Indice

Capitolo 1

Algoritmo di Euclide, teorema cinese e interpolazione

1.1 Algoritmo di Euclide

Siano m un intero qualunque (positivo, negativo o nullo), n un intero positivo, e

$$\ldots, -kn, \ldots, -2n, -n, 0, n, 2n, \ldots, kn, \ldots$$

l'insieme dei multipli di n. Esistono allora due termini consecutivi di questa successione, qn e $(q+1)n$ tali che:

$$qn \leq m < (q+1)n. \tag{1.1}$$

Sia r la differenza:

$$r = m - qn.$$

L'operazione che consiste nel determinare i due numeri q ed r si chiama *divisione* di m (dividendo) per n (divisore). L'intero q è il *quoziente* (è il minimo intero il cui prodotto per n non supera m, e come tale è univocamente determinato), e r il *resto* della divisione (anch'esso allora univocamente determinato). Dalla (1.1) si ha, sottraendo qn dai tre membri,

$$0 \leq r < n$$

e dunque: *il resto non è mai negativo ed è minore del divisore.* Se $r = 0$, si dice che m è un *multiplo* di n, o che n è un *divisore* di m, e si scrive $n|m$. Se $m \neq 1$ non ha altri divisori all'infuori di se stesso e dell'unità, allora m è *primo*. Consideriamo ora due interi m e n, $m \geq n > 0$, e cerchiamo gli interi che sono divisori comuni di m e n. Vedremo che il problema si riduce a quello di trovare i divisori di *un solo intero* d. Dividiamo m per n:

$$m = qn + r \qquad\qquad 0 \leq r < n.$$

Ne segue $r = m - qn$. Si vede allora che un intero che divide m e n divide anche r. D'altra parte, se un intero divide n e r, la stessa uguaglianza ci dice che questo intero divide anche m, e dunque che esso divide m e n. In altri termini, i divisori comuni di m e n coincidono con quelli di n e r. Dividendo ora n per r, si ha, come sopra che i divisori comuni di n e r (e dunque quelli di m e n), sono quelli di r e del resto di quest'ultima divisione. Proseguendo in questo modo, si ha una successione di divisioni che ad un certo punto deve dare resto zero, in quanto i resti sono interi positivi strettamente decrescenti (si è posto $q = q_1$ e $r = r_1$):

$$\begin{aligned}
m &= nq_1 + r_1, & r_1 &< n,\\
n &= r_1q_2 + r_2, & r_2 &< r_1,\\
r_1 &= r_2q_3 + r_3, & r_3 &< r_2,\\
&\vdots\\
r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1}, & r_{k-1} &< r_{k-2},\\
r_{k-2} &= r_{k-1}q_k,
\end{aligned}$$

con il $k-$esimo resto r_k uguale a zero. Per l'argomento di sopra abbiamo allora che i divisori comuni di m e n sono i divisori comuni di r_{k-1} (l'ultimo resto non nullo) e 0, e poichè tutti gli interi dividono 0, si ha che *i divisori comuni di m e n sono, tutti e soli, i divisori di r_{k-1}*. Posto $d = r_{k-1}$, si scrive $d = (m, n)$ o $d =$MCD(m, n). Ora, d divide sia m che n, e poichè tra i divisori di d c'è d stesso, d è il più grande divisore comune di m e n, d'onde il nome di *massimo comun divisore* di m e n. Questa terminologia, tuttavia, nasconde la proprietà saliente di questo numero, che non è tanto quella di essere il più grande tra i divisori comuni di m e n, quanto quella di esaurire, con i suoi divisori, tutti i divisori di m e n.

Abbiamo allora il seguente *algoritmo di Euclide*:

input: a, b,
$u : a$, $v : b$,
mentre $v \neq 0$ fare:
$(q : quoziente(u, v)$, $t : u, u : v, v : t - qv)$,
output: u.

Se $d = (m, n) = 1$, allora m e n non hanno divisori comuni diversi da 1: sono *primi tra loro* (o *relativamente primi*).

Il resto $r_1 = m - qn$ è una combinazione lineare di m e n:

$$r_1 = 1 \cdot m + (-q_1) \cdot n,$$

e ciò è vero anche per r_2: si ha $r_2 = n - q_2r_1 = n - q_2m + q_1q_2n$, da cui:

$$r_2 = (-q_2) \cdot m + (1 - q_1 q_2) \cdot n.$$

Ciò accade per tutti i resti r_i, $i = 1, 2, \ldots, k$, e dunque anche per $r_{k-1} = d$. Si ha così:

Teorema 1.1. (IDENTITÀ DI BÉZOUT) *Dati due interi m e n, esistono due interi h e k tali che $d = (m, n)$ è combinazione lineare di m e n:*

$$d = hm + kn. \qquad \diamondsuit$$

Nota. I due interi h e k del Teorema 1.1 non sono univocamente determinati. Per ogni intero s si ha infatti:

$$d = (h \pm sn)m + (k \mp sm)n.$$

Modificando il programma per l'algoritmo di Euclide si ottiene l'algoritmo di Bézout. Esso fornisce la terna $[h, k, d]$:

input: m, n,
$u : [1, 0, m], v : [0, 1, n]$,
mentre $v_3 \neq 0$ fare:
$(q : quoziente(u, v), t : u, u : v, v : t - qv)$,
output: u.

L'input dell'algoritmo consta dei due interi m e n. Nella forma data dal teorema di Bézout essi si scrivono:

$$m = 1 \cdot m + 0 \cdot n \text{ e } n = 0 \cdot m + 1 \cdot n,$$

che danno le due terne iniziali dell'algoritmo. Si ha infatti $m = (m, m)$ e $n = (n, n)$.

Ogni intero m diviso per un intero n, dà un resto non negativo che è minore di n. I resti possibili sono dunque gli interi $0, 1, \ldots, n - 1$ (e si ottengono tutti perchè un numero m minore di n diviso per n dà resto m, con quoziente 0). Se il resto è r si dice che *m è congruo a r modulo n*, e si scrive $m \equiv r \mod n$. Ricordiamo infine il *teorema fondamentale dell'aritmetica: ogni numero intero diverso da 1 o è primo, oppure si può decomporre in un prodotto di fattori primi, e ciò, a meno dell'ordine dei fattori, in modo unico.* (L'unicità di questa decomposizione è un'altra conseguenza dell'esistenza del massimo comun divisore; v. l'esercizio 3 qui sotto).

Esercizi

1. Dimostrare che se quattro numeri m, n, q, r sono tali che $m = qn + r$ e $0 \leq r < n$, allora q e r sono quoziente e resto della divisione di m per n.

2. Sia $m|ab$ e $(m, a) = 1$. Dimostrare che allora $m|b$.

3. Dimostrare che $(m, ab) = 1$ se e solo se $(m, a) = 1$ e $(m, b) = 1$. Estendere al caso di più interi. Usare questo fatto per dimostrare che la fattorizzazione di un intero nel prodotto di primi è unica.

4. Sia $(m, n) = 1$. Dimostrare che se $hm + kn = 1$ e $h'm + k'n = 1$, allora $h' \equiv h \bmod n$ e $k' \equiv k \bmod m$.

5. Siano $a_1, a_2, \ldots, a_n$ interi positivi, e sia a_n il più piccolo. Sia r_i il resto della divisione di a_i per a_n, $i \neq n$. Dimostrare che:

$$\mathrm{MCD}(a_1, a_2, \ldots, a_n) = \mathrm{MCD}(r_1, r_2, \ldots, r_{n-1}, a_n).$$

(Si noti che il più piccolo intero della prima $n-$pla è il più grande della seconda). Ripetendo l'operazione sulla seconda $n-$pla, e così di seguito, si arriva ad una $n-$pla nella quale tutti gli elementi sono uguali a zero salvo uno. Dimostrare che questo è il $\mathrm{MCD}(a_1, a_2, \ldots, a_n)$.

6. Nella *successione di Fibonacci*:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

ogni termine, a partire dal terzo, si ottiene sommando i due che lo precedono:

$$f_{n+2} = f_{n+1} + f_n,$$

$n \geq 0$, e $f_0 = 0$, $f_1 = 1$.
a) Dimostrare che due numeri di Fibonacci consecutivi f_{k+1} e f_k sono relativamente primi.
b) Dimostrare che l'algoritmo di Euclide applicato a f_{n+2} e f_{n+1} consta esattamente di n passi.
(*Sugg.:* si osservi che scrivendo la relazione che lega i numeri di Fibonacci come $f_{n+2} = f_{n+1} \cdot 1 + f_n$ si ha, essendo $f_n \leq f_{n+1}$ che f_n è il resto della divisione di f_{n+2} per f_{n+1} (e il quoziente è 1)).
c) (Teorema di Lamé) Dimostrare che se $u > v > 0$ sono tali che l'algoritmo della divisione di u per v consta esattamente di n passi, e u è minimo con questa proprietà, allora $u = f_{n+2}$ e $v = f_{n+1}$.
(*Sugg.:* si osservi che $r_{n-2} \geq 2 = f_3$, e dunque $r_{n-3} \geq 2 + 1 = 3 = f_4$, e che in generale ogni resto è maggiore o uguale della somma dei due resti successivi).

7. Dati due interi m e n, sostituendo nella definizione di MCD la parola "massimo" con "minimo" e "divisore" con "multiplo", si ottiene la definizione "duale"

di *minimo comune multiplo*: è *il numero μ tale che i multipli comuni di m e n sono, tutti e soli, i multipli di μ*. Si scrive $\mu = mcm(m, n)$.
a) Dimostrare che μ esiste ed è uguale a $mn/(m, n)$.
b) Estendere al caso di più interi.

8. Dimostrare che qualunque sia n nessuno dei numeri:

$$n! + 2, n! + 3, \ldots, n! + n$$

è primo. Lo stesso se invece di $n!$ si prende $mcm(1, 2, \ldots, n)$. (Si ha così– prendendo il più grande primo minore di $n! + 2$ e il più piccolo primo maggiore di $n! + n$– che nella serie dei numeri primi esistono lacune arbitrariamente grandi).

1.2 Il teorema cinese e i numeri di Lagrange

Siano ora m, n e a, b due coppie di interi. Ci poniamo il seguente problema: esiste un intero c che diviso per m dà resto a e diviso per n dà resto b? Questo problema non ha sempre soluzione. Ad esempio, con $m = 4$, $n = 6$, $a = 1$ e $b = 2$ dovrebbe aversi $c = 4q_1 + 1 = 6q_2 + 2$, cioè c insieme dispari e pari. Con $a = 2$ e $b = 4$ si ha la soluzione $c = 10$. Infatti, $10 = 4 \cdot 2 + 2 = 1 \cdot 6 + 4$.

Come si vede, l'esistenza della soluzione dipende dalla scelta della coppia a, b. Una condizione sufficiente affinchè, dati m e n la soluzione esista qualunque siano a e b è che m e n siano primi tra loro, come dimostra il teorema che segue.

Teorema 1.2. (TEOREMA CINESE DEI RESTI) *Siano m e n primi tra loro. Allora comunque si scelgano due interi a e b esiste un intero c tale che*

$$c \equiv a \bmod m,$$
$$c \equiv b \bmod n.$$

Inoltre, tale soluzione è unica mod mn (cioè: c è l'unico intero maggiore o uguale a 0 e minore di mn che risolve entrambe le congruenze).

Dim. Essendo $(m, n) = 1$, esistono h e k tali che $hm + kn = 1$. Si ha da qui che $kn \equiv 1 \bmod m$ e $hm \equiv 1 \bmod n$. Se $a = 1$ e $b = 0$ abbiamo già la soluzione: $c = kn$ (e per $a = 0$ e $b = 1$ la soluzione $c = hm$). In generale, dico che $c = bhm + akn$ è l'intero cercato. Infatti, modulo m, si ha $c \equiv akn \equiv a \cdot 1 = a \bmod m$, e, modulo n, $c \equiv bhm \equiv b \cdot 1 = b \bmod n$. Per quanto riguarda l'unicità, se d è un'altra soluzione, essendo d congruo ad a e b modulo m e n, rispettivamente, si ha $d \equiv c$ modulo m e n, e pertanto m e n dividono $d - c$. Ma essendo m e n primi tra loro, anche il loro prodotto mn divide $d - c$, cioè $d \equiv c \bmod mn$. Dunque la soluzione modulo mn è unica. In altre parole, esiste ed è unico l'intero c, $0 \leq c < mn$ che risolve le due congruenze. Ogni altra soluzione si ottiene aggiungendo a c un multiplo di mn. $\diamondsuit$

Nota. I due interi a e b del teorema risultano allora essere i coefficienti che servono per scrivere c come combinazione lineare di hm e kn. Si osservi inoltre che nell'esempio visto sopra, con $m = 4$, $n = 6$, $a = 2$ e $b = 4$ oltre alla soluzione $c = 10$ si ha anche la soluzione $c = 22$: $22 = 4 \cdot 5 + 2 = 6 \cdot 3 + 4$, e 10 e 22 non sono congrui modulo $4 \cdot 6 = 24$. Dunque, se m e n non sono primi tra loro, non solo una soluzione può non esistere, ma se esiste può non essere unica.

Esempi. 1. Dimostriamo che il gruppo $Z_3 \oplus Z_4$ è isomorfo al gruppo Z_{12}. Il primo consta delle coppie (x, y) con $x = 0, 1, 2$ e $y = 0, 1, 2, 3$ con l'operazione

$$(x_1, y_1) + (x_2, y_2) = ((x_1 + x_2) \bmod 3, (y_1 + y_2) \bmod 4);$$

il secondo degli interi 0,1,...,11 con la somma mod 12. Data la coppia $(x, y) \in Z_3 \oplus Z_4$, per il teorema cinese esiste ed è unico l'intero c, $0 \leq c < 3 \cdot 4 = 12$, congruo a x mod 3 e a y mod 4. La corrispondenza $(x, y) \to c$ è l'isomorfismo cercato. Più in generale, per (m, n)=1, si ha $Z_m \oplus Z_n$ isomorfo a Z_{mn}.

2. Sia $\varphi(n)$ la *funzione di Eulero*, così definita:

$\varphi(1) = 1$,

$\varphi(n) =$ numero degli interi minori di n e primi con n.

Facciamo vedere che se $(m, n) = 1$ allora $\varphi(mn) = \varphi(m)\varphi(n)$. Denotiamo con C_n l'insieme (il gruppo) degli interi minori di n e primi con n. Se $(x, m) = (y, n) = 1$, allora l'intero c del teorema cinese, cioè quello che è congruo a x e a y modulo m e n, rispettivamente, è primo con m e n, e dunque anche con il prodotto mn. Allora la corrispondenza $C_m \times C_n \longrightarrow C_{mn}$ data da $(x, y) \to c$ è ben definita per l'unicità di c. Viceversa, se $c \in C_{mn}$, allora prendendo per x e y i resti della divisione di c per m e per n si ha che anche la corrispondenza inversa $c \to (x, y)$ è ben definita (unicità del resto). Si ha quindi corrispondenza biunivoca.

3. Se $(m, n) = 1$, si ha $am + bn = 1$, per certi a e b. Poniamo $e = am$, $e' = bn$. Si ha:

$$e^2 = (am)^2 = am \cdot am = am(1 - bn) = am - abmn \equiv am = e \bmod mn,$$

e analogamente $e'^2 \equiv e' \bmod mn$. Questo fatto si esprime dicendo che, nell'anello delle classi resto mod mn, e ed e' sono *idempotenti*. Inoltre sono *ortogonali*:

$$ee' = am \cdot bn = abmn \equiv 0 \bmod mn,$$

e la loro somma è 1: $e + e' = 1$.

Il teorema cinese si generalizza al caso di più moduli.

Teorema 1.3. *Siano $m_0, m_1, \ldots, m_n$ interi a due a due primi tra loro, e siano $u_0, u_1, \ldots, u_n$ interi qualunque. Allora esiste un intero u tale che*

$$u \equiv u_i \bmod m_i,$$

$i = 0, 1, \ldots, n$, e questo u è unico modulo il prodotto $m_0 m_1 \cdots m_n$. In altri termini, risolvere il sistema di congruenze $x \equiv u_i$ mod m_i, $i = 0, 1, \ldots, n$, equivale a risolvere la sola congruenza $x \equiv u$ mod $m_0 m_1 \cdots m_n$.

Di questo teorema daremo due dimostrazioni, una di esistenza e l'altra costruttiva.

Prima dimostrazione. (v. Esempio 1.) Dimostriamo innanzitutto che se u esiste allora è unico modulo il prodotto $m = m_0 m_1 \cdots m_n$. Se infatti $v \equiv u_i$ mod m_i, per tutti gli i, allora $u - v \equiv 0$ mod m_i, e dunque (gli m_i sono primi a due a due) $u - v \equiv 0$ mod m, cioè $u \equiv v$ mod m. Consideriamo ora per ogni $u = 0, 1, \ldots, m-1$, la $(n+1)-$pla $(u \bmod m_0, u \bmod m_1, \ldots, u \bmod m_n)$. Queste $(n+1)-$ple sono, al variare di u, tutte distinte, in quanto se per certi u e v tra 0 e $m-1$ si avesse:

$$(u \bmod m_0, \ldots, u \bmod m_n) = (v \bmod m_0, \ldots, v \bmod m_n),$$

allora $u \equiv v$ mod m. Ma le $(n+1)-$ple $(v_0, v_1, \ldots, v_n)$, dove $0 \leq v_i < m_i$ sono anch'esse tutte distinte, e il loro numero è uguale a quello delle precedenti, cioè m. Dunque per la data $(n+1)-$pla $(u_0, u_1, \ldots, u_n)$ esiste una delle $(u \bmod m_0, u \bmod m_1, \ldots, u \bmod m_n)$ che la eguaglia.

Seconda dimostrazione. Questa dimostrazione estende quella del caso di due interi già vista, e come in quel caso si dà un metodo per costruire la soluzione. Posto $m = m_0$ e $n = m_1 m_2 \cdots m_n$, si ha che esistono due interi h e k tali che $hm + kn = 1$, e dunque, posto $L_0 = kn$,

$$\begin{aligned} L_0 &\equiv 1 \bmod m, \\ L_0 &\equiv 0 \bmod n. \end{aligned}$$

L_0 è divisibile per il prodotto $m_1 m_2 \cdots m_n$, e dunque in particolare per m_i, $i = 1, 2, \ldots, n$. Ne segue:

$$\begin{aligned} L_0 &\equiv 1 \bmod m_0, \\ L_0 &\equiv 0 \bmod m_i, \end{aligned}$$

$i = 1, 2, \ldots, n$. (Si noti che L_0 risolve il problema per la $(n+1)-$pla $u_0 = 1, u_1 = u_2 = \ldots = u_n = 0$). Con stesso argomento applicato agli altri m_i abbiamo allora $n+1$ interi $L_0, L_1, \ldots, L_n$ tali che:

$$\begin{aligned} L_k &\equiv 1 \bmod m_k, \\ L_k &\equiv 0 \bmod m_j, \end{aligned}$$

per $j \neq k$. L'intero:

$$u_0 L_0 + u_1 L_1 + \ldots + u_n L_n$$

è una soluzione comune delle date congruenze. Per l'unicità si veda la prima dimostrazione. $\diamondsuit$

Nota. Gli L_k formano una "base mista" per gli interi mod m, dove $m = m_0 m_1 \cdots m_n$, nel senso che per ogni tale intero u esiste ed è unica la $(n+1)-$pla $(u_0, u_1, \ldots, u_n)$, con $0 \leq u_k < m_k$ tale che $u = \sum_{k=0}^{n} u_k L_k$. Questa $(n+1)-$pla si può allora considerare come una rappresentazione di u: la chiameremo *rappresentazione modulare* di u, rispetto ai moduli $m_0, m_1, \ldots, m_n$. Rappresentare un intero in questo modo non dà luogo ad una perdita di informazione, in quanto, per il teorema cinese, possiamo ritrovare u univocamente a partire dagli u_i.

Chiameremo gli L_k *numeri di Lagrange.*

Siano $A_1, A_2, \ldots, A_r$ anelli commutativi con unità. La *somma diretta* degli A_k:

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_r,$$

è l'anello che ha come elementi le $r-$ple $(a_1, a_2, \ldots, a_r)$, e come operazioni la somma e il prodotto di queste $r-$ple componente per componente. Le $r-$ple $(0, 0, \ldots, 0, a_k, 0, \ldots, 0)$ formano un sottoanello $\overline{A}_k$ isomorfo ad A_k. L'unità di A è la $r-$pla $1 = (1, 1, \ldots, 1)$, e quella di $\overline{A}_k$ è $e_k = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$. Allora, la somma degli e_k è 1, l'unità di A:

$$e_1 + e_2 + \cdots + e_r = 1,$$

mentre il prodotto di e_i ed e_j, con $i \neq j$ è zero:

$$e_i e_j = 0;$$

inoltre:

$$e_k^2 = e_k.$$

Le unità degli A_k sono dunque idempotenti ortogonali. Dato un elemento $a = (a_1, a_2, \ldots, a_k, \ldots, a_r) \in A$, esso è somma delle proprie componenti $\overline{a}_k = (0, 0, \ldots, 0, a_k, 0, \ldots, 0)$; ma $(0, 0, \ldots, 0, a_k, 0, \ldots, 0) = ae_k$, e dunque:

$$\overline{a}_k = ae_k.$$

Allora $A = \overline{A}_1 \oplus \overline{A}_2 \oplus \cdots + \oplus \overline{A}_r$, cioè A è somma diretta dei propri sottoanelli $\overline{A}_k$ (somma diretta *interna*).

Viceversa, sia A un anello commutativo con unità 1 tale che 1 ammetta una partizione in idempotenti ortogonali: $e_1 + e_2 + \cdots + e_r = 1$. Allora gli elementi ae_k, $a \in A$, formano un sottoanello in quanto:

$$ae_k \pm be_k = (a \pm b)e_k,$$
$$(ae_k)(be_k) = abe_k^2 = abe_k.$$

Denotiamo con $\overline{A}_k$ questo sottoanello, e con $\overline{a}_k$ l'elemento ae_k. $\overline{A}_k$ ha e_k come unità:

$$\overline{a}_k e_k = ae_k e_k = ae_k^2 = ae_k = \overline{a}_k,$$

e gli elementi $a \in A$ ammettono la decomposizione:

$$a = a \cdot 1 = a(e_1 + e_2 + \cdots + e_r) = ae_1 + ae_2 + \cdots + ae_r = \overline{a}_1 + \overline{a}_2 + \cdots + \overline{a}_r,$$

con $ae_k \in \overline{A}_k$, e dove si è posto $\overline{a}_k = ae_k$. Questa decomposizione è unica; se infatti si ha anche:

$$a = x_1e_1 + x_2e_2 + \cdots + x_re_r,$$

con $x_k \in A$ e $x_ke_k \in \overline{A}_k$, allora, moltiplicando per e_j si ha $x_je_j = ae_j$. Dunque $A = \overline{A}_1 \oplus \overline{A}_2 \oplus \cdots + \oplus\overline{A}_r$.

Nell'Esempio 3 di sopra abbiamo visto che $e = L_0$ e $e' = L_1$ sono idempotenti ortogonali e a somma 1. Questo accade per tutti gli L_k. Si ha, con $m = m_0m_1 \cdots m_n$:

1. $L_0 + L_1 + \ldots + L_n \equiv 1 \bmod m$.

   Prendendo $u_0 = u_1 = \ldots = u_n = 1$ si ha $\sum L_i \equiv 1 \bmod m_i$. Ne segue che $\sum L_i - 1$ è divisibile per m_i per tutti gli i, e dunque è divisibile per il loro prodotto m.

2. $L_iL_j \equiv 0 \bmod m, i \neq j$.

   Ciò si vede osservando che il prodotto L_iL_j contiene come fattori sia $\prod_{s\neq i} m_s$ che $\prod_{s\neq j} m_s$ e dunque tutti gli m_i e il loro prodotto m.

3. $L_k^2 \equiv L_k \bmod m$.

   Segue da 1. che

$$L_k = L_k \cdot 1 \equiv L_k \cdot (L_0 + L_1 + \ldots + L_k + \ldots + L_n) \bmod\ m.$$

Per 2., tutti i prodotti $L_kL_j, j \neq k$, sono zero modulo m e resta solo L_k^2.

Sia ora $A = Z_m$ l'anello delle classi resto modulo m, con $m = m_0 \cdots m_n$. Per quanto visto sopra gli L_k permettono una decomposizione di A in somma diretta dei sottoanelli $A_k = \{aL_k \bmod m, a \in A\}$. Posto $\overline{a}_k = aL_k \bmod m$ (dunque $aL_k = mq + \overline{a}_k$, per un certo q), l'elemento a (la classe resto a mod m) si decompone in:

$$a \equiv \overline{a}_1 + \overline{a}_2 + \cdots + \overline{a}_r \bmod m,$$

ed essendo $L_k \equiv 1 \bmod m_k$ e $L_k \equiv 0 \bmod m_i$, $i \neq k$, si ha:

$$\overline{a}_k \equiv a \bmod m_k,\ \overline{a}_k \equiv 0 \bmod m_i,\ i \neq k.$$

Il sottoanello A_k è isomorfo all'anello delle classi resto mod m_k. Infatti, consideriamo la corrispondenza $Z \longrightarrow A_k$ data da $a \longrightarrow \overline{a}_k$. Si tratta evidentemente di un omomorfismo surgettivo. Se $\overline{a}_k = 0$, allora aL_k è divisibile per m, e dunque per tutti gli m_i, e in particolare per m_k; ma essendo $L_k \equiv 1 \bmod m_k$,

m_k deve dividere a, cioè $a \equiv 0 \bmod m_k$. Viceversa, se $a \equiv 0 \bmod m_k$ allora $aL_k \equiv 0 \bmod m_k$; ma essendo sempre $aL_k \equiv 0 \bmod m_i$, per $i \neq k$ (perchè ciò accade per gli L_k) si ha che aL_k è divisibile per tutti gli m_i, e dunque per m. In altri termini $\overline{a}_k \equiv 0 \bmod m$. In questo omomorfismo allora gli elementi del nucleo sono tutti e soli i multipli di m_k, e per il teorema di omomorfismo si ha $A_k \simeq Z/m_k Z = Z_{m_k}$.

In definitiva,

$$Z_m = A_0 \oplus A_1 \oplus \cdots \oplus A_n$$

(somma diretta interna), dove la componente in A_k di $a \in Z_m$ è il resto della divisione di a per m_k.

Torniamo ora al teorema cinese. Per calcolare u si può procedere in due modi:

1. Come visto nel teorema: dati gli m_k si calcolano una volta per tutte gli L_k e poi, per ogni scelta degli u_i, si determina u come combinazione lineare degli L_k a coefficienti gli u_i. E' questo il *metodo di Lagrange*.

2. Si considerano *insieme* i dati m_i e u_i, e si costruisce u ricorsivamente a partire dai dati m_0 e u_0, quindi m_0, m_1 e u_0, u_1, ecc. Questo è il *metodo di Newton*.

Vediamo ora in dettaglio questi due metodi.

1.2.1 Calcolo degli L_k e di u (metodo di Lagrange)

Siano dati $m_0, m_1, \ldots, m_n$ a due a due relativamente primi. Per ogni coppia (m_i, m_k), esistono allora $s_i^{(k)}$ e $s_k^{(i)}$ tali che:

$$s_i^{(k)} m_i + s_k^{(i)} m_k = 1,$$

ovvero:

$$s_i^{(k)} m_i = 1 - s_k^{(i)} m_k.$$

Tutti gli $s_i^{(k)} m_i, i \neq k$, sono allora congrui a 1 modulo m_k, come pure il loro prodotto L'_k:

$$L'_k = \prod_{i \neq k} s_i^{(k)} m_i \equiv 1 \bmod m_k.$$

Per $i \neq k$ questo prodotto ha come fattore m_i, per cui:

$$L'_k \equiv 0 \bmod m_i, \ i \neq k.$$

Per operare con numeri più piccoli trasformiamo L'_k come segue:

$$L'_k = \textstyle\prod_{i \neq k} s_i^{(k)} m_i = \prod_{i \neq k} s_i^{(k)} \cdot \prod_{i \neq k} m_i,$$

e sostituiamo $\prod_{i\neq k} s_i^{(k)}$ con il resto che dà nella divisione per m_k. Ciò lascia la congruenza inalterata in quanto se $\prod_{i\neq k} s_i^{(k)} = qm_k + r$ allora:

$$\begin{aligned} L'_k &= (qm_k + r)\prod_{i\neq k} m_i = qm_k \prod_{i\neq k} m_i + r\prod_{i\neq k} m_i \\ &\equiv r\prod_{i\neq k} m_i \bmod m_k. \end{aligned}$$

Poniamo $L_k = r\prod_{i\neq k} m_i$. Poichè $L_k \equiv L'_k \equiv 1 \bmod m_k$, abbiamo:

$$\begin{aligned} L_k &\equiv 1 \mod m_k, \\ L_k &\equiv 0 \mod m_i, \quad i \neq k. \end{aligned}$$

Riassumendo, per calcolare L_k:

1. Per ogni i, determinare due interi $s_i^{(k)}$ e $s_k^{(i)}$ tali che:

$$s_i^{(k)} m_i + s_k^{(i)} m_k = 1.$$

2. Fare il prodotto di tutti gli $s_i^{(k)}$, $i \neq k$, dividerlo per m_k e prendere il resto r_k.

3. Allora $L_k = r_k \prod_{i\neq k} m_i$.

Esempio. Siano $m_0 = 7$, $m_1 = 11$, $m_2 = 13$, $m_3 = 15$. Procedendo come visto sopra si ha:

$$\begin{array}{llll} s_0^{(1)}7 & + & s_1^{(0)}11 = 1, \\ -3 & & 2 \\ s_0^{(2)}7 & + & s_2^{(0)}13 = 1, \\ 2 & & -1 \\ s_0^{(3)}7 & + & s_3^{(0)}15 = 1, \\ -2 & & 1 \\ s_1^{(2)}11 & + & s_2^{(1)}13 = 1, \\ 6 & & -5 \\ s_1^{(3)}11 & + & s_3^{(1)}15 = 1, \\ -4 & & 3 \\ s_2^{(3)}13 & + & s_3^{(2)}15 = 1. \\ 7 & & -6 \end{array}$$

Con questi valori abbiamo:

$$\begin{aligned} L_0 &= s_1^{(0)} s_2^{(0)} s_3^{(0)} \pmod 7 \cdot 11 \cdot 13 \cdot 15 \\ &= 2 \cdot -1 \cdot 1 \pmod 7 \cdot 11 \cdot 13 \cdot 15 \end{aligned}$$

$$\begin{aligned} &= -2 \pmod 7 \cdot 2145 \\ &= -4290. \end{aligned}$$

$$\begin{aligned} L_1 &= s_0^{(1)} s_2^{(1)} s_3^{(1)} \pmod{11} \cdot 7 \cdot 13 \cdot 15 \\ &= -3 \cdot -5 \cdot 3 \pmod{11} \cdot 1365 \\ &= 45 \pmod{11} \cdot 1365 \\ &= 1 \cdot 1365 \\ &= 1365. \end{aligned}$$

$$\begin{aligned} L_2 &= s_0^{(2)} s_1^{(2)} s_3^{(2)} \pmod{13} \cdot 7 \cdot 11 \cdot 15 \\ &= 2 \cdot 6 \cdot -6 \pmod{13} \cdot 1155 \\ &= -72 \pmod{13} \cdot 1155 \\ &= -7 \cdot 1155 \\ &= -8085. \end{aligned}$$

$$\begin{aligned} L_3 &= s_0^{(3)} s_1^{(3)} s_2^{(3)} \pmod{15} \cdot 7 \cdot 11 \cdot 13 \\ &= -2 \cdot -4 \cdot 7 \pmod{15} \cdot 1001 \\ &= 56 \pmod{15} \cdot 1001 \\ &= -4 \cdot 1001 = -4004. \end{aligned}$$

Scegliamo ora quattro interi:

$$u_0 = -1 \, , u_1 = -2 \, , u_2 = 2 \, , u_3 = 6;$$

un intero congruo a $u_i \bmod m_i$, $i = 0, 1, 2, 3$, è

$$4290 - 2 \cdot 1365 - 2 \cdot 8085 - 6 \cdot 4004 = -38634,$$

e l'unica soluzione modulo $m_0 m_1 m_2 m_3 = 7 \cdot 11 \cdot 13 \cdot 15 = 15015$ si ottiene aggiungendo a -38634 l'intero $3 \cdot 15015$. Si trova $u = 6411$.

Come visto in precedenza, i quattro interi L_k ora trovati permettono di decomporre l'anello Z_m, con $m = 15015$, nella somma diretta di quattro sottoanelli. Se $a \in Z_m$, le sue componenti nei quattro addendi sono $aL_k \bmod m$. Ad esempio, sia $a = 156$; allora:

0. $\overline{a}_0 = aL_0 \bmod 15015 = 156 \cdot -4290 \bmod 15015 = 6435$;
1. $\overline{a}_1 = aL_1 \bmod 15015 = 156 \cdot 1365 \bmod 15015 = 2730$;
2. $\overline{a}_2 = aL_2 \bmod 15015 = 156 \cdot -8085 \bmod 15015 = 0$;
3. $\overline{a}_3 = aL_3 \bmod 15015 = 156 \cdot -4004 \bmod 15015 = 6006$.

La somma dei quattro numeri trovati vale 15171 che mod 15015 è proprio 156. Inoltre, $\overline{a}_k \equiv a \bmod m_i$; infatti:
$6435-156 = 897\cdot 7; 2730-156 = 234\cdot 11; 0-156 = -12\cdot 13; 6006-156 = 390\cdot 15.$

1.2.2 Calcolo di u (metodo di Newton)

Nel metodo di Newton, che ora consideriamo, la soluzione u si costruisce ricorsivamente usando sia gli m_i che gli u_i. Se $u^{(k-1)}$ è una soluzione per i dati:

$$m_0, m_1, \ldots, m_{k-1},$$
$$u_0, u_1, \ldots, u_{k-1},$$

il metodo fornisce una soluzione $u^{(k)}$ per i dati:

$$m_0, m_1, \ldots, m_{k-1}, m_k,$$
$$u_0, u_1, \ldots, u_{k-1}, u_k.$$

Sia $k = 0$. In tal caso i dati sono:

$$m_0$$
$$u_0.$$

Sia $u^{(0)}$ il resto della divisione di u_0 per m_0. Allora:

$$u^{(0)} \equiv u_0 \bmod m_0$$

con $u^{(0)} < m_0$. Se $k = 1$ e

$$m_0, m_1$$
$$u_0, u_1$$

sono i dati, sia:

$$s_0^{(1)} m_0 + s_1^{(0)} m_1 = 1.$$

Sappiamo che una soluzione è data da:

$$u_1 s_0^{(1)} m_0 + u_0 s_1^{(0)} m_1.$$

Se invece di u_0 prendiamo il resto della divisione di u_0 per m_0, e cioè $u^{(0)}$, allora il numero:

$$u_1 s_0^{(1)} m_0 + u^{(0)} s_1^{(0)} m_1$$

è anch'esso una soluzione perchè questo numero è congruo a $u^{(0)}$, e quindi a u_0, modulo m_0. Perciò sia:

$$u^{(1)} = u_1 s_0^{(1)} m_0 + u^{(0)} s_1^{(0)} m_1.$$

Poichè $s_1^{(0)} m_1 = 1 - s_0^{(1)} m_0$, possiamo scrivere:

$$u^{(1)} = u_1 s_0^{(1)} m_0 + u^{(0)}(1 - s_0^{(1)} m_0),$$

ovvero:

$$u^{(1)} = u^{(0)} + (u_1 - u^{(0)}) s_0^{(1)} m_0.$$

Questa è una soluzione per questo caso in quanto:

$$u^{(1)} \equiv u^{(0)} \equiv u_0 \bmod m_0,$$

e poichè $s_0^{(1)} m_0 = 1 - s_1^{(0)} m_1$,

$$u^{(1)} = u^{(0)} + (u_1 - u^{(0)})(1 - s_1^{(0)} m_1),$$

per cui:

$$u^{(1)} \equiv u_1 \bmod m_1.$$

Così, per passare da $k = 0$ a $k = 1$ si aggiunge alla soluzione $u^{(0)}$ del caso $k = 0$ la differenza tra il nuovo valore u_1 di u e $u^{(0)}$ moltiplicata per $s_0^{(1)} m_0$.

Sia ora $k = 2$. Abbiamo:

$$\begin{aligned} s_0^{(1)} m_0 + s_1^{(0)} m_1 &= 1, \\ s_0^{(2)} m_0 + s_2^{(0)} m_2 &= 1, \\ s_1^{(2)} m_1 + s_2^{(1)} m_2 &= 1. \end{aligned}$$

Poniamo:

$$u^{(2)} = u^{(0)} + (u_1 - u^{(0)}) s_0^{(1)} m_0 + (u_2 - u^{(1)}) s_0^{(2)} m_0 \cdot s_1^{(2)} m_1.$$

Qui abbiamo aggiunto a $u^{(1)}$, che è la soluzione nel caso $k = 1$, la differenza $u_2 - u^{(1)}$ moltiplicata per $s_0^{(2)} m_0 \cdot s_1^{(2)} m_1$. Si tratta effettivamente di una soluzione in quanto:

$$u^{(2)} \equiv u^{(0)} \equiv u_0 \bmod m_0,$$

e

$$u^{(2)} \equiv u^{(1)} \equiv u_1 \bmod m_1.$$

Inoltre, se scriviamo $s_0^{(2)} m_0 = 1 - s_2^{(0)} m_2$ e $s_1^{(2)} m_1 = 1 - s_2^{(1)} m_2$ abbiamo:

$$u^{(2)} = u^{(0)} + (u_1 - u^{(0)}) s_0^{(1)} m_0 + (u_2 - u^{(1)})(1 - s_2^{(0)} m_2)(1 - s_2^{(1)} m_2),$$

che fornisce:

$$u^{(2)} \equiv u^{(1)} + (u_2 - u^{(1)}) = u_2 \bmod m_2.$$

Il funzionamento del metodo è ora chiaro: supponiamo nota la soluzione

$$u^{(k-1)} \equiv u_j \bmod m_j,$$

$j = 0, 1, \ldots, k-1$. Allora:

$$u^{(k)} = u^{(k-1)} + (u_k - u^{(k-1)}) \prod_{j=0}^{k-1} s_j^{(k)} m_j \tag{1.2}$$

($u^{(0)} = u_0 \bmod m_0$). L'intero richiesto è allora $u = u^{(n)}$.

Nota. 1. Conviene spezzare il prodotto $\prod_{j=0}^{k-1} s_j^{(k)} m_j$ e calcolare separatamente i fattori $s_k = \prod_{j=0}^{k-1} s_j^{(k)}$, e $q_k = \prod_{j=0}^{k-1} m_j$, per $k = 1, 2, \ldots, n$.

2. Poichè

$$s_i^{(k)} m_i + s_k^{(i)} m_k = 1,$$

abbiamo:

$$s_i^{(k)} m_i \equiv 1 \bmod m_k, \quad i \neq k.$$

Ne segue:

$$s_i^{(k)} \equiv m_i^{-1} \bmod m_k.$$

In altri termini, $s_i^{(k)}$ è l'inverso di m_i modulo m_k.

Poniamo ora:

$$a_k = (u_k - u^{(k-1)}) \cdot s_k \bmod m_k,$$

con $a_0 = u^{(0)} = u_0 \bmod m_0$. La formula (1.2) diventa:

$$u^{(k)} = u^{(k-1)} + a_k q_k,$$

e abbiamo il seguente algoritmo (per semplificare i calcoli conviene ridurre subito il valore attuale di u modulo l'm_k successivo):

input: m_i, u_i, s_i, q_i,
$u : u_0$,
per k: 0 a $n-1$ fare:
($u : u \bmod m_k$,
$a : (u_k - u)s_{k+1} \bmod m_{k+1}$,
$u : u + aq_{k+1}$),
output: u.

Esempio. Vediamo come funziona il metodo di Newton sull'esempio visto in precedenza. Calcoliamo i q_k:

$$\begin{aligned} q_1 &= m_0 = 7, \\ q_2 &= m_0 m_1 = 7 \cdot 11 = 77, \\ q_3 &= m_0 m_1 m_2 = 7 \cdot 11 \cdot 13 = 1001. \end{aligned}$$

Per gli s_k abbiamo:

k=1:

$$s_1 = s_0^{(1)} \equiv m_0^{-1} = 7^{-1} \bmod 11 = 8;$$

k=2:

$$\begin{aligned} s_0^{(2)} &\equiv m_0^{-1} = 7^{-1} \bmod 13 = 2, \\ s_1^{(2)} &\equiv m_1^{-1} = 11^{-1} \bmod 13 = 6, \end{aligned}$$

per cui:

$$s_2 \equiv 2 \cdot 6 \bmod 13 = 12 \bmod 13 = 12;$$

k=3:

$$\begin{aligned} s_0^{(3)} &\equiv m_0^{-1} = 7^{-1} \bmod 15 = 13, \\ s_1^{(3)} &\equiv m_1^{-1} = 11^{-1} \bmod 15 = 11, \\ s_2^{(3)} &\equiv m_2^{-1} = 13^{-1} \bmod 15 = 7, \end{aligned}$$

e

$$s_3 \equiv -2 \cdot -4 \cdot 7 = 56 \bmod 15 = 11.$$

L'algoritmo dà allora:

k=0:

$$u = u_0 \bmod 7 = -1 \bmod 7 = 6;$$

k=1:

$$\begin{aligned} u &: 6, \\ a &: (-2 - (6)) \cdot 8 = -64 \bmod 11 = 2, \\ u &: 6 + \cdot 7 = 20; \end{aligned}$$

abbiamo a questo punto:

$$\begin{aligned} 20 &\equiv -1 \bmod 7, \\ 20 &\equiv -2 \bmod 11; \end{aligned}$$

k=2:

$$\begin{aligned} u &: 20 \bmod 13 = 7, \\ a &: (2-7) \cdot 2 = -10 \bmod 15 = 5, \\ u &: 20 + 5 \cdot 77 = 405; \end{aligned}$$

qui abbiamo:

$$\begin{aligned} 405 &\equiv -1 \bmod 7, \\ &\equiv -2 \bmod 11, \\ &\equiv 2 \bmod 13; \end{aligned}$$

k=3:

$$\begin{aligned} u &: 405 \bmod 15 = 0, \\ a &: (6-0)\cdot 11 = 66 \bmod 15 = 6, \\ u &: 405 + 6 \cdot 1001 = 6411, \end{aligned}$$

che è l'intero trovato col metodo di Lagrange.

Si osservi ora che:

$$u = u^{(n)} = (u^{(0)} - u^{(-1)}) + (u^{(1)} - u^{(0)}) + \ldots + (u^{(n)} - u^{(n-1)}).$$

Posto $u^{(-1)} = 0$ abbiamo:

$$u = a_0 + a_1 m_0 + a_2 m_0 m_1 + \ldots + a_n m_0 m_1 \cdots m_{n-1}. \tag{1.3}$$

Gli interi a_i forniscono quella che si chiama la *rappresentazione newtoniana* di u nella "base mista" $1, m_0, m_0 m_1, \ldots, m_0 m_1 \cdots m_{n-1}$:

$$u =< a_0, a_1, \ldots, a_n > .$$

Nell'esempio visto si ha $6411 = 6 + 2 \cdot 7 + 5 \cdot 77 + 6 \cdot 1001$, e dunque:

$$6411 =< 6, 2, 5, 6 > .$$

1.3 Polinomi

Come nel caso degli interi, esiste tra i polinomi a coefficienti in un campo una divisione con resto: se $f = f(x)$ e $g = g(x)$ sono due polinomi, esiste una (unica) coppia di polinomi $q = q(x)$ e $r = r(x)$, con $\partial r < \partial g$, tale che:

$$f = gq + r.$$

(Il simbolo ∂ indica il grado del polinomio. Ricordiamo che gli elementi del campo (*costanti*) hanno grado 0, ad esclusione dello 0 (il *polinomio nullo*), al quale non si assegna alcun grado). Vediamo come si trovano q e r. All'inizio abbiamo un q e un r, e sono:

$$q = 0 \text{ e } r = f;$$

infatti:

$$f = 0 \cdot g + f,$$

ma la condizione $\partial r < \partial g$ non sarà in generale soddisfatta. (Si osservi che $q = 0$ e $r = f$ è la soluzione quando $\partial g > \partial f$). Se $r \neq 0$ e $\partial r \geq \partial g$, consideriamo i monomi di grado massimo di r e g, e siano $m(r)$ e $m(g)$, e il loro quoziente $m(r)/m(g)$. I nuovi valori di q e r saranno:

$$q + \tfrac{m(r)}{m(g)} \text{ e } r - \tfrac{m(r)}{m(g)}g.$$

Quando $r = 0$ o $\partial r < \partial g$, il procedimento termina. Abbiamo dunque il seguente algoritmo.

input: f, g,
$q : 0,\ r : f$,
mentre $r \neq 0$ e $\partial r > \partial g$ fare:
$(q : q + \frac{m(r)}{m(g)},\ r : r - \frac{m(r)}{m(g)}g)$,
output: q,r.

Esempio. $f = x^4 - 2x + 1$, $g = x^2 + 1$,
$q : 0,\ r = f$.
$r \neq 0$? Sì. $\partial r > \partial g$? Sì.
$m(r)/m(g) = x^4/x^2 = x^2$,
$q : 0 + x^2,\ r : f - x^2 g = -2x$,
$\partial r > \partial g$? No.

L'algoritmo termina, con output i valori attuali di q e r, cioè x^2 e $-2x$, che sono il quoziente e il resto della divisione.

Vediamo ora perchè l'algoritmo funziona, cioè fa effettivamente quello che vogliamo (fornire q ed r con $f = qg + r$ e $0 \leq \partial r < \partial g$). Intanto perchè $f = qg + r$ è vera per i valori iniziali 0 ed f di q ed r, e inoltre perchè questa uguaglianza resta vera quando si sostituiscono a q ed r i nuovi valori:

$$f = qg + r = (q + \frac{m(r)}{m(g)})g + (r - \frac{m(r)}{m(g)}g). \tag{1.4}$$

Infine perchè il valore finale di r è $r = 0$ oppure è tale che $\partial r < \partial g$ (e l'algoritmo si ferma). Infatti, il grado di $r - \frac{m(r)}{m(g)}g$ è inferiore al grado di r; siano:

$$\begin{aligned} r &= a_0 x^m + a_1 x^{m-1} + \cdots + a_m, \\ g &= b_0 x^k + b_1 x^{k-1} + \cdots + b_k, \end{aligned}$$

e sia $m \geq k$. Allora:

$$\begin{aligned} r - \frac{m(r)}{m(g)}g &= (a_0 x^m + a_1 x^{m-1} + \cdots) - \frac{a_0}{b_0} x^{m-k}(b_0 x^k + b_1 x^{k-1} + \cdots) \\ &= a_0 x^m + a_1 x^{m-1} + \cdots + a_m - a_0 x^m - \cdots \\ &= a_1 x^{m-1} + \cdots \end{aligned}$$

con gli altri termini di grado inferiore a $m-1$ (oppure l'intera espressione si annulla).

Nota. L'uguaglianza (1.4) è ovviamente vera per qualunque polinomio si metta al posto di $m(r)/m(g)$. La scelta di quest'ultimo, però, è quella che fa sì che il grado diminuisca.

Se $r=0$, allora si dice che g *divide* f o che f *è multiplo di* g. Se un polinomio non ha altri divisori all'infuori di se stesso e delle costanti esso è *irriducibile*. (Quest'ultima nozione corrisponde a quella di numero primo nel caso degli interi). Nell'altro caso, quando cioè esso è prodotto di due polinomi, entrambi di grado inferiore al proprio, il polinomio si dice *riducibile*.

Corollario 1.4. *Se il polinomio $f(x)$ ha una radice a nel campo, $f(a)=0$, allora $f(x)$ è multiplo di $x-a$.*

Dim. La divisione di $f(x)$ per $x-a$ fornisce $f(x)=(x-a)q(x)+r(x)$, con $\partial r(x) < \partial(x-a)=1$, e dunque o $r(x)=0$, oppure $\partial r(x)=0$, cioè $r(x)=c$, una costante. Ma si ha $0=f(a)=(a-a)q(a)+r(a)$, e dunque $r(a)=0$. Ma essendo $r(x)$ costante, se assume una volta il valore 0 lo assume sempre; dunque $r(x)=0$. $\diamondsuit$

Se $f(x)=(x-a)q(x)$ e $q(a)=0$ allora a è radice *doppia* (almeno) di $f(x)$; si ha in questo caso che $(x-a)^2$ divide $f(x)$. In generale, a è radice di *molteplicità* m (almeno) se $(x-a)^m$ divide $f(x)$.

Corollario 1.5. *Un polinomio $f(x)$ di grado $n \geq 1$ ha al più n radici (nel campo o in un suo ampliamento).*

Dim. Induzione su n. Se $n=1$, $f(x)=ax+b$ ha la sola radice $x=-b/a$. Sia $\partial f > 1$. Se $f(x)$ non ha radici, non c'è più niente da dimostrare. Altrimenti, sia a una radice. Per il corollario precedente, $f(x)$ è multiplo di $x-a$: $f(x)=(x-a)q(x)$. Se ora $b \neq a$ è una radice di $f(x)$, lo è anche di $q(x)$, in quanto $0=f(b)=(b-a)q(b)$, ed essendo $b-a \neq 0$ è $q(b)=0$. Il polinomio $q(x)$ è di grado $n-1$, e dunque, per induzione, ha al più $n-1$ radici. Queste sono anche radici di $f(x)$; aggiungendo la radice a, $f(x)$ ne ha al più n. $\diamondsuit$

Tenuto conto del teorema fondamentale dell'algebra: *un polinomio di grado $n \geq 1$ a coefficienti nel campo complesso $\mathcal{C}$ ha almeno una radice in $\mathcal{C}$*, si ha:

Corollario 1.6. *Un polinomio di grado $n \geq 1$ a coefficienti in $\mathcal{C}$ ha esattamente n radici in $\mathcal{C}$ (contando le molteplicità).* $\diamondsuit$

Corollario 1.7. *Se due polinomi $f(x)$ e $g(x)$ di grado al più n hanno gli stessi valori per $n+1$ valori distinti della variabile, allora essi coincidono: $f(x)=g(x)$.*

Dim. Il polinomio $f(x) - g(x)$ è di grado al più n e ammette $n+1$ radici. Non può avere grado positivo perchè allora, per il corollario precedente, avrebbe al più n radici, e non può avere grado zero perchè allora sarebbe una costante non nulla, e in tal caso non avrebbe radici. Allora si tratta del polinomio nullo: $f(x) - g(x) = 0$, e dunque $f(x) = g(x)$. $\diamondsuit$

In particolare, se assegnati $n+1$ valori distinti $x_0, x_1, \ldots, x_n$ della variabile esiste un polinomio di grado al più n (o nullo) che assume $n+1$ valori dati sugli x_k, allora questo polinomio è unico. Che esso effettivamente esista lo vedremo nel prossimo paragrafo.

Come nel caso degli interi, si definisce il *massimo comun divisore* di due polinomi $f(x)$ e $g(x)$: è *il polinomio $d(x)$ che ha come divisori tutti e soli i divisori comuni di $f(x)$ e $g(x)$*. (Nel caso di polinomi, i divisori sono definiti a meno di costanti moltiplicative). La dimostrazione dell'esistenza di $d(x)$ è costruttiva. Come per gli interi essa si basa sull'algoritmo di Euclide, che ora ha la forma seguente: dividendo $f = f(x)$ per $g = g(x)$ si ha:

$$f = gq + r, \qquad \partial r < \partial g,$$

e proseguendo la divisione, si ha (posto $r = r_1, q = q_1$):

$$\begin{aligned}
g &= r_1 q_2 + r_2, && \partial r_2 < \partial r_1,\\
r_1 &= r_2 q_3 + r_3, && \partial r_3 < \partial r_2,\\
&\vdots\\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1}, && \partial r_{k-1} < \partial r_{k-2},\\
r_{k-2} &= r_{k-1} q_k,
\end{aligned}$$

e $r_k = 0$. L'ultimo resto non nullo r_{k-1} è il massimo comun divisore $d = (f, g)$ dei due polinomi. (Se $r = 0$, allora $(f, g) = g$).

Se $d(x)$ è una costante, allora $f(x)$ e $g(x)$ sono *relativamente primi*.

L'esistenza del massimo comun divisore permette di estendere ai polinomi alcuni dei risultati visti per gli interi. In particolare si ha che *ogni polinomio si decompone nel prodotto di polinomi irriducibili*, e ciò, a meno dell'ordine dei fattori e della moltiplicazione per costanti, *in modo unico*.

Abbiamo visto (Corollario 1.4) che se un polinomio ha una radice, allora esso si riduce. Il viceversa non è vero in generale. Ad esempio, nel campo reale, il polinomio $x^4 + 2x^2 + 1$ si spezza in $(x^2 + 1)(x^2 + 1)$, ma radici reali non ne ha.

Esempi. 1. (*Derivata di un polinomio*) La possibilità di eseguire la divisione permette di definire la derivata di un polinomio in modo puramente algebrico. Sia infatti:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

un polinomio su un campo e α un elemento del campo o di un suo ampliamento. Allora dividendo $f(x)$ per $x-\alpha$ si ha:

$$f(x) = (x-\alpha)q(x) + r(x), \tag{1.5}$$

con $r(x)$ costante. Eseguendo esplicitamente la divisione si trova, per il quoziente:

$$\begin{aligned} q(x) &= a_0 x^{n-1} + (a_0\alpha + a_1)x^{n-2} + (a_0\alpha^2 + a_1\alpha + a_2)x^{n-3} + \cdots \\ &+ a_0\alpha^{n-1} + a_1\alpha^{n-2} + \cdots + a_{n-2}\alpha + a_{n-1}, \end{aligned}$$

e per il resto:

$$r(x) = a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n.$$

(Si noti come $r(x)$ sia il valore di $f(x)$ in α, e dunque vale 0 se α è radice di $f(x)$, e viceversa). I coefficienti di $q(x)$ sono dunque polinomi in α di grado 0,1,..., $n-1$, dove il $k-$esimo polinomio ha per coefficienti i primi k coefficienti di $f(x)$. Calcolando $q(x)$ in α si trova $n-k$ volte il termine $a_k\alpha^{n-k-1}$, $k = 0, 1, \ldots, n-1$, e dunque:

$$q(\alpha) = na_0\alpha^{n-1} + (n-1)a_1\alpha^{n-2} + 2a_{n-2}\alpha + a_{n-1}.$$

Scrivendo il polinomio a secondo membro come polinomio in x, si ottiene l'espressione di quella che definiamo come *derivata* del polinomio $f(x)$.

(La derivata della (1.5) eseguita secondo il metodo dell'analisi è:

$$f'(x) = q(x) + (x-\alpha)q'(x),$$

da cui appunto $f'(\alpha) = q(\alpha)$).

2. (*Il metodo di Horner*) Dalla (1.5) vediamo che il valore $f(\alpha)$ di un polinomio $f(x)$ in un punto α è il resto della divisione di $f(x)$ per $x-\alpha$. Questa divisione fornisce un metodo che permette di calcolare $f(\alpha)$, e che è più economico del metodo standard che consiste nel calcolo delle potenze di α. Col metodo standard occorre eseguire le $n-1$ moltiplicazioni $\alpha\cdot\alpha = \alpha^2$, $\alpha^2\cdot\alpha = \alpha^3$,..., $\alpha^{n-1}\cdot\alpha = \alpha^n$, e quindi le n moltiplicazioni $a_i\alpha^i$; in tutto $2n-1$ moltiplicazioni. Si osservi invece come si ottengono i coefficienti del quoziente $q(x)$ a partire da quelli di $f(x)$: cominciando da a_0, si moltiplica per α e si aggiunge il coefficiente successivo:

$$a_0,\ a_0\alpha + a_1,\ (a_0\alpha + a_1)\alpha + a_2, \ldots$$

L'ultimo coefficiente di $q(x)$ è un polinomio di grado $n-1$ in α; moltiplicando ancora per α e aggiungendo a_n si ha il resto della divisione, cioè il valore di $f(x)$ in α:

$$f(\alpha) = ((\ldots(a_0\alpha + a_1)\alpha + a_2)\alpha + \cdots) + a_n.$$

Quest'ultima uguaglianza fornisce un metodo (*metodo di Horner*) per il calcolo di un polinomio in un punto α che richiede n moltiplicazioni, cioè circa la metà di quelle richieste dal metodo standard, e n addizioni.

Come per gli interi abbiamo, con la stessa dimostrazione, l'identità di Bézout per i polinomi:

Teorema 1.8. (IDENTITA' DI BÉZOUT). *Sia $d(x) = (f(x), g(x))$. Allora esistono due polinomi $a(x)$ e $b(x)$ tali che:*

$$d(x) = a(x)f(x) + b(x)g(x). \qquad \diamondsuit$$

Nota. In particolare, se $f(x)$ e $g(x)$ sono relativamente primi allora si ha l'uguaglianza di sopra con $d(x) = d$, una costante. Dividendo $a(x)$ e $b(x)$ per d si hanno due polinomi $a'(x)$ e $b'(x)$ tali che $a'(x)f(x) + b'(x)g(x) = 1$.

Il teorema cinese, che si basa sull'identità di Bézout, sussiste anche per i polinomi, con dimostrazione analoga :

Teorema 1.9. (TEOREMA CINESE PER POLINOMI.) *Siano:*

$$m_0(x), m_1(x), \ldots, m_n(x),$$

polinomi a due a due relativamente primi, e siano:

$$u_0(x), u_1(x), \ldots, u_n(x)$$

polinomi qualunque. Allora esiste un polinomio $u(x)$ tale che:

$$u(x) \equiv u_k(x) \bmod m_k(x),\ k = 0, 1, \ldots, n,$$

e questo $u(x)$ è unico modulo il prodotto $m(x) = m_0(x)m_1(x)\cdots m_n(x)$. (Cioè: $u(x)$ è l'unico polinomio di grado inferiore al grado di $m(x)$ che risolve il dato sistema di congruenze).

Dimostriamo prima un lemma.

Lemma 1.10. *Siano f,g e h tre polinomi con $\partial h < \partial f + \partial g$, e si abbia, per certi polinomi a e b, la relazione:*

$$af + bg = h.$$

Allora la stessa relazione sussiste con due polinomi a_1 e b_1, tali che $\partial a_1 < \partial g$ e $\partial b_1 < \partial f$.

Dim. Osserviamo intanto che se $\partial a < \partial g$ allora è necessariamente $\partial b < \partial f$ altrimenti, $\partial h = \partial(af + bg) = \partial bg \geq \partial f + \partial g$, contro l'ipotesi. Supponiamo allora $\partial a \geq \partial g$; dividendo si ha $a = gq + r$ con $\partial r < \partial g$; posto allora $a_1 = a - gq$

e $b_1 = b + fq$, si ha $a_1 f + b_1 g = h$, ed essendo $\partial a_1 < \partial$g è anche $\partial b_1 < \partial f$, per quanto osservato sopra. $\diamondsuit$

Corollario 1.11. *Siano f e g due polinomi relativamente primi. Esistono allora due polinomi a e b con $\partial a < \partial g$ e $\partial b < \partial f$ e tali che:*

$$af + bg = 1.$$

Inoltre, a e b sono univocamente determinati.

Dim. Due polinomi a e b tali che $af + bg = 1$ esistono in quanto a e b sono relativamente primi. Allora la tesi segue dal lemma dove si prenda per h il polinomio identicamente uguale a 1. Se a_1, b_1 è un'altra tale coppia, allora sottraendo la relazione $a_1 f + b_1 g = 1$ dalla precedente si ha $(a - a_1)f = (b_1 - b)g$, ed essendo $(f, g) = 1$, g deve dividere $a - a_1$; ma $\partial(a - a_1) < \partial g$, e dunque $a - a_1 = 0$ e $a_1 = a$, per cui è anche $b_1 = b$. $\diamondsuit$

Veniamo ora alla dimostrazione del Teorema 1.9.

Dim. Sia $m(x) = \prod_{k=0}^{n} m_k(x)$ e sia $l_k(x) = \frac{m(x)}{m_k(x)}$. Allora $(m_k(x), l_k(x)) = 1$, e per il corollario esistono e sono unici $a_k(x)$ e $b_k(x)$ tali che $\partial a_k(x) < \partial l_k(x)$ e $\partial b_k(x) < \partial m_k(x)$ e

$$a_k(x)m_k(x) + b_k(x)l_k(x) = 1.$$

Si ponga $L_k(x) = b_k(x)l_k(x)$, e si osservi che essendo $\partial b_k(x) < \partial m_k(x)$, il grado di L_k è minore del grado di $m(x)$. Inoltre, per costruzione,

$$\begin{aligned} L_k(x) &\equiv 1 \mod m_k(x), \\ L_k(x) &\equiv 0 \mod m_i(x),\ i \neq k. \end{aligned}$$

Allora,

$$u(x) = \sum_{k=0}^{n} u_k L_k(x)$$

è il polinomio cercato. $\diamondsuit$

Nell'anello $A = K[x]/(m(x))$ dei polinomi a coefficienti nel campo K e di grado inferiore al grado di $m(x)$, con la somma usuale e prodotto seguito dalla riduzione mod $m(x)$, i polinomi $L_k(x)$ sono idempotenti ortogonali e a somma 1:

1. $L_0(x) + L_1(x) + \ldots + L_n(x) \equiv 1 \mod m(x)$.
   Ciò segue dal fatto che $\sum L_k(x) - 1$ è divisibile per tutti gli $m_k(x)$, e dunque per $m(x)$.

2. $L_i(x)L_j(x) \equiv 0 \mod m(x), i \neq j$.

Il fattore $m_i(x)$ che manca in $L_i(x)$ compare in $L_j(x)$. Nel prodotto $L_i(x)L_j(x)$ compaiono allora tutti i fattori $m_k(x)$, e dunque $m(x)$ è un fattore di questo prodotto.

3. $L_k(x)^2 \equiv L_k(x) \bmod m(x)$.
Segue moltiplicando 1. per $L_k(x)$ e tenendo poi conto di 2.

Ogni elemento di $f(x) \in A$ ammette poi un'unica decomposizione della forma:

$$f(x) \equiv f_0(x)L_0(x) + f_1(x)L_1(x) + \cdots + f_n(x)L_n(x) \bmod m(x),$$

dove $f_i(x)$ è il resto della divisione di $f(x)$ per $m_i(x)$. Come nel caso degli interi le proprietà suddette ci permettono di decomporre l'anello A nella somma diretta dei sottoanelli $A_k = \{f(x)L_k(x) \bmod m(x)\}$. Infine, con la stessa dimostrazione del caso degli interi si ha $A_k \simeq K[x]/(m_k(x))$.

Nota. L'anello A ha anche una struttura di spazio vettoriale su K, come subito si vede; si tratta dunque un'*algebra*.

Un caso particolare, ma molto importante, del teorema cinese è quello in cui i polinomi $m_k(x)$ sono di primo grado e della forma $x - x_k$, e gli $u_k(x)$ sono costanti. E' il caso che tratteremo in dettaglio nel prossimo paragrafo.

Esercizi

9. Enunciare e svolgere gli esercizi dal n. 1 al 5 e il n. 7 per il caso dei polinomi.

10. Dimostrare che se $f = \prod_i f_i$ con $(f_i, f_j) = 1$, e a è un polinomio qualunque, si ha:

$$\frac{a}{f} = g + \frac{a_1}{f_1} + \frac{a_2}{f_2} + \cdots + \frac{a_n}{f_n}$$

dove g è un polinomio e $\partial a_i < \partial f_i$, e gli a_i sono unici soggetti a queste condizioni. Inoltre, se $\partial a < \partial f$ allora $g = 0$. (La detta decomposizione di a/f si chiama *decomposizione in frazioni semplici*).

11. Un polinomio di grado ≤ 3 su un campo qualunque è riducibile se e solo se ammette una radice.

12. Dare un esempio che dimostri come venga meno l'unicità della fattorizzazione in polinomi irriducibili se i coefficienti non sono in un campo.

13. Dimostrare che nel campo complesso due polinomi non sono primi tra loro se e solo se hanno una radice in comune.

14. Dimostrare che il MCD di due polinomi $f(x)$ e $g(x)$ non dipende dal campo dei coefficienti (nel senso che se i coefficienti di $f(x)$ e $g(x)$ appartengono sia ad un campo K che ad un campo L, il MCD è sempre lo stesso).

1.4 Interpolazione polinomiale

Il classico problema dell'interpolazione polinomiale ha la forma seguente: dati $n+1$ numeri distinti ($n+1$ elementi di un campo):

$$x_0, x_1, \ldots, x_n,$$

e $n+1$ numeri qualsiasi:

$$u_0, u_1, \ldots, u_n,$$

trovare un polinomio $u(x)$ di grado al più n il cui valore in x_k sia u_k, $k = 0, 1, \ldots, n$:

$$u(x_k) = u_k$$

(sappiamo, per il Corollario 1.7, che tale polinomio se esiste è unico).

Questo problema è un caso particolare di quello risolto dal teorema cinese. Infatti, se $u(x)$ è tale che $u(x_k) = u_k$, allora il polinomio

$$u(x) - u_k$$

ha la radice x_k, e dunque è divisibile per $x - x_k$; in altri termini, $u(x) - u_k \equiv 0 \bmod (x - x_k)$, ovvero:

$$u(x) \equiv u_k \bmod (x - x_k), \tag{1.6}$$

$k = 0, 1, \ldots, n$. Poichè gli x_k sono distinti, i polinomi $x - x_k$ sono a due a due relativamente primi. Siamo allora nelle ipotesi del teorema cinese, con $m_k(x) = x - x_k$ e i polinomi $u_k(x) = u_k$ di grado zero (costanti). Il teorema assicura allora l'esistenza di un polinomio $u(x)$ tale che valga la (1.6) e la sua unicità modulo il prodotto $\prod_{i=0}^{n}(x - x_k)$. Poichè questo prodotto è di grado $n + 1$, $u(x)$ è l'unico polinomio di grado al più n (o eventualmente nullo) che soddisfa le condizioni date. Esso prende il nome di *polinomio interpolatore di Lagrange*.

Che un tale $u(x)$ esista e sia unico si può vedere anche dalla teoria dei sistemi di equazioni lineari. Per il polinomio incognito $u(x) = \sum_{i=0}^{n} a_i x^i$ deve aversi $\sum_{i=0}^{n} a_i x_k^i = u_k$, $k = 0, 1, \ldots, n$. Abbiamo così un sistema di $n + 1$ equazioni nelle $n + 1$ incognite $a_0, a_1, \ldots, a_n$, il cui determinante è il Vandermonde V degli x_i. Poichè gli x_i sono distinti, è $V \neq 0$, e dunque la soluzione esiste ed è unica.

Per il calcolo di $u(x)$ abbiamo due metodi, come nel caso degli interi.

1.4.1 Il metodo di Lagrange

Determiniamo i polinomi $L_k(x)$, visti nel paragrafo precedente. In questo caso essi prendono il nome di *polinomi di Lagrange*, e il loro calcolo è grandemente facilitato dal fatto che gli $m_k(x)$ sono ora lineari. Infatti, dati $x - x_i$ e $x - x_j$ è immediato trovare $a(x)$ e $b(x)$ tali che $a(x)(x - x_i) + b(x)(x - x_j) = 1$: basta prendere le due costanti:

$$a(x) = \frac{1}{x_j - x_i}, \quad b(x) = \frac{1}{x_i - x_j}.$$

Si ha:

$$\frac{1}{x_j - x_i}(x - x_i) + \frac{1}{x_i - x_j}(x - x_j) = \frac{x - x_i - (x - x_j)}{x_j - x_i} = \frac{x_j - x_i}{x_j - x_i} = 1.$$

Ne segue:

$$L_k(x) = \prod_{i \neq k} s_i^{(k)} \cdot \prod_{i \neq k}(x - x_i) = \frac{\prod_{i \neq k}(x - x_i)}{\prod_{i \neq k}(x_k - x_i)}.$$

Gli $L_k(x)$ sono dunque tutti di grado n, e il polinomio $u(x)$ cercato è

$$u(x) = \sum_{k=0}^{n} u_k L_k(x).$$

Questo polinomio è tale che $u(x_k) = u_k$ in quanto $L_k(x_k) = 1$ e $L_k(x_j) = 0$, $j \neq k$. Esso prende il nome di *polinomio interpolatore di Lagrange*.

Per il calcolo di $u(x)$ con questo metodo occorre eseguire $2(n-1)$ moltiplicazioni per ciascuno degli $L_k(x)$ ($n-1$ a numeratore e altrettante a denominatore),

e dunque il calcolo degli $L_k(x)$ costa in tutto $2(n-1)(n+1) = 2n^2 - 2$ moltiplicazioni. Occorre poi aggiungere le $n+1$ moltiplicazioni per gli u_k; in tutto allora $2n^2 + n - 1$ moltiplicazioni.

Esempio. Siano:

$$x_0 = 1, x_1 = 4, x_2 = 6, x_3 = 11,$$
$$u_0 = 10, u_1 = 334, u_2 = 1040, u_3 = 5920.$$

Allora:

$$\begin{aligned}
L_0(x) &= \frac{(x-4)(x-6)(x-11)}{(1-4)(1-6)(1-11)} = \frac{x^3 - 21x^2 + 134x - 264}{-150}, \\
L_1(x) &= \frac{(x-1)(x-6)(x-11)}{(4-1)(4-6)(4-11)} = \frac{x^3 - 18x^2 + 83x - 66}{42}, \\
L_2(x) &= \frac{(x-1)(x-4)(x-11)}{(6-1)(6-4)(6-11)} = \frac{x^3 - 16x^2 + 59x - 44}{-50}, \\
L_3(x) &= \frac{(x-1)(x-4)(x-6)}{(11-1)(11-4)(11-6)} = \frac{x^3 - 11x^2 + 34x - 24}{350}.
\end{aligned}$$

Ne segue:

$$u(x) = 10L_0(x) + 334L_1(x) + 1040L_2(x) + 5920L_3(x) = 4x^3 + 5x^2 - x + 2.$$

Sia $m(x) = (x - x_0)(x - x_1)\cdots(x - x_n)$. Sappiamo che gli $L_k(x)$ sono idempotenti ortogonali a somma 1 mod $m(x)$; ma qui la loro somma vale 1, e non solo 1 mod $m(x)$:

$$L_0(x) + L_1(x) + \cdots + L_n(x) = 1.$$

Ciò segue calcolando, o osservando che la somma a primo membro è un polinomio di grado $\leq n$ che vale 1 per gli $n+1$ valori $x_0, x_1, \ldots, x_n$ della variabile x, e dunque è identicamente uguale a 1.

Nella scrittura:

$$f(x) \equiv f_0(x)L_0(x) + f_1(x)L_1(x) + \cdots + f_n(x)L_n(x) \bmod m(x),$$

che dà la decomposizione dell'algebra $A = K[x]/(m(x))$ dei polinomi di grado al più n, gli $f_k(x)$ sono ora i resti della divisione di $f(x)$ per $x - x_k$, e dunque $f_k(x) = f(x_k)$; i polinomi $f_k(x)$ sono cioè delle costanti, e i sottoanelli $A_k \simeq K[x]/(m_k(x))$ sono tutti isomorfi a K:

$$K/(m(x)) = K \oplus K \oplus \cdots \oplus K.$$

La base standard di questo spazio vettoriale di dimensione $n+1$ è data dai monomi $1, x, x^2, \ldots, x^n$. Dimostriamo ora che anche gli $L_k(x)$ formano una base di questo spazio.

Teorema 1.12. *Gli $L_k(x)$ formano una base dello spazio vettoriale dei polinomi di grado al più n.*

Dim. Sia $f(x)$ un polinomio di grado al più n. Allora:

$$f(x_0)L_0(x) + f(x_1)L_1(x) + \cdots + f(x_n)L_n(x)$$

è un polinomio di grado al più n che ha gli stessi valori di $f(x)$ sugli $n+1$ punti $x_0, x_1, \ldots, x_n$, e dunque coincide con $f(x)$. Si ha allora che $f(x)$ è combinazione lineare degli $L_k(x)$ (e i coefficienti sono gli $f(x_k)$); ciò dimostra che gli $L_k(x)$ generano il detto spazio. Inoltre, quella scritta è l'unica combinazione lineare degli $L_k(x)$ che dà $f(x)$, perchè se

$$f(x) = a_0L_0(x) + a_1L_1(x) + \cdots + a_nL_n(x),$$

allora calcolando successivamente in $x_0, x_1, \ldots, x_n$ si trova $a_k = f(x_k)$. Gli $L_k(x)$ sono dunque linearmente indipendenti. $\diamondsuit$

Nota. Contrariamente alla base standard, gli elementi di questa base hanno tutti lo stesso grado n. Così, ogni scelta di $n+1$ numeri $x_0, x_1, \ldots, x_n$ distinti determina una base dello spazio tutti gli elementi della quale hanno lo stesso grado n.

Vediamo ora come passare da una base data dagli $L_k(x)$ (per una scelta degli x_i), alla base standard $1, x, x^2, \ldots, x^n$. Per un monomio x^k si ha:

$$x^k = x_0^k L_0(x) + x_1^k L_1(x) + \ldots + x_n^k L_n(x).$$

Ne segue che la matrice di passaggio dalla base degli $L_k(x)$ a quella degli x^i è la matrice di Vandermonde $(n+1) \times (n+1)$:

$$V = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_0 & x_1 & \ldots & x_n \\ x_0^2 & x_1^2 & \ldots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_0^n & x_1^n & \ldots & x_n^n \end{pmatrix}.$$

(Trattandosi di una matrice di cambiamento di base, V è non singolare. Si ha così una dimostrazione del fatto che il determinante di Vandermonde è diverso da zero). La matrice inversa V^{-1} della V è la matrice di passaggio dalla base degli x^i a quella degli $L_k(x)$. Gli elementi di V^{-1} ci permettono dunque di scrivere gli $L_k(x)$ in termini delle potenze di x. Ma ciò significa semplicemente

scrivere gli $L_k(x)$ nell'usuale forma di polinomi in x. Ne segue che V^{-1} *è la matrice nella quale gli elementi della k-esima riga sono i coefficienti del k-esimo polinomio di Lagrange* $L_k(x)$, $k = 0, 1, \ldots, n$.

Esempio. Come nell'esempio precedente, prendiamo:

$$x_0 = 1, x_1 = 4, x_2 = 6, x_3 = 11.$$

La matrice di Vandermonde è in questo caso:

$$V = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 4 & 6 & 11 \\ 1 & 16 & 36 & 121 \\ 1 & 64 & 216 & 1331 \end{pmatrix}.$$

Il polinomio $L_0(x)$ è

$$L_0(x) = \frac{264}{150} - \frac{134}{150}x + \frac{21}{150}x^2 - \frac{1}{150}x^3,$$

e analogamente per gli altri. La matrice V^{-1} è

$$V^{-1} = \begin{pmatrix} \frac{264}{150} & -\frac{134}{150} & \frac{21}{150} & -\frac{1}{150} \\ -\frac{66}{42} & \frac{83}{42} & -\frac{18}{42} & \frac{1}{42} \\ \frac{44}{50} & -\frac{59}{50} & \frac{16}{50} & -\frac{1}{50} \\ -\frac{24}{350} & \frac{34}{350} & -\frac{11}{350} & \frac{1}{350} \end{pmatrix}.$$

Vediamo ora un'altra espressione per gli $L_k(x)$. Sia:

$$m(x) = (x - x_0)(x - x_1)\cdots(x - x_n).$$

Abbiamo:

$$L_k(x) = \frac{\prod_{i\neq k}(x - x_i)}{\prod_{i\neq k}(x_k - x_i)} = \frac{1}{\prod_{i\neq k}(x_k - x_i)} \cdot \frac{m(x)}{x - x_k},$$

e si osservi che $\prod_{i\neq k}(x_k - x_i)$ è $\frac{m(x)}{x-x_k}$ calcolato in x_k. Posto allora $\frac{m(x)}{x-x_k} = q_k(x)$ si ha $L_k(x) = \frac{q_k(x)}{q_k(x_k)}$. Derivando $m(x) = (x - x_k)q_k(x)$ si ottiene $m'(x) = q_k(x) + (x - x_k)q_k'(x)$, da cui $q_k(x_k) = m'(x_k)$, e infine:

$$\begin{aligned} L_k(x) &= \frac{q_k(x)}{m'(x_k)} = \frac{m(x)}{m'(x_k)(x - x_k)} = \frac{1}{m'(x_k)} \cdot \frac{m(x)}{x - x_k} \\ &= \frac{1}{m'(x_k)}(x - x_0)\cdots(x - x_{k-1})(x - x_{k+1})\cdots(x - x_n). \end{aligned}$$

In altri termini, i coefficienti di $L_k(x)$ sono, a meno del fattore $m'(x_k)$, quelli di $\frac{m(x)}{x-x_k}$.

Esercizi

Ricordiamo che il duale di uno spazio vettoriale V su un campo K è lo spazio V^* delle trasformazioni lineari $f : V \longrightarrow K$. Se $\{v_i\}$ è una base di V, la base di V^* duale della $\{v_i\}$ è data dagli f_i tali che $f_i(v_j) = \delta_{i,j}$. Negli esercizi che seguono lo spazio è quello dei polinomi di grado al più n considerato in questo paragrafo.

15. Determinare la base duale della base degli $L_k(x)$.

16. Determinare la base duale della base standard $1, x, \ldots, x^n$.

17. Dimostrare che i polinomi $(x-a)^k$, $k = 0, 1, \ldots, n$, sono una base. Qual è la sua base duale?

18. Dimostrare che qualunque insieme di polinomi $p_k(x)$, di gradi $k = 0, 1, \ldots, n$ forma una base.

19. Dimostrare che la matrice di Vandermonde è non singolare usando il Corollario 1.5.

20. Dimostrare che, oltre alle $2n^2 + n - 1$ moltiplicazioni, il calcolo di $u(x)$ con il metodo di Lagrange richiede n addizioni, $2n^2 + 2$ sottrazioni e $n + 1$ divisioni.

1.4.2 Il metodo di Newton

Il polinomio interpolatore si può calcolare, come nel caso degli interi, alla Newton. Se

$$L_0^{(r)}, L_1^{(r)}, \ldots, L_r^{(r)},$$

sono gli interi forniti dal metodo di Lagrange nel caso di $r+1$ moduli $m_0, m_1, \ldots, m_r$, e se $u_0, u_1, \ldots, u_r$ sono $r+1$ interi qualunque, una soluzione è data da:

$$u^{(r)} = u_0 L_0^{(r)} + u_1 L_1^{(r)} + \cdots + u_r L_r^{(r)}.$$

Consideriamo la differenza $u^{(n)} - u^{(n-1)}$; abbiamo:

$$u^{(n)} - u^{(n-1)} = u_0(L_0^{(n)} - L_0^{(n-1)}) + \cdots + u_{n-1}(L_{n-1}^{(n)} - L_{n-1}^{(n-1)}) + u_n L_n^{(n)}.$$

Ora, $L_k^{(n)}$ e $L_k^{(n-1)}$ sono entrambi congrui a 1 modulo m_k e a 0 modulo m_i, $i \neq k$, $k = 0, 1, \ldots, n-1$, e dunque la differenza $u^{(n)} - u^{(n-1)}$ è congrua a 0 modulo $m_0, m_1, \ldots, m_{n-1}$ e perciò anche modulo il loro prodotto q_n:

$$u^{(n)} - u^{(n-1)} \equiv 0 \bmod q_n,$$

ovvero:

$$u^{(n)} = u^{(n-1)} + a_n q_n.$$

Analogamente:

$$u^{(n-1)} = u^{(n-2)} + a_{n-1}q_{n-1}$$

e

$$u = u^{(n)} = a_0 + a_1q_1 + \cdots + a_nq_n. \tag{1.7}$$

La situazione è del tutto analoga nel caso dei polinomi. Si considerano i polinomi di Lagrange nel caso di $r+1$ punti: $x_0, x_1, \ldots, x_r$, e $r+1$ valori $u(x_0), u(x_1), \ldots, u(x_r)$ di $u(x)$:

$$L_0^{(r)}(x), L_1^{(r)}(x), \ldots, L_r^{(r)}(x).$$

La soluzione per il caso di $n+1$ punti è

$$u(x) = u^{(n)}(x) = u_0L_0^{(n)}(x) + \cdots + u_{n-1}L_{n-1}^{(n)}(x) + u_nL_n^{(n)}(x).$$

Per $k = 0, 1, \ldots, n-1$ il valore di $L_k^{(n)}(x)$ e $L_k^{(n-1)}(x)$ in $x = x_k$ è 1, e in $x = x_j$, $j \neq k$, è 0. $L_n^{(n)}$ vale zero negli stessi punti. Ne segue che la differenza $u^{(n)}(x) - u^{(n-1)}(x)$ è divisibile per $(x-x_0)(x-x_1)\cdots(x-x_{n-1})$, per cui:

$$u^{(n)}(x) = u^{(n-1)}(x) + a_n(x-x_0)(x-x_1)\cdots(x-x_{n-1}).$$

Tutto questo conduce alla *formula di interpolazione di Newton*:

$$\begin{aligned} u(x) = u^{(n)}(x) &= a_0 + a_1(x-x_0) + a_2(x-x_0)(x-x_1) + \cdots \\ &+ a_n(x-x_0)(x-x_1)\cdots(x-x_{n-1}). \end{aligned} \tag{1.8}$$

L'analogia con la formula (1.3) è evidente. Inoltre, come nella (1.3), il coefficiente a_k della (1.8) non dipende né da $x_{k+1}, \ldots, x_n$ né da $u_{k+1}, \ldots, u_n$.

Il calcolo degli a_i procede come nel caso degli interi:

$$\begin{aligned} u_0 &= u(x_0) = a_0, \\ u_1 &= u(x_1) = a_0 + a_1(x_1 - x_0), \end{aligned}$$

da cui:

$$a_1 = \frac{u_1 - u_0}{x_1 - x_0}.$$

Inoltre,

$$\begin{aligned} u_2 = u(x_2) &= a_0 + a_1(x_2 - x_0) + a_2(x_2 - x_0)(x_2 - x_1) \\ &= u_0 + \frac{u_1 - u_0}{x_1 - x_0}(x_2 - x_0) + a_2(x_2 - x_0)(x_2 - x_1), \end{aligned}$$

da cui:

$$a_2 = \frac{(u_2 - u_0)(x_1 - x_0) - (u_1 - u_0)(x_2 - x_0)}{(x_1 - x_0)(x_2 - x_0)(x_2 - x_1)},$$

e così di seguito.

Abbiamo parlato di analogia tra la (1.3) e la (1.8): ma si tratta in realtà della stessa formula. Prendere un intero mod m_k significa prenderne il resto nella divisione per m_k. Prendere un polinomio mod $(x - x_k)$ significa prenderne il resto nella divisione per $x - x_k$, e dunque il valore in x_k. In particolare il resto della divisione di $x - x_i$ per $x - x_k$ è $x_k - x_i$. Viste sotto questa luce le due formule sono la stessa. Infatti, nel caso di (1.3), $a_0 \equiv u_0 \bmod m_0$, cioè a_0 è il resto della divisione di u_0 per m_0. Per a_1 la (1.3) dà:

$$a_1 \equiv \frac{u_1 - u_0}{m_0} \bmod m_1, \tag{1.9}$$

e la (1.8):

$$a_1 = \frac{u_1 - u_0}{x_1 - x_0}. \tag{1.10}$$

Ora $x_1 - x_0$ è il resto della divisione di $x - x_0$ per $x - x_1$, ciò che corrisponde a $m_0 \bmod m_1$ nella (1.9). La cosa risalta ancora di più scrivendo la (1.9) come:

$$a_1 \equiv \frac{(u_1 - u_0) \bmod m_1}{m_0 \bmod m_1}, \tag{1.11}$$

e la (1.10) come:

$$a_1 \equiv \frac{(u_1 - u_0) \bmod (x - x_0)}{(x - x_0) \bmod (x - x_1)}, \tag{1.12}$$

($(u_1 - u_0) \bmod (x - x_0)$ è semplicemente $u_1 - u_0$ in quanto $u_1 - u_0$ è una costante). Analogamente per gli altri a_i.

Esempio. Vogliamo determinare il polinomio $u(x)$ di grado al più 3 tale che, per

$$x_0 = -2, x_1 = -1, x_2 = 0, x_3 = 1,$$

si abbia:

$$\begin{aligned} u_0 &= u(-2) = -1, \\ u_1 &= u(-1) = 2, \\ u_2 &= u(0) = 1, \\ u_3 &= u(1) = -2. \end{aligned}$$

Gli a_i della (1.8) sono in questo caso:

$$\begin{aligned} a_0 &= u_0 = -1; \\ a_1 &= \frac{u_1 - u_0}{x_1 - x_0} = \frac{3}{1} = 3; \\ a_2 &= \frac{2 \cdot 1 - 3 \cdot 2}{1 \cdot 2 \cdot 1} = \frac{-4}{2} = -2. \end{aligned}$$

Per a_3 abbiamo:

$$u_3 = u(1) = a_0 + a_1 \cdot 3 + a_2 \cdot 6 + a_3 \cdot 6 = -1 + 3 \cdot 3 - 2 \cdot 6 + a_3 \cdot 6,$$

che dà:

$$a_3 = \frac{1}{3}.$$

Pertanto,

$$\begin{aligned} u(x) &= -1 + 3(x+2) - 2(x^2 + 3x + 2) + \frac{1}{3}(x^3 + 3x^2 + 2x) \\ &= \frac{1}{3}x^3 - x^2 - \frac{7}{3}x + 1. \end{aligned}$$

1.4.3 Differenze divise

Gli a_i del metodo di Newton sono particolari *differenze divise*, nel senso che ora vediamo. Sia $f(x)$ una funzione qualunque (non necessariamente un polinomio), e siano $y_0, y_1, \ldots, y_n$ i suoi valori nei punti $x_0, x_1, \ldots, x_n$. La frazione $\frac{y_i - y_j}{x_i - x_j}$ si denota con $[x_i x_j]$:

$$[x_0 x_1] = \frac{y_0 - y_1}{x_0 - x_1}, \quad [x_1 x_2] = \frac{y_1 - y_2}{x_1 - x_2}, \ldots.$$

Si osservi che il valore di $[x_i x_j]$ non dipende dall'ordine degli argomenti: $[x_i x_j] = [x_j x_i]$. Le $[x_i x_j]$ si chiamano *differenze divise del primo ordine* della funzione $f(x)$. Le frazioni:

$$[x_0 x_1 x_2] = \frac{[x_0 x_1] - [x_1 x_2]}{x_0 - x_2},$$

e

$$[x_1 x_2 x_3] = \frac{[x_1 x_2] - [x_2 x_3]}{x_1 - x_3},$$

etc., sono le *differenze divise del secondo ordine*. In generale,

$$[x_0 x_1 \ldots x_n] = \frac{[x_0 x_1 \ldots x_{n-1}] - [x_1 x_2 \ldots x_n]}{x_0 - x_n}$$

sono le differenze divise di ordine n. Per definizione, $[x_i] = y_i$, il valore di $f(x)$ in x_i; queste sono le *differenze divise di ordine* 0. Come nel caso $n = 1$, le differenze di ordine n non dipendono dall'ordine degli x_i: $[x_0 x_1 \ldots x_k] = [x_{i_0} x_{i_1} \ldots x_{i_k}]$, dove $i_0, i_1, \ldots, i_k$ è una qualunque permutazione di $0, 1, \ldots, k$.

La tavola che segue mostra come calcolare le varie differenze ($n = 4$):

$$
\begin{array}{cccccc}
x & y & & & & \\
x_0 & y_0 & & & & \\
 & & [x_0x_1] & & & \\
x_1 & y_1 & & [x_0x_1x_2] & & \\
 & & [x_1x_2] & & [x_0x_1x_2x_3] & \\
x_2 & y_2 & & [x_1x_2x_3] & & [x_0x_1x_2x_3x_4] \\
 & & [x_2x_3] & & [x_1x_2x_3x_4] & \\
x_3 & y_3 & & [x_2x_3x_4] & & \\
 & & [x_3x_4] & & & \\
x_4 & y_4 & & & &
\end{array}
$$

Il valore di una parentesi quadra $[\ldots]$ si ottiene dividendo la differenza tra le due parentesi che la precedono per la differenza tra la prima e l'ultima x della parentesi. Detta altrimenti: il valore di una parentesi si ottiene prendendo la differenza tra le due parentesi ottenute cancellando due valori differenti di x e dividendola per la differenza di questi due valori.

Esempio.

$$
\begin{array}{cccccc}
x & y & & & & \\
-2 & -1 & & & & \\
 & & 3 & & & \\
-1 & 2 & & -2 & & \\
 & & -1 & & \frac{1}{3} & \\
0 & 1 & & -1 & & \\
 & & -3 & & & \\
1 & -2 & & & &
\end{array}
$$

Nel caso in cui $f(x)$ sia un polinomio $u(x)$, come nel paragrafo precedente, si vede subito che gli a_i della (1.8) sono dati da:

$$a_0 = y_0, a_1 = [x_0x_1], \ldots, a_i = [x_0x_1 \ldots x_i], \ldots, a_n = [x_0x_1 \ldots x_n].$$

Questo calcolo degli a_i richiede allora n divisioni per le differenze di ordine 1, $n-1$ per quelle di ordine 2,..., 1 divisione per quella di ordine n; in tutto $\frac{1}{2}(n^2+n)$ divisioni, a cui vanno aggiunte n^2+n sottrazioni, con un risparmio di circa 3/4 delle operazioni richieste dal metodo di Lagrange.

1.5 Applicazioni

Vediamo ora un'applicazione del teorema cinese ad un problema di probabilità, e tre esempi di applicazione dei polinomi di Lagrange: una ad un problema di

matrici, un' altra al calcolo del prodotto di due polinomi, e una terza ad un problema di crittografia.

1. Si può definire una misura[1]sul gruppo degli interi Z, cioè una funzione μ definita sui sottoinsiemi S di Z a valori in $[0,1]$ e tale che:

(i) $\mu(Z) = 1$;
(ii) $\mu(i + S) = \mu(S)$, $i \in Z$, (invarianza per traslazione);
(iii) $\mu(S \cup T) = \mu(S) + \mu(T)$, se $S \cap T = \emptyset$.

(La (iii)– additività finita– si estende alle unioni finite disgiunte). Queste tre proprietà permettono di definire una probabilità su Z: per ogni $S \subseteq Z$, la probabilità che un elemento x di Z appartenga ad S è data dalla misura di S:

$$\mu(S) = p(x \in S).$$

Sia m un intero positivo, e siano $S_0, S_1, \ldots, S_{m-1}$ le classi resto mod m. Poichè $S_i = i + S_0$, dalla (ii) si ha $\mu(S_i) = \mu(S_0)$, e dunque tutte le classi resto mod m hanno la stessa misura, e quindi, ricordando la (i) e la (iii),

$$1 = \mu(Z) = \mu(S_0 \cup S_1 \cup \ldots \cup S_{m-1}) = m\mu(S_i).$$

Gli S_i hanno dunque tutti misura $\mu(S_i) = 1/m$. In altri termini, ciò significa che dati a e m in Z, la probabilità che un intero x sia congruo ad a mod m (cioè che x appartenga alla classe S_i dove si trova a), è $1/m$:

$$p(x \equiv a \bmod m) = \frac{1}{m}.$$

Siano ora $m_0, m_1, \ldots, m_n$ interi a due a due primi tra loro. Il teorema cinese ci dice che ogni sistema di congruenze:

$$x \equiv a_i \bmod m_i,\ i = 0, 1, \ldots, n, \tag{1.13}$$

è equivalente ad una sola congruenza:

$$x \equiv a \bmod m, \tag{1.14}$$

dove m è il prodotto degli m_i. Per quanto visto sopra, la (1.14) ha probabilità $1/m$ di verificarsi, e cioè $\frac{1}{m_0} \cdot \frac{1}{m_1} \cdots \frac{1}{m_n}$. In altri termini, la probabilità del verificarsi simultaneo delle (1.13) (cioè la probabilità del verificarsi della (1.14)) è il prodotto delle probabilità del verificarsi di ciascuna di esse, se ne conclude che *le congruenze i cui moduli sono a due a due relativamente primi sono statisticamente indipendenti.*

[1]La dimostrazione dell'esistenza di una tale misura non è semplice.

2. Se $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ è un polinomio e A una matrice quadrata, con $f(A)$ intendiamo la matrice ottenuta sommando le matrici a_kA^k (i cui elementi sono quelli della potenza $k-$esima di A moltiplicati per a_k), per $k = 0, 1, \ldots, n$ (la matrice A^0 è la matrice identità I). Si può dimostrare che data una matrice A esiste sempre un polinomio $f(x)$ tale che $f(A) = 0$, dove 0 è la matrice nulla, quella con tutti zeri. (Per esempio, per il teorema di Hamilton-Cayley, il polinomio caratteristico di A, cioè $det(A - xI)$, che è di grado n se A è una matrice $n \times n$). Tra questi ne esiste allora uno di grado minimo $m + 1$ e monico, $m(x)$, il *polinomio minimo di A*. Supponiamo che $m(x)$ abbia tutte le radici distinte $\lambda_0, \lambda_1, \ldots, \lambda_m$. Possiamo allora considerare i polinomi di Lagrange $L_k(x)$, $k = 0, 1, \ldots, m$, relativi ai λ_i, e le matrici $A_k = L_k(A)$. Sappiamo che gli $L_k(x)$ sono idempotenti ortogonali, e che hanno somma 1, ciò che si traduce ora nelle tre relazioni:

1. $I = A_0 + A_1 + \cdots + A_m$,
2. $A_iA_j = 0$, $i \neq j$,
3. $A_i^2 = A_i$, per ogni i.

(La 2. e la 3. provengono da congruenze mod $m(x)$, che diventano congruenze mod $m(A)$; ma $m(A) = 0$, e dunque le congruenze sono uguaglianze).

La matrice A rappresenta una trasformazione lineare di uno spazio vettoriale V. Facciamo vedere come 1., 2., e 3. permettano di decomporre lo spazio in somma diretta di sottospazi. Se $v \in V$, si ha, dalla 1.,

$$v = Iv = A_0v + A_1v + \cdots + A_mv,$$

per cui:

$$V = A_0(V) + A_1(V) + \cdots + A_m(V),$$

e V è la somma dei sottospazi $A_i(V)$. Inoltre, questa somma è diretta. Se infatti:

$$A_iv_i = A_0v_0 + \cdots + A_{i-1}v_{i-1} + A_{i+1}v_{i+1} \cdots + A_mv_m,$$

per certi $v_0, v_1, \ldots, v_m$, allora, moltiplicando per A_i e tenendo conto di 2. e 3. si ha $A_iv_i = 0$.

Dimostriamo ora che se $v \in A_i(V)$, allora $Av = \lambda_iv$, per ogni i. Sappiamo che

$$x = \lambda_0L_0(x) + \lambda_1L_1(x) + \cdots + \lambda_mL_m(x);$$

questa, per $x = A$ diventa:

$$A = \lambda_0A_0 + \lambda_1A_1 + \cdots + \lambda_mA_m.$$

Ora, se $v = A_i(u)$, è $(A - \lambda_iI)v = (A - \lambda_iI)A_iu = AA_iu - A_i\lambda_iu$. Quest'ultima quantità è zero. Infatti, dall'espressione di A data qui sopra si ha $AA_i =$

$\lambda_i A_i^2 = \lambda_i A_i$, e dunque $AA_i u - A_i\lambda_i u = A_i\lambda_i u - A_i\lambda_i u = 0$. Perciò $Av - \lambda_i v = (A - \lambda_i I)v = 0$, e $Av = \lambda_i v$, come si voleva.

Abbiamo dimostrato che $A_i(V) \subseteq Ker(A - \lambda_i I)$. Ma anche la somma dei $K_i = Ker(A - \lambda_i I)$ è diretta (in quanto autovettori corrispondenti ad autovalori distinti sono indipendenti), e dunque, per ragioni di dimensione, V è somma diretta dei K_i. Scegliendo una base in ciascuno di questi, la matrice A si trasforma in una matrice diagonale a blocchi: ciascun blocco è scalare, perchè corrisponde ad uno dei K_i, e dunque ha tutti λ_i sulla diagonale e zero altrove. Abbiamo così: *se il polinomio minimo di una matrice A si spezza sul campo dei coefficienti in fattori lineari distinti, allora A è diagonalizzabile.* (E' vero anche il viceversa).

3. Se $g(x)$ e $h(x)$ sono due polinomi, di grado n, il prodotto $f = gh$ si può calcolare in questo modo. Siano $x_0, x_1, \ldots, x_{2n}$ punti distinti; allora i prodotti $y_i = g(x_i)h(x_i)$ forniscono $2n + 1$ valori di f, che è di grado $2n$, e dunque individuano f. L'espressione esplicita di f si può allora ottenere col metodo di Lagrange a partire dagli x_i e y_i. Se g e h sono di grado diverso, $m = \partial g < \partial h = n$, si può rendere g di grado fittizio n aggiungendo monomi del tipo $0 \cdot x^k$.

Il calcolo di un polinomio di grado n in un punto richiede un numero di moltiplicazioni dell'ordine di n, e dunque, per avere i valori in n punti, o in una funzione lineare di n, occorrono un numero di moltiplicazioni dell'ordine di n^2. Vedremo in seguito (Cap. 5) che scegliendo come punti le radici $n-$esime dell'unità, il numero di moltiplicazioni si può abbassare a $n \log n$.

4. In questo esempio si tratta di suddividere un dato segreto D (ad esempio un numero che dà la combinazione per aprire una cassaforte) in n parti $D_0, D_1, \ldots, D_{n-1}$ in modo tale che:
a) la conoscenza di k tra i D_i permette di calcolare D;
b) la conoscenza di $k - 1$ tra i D_i lascia D indeterminato, nel senso che i suoi possibili valori sono tutti ugualmente probabili.

A tale scopo consideriamo un polinomio di grado $k - 1$:

$$p(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1},$$

dove $a_0 = D$, e gli altri coefficienti scelti in modo casuale. Se $x_0, x_1, \ldots, x_{n-1}$, $n \geq k$, sono numeri distinti, consideriamo i numeri:

$$p(x_0), p(x_1), \ldots, p(x_{n-1}).$$

Ora, k coppie $D_i = (x_i, p(x_i))$ permettono di determinare $p(x)$ per interpolazione, e dunque D come $p(0)$, ma $k - 1$ non bastano a determinare il polinomio e quindi D. In altri termini, per tornare all'esempio della cassaforte, se le n coppie $(x_i, p(x_i))$ vengono messe a conoscenza di n persone, una coppia per ogni persona, per aprire la cassaforte è necessario l'accordo di almeno k persone.

Lo stesso problema si può affrontare usando l'aritmetica modulare. Dato un intero D, sia p un primo maggiore di D e n. Scegliamo i coefficienti $a_1, a_2, \ldots, a_{k-1}$ di $p(x)$ in modo casuale tra $0, 1, \ldots, p-1$, come pure gli n valori x_i, con la sola avvertenza che $x_i \neq 0$. Il calcolo dei $p(x_i)$ si fa modulo p. Ora, conoscendo $k-1$ coppie $D_i = (x_i, p(x_i))$, per ogni possibile valore di D si può costruire un polinomio $p'(x)$, ed uno solo, tale che $p'(0) = D$. Questi p polinomi sono per costruzione tutti ugualmente probabili, per cui nulla si può sapere sull'effettivo valore di D.

Nota bibliografica

Per tutto il capitolo si vedano [**A**] e [**C**]. Per l'algoritmo di Euclide [**Kn**] §4.5.2. Per il teorema cinese e i metodi di Lagrange e Newton l'articolo di M. Lauer "*Computing by homomorphic images*" in [**CA**], da cui è preso anche l'esempio discusso nel testo. Per il teorema cinese e l'interpolazione il §4.6.4 di [**Kn**] e [**Li**]. Il numero 4 delle Applicazioni è in [**Kn**], p. 486.

Capitolo 2

Sviluppi in serie p-adici

2.1 Numeri razionali

In questo paragrafo ci occupiamo dello sviluppo di un numero razionale in serie di potenze di un numero $p \geq 2$, non necessariamente primo. Si vedrà come la tecnica che useremo estenda al caso dei numeri razionali quella che dà la scrittura in base p di un numero intero positivo. Lì lo sviluppo è finito, si ha cioè un polinomio in p a coefficienti compresi tra 0 e $p-1$, estremi inclusi; qui sarà infinito, si avrà cioè una serie di potenze di p, con lo stesso insieme di variabilità dei coefficienti.

Per scrivere un intero $x \geq 0$ in una certa base p si divide x per p ottenendo un resto c_0 e un quoziente q: $x = c_0 + pq$. Il resto c_0 è la prima cifra dello sviluppo, e rappresenta la "prima approssimazione" del numero x, cioè il numero x "a meno di multipli di p". Per trovare la seconda cifra, si divide q per p: $q = c_1 + pq_1$, per cui, sostituendo q con l'espressione trovata, $x = c_0 + c_1 p + q_1 p^2$. Il numero $c_0 + c_1 p$ è la "seconda approssimazione" di x, cioè x "a meno di multipli di p^2"; e così di seguito. Poichè per qualche n si ha $x < p^n$, se n è il minimo esponente per cui ciò accade i coefficienti da c_n in poi sono tutti zero: $x = c_0 + c_1 p + \cdots + c_{n-1} p^{n-1} + 0 \cdot p^n + \cdots$. Si scrive $x = c_0, c_1 \ldots c_{n-1}$.

Il procedimento è dunque il seguente: trovato $c_0 \equiv x \bmod p$, per trovare c_1 si considera q, cioè l'intero:

$$\frac{x - c_0}{p}$$

e lo si divide per p; c_1 sarà il resto di questa divisione:

$$c_1 \equiv \frac{x - c_0}{p} \bmod p.$$

Per c_2, si prende l'intero:

$$\frac{x - (c_0 + c_1 p)}{p^2}$$

e lo si divide per p; c_2 è il resto di questa divisione:

$$c_2 \equiv \frac{x - (c_0 + c_1 p)}{p^2} \bmod p,$$

e così di seguito. In generale, sia $e_n = c_0 + c_1 p + \cdots + c_{n-1} p^{n-1}$ l'approssimazione di x di ordine n; la quantità $x - e_n = R_n$ è il *resto* di ordine n. La nuova approssimazione sarà $e_{n+1} = e_n + c_n p^n$, dove c_n è il resto della divisione di $\frac{x-e_n}{p^n}$ per p; dunque, per $n > 0$ abbiamo la formula generale:

$$c_n \equiv \frac{x - (c_0 + c_1 p + \cdots + c_{n-1} p^{n-1})}{p^n} \bmod p, \tag{2.1}$$

dove i coefficienti c_i sono tali che $0 \leq c_i < p$.

Sia ora a/b un numero razionale. Sussiste il seguente teorema.

Teorema 2.1. *Sia a/b un numero razionale, $b \geq 1$, e $p \geq 2$ un intero con $(p, b) = 1$. Allora esiste ed è unica la coppia di interi c, d, con $0 \leq c < p$ e tale che:*

$$\frac{a}{b} = c + \frac{d}{b} p. \tag{2.2}$$

Dim. Sia $bx + py = 1$. Allora $b(ax) + p(ay) = a$. Se $0 \leq ax < p$, si ha il risultato con $c = ax$ e $d = ay$. Altrimenti, dividiamo ax per p; otteniamo $ax = pq + r$, con $0 \leq r < p$, e posto:

$$c = ax - pq \text{ e } d = ay + bq,$$

si ha:

$$bc + pd = a,$$

da cui, dividendo per b, la (2.2). (Si osservi che $c \equiv ab^{-1} \bmod p$, e che b^{-1} esiste mod p in quanto $(p, b) = 1$). Ciò dimostra l'esistenza. Per l'unicità, sia c', d' un'altra coppia con le proprietà dette; allora $bc' + pd' = a$, da cui, sottraendo dalla precedente, $b(c - c') = p(d' - d)$. Ne segue che p divide $b(c - c')$, ed essendo $(p, b) = 1$, p divide $c - c'$. Ma c e c' sono entrambi inferiori a p e non negativi, e perciò $-p < c - c' < p$. Ne segue $c - c' = 0$ e $c = c'$, e dunque anche $d = d'$. $\diamondsuit$

Si osservi come nel caso di a/b intero, cioè $b = 1$, la (2.2) diventi $a = c + dp$, per cui c è il resto e d il quoziente della divisione di a per p.

L'intero c della (2.2) è la prima approssimazione di a/b. Poniamo $c = c_0$, e applichiamo il teorema alla coppia d, b. Otteniamo, come sopra,

$$\frac{d}{b} = c_1 + \frac{d_1}{b} p,$$

e analogamente:

$$\frac{d_1}{b} = c_2 + \frac{d_2}{b}p.$$

Proseguendo in questo modo, e sostituendo ad ogni passo $\frac{d_i}{b}$ con la sua espressione $c_{i+1} + \frac{d_{i+1}}{b}p$, otteniamo lo sviluppo:

$$\frac{a}{b} = c_0 + c_1 p + c_2 p^2 + \cdots + c_{n-1}p^{n-1} + \frac{d_{n-1}}{b}p^n, \tag{2.3}$$

per $n = 1, 2, \ldots$. Ne segue:

$$a = b(c_0 + c_1 p + \cdots + c_{n-1}p^{n-1}) + d_{n-1}p^n, \tag{2.4}$$

e dunque:

$$a \equiv b(c_0 + c_1 p + \cdots + c_{n-1}p^{n-1}) \bmod p^n, \tag{2.5}$$

dove $0 \leq c_i < p$. Per ogni $n = 1, 2, \ldots$ abbiamo allora una delle congruenze (2.5). Si suole scrivere simbolicamente:

$$\frac{a}{b} = c_0 + c_1 p + c_2 p^2 + \cdots = \sum_{k \geq 0} c_k p^k,$$

o anche:

$$\frac{a}{b} = c_0, c_1 c_2 \ldots.$$

Sottolineamo tuttavia il fatto che queste due scritture non sono altro che un modo simbolico di esprimere la successione infinita di congruenze data dalla (2.5). Il termine $R_n = d_{n-1}p^n$ della (2.4) è il *resto di ordine n* dello sviluppo.

Lo sviluppo di un numero razionale in serie di potenze di p si riduce dunque alla risoluzione delle congruenze (2.5) per $n = 1, 2 \ldots$.

Riassumiamo quanto sopra nel seguente:

Teorema 2.2. *Ogni numero razionale a/b, con $b \geq 1$, si può sviluppare in serie di potenze positive di un numero intero $p \geq 2$ e tale che $(p, b) = 1$, e ciò con precisione arbitraria, nel senso che il resto R_n della (2.4), proseguendo opportunamente lo sviluppo, si può rendere divisibile per una potenza comunque elevata di p.* $\diamondsuit$

Lo sviluppo del Teorema 2.2 si chiama *sviluppo p-adico* del numero razionale a/b.

Se denotiamo con $e_n = c_0 + c_1 p + \cdots + c_{n-1}p^{n-1}$ l'approssimazione di ordine n di a/b data dalla (2.5), abbiamo:

$$\frac{a}{b} \equiv e_n \bmod p^n,$$

ovvero $be_n - a \equiv 0 \bmod p^n$. In altri termini, e_n è una soluzione dell'equazione $bx - a = 0$ negli interi mod p^n. Abbiamo così un modo equivalente di enunciare il Teorema 2.1:

Teorema 2.3. *Se a, b e p sono come nel Teorema 2.1, allora l'equazione $bx - a = 0$ ammette una soluzione negli interi modulo p^n, per ogni n.* $\diamondsuit$

Esempio. Determiniamo lo sviluppo 7−adico di 1/12. Si ha:

$$12 \cdot 3 + 7 \cdot -5 = 1, \tag{2.6}$$

e dunque:

$$\frac{1}{12} = 3 - \frac{5}{12}7.$$

Dalla (2.6) moltiplicata per -5 abbiamo $12 \cdot -15 + 7 \cdot 25 = -5$. Poichè -15 non è compreso tra 0 e 7, dividiamolo per 7: $-15 = 7 \cdot -3 + 6$. Ne segue $12 \cdot 6 + 7 \cdot -11 = -5$ e pertanto:

$$-\frac{5}{12} = 6 - \frac{11}{12}7.$$

Analogamente, $12 \cdot -33 + 7 \cdot 55 = -11$, $-33 = 7 \cdot -5 + 2$ e $12 \cdot 2 + 7 \cdot (55 + 12 \cdot -5) = 12 \cdot 2 + 7 \cdot -5 = -11$, e

$$-\frac{11}{12} = 2 - \frac{5}{12}7.$$

Si ricomincia dunque con $-5/12$, per cui la cifra successiva sarà di nuovo 6. Ne segue:

$$\frac{1}{12} = 3,6262\ldots \bmod 7.$$

Lo sviluppo è allora *periodico*, di periodo 2 (le due cifre 6 e 2). Si scrive:

$$\frac{1}{12} = 3,\overline{62} \bmod 7.$$

Nei termini del Teorema 2.3 abbiamo allora che l'equazione $12x - 1 = 0$ ha la soluzione 3 negli interi mod 7, la soluzione $3 + 6 \cdot 7 = 45$ negli interi mod 7^2 (infatti $12 \cdot 45 - 1 = 540 - 1 = 539 = 11 \cdot 7^2 \equiv 0 \bmod 7^2$), ecc.

Come si vede, il procedimento è analogo a quello del caso di un intero. Più precisamente, dalla $\frac{a}{b} = c_0 + \frac{d}{b}p$ si ha:

$$\frac{\frac{a}{b} - c_0}{p} = \frac{1}{b}\frac{a - bc_0}{p} = \frac{d}{b},$$

per cui $d = \frac{a - bc_0}{p}$. Ora, $d = bc_1 + pd_1 \equiv bc_1 \bmod p$, e dunque:

$$c_1 \equiv db^{-1} = \frac{1}{b}\frac{a - bc_0}{p} \bmod p.$$

Analogamente, $d_1 = \frac{a-b(c_0+c_1p)}{p^2}$ e

$$c_2 = \frac{1}{b}\frac{a-b(c_0+c_1p)}{p^2} \bmod p,$$

e in generale:

$$c_n \equiv \frac{1}{b}\frac{a-b(c_0+c_1p+\cdots+c_{n-1}p^{n-1})}{p^n} \bmod p,$$

che concide con la (2.1) quando $b = 1$. Si osservi come ogni volta l'espressione:

$$\frac{a-b(c_0+c_1p+\cdots+c_{n-1}p^{n-1})}{p^n}$$

sia un intero. Si tratta infatti dell'intero d_{n-1} della (2.3) (o (2.4)).

Indicando anche qui con e_n l'approssimazione di a/b di ordine n:

$$e_n = c_0 + c_1p + \cdots + c_{n-1}p^{n-1}.$$

abbiamo il seguente algoritmo che fornisce i coefficienti $c_0, c_1, \ldots, c_{n-1}$ o i valori approssimati $e_1, e_2, \ldots, e_n$, per ogni n:

input: a,b,p,n,
$d : \frac{1}{b} \bmod p$, $c_0 : ad \bmod p$, $e_1 = c_0$,
per $k : 1$ a $n-1$ fare:
($q_k : quoziente(a - be_k, p^k)$,
$c_k : dq_k \bmod p$,
$e_{k+1} : e_k + c_kp^k$),
output: $c_0, c_1, \ldots c_{n-1}$ (oppure: $e_1, e_2, \ldots, e_n$).

Esempi. 1. Determiniamo lo sviluppo $p-$adico di

$$\frac{1}{1-p}.$$

Col metodo del Teorema 2.1 abbiamo:

$$1 \cdot (1-p) + 1 \cdot p = 1,$$

e dunque:

$$\frac{1}{1-p} = 1 + \frac{1}{1-p}p,$$

e $c_0 = 1$. Ne segue:

$$\frac{1}{1-p} = 1 + (1 + \frac{1}{1-p}p)p = 1 + p + \frac{1}{1-p}p^2,$$

e $c_1 = 1$. Proseguendo in questo modo, o per induzione, si trova:

$$\frac{1}{1-p} = 1 + p + p^2 + \cdots .$$

2. Più in generale sviluppiamo:

$$\frac{1}{1-p^n},$$

questa volta facendo girare l'algoritmo. Abbiamo:

$$1 \equiv (1-p^n)c_0 = c_0 - p^n c_0 \bmod p,$$

e dunque $c_0 = 1$. Inoltre,

$$1 \equiv (1-p^n)(1+c_1 p) = 1 - p^n + c_1 p - c_1 p^{n-1} \bmod p^2.$$

Se $n \geq 2$ si ha $c_1 \equiv 0 \bmod p$. Analogamente sono uguali a zero tutti i c_i con $i < n$. Allora:

$$1 \equiv (1-p^n)(1+c_n p^n) = 1 + c_n p^n - p^n - c_n p^{2n} \bmod p^{n+1},$$

e dunque $0 \equiv c_n - 1 \bmod p$, e $c_n = 1$. Come sopra, sono zero tutti i coefficienti da c_{n+1} a c_{2n-1}, e $c_{2k} = 1$. In definitiva, $c_i = 1$ per i multiplo di n, e $c_i = 0$ altrimenti:

$$\frac{1}{1-p^n} = 1 + p^n + p^{2n} + \cdots + p^{kn} + \cdots .$$

Nota. Gli sviluppi degli esempi precedenti si possono ritrovare come caso particolare dello sviluppo formale:

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots,$$

con il quale intendiamo la successione di congruenze:

$$1 \quad \equiv \quad (1-x)(1 + x + \cdots + x^{n-1}) \bmod x^n$$

(il secondo membro è uguale infatti a $1 - x^n \bmod x^n$, e questo è equivalente a $1 \bmod x^n$, $n = 1, 2 \ldots$; con "mod x^n" si intende "quando si ponga $x^n = 0$"). Con $x = p$, o $x = p^n$ si ottengono le espressioni viste, come pure con $x = a$, $a \neq 1$, ogni espressione $\frac{1}{1-a^n}$. Ritorneremo su questo punto quando parleremo degli sviluppi in serie delle funzioni razionali.

Lo sviluppo di un numero intero nella base p è periodico, di periodo 1: il periodo consta di una sola cifra, lo zero. Vedremo tra un momento che un numero intero negativo ha uno sviluppo periodico anch'esso di periodo 1, ma

la cifra che si ripete è $p-1$, e che in generale lo sviluppo in serie di un numero razionale è sempre periodico, cioè della forma:

$$\frac{a}{b} = c_0, c_1 \dots c_k \overline{c_{k+1} c_{k+2} \dots c_{k+d}} \,,$$

dove questa scrittura significa che $c_{k+1} = c_{k+d+1} = c_{k+2d+1} = \dots$, e analogamente per gli altri c_i. Se d è la lunghezza minima per la quale si hanno queste uguaglianze si dice allora che a/b è periodico di periodo d. Viceversa, uno sviluppo periodico rappresenta un numero razionale (v. Teorema 2.5 più avanti).

Consideriamo ora uno sviluppo della forma:

$$\frac{a}{b} = a_0 + a_1 p + a_2 p^2 + \cdots,$$

dove gli a_i sono interi arbitrari, e vediamo come portare questo sviluppo alla forma in cui i coefficienti sono compresi tra 0 e $p-1$, forma che chiameremo *ridotta*. Se a_0 non è compreso tra 0 e $p-1$ dividiamolo per p, $a_0 = pq_1 + r_1$, e sostituiamo nello sviluppo a_0 con $a_0 - pq_1$. Avendo tolto pq_1 dobbiamo ora aggiungerlo, e troviamo:

$$(a_0 - pq_1) + (a_1 + q_1)p + \cdots,$$

e proseguendo, $a_1 + q_1 = pq_2 + r_2$ e

$$(a_0 - pq_1) + (a_1 + q_1 - pq_2)p + (a_2 + q_2)p^2 + \cdots.$$

Allora,

$$\frac{a}{b} = c_0 + c_1 + \cdots,$$

dove $c_i = a_i + q_i - pq_{i+1}$, e $0 \le c_i < p$ in quanto si tratta di resti di divisioni per p.

Se uno sviluppo ha la forma $a_0, a_1 a_2 \dots$, esso si riscrive in forma ridotta sostituendo ogni cifra, cominciando dalla prima, con il resto che si ottiene dividendola per p e aggiungendo il quoziente ottenuto (il "riporto") alla cifra successiva.

Esempi. 1. Sia $7,530860\overline{0}$ un intero mod 3. Esso si trasforma successivamente come segue:

$$\begin{aligned} 7,530860\overline{0} &= 1,730860\overline{0} = 1,150860\overline{0} \\ &= 1,121860\overline{0} = 1,121280\overline{0} \\ &= 1,1212220\overline{0}, \end{aligned}$$

che è la scrittura in base 3 di 2155: $1 + 1\cdot 3 + 2\cdot 3^2 + \cdots + 2\cdot 3^6 + 0\cdot 3^7 + 0\cdot 3^8 + \cdots$

2. Consideriamo, sempre nella base 3, il numero negativo -2155. Per l'esempio precedente si ha $-2155 = -1 - 1\cdot 3 - 2\cdot 3^2 - \cdots - 2\cdot 3^6 + 0\cdot 3^7 + 0\cdot 3^8 + \cdots$. Qui i coefficienti sono in modulo minori di 3, e la divisione per p dà quindi sempre quoziente -1: $-k = p\cdot -1 + (p-k)$. La riduzione avviene perciò sostituendo due coefficienti consecutivi a_k, a_{k+1} con $a_k + p, a_{k+1} - 1$. Si ha allora: $-2155 = 2 - 2\cdot 3 - 2\cdot 3^2 - \cdots$, e proseguendo:

$$-2155 = 2 + 1\cdot 3 + 0\cdot 3^2 - 2\cdot 3^3 + \cdots .$$

Arrivati a $2 + 1\cdot 3 + \cdots + 1\cdot 3^5 - 3\cdot 3^6 + 0\cdot 3^7 + \cdots$, abbiamo: $\cdots - 3\cdot 3^6 + 0\cdot 3^7 + 0\cdot 3^8 + \cdots = 0\cdot 3^6 - 1\cdot 3^7 + 0\cdot 3^8 + \cdots = \cdots 2\cdot 3^7 - 1\cdot 3^8 + \cdots$. In altre parole, i coefficienti delle potenze da 3^7 in poi sono tutti uguali a 2. Si osservi che quello di 3^6 è l'ultimo coefficiente di 2155 prima che cominci il periodo 0. Dunque, -2155 è periodico, di periodo 1. Scriviamo allora $-2155 = 2, 1010002\overline{2}$. La cifra che si ripete è 2, cioè $3 - 1$. Quest'ultimo fatto è generale.

Teorema 2.4. *Uno sviluppo in serie modulo p nel quale i coefficienti da un certo punto in poi sono tutti uguali a $p-1$ rappresenta un numero intero negativo, e viceversa.*

Dim. Sia $x = c_0, c_1c_2\ldots c_k\ p-1\ p-1\ldots$ lo sviluppo in questione. Possiamo supporre che si tratti di uno sviluppo ridotto perchè un eventuale processo di riduzione non fa che spostare verso destra l'inizio del periodo. Allora $-x = -c_0 - c_1p - \cdots - c_kp^k + (1-p)p^{k+1} + (1-p)p^{k+2} + \cdots$. Riducendo, si arriva a $\cdots + (p-c_k-1)p^k + (1-p-1)p^{k+1} + \cdots = \cdots + 0\cdot p^{k+1} + (1-p-1)p^{k+2} + \cdots$, ecc., per cui $c_i = 0$ per $i > k$. Ne segue che $-x$ è un intero positivo, per cui x è un intero negativo. Viceversa, se x è negativo, $-x$ è positivo, e dunque $-x = d_0, d_1d_2\ldots\overline{0}$, e perciò $x = -d_0 - d_1p - \cdots - d_kp^k + 0\cdot p^{k+1} + \cdots$. Nella solita riduzione si ha: $\cdots + (p-d_k-1)p^k - 1\cdot p^{k+1} + 0\cdot p^{k+2} + \cdots = \cdots (p-1)p^{k+1} - 1\cdot p^{k+2} + \cdots$. Si vede allora che i coefficienti delle potenze p^i con $i > k$ sono tutti uguali a $p-1$. $\diamondsuit$

Esercizi

1. Che numero rappresenta lo sviluppo:

$$9, 999\ldots = 9, \overline{9}$$

in base 10? Più in generale, che numero rappresenta lo sviluppo:

$$p-1, p-1\ p-1\ \ldots = p-1, \overline{p-1}$$

in base p?

2. Qual è lo sviluppo in base 10 di -327?

3. Scrivere la forma ridotta mod 3 di 1,234...k... (tutti gli interi positivi).

4. Che numero rappresenta lo sviluppo $p-$adico: $p, \overline{p-1}$?

5. Che numero rappresenta lo sviluppo $p-$adico:

$$p, 2p-1\ 3p-2\ \ldots (k+1)p-k \ldots ?$$

6. Qual è la condizione necessaria e sufficiente affinchè uno sviluppo $p-$adico rappresenti lo zero?

7. Dimostrare che $c_0 + c_1 p + \cdots + c_{n-1}p^{n-1} = p^n - 1$ se e solo se tutti i c_i sono uguali a $p-1$.

8. Cosa significa il fatto che in uno sviluppo p-adico un coefficiente è uguale a zero?

9. Calcolare la seguente somma mod 5:

$$2, 3102114\overline{0} + 3, 1412021310.$$

Vediamo ora un classico teorema.

Teorema 2.5. *Uno sviluppo p-adico rappresenta un numero razionale se e solo se è periodico.*

Dim. Supponiamo dapprima di avere un numero periodico *puro* (il periodo comincia cioè con la prima cifra) di periodo d:

$$x = \overline{c_0, c_1 c_2 \ldots c_{d-1}}\ ,$$

ovvero:

$$x = c_0 + c_1 p + \cdots + c_{d-1}p^{d-1} + c_0 p^d + \cdots + c_{d-1}p^{2d-1} + \cdots .$$

Mettendo in evidenza p^d questa espressione si può scrivere:

$$x = c_0 + c_1 p + \cdots + c_{d-1}p^{d-1} + (c_0 + c_1 p + \cdots + c_{d-1}p^{d-1})p^d + \cdots ,$$

cioè:

$$x = (c_0 + c_1 p + \cdots + c_{d-1}p^{d-1})(1 + p^d + p^{2d} + \cdots),$$

e ricordando che la serie a secondo membro ha per somma $1/(1-p^d)$,

$$x = c_0 + c_1 p + \cdots + c_{d-1}p^{d-1} \cdot \frac{1}{1-p^d} = \frac{c_0 + c_1 p + \cdots + c_{d-1}p^{d-1}}{1-p^d}.$$

Il numero x è dunque rapporto di due interi e perciò è razionale. Si osservi che si ottiene così un numero razionale negativo (perchè $1-p^d$ è negativo), che è

una frazione propria in quanto $1 - p^d$ è superiore (in modulo) al numeratore (per l'es. 7, si ha uguaglianza se e solo se tutti i c_i sono uguali a $p-1$, e dunque $x = -1$, intero), e il cui denominatore è primo con p. Inoltre, d è il più piccolo esponente tale che $x(1-p^d)$ è periodico, altrimenti il periodo sarebbe minore di d. Viceversa, sia $-\frac{a}{b}$ un numero razionale negativo (ridotto ai minimi termini) con $(b,p) = 1$, e sia d l'*ordine di p modulo b*, cioè il più piccolo intero positivo tale che $p^d \equiv 1 \bmod b$.[1] Allora $p^d - 1 = bt$, per un certo intero positivo t, $b = \frac{p^d-1}{t}$, e dunque:

$$-\frac{a}{b} = -\frac{at}{p^d-1} = \frac{m}{1-p^d},$$

dove si è posto $m = at$, che è un intero. Ora $m = at < bt$ in quanto $a < b$ e perciò $m < p^d - 1$; m ha quindi una scrittura in base p che arriva fino a p^{d-1}: $m = c_0 + c_1 p + \ldots + c_{d-1}p^{d-1}$, $0 \le c_i < p$. Ne segue:

$$\begin{aligned} -\frac{a}{b} &= \frac{m}{1-p^d} = m(1 + p^d + p^{2d} + \cdots) \\ &= (c_0 + c_1 p + \cdots + c_{d-1}p^{d-1})(1 + p^d + p^{2d} + \cdots) \\ &= \overline{c_0, c_1 c_2 \ldots c_{d-1}}\ , \end{aligned}$$

per cui il nostro numero razionale è un numero periodico puro.

Per quanto riguarda il caso generale, sia $x = a_0, a_1 \cdots a_k \overline{c_0 c_1 \ldots c_{d-1}}$, e sia s l'intero positivo $s = a_0, a_1 \cdots a_k$. Sottraendo s da x otteniamo $x - s = 0, 00 \ldots 0\overline{c_0 c_1 \ldots c_{d-1}}$, da cui, moltiplicando per $p^{-(k+1)}$, $p^{-(k+1)}(x - s) = \overline{c_0, c_1 c_2 \ldots c_{d-1}}$. Per quanto visto sopra, il secondo membro è un numero razionale, e dunque anche il primo lo è. Ne segue che x è razionale.

Viceversa, se x è un numero razionale il cui denominatore è primo con p, moltiplicando x per una opportuna potenza di p e aggiungendo o togliendo un intero, ci si riduce ad un numero razionale negativo. $\diamondsuit$

Nota. Per quanto ora visto il periodo di un numero razionale è 1 se e solo se l'ordine di $p \bmod b$ è 1, cioè se e solo se $p \equiv 1 \bmod b$. Se $\frac{a}{b}$ è intero, cioè se $b = 1$, allora l'ordine di $p \bmod 1$ è 1. Infatti, poichè due interi qualunque sono sempre tra loro congrui mod 1, il più piccolo intero positivo d tale che $p^d \equiv 1 \bmod b$ è 1. Si ritrova così il fatto che il periodo di un intero è 1.

Esempi. 1. Sviluppiamo $-\frac{1}{3} \bmod 5$. Si ha $5^2 \equiv 1 \bmod 3$, e dunque il periodo è $d = 2$. Inoltre, $5^2 - 1 = 24 = 3 \cdot 8$ e dunque $t = 8$, $m = 1 \cdot 8 = 8$, $8 = 3 + 1 \cdot 5$, e infine:

$$-\frac{1}{3} = \frac{3 + 1 \cdot 5}{1 - 5^2} \quad = \quad (3 + 1 \cdot 5)(1 + 5^2 + 5^4 \cdots)$$

[1] Essendo p primo con b, $p \bmod b$ appartiene al gruppo degli elementi invertibili di Z/bZ, e come tale ha un ordine, cioè il minimo intero d tale che l'elemento elevato a d è uguale all'unità.

$$\begin{aligned} &= 3 + 1\cdot 5 + 3\cdot 5^2 + 1\cdot 5^3 + \cdots \\ &= \overline{3,1}. \end{aligned}$$

Sviluppiamo ora $\frac{1}{3}$ mod 5. Scrivendo $\frac{1}{3} = 2 - \frac{1}{3}5$ e usando l'esempio precedente abbiamo $5 \cdot -\frac{1}{3} = 3\cdot 5 + 1\cdot 5^2 + \cdots = 0,\overline{31}$, e aggiungendo 2 si trova $\frac{1}{3} = 2,\overline{31}$. Facendo la somma (con riporto, e cominciando da sinistra) si trova $2,\overline{31} + \overline{3,1} = 0,00\ldots = 0$.

2. E' istruttivo ora sviluppare $\frac{1}{3}$ in serie di potenze di $\frac{1}{5}$. Tenuto conto di quanto visto prima si ha, dividendo sopra e sotto per 5^2,

$$\frac{1}{3} = \frac{3+1\cdot 5}{5^2-1} = \frac{\frac{3}{5^2}+\frac{1}{5}}{1-(\frac{1}{5})^2} = (\frac{1}{5}+\frac{3}{5^2})(1+\frac{1}{5^2}+\frac{1}{5^4}+\cdots),$$

e dunque:

$$\frac{1}{3} = \frac{1}{5}+\frac{3}{5^2}+\frac{1}{5^3}+\frac{3}{5^4}+\cdots = 0,\overline{13}.$$

Si vede allora che rispetto a $-\frac{1}{3}$ il periodo si inverte e comincia dopo la virgola, cioè dalle potenze positive di $\frac{1}{5}$. Inoltre, prima della virgola c'è 0. E' facile vedere che questo fatto è generale.

3. Vediamo ora un esempio con $p = 10$. Sviluppiamo $-\frac{3}{11}$. Si ha $10^2 \equiv 1 \bmod 11$, e dunque il periodo è $d = 2$. Inoltre, $10^2 - 1 = 11\cdot 9$, per cui $m = at = 3\cdot 9 = 27$. Allora:

$$\begin{aligned} -\frac{3}{11} &= \frac{-3\cdot 9}{10^2-1} = \frac{27}{1-10^2} = \frac{7+2\cdot 10}{1-10^2} \\ &= (7+2\cdot 10)(1+10^2+10^4+\cdots) \\ &= 7+2\cdot 10+7\cdot 10^2+2\cdot 10^3+\cdots \\ &= \overline{7,2}. \end{aligned}$$

Nota. L'usuale scrittura decimale di una frazione propria $\frac{a}{b}$ con denominatore primo con 10 si ottiene come sopra con $p = 10$. Più precisamente, trovato d minimo tale che $10^d \equiv 1 \bmod b$, cioè il periodo, sia $10^d - 1 = bt$. Allora, come prima,

$$\frac{a}{b} = \frac{at}{10^d-1} = \frac{m}{10^d-1}.$$

Dividiamo sopra e sotto per 10^d:

$$\frac{a}{b} = \frac{\frac{m}{10^d}}{1-(\frac{1}{10})^d}.$$

Scrivendo l'intero m in base 10, $m = c_0 + c_1 10 + c_2 10^2 + \cdots + c_{d-1}10^{d-1}$, e sviluppando $1-(\frac{1}{10})^d$ si ottiene:

$$\frac{a}{b} = \frac{c_{d-1}}{10}+\frac{c_{d-2}}{10^2}+\cdots+\frac{c_0}{10^d}(1+\frac{1}{10^d}+\frac{1}{10^{2d}}+\cdots),$$

e perciò:

$$\frac{a}{b} = 0, \overline{c_{d-1} c_{d-2} \dots c_0} \ .$$

Si ritrova in particolare il fatto ben noto che se il denominatore di una frazione è primo con 10 (cioè non è divisibile né per 2 né per 5), non vi sono cifre decimali prima di quelle periodiche, e viceversa.

Esempio. Cerchiamo lo sviluppo decimale usuale di $\frac{3}{11}$. Dalla $10^d \equiv 1 \bmod 11$ abbiamo $d = 2$. Inoltre, $10^2 - 1 = 11 \cdot 9$, per cui $m = at = 3 \cdot 9 = 27 = 7 + 2 \cdot 10$. Ne segue:

$$\frac{3}{11} = \frac{7 + 2 \cdot 10}{10^2 - 1} = \frac{\frac{7+2\cdot 10}{10^2}}{1 - \frac{1}{10^2}},$$

dove si è diviso sopra e sotto per 10^2. Dunque:

$$\begin{aligned}
\frac{3}{11} &= \frac{7 + 2 \cdot 10}{10^2} \cdot \frac{1}{1 - \frac{1}{10^2}} \\
&= \frac{7 + 2 \cdot 10}{10^2} \cdot (1 + \frac{1}{10^2} + \frac{1}{10^4} + \cdots) \\
&= (\frac{2}{10} + \frac{7}{10^2})(1 + \frac{1}{10^2} + \frac{1}{10^4} + \cdots) \\
&= \frac{2}{10} + \frac{7}{10^2} + \frac{2}{10^3} + \frac{7}{10^4} + \cdots \\
&= 0, \overline{27}.
\end{aligned}$$

Per ottenere un numero razionale a partire dalla sua espressione decimale basta fare il percorso ora visto a ritroso, cioè scrivere il periodo sotto forma di numero intero (nell'esempio: 27), e dividerlo per $10^d - 1 = 99 \dots 9$ (cioè tanti 9 quante sono le cifre del periodo; nell'esempio: 99), e poi ridurre ai minimi termini (nell'esempio: $\frac{27}{99} = \frac{3}{11}$). (Lo sviluppo in potenze di 10 di $-\frac{3}{11}$ visto prima dava $-\frac{3}{11} = \overline{7, 2}$).

2.2 Numeri algebrici

Un numero algebrico è una radice di un polinomio a coefficienti razionali. Lo sviluppo $p-$adico di un numero razionale $\frac{a}{b}$, $(p, b) = 1$, permette di trovare una radice del polinomio $p(x) = bx - a$, cioè una soluzione dell'equazione lineare $bx - a \equiv 0 \bmod p^n$, per ogni $n = 1, 2, \dots$ (Teorema 2.3). Vediamo ora il caso di un'equazione quadratica, $x^2 - a = 0$, con p primo e p che non divide a (cioè a non è zero modulo p). Limitiamoci per il momento al caso $p \neq 2$. Osserviamo subito che, contrariamente al caso lineare, questa equazione può non avere soluzioni già per $n = 1$. E' il caso per esempio della $x^2 - 2 = 0$ con $p = 3$. Ma basta che ne abbia una mod p perchè poi ne abbia una mod p^n per ogni n. Indichiamo questa soluzione con $\sqrt{a}$.

Teorema 2.6. *Sia p primo e $p > 2$. Se l'equazione $x^2 - a = 0$, $p \not| a$, ha una soluzione negli interi* mod p*, allora ne ha una negli interi* mod p^n *per ogni n.*

Dim. Come nel caso lineare si tratta di trovare uno sviluppo in serie di potenze di p:

$$\sqrt{a} = c_0 + c_1 p + c_2 p^2 + \cdots .$$

Sia e_1 una soluzione mod$p$. Poniamo $e_1 = c_0$, e supponiamo, per induzione, di aver trovato una soluzione e_n mod p^n nella forma:

$$e_n = c_0 + c_1 p + \cdots + c_{n-1} p^{n-1},$$

di avere cioè:

$$e_n^2 \equiv a \bmod p^n.$$

Cerchiamo allora una soluzione mod p^{n+1} nella forma $e_{n+1} = e_n + cp^n$. Dovendo essere:

$$e_{n+1}^2 \equiv a \bmod p^{n+1},$$

dobbiamo risolvere rispetto all'incognita c la seguente congruenza:

$$e_n^2 + 2ce_n p^n + c^2 p^{2n} \equiv a \bmod p^{n+1},$$

ovvero, essendo $2n > n + 1$ per $n > 1$,

$$e_n^2 + 2ce_n p^n \equiv a \bmod p^{n+1}. \tag{2.7}$$

Per ipotesi induttiva, $e_n^2 \equiv a \bmod p^n$, cioè $a - e_n^2 \equiv 0 \bmod p^n$, ovvero $a - e_n^2$ è divisibile per p^n. Ne segue che $\frac{a-e_n^2}{p^n}$ è un intero. Allora la (2.7) ha una soluzione c negli interi mod p^{n+1} se e solo se l'equazione in c:

$$\frac{a - e_n^2}{p^n} \equiv 2e_n c \tag{2.8}$$

ha una soluzione negli interi mod p. Ora, essendo $e_n \equiv e_1 \not\equiv 0 \bmod p$, l'inverso di e_n mod p esiste, come pure l'inverso di 2, in quanto $p \neq 2$. La (2.8), e perciò la (2.7), ha dunque la soluzione:

$$c \equiv \frac{1}{2e_1} \frac{a - e_n^2}{p^n} \bmod p,$$

cioè il resto della divisione di $\frac{1}{2e_1}\frac{a-e_n^2}{p^n}$ per p. Con questo c, che chiamiamo c_n, abbiamo allora la nuova soluzione:

$$e_{n+1} = e_n + c_n p^n,$$

negli interi modulo p^{n+1}. $\diamondsuit$

Un altro modo di esprimere questo risultato è il seguente:

Teorema 2.7. *Nelle ipotesi del Teorema* 2.6 *si ha lo sviluppo in serie:*

$$\sqrt{a} = c_0 + c_1 p + c_2 p^2 + \cdots . \qquad \diamondsuit$$

Esempio. Calcoliamo $\sqrt{2}$ con $p = 7$. Modulo 7, l'equazione $x^2 - 2 = 0$ ha la soluzione $x = 3$ in quanto $3^2 - 2 = 7 \equiv 0 \bmod 7$ (ha pure un'altra soluzione, $x = 4 \equiv -3 \bmod 7$). Il procedimento visto nel teorema può allora cominciare: $e_1 = c_0 = 3$, e

$$c_1 = \frac{1}{2 \cdot 3} \frac{2 - 3^2}{7} = \frac{1}{6} \cdot -\frac{7}{7} = -\frac{1}{6} = -6 \equiv 1 \bmod 7,$$

da cui: $e_2 = c_0 + c_1 \cdot 7 = 3 + 1 \cdot 7$. Analogamente:

$$c_2 = 6 \cdot \frac{2 - e_2^2}{7^2} = 6 \cdot \frac{2 - 100}{7^2} = 6 \cdot -2 \equiv 2 \bmod 7,$$

e dunque $e_3 = 3 + 1 \cdot 7 + 2 \cdot 7^2$. Proseguendo si trova:

$$\sqrt{2} = 3,12612124 \cdots .$$

Nella dimostrazione del Teorema 2.6 è contenuto il seguente algoritmo, dove e_1 è una soluzione dell'equazione mod p:

input: a, p, b, e_1,
$c_0 : e_1$, $m : 2e^{-1} \bmod p$,
per $k : 1$ a n fare:
($q_k : quoziente(a - e_k^2, p^k)$,
$c_k : q_k m \bmod p$,
$e_{k+1} : e_k + c_k \cdot p^k$),
output: $c_0, c_1, \ldots, c_n$ (oppure: $e_1, e_2, \ldots, e_{n+1}$).

Come si vede, l'algoritmo è del tutto analogo a quello del caso dei numeri razionali. Si tratta in effetti di casi particolari di uno stesso algoritmo, che vedremo tra un momento. Prima però consideriamo il caso $p = 2$, che abbiamo tralasciato, e che richiede un trattamento a parte.

Intanto, se a è dispari, l'equazione $x^2 - a = 0$ ha sempre una soluzione mod 2, ed è $x = 1$ ($1 - a$ è pari e dunque 0 mod 2). Ma contrariamente al caso $p > 2$ non è detto che ne abbia una mod 4. Ad esempio, $x^2 - 7 = 0$ non ha soluzione negli interi mod 4, come subito si verifica. La ragione è che $7 \not\equiv 1 \bmod 4$. Infatti se $x^2 - a$ ha una soluzione mod 4, questa soluzione è $x = 1$ o $x = 3 \equiv -1 \bmod 4$ (in quanto a è dispari). Allora $1 - a \equiv 0 \bmod 4$ e $a \equiv 1 \bmod 4$. Analogamente per $x = 3$ si ha $a \equiv 9 \equiv 1 \bmod 4$. Viceversa, se $a \equiv 1 \bmod 4$ si hanno le soluzioni $x = 1$ e $x = 3$. Dunque, *condizione necessaria e sufficiente affinchè*

l'equazione $x^2 - a = 0$, *a dispari, abbia una soluzione negli interi* mod 4 *è che* $a \equiv 1 \bmod 4$.

Ma l'equazione $x^2 - a = 0$ può avere una soluzione mod 4 senza averne una mod 8. E' il caso ad esempio della $x^2 - 21 = 0$. I numeri dispari mod 8 sono 1,3,5 e 7, i cui quadrati 1,9, 25 e 49 sono congrui a 1 mod 8, mentre 21 non lo è. Perchè l'equazione abbia soluzione è dunque necessario che si abbia $a \equiv 1 \bmod 8$. Questa condizione è ovviamente anche sufficiente, perchè allora $x = 1$ è una soluzione. Ma non solo: essa è anche sufficiente affinchè l'equazione abbia soluzione mod 2^n per ogni $n \geq 3$ (e dunque anche per $n = 1$ e 2). E' quanto afferma il teorema che segue.

Teorema 2.8. *Sia* $a \equiv 1 \bmod 8$. *Allora l'equazione:*

$$x^2 - a = 0$$

ha una soluzione negli interi mod 2^n *per ogni* $n = 1, 2, \ldots$.

Dim. Si ha intanto la soluzione $x = 1$ per $n = 1, 2$ e 3. Sia $n > 3$, e sia e_n una soluzione mod 2^n. Cerchiamo questa volta la soluzione sotto la forma:

$$e_{n+1} = e_n + c \cdot 2^{n-1}$$

(e non 2^n come nel caso $p \neq 2$). Deve essere $e_{n+1}^2 \equiv a \bmod 2^{n+1}$, cioè:

$$e_n^2 + 2^n e_n c + 2^{2n-2} c^2 \equiv a \bmod 2^{n+1},$$

ed essendo $2n - 2 > n + 1$ in quanto $n > 3$, il coefficiente di c^2 è zero, e restiamo con:

$$e_n^2 + 2^n e_n c \equiv a \bmod 2^{n+1}.$$

Per ipotesi, $e_n^2 \equiv a \bmod 2^n$, e la soluzione della precedente equazione è allora l'intero c tale che:

$$c \equiv \frac{e_n^2 - a}{2^n e_n} \bmod 2.$$

Con questo valore di c, $e_{n+1} = e_n + c \cdot 2^{n-1}$ è la soluzione mod 2^{n+1}. $\diamondsuit$

Esempio. Consideriamo l'equazione $x^2 - 41 = 0$. Abbiamo la soluzione $x = 1$ per $n = 1, 2, 3$. Una soluzione per $n = 4$, cioè mod 2^4, si trova in questo modo. Con $e_3 = 1$ si ha:

$$\begin{aligned} (1 + 2^2 c)^2 &= 1 + 2^3 c + 2^4 c^2 \equiv 41 \bmod 2^4, \\ c &\equiv \frac{1 - 41}{8} = -5 \equiv 1 \bmod 2, \end{aligned}$$

e dunque $e_4 = 1 + 1 \cdot 2^2 = 5$, ed effettivamente $5^2 = 25 \equiv 41 \bmod 2^4$.

Riassumiamo quanto detto sopra nel teorema seguente.

Teorema 2.9. *Sia a un numero dispari. Allora:*
i) a è sempre un quadrato mod 2*;*
ii) a è un quadrato mod 4 *se e solo se $a \equiv 1 \bmod 4$;*
iii) a è un quadrato mod 2^n, $n \geq 3$, *se e solo se $a \equiv 1 \bmod 8$.* $\diamondsuit$

2.3 Il metodo di Newton

Come già accennato, gli sviluppi in serie, che danno approssimazioni successive di un numero, sono casi particolari di un metodo generale. Si tratta del *metodo di Newton delle approssimazioni successive*. Esso consiste, data una funzione $f(x)$ (a noi interessa il caso di un polinomio a coefficienti interi) e un valore approssimato x_n di una sua radice, nel determinare una migliore approssimazione x_{n+1}, prendendo come x_{n+1} il punto di intersezione della tangente alla curva che rappresenta $f(x)$ nel punto $(x_n, f(x_n))$ con l'asse delle x. Poichè questa tangente ha equazione $y - f(x_n) = f'(x_n)(x - x_n)$, questo punto è

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}. \tag{2.9}$$

Ora, nel caso di un numero razionale a/b abbiamo che questo numero è radice di $f(x) = bx - a$. La formula vista nel paragrafo precedente era, con $(b, p) = 1$, $e_{n+1} = e_n + c_n p^n$, dove:

$$c_n \equiv \frac{1}{b} \frac{a - be_n}{p^n} \bmod p.$$

Ma $f(e_n) = be_n - a$, e $f'(x) = b$, costante. Il nostro c_n si può dunque scrivere:

$$c_n = -\frac{f(e_n)}{f'(e_n)p^n} \bmod p,$$

e dunque:

$$e_{n+1} = e_n - \frac{f(e_n)}{f'(e_n)} \bmod p,$$

che è la forma che assume la (2.9) nel caso in questione. Analogamente, nel caso di una radice quadrata ($p \neq 2$), è $f(x) = x^2 - a$, $f'(x) = 2x$, per cui:

$$c_n \equiv \frac{1}{2e_n} \frac{a - e_n^2}{p^n} \bmod p,$$

ovvero:

$$c_n = -\frac{f(e_n)}{f'(e_n)p^n} \bmod p,$$

e dunque la (2.9) assume la forma:

$$e_{n+1} = e_n - \frac{f(e_n)}{f'(e_n)} \bmod p.$$

Questo procedimento vale in generale: se il polinomio ha una radice e_1 mod p, e se $f'(e_1) \not\equiv 0 \bmod p$, allora la (2.9) permette di trovare una radice di $f(x)$ mod p^n per ogni n. In altri termini, essa permette di trovare lo sviluppo $p-$adico di una radice di un qualunque polinomio $f(x)$ a coefficienti interi (con le limitazioni dette). Sia infatti:

$$f(x) = \sum_{k=0}^{m} a_k x^k;$$

osserviamo che, per ogni intero c,

$$(x+cp)^k = \sum_{i=o}^{k} \binom{k}{i} x^{k-i}(cp)^i \equiv x^k + kcpx^{k-1} \bmod p^2,$$

in quanto, per $i > 1$, $(cp)^i = c^i p^i \equiv 0 \bmod p^2$. Ne segue:

$$f(x+cp) = \sum_{k=0}^{m} a_k (x+cp)^k \equiv \sum_{k=0}^{m} a_k x^k + cp \sum_{k=0}^{m} a_k k x^{k-1} \bmod\ p^2,$$

e dunque,

$$f(x+cp) \equiv f(x) + cpf'(x) \bmod p^2.$$

Se ora e_1 è una radice di $f(x)$ mod p tale che $f'(e_1) \not\equiv 0 \bmod p$, per una radice $e_2 \equiv e_1 + cp \bmod p^2$ deve essere:

$$0 \equiv f(e_1 + cp) = f(e_1) + cpf'(e_1) \bmod p^2.$$

Ora, $f(e_1) \equiv 0 \bmod p$, e dunque c risolve la precedente congruenza mod p^2 se e solo se risolve la

$$cf'(e_1) \equiv -\frac{f(e_1)}{p} \bmod p.$$

Ma questa ha la soluzione:

$$c \equiv -\frac{f(e_1)}{f'(e_1)p} \bmod\ p.$$

Abbiamo così la nuova approssimazione:

$$e_2 = e_1 - \frac{f(e_1)}{f'(e_1)}.$$

In generale, per passare da e_n ad e_{n+1}, si considera la congruenza:

$$f(x + cp^n) \equiv f(x) + cp^n f'(x) \bmod p^{n+1},$$

che dà il valore:

$$c \equiv -\frac{f(e_n)}{f'(e_n)p^n} \bmod p,$$

e la nuova approssimazione:

$$e_{n+1} = e_n - \frac{f(e_n)}{f'(e_n)}.$$

Abbiamo quindi il seguente algoritmo, che riassume i due visti in precedenza. Si osservi che $f'(e_k) \equiv f'(e_1) \bmod p$, in quanto e_k è uguale ad e_1 più un multiplo di p, $e_k = e_1 + tp$, e per quanto visto sopra con $t = c$ è $f'(e_k) = f'(e_1 + tp) \equiv f'(e_1) \bmod p$. Poniamo $d = \frac{1}{f'(e_1)}$, e $e_1 = e$, valore iniziale della radice.

input: $f(x), p, e, d$,
$e_1 : e$,
per k: 1 a $n-1$ fare:
$(q_k : quoziente(-f(e_k), p^k) \cdot d$,
$c_k : q_k \bmod p$,
$e_{k+1} : e_k + c_k \cdot p^k)$,
output: $c_0, c_1, \ldots, c_{n-1}$ (oppure $e_1, e_2, \ldots, e_n$).

Esempio. Calcoliamo alcune cifre dello sviluppo 7−adico di una radice cubica di -1. Si tratta di una delle tre soluzioni mod 7 dell'equazione $x^3 + 1 = 0$, e che sono $x = 3$,5 e 6. Sviluppiamo la prima, $x = 3$. Abbiamo $f(x) = x^3 + 1$, $f'(x) = 3x^2$, e, con $e_1 = 3$, $f'(e_1) = f'(3) = 27 \equiv 6 \bmod 7$, e dunque $d = 6$. Facendo girare l'algoritmo si ha:

$k = 1$:

$$q_1 : -\tfrac{f(e_1)}{7} \cdot 6 = -\tfrac{28}{7} \cdot 6 = -\tfrac{168}{7} = -24,$$
$$c_1 : -24 \bmod 7 = 4,$$
$$e_2 : 3 + 4 \cdot 7 = 31;$$

$k = 2$:

$$q_2 : -\tfrac{f(e_2)}{7^2} \cdot 6 = -\tfrac{f(31)}{7^2} \cdot 6 = -608 \cdot 6 = -3648 \equiv 1 \bmod 7,$$

e così proseguendo si trova:

$$3,4630262434\ldots \bmod 7.$$

Nel caso classico, la (2.9) si può usare per calcolare una radice quadrata. Calcoliamo alcune cifre di $\sqrt{2}$, partendo da un valore approssimato, diciamo $x_1 = 1$. Ora, $f(x) = x^2 - 2$, $f'(x) = 2x$ e dunque $f(x_1) = -1$, $f'(x_1) = 2$, e:

$$x_2 = 1 - \frac{-1}{2} = \frac{3}{2} = 1,5.$$

Con questo valore,

$$x_3 = 1,5 - \frac{2,25-2}{3} = \frac{4,5-0,25}{3} = 1,41\overline{6}.$$

Come si vede, la convergenza al valore di $\sqrt{2}$ è in questo caso molto rapida. Il metodo usuale di calcolo di una radice quadrata ricalca il metodo di Newton visto qui.

2.4 Sviluppi in serie di funzioni razionali

Un polinomio $f(x)$ a coefficienti in un campo (che nelle nostre considerazioni sarà il campo Q dei razionali) è una combinazione lineare dei monomi $1, x, x^2, \ldots$, con coefficienti che sono zero da un certo punto in poi:

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n + 0 \cdot x^{n+1} + \cdots.$$

Sotto questa forma un polinomio è uno sviluppo (finito) in serie di potenze di x, ovvero *in base x*. Se $p(x)$ è un qualunque polinomio di primo grado, si ha analogamente lo sviluppo:

$$f(x) = c_0 + c_1 p(x) + c_2 p(x)^2 + \cdots + c_n p(x)^n + 0 \cdot p(x)^{n+1} + \cdots$$

in base $p(x)$. Il procedimento che porta ad una scrittura di questo tipo è lo stesso di quello usato per gli interi. Si divide $f(x)$ per $p(x)$ (in particolare, per x): $f(x) = r(x) + p(x)q(x)$, $0 \leq \partial r(x) < \partial p(x)$, e si prende il resto $r(x) = c_0$, che è una costante perchè di grado zero. Questa sarà la prima approssimazione del polinomio: $f(x) \equiv c_0 \bmod p(x)$. Si prende poi $\frac{f(x)-c_0}{p(x)}$, si divide per $p(x)$ e si prende il resto c_1, anch'esso una costante:

$$c_1 \equiv \frac{f(x) - c_0}{p(x)} \bmod\ p(x),$$

e in generale:

$$c_k \equiv \frac{f(x) - (c_0 + c_1 p(x) + \cdots + c_{k-1} p(x)^{k-1})}{p(x)^k} \bmod\ p(x).$$

Se ora $g(x)$ è un altro polinomio, cerchiamo uno sviluppo analogo per la funzione razionale $f(x)/g(x)$. Abbiamo un teorema del tutto simile al Teorema 2.1.

Teorema 2.10. *Sia $f(x)/g(x)$ una funzione razionale, $p(x)$ un polinomio di primo grado con $(p(x), g(x)) = 1$. Allora esiste ed è unica la coppia di polinomi $c = c(x)$ e $d(x)$, con c costante, tale che*:

$$\frac{f(x)}{g(x)} = c + \frac{d(x)}{g(x)} p(x). \tag{2.10}$$

Dim. Esistono $c_0(x)$ e $d_0(x)$ tali che:

$$g(x)c_0(x) + p(x)d_0(x) = 1,$$

da cui:

$$g(x)(c_0(x)f(x)) + p(x)(d_0(x)f(x)) = f(x).$$

Dividiamo $c_0(x)f(x)$ per $p(x)$: $c_0(x)f(x) = p(x)q(x) + r(x)$, con $\partial r(x) = 0$. Posto:

$$c = r(x) = c_0(x)f(x) - p(x)q(x) \text{ e } d(x) = d_0(x)f(x) + q(x)g(x),$$

si ha:

$$g(x) \cdot c + p(x)d(x) = f(x),$$

e dunque la (2.10). Se c'=costante e $d'(x)$ è un'altra coppia tale che:

$$g(x)c' + p(x)d'(x) = f(x),$$

sottraendo dalla precedente si ha:

$$g(x)(c - c') = p(x)(d'(x) - d(x)),$$

da cui, essendo $(p(x), g(x)) = 1$, $p(x)$ divide $c - c'$. Ma $\partial p(x) = 1$ e $\partial(c - c') = 0$; la sola possibilità è che $c - c' = 0$, cioè $c' = c$, e dunque anche $d'(x) = d(x)$. $\diamondsuit$

Nota. Essendo $p(x)$ di primo grado, $p(x) = ax + b$, la condizione $(p(x), g(x)) = 1$ equivale alla condizione che $-\frac{b}{a}$ non sia radice di $g(x)$.

Applicando il teorema alla coppia $d(x), g(x)$, si ottengono una costante c_1 e un polinomio $d_1(x)$, e, proseguendo, una costante c_i e un polinomio $d_i(x)$. Sostituendo $d_i(x)/g(x)$ con la sua espressione:

$$\frac{d_i(x)}{g(x)} = c_{i+1} + \frac{d_{i+1}(x)}{g(x)}p(x),$$

otteniamo lo sviluppo:

$$\frac{f(x)}{g(x)} = c_0 + c_1p(x) + \cdots + c_{n-1}p(x)^{n-1} + \frac{d_{n-1}(x)}{g(x)}p(x)^n,$$

$n = 1, 2, \ldots$. Ne segue:

$$f(x) = g(x)(c_0 + c_1p(x) + \cdots + c_{n-1}p(x)^{n-1}) + d_{n-1}(x)p(x)^n.$$

Il termine $R_n = d_{n-1}(x)p(x)^n$ è il *resto di ordine n* dello sviluppo. Dalla precedente segue:

$$f(x) \equiv g(x)(c_0 + c_1p(x) + \cdots + c_{n-1}p(x)^{n-1}) \bmod p(x)^n, \qquad (2.11)$$

$n = 1, 2, \ldots$. La successione infinita di congruenze (2.11) si suole riassumere simbolicamente nella forma:

$$\frac{f(x)}{g(x)} = c_0 + c_1 p(x) + \cdots = \sum_{k \geq 0} c_k p(x)^k.$$

Il calcolo dei coefficienti c_i si effettua risolvendo ricorsivamente le congruenze (2.11). Risolvere la prima:

$$f(x) \equiv c_0 g(x) \bmod p(x),$$

significa determinare c_0 in modo che $f(x)$ e $c_0 g(x)$ divisi per $p(x)$ diano lo stesso resto. Essendo $p(x) = ax + b$, di primo grado, questo resto è il valore di $f(x)$ e $c_0 g(x)$ in $-\frac{b}{a}$. Deve quindi essere $f(-\frac{b}{a}) = c_0 g(-\frac{b}{a})$, cioè $c_0 = f(-\frac{b}{a})/g(-\frac{b}{a})$.

Per semplicità ci limiteremo d'ora in poi al polinomio $p(x) = x - a$. Allora:

$$c_0 = \frac{f(a)}{g(a)}.$$

Per trovare c_1 consideriamo, con questo valore di c_0, la congruenza:

$$f(x) \equiv g(x)(c_0 + c_1(x - a)) \bmod (x - a)^2.$$

Poichè c_0 è tale che $f(x) - c_0 g(x)$ è divisibile per $x - a$, il quoziente $q_1(x) = (f(x) - c_0 g(x))/(x - a)$ è un polinomio. La congruenza precedente è allora equivalente alla:

$$q_1(x) \equiv c_1 g(x) \bmod (x - a),$$

e come prima:

$$c_1 = \frac{q_1(a)}{g(a)}.$$

In generale,

$$c_n = \frac{1}{g(a)} \frac{f(x) - g(x)(c_0 + c_1(x - a) + \cdots + c_{n-1}(x - a)^{n-1})}{(x - a)^n} \qquad (2.12)$$

mod $(x - a)$. Abbiamo così l'algoritmo (per $g(a) \neq 0$):

input: $f(x), g(x), a$,
$d : \frac{1}{g(a)}$, $c_0 : f(a)d$, $e_1 : c_0$,
per k : 1 a $n - 1$ fare:
$(q_k : quoziente(f(x) - e_k g(x), (x - a)^k) \cdot d$,
$c_k : resto(q_k, x - a)$,
$e_{k+1} : e_k + c_k \cdot (x - a)^k)$,
output: $c_0, c_1, \ldots, c_{n-1}$ (oppure: $e_1, e_2, \ldots, e_n$).

Esempi. 1. Abbiamo già visto che la funzione $\frac{1}{1-x}$ si sviluppa come $1+x+x^2+\cdots$ (in serie di potenze di $x-a$ con $a=0$), cioè con i coefficienti tutti uguali a 1. Ritroviamo questo risultato facendo girare l'algoritmo. Qui $f(x)=1$, $g(x)=1-x$. Allora $g(0)=1$, $d=1$, $q_0=1$, $c_0=\frac{1}{1}=1$, $e_1=1$.
$k=0$:

$$\begin{aligned} & q_1 : quoziente(1-1\cdot(1-x),x)\cdot 1 = 1, \\ & c_1 : 1, \\ & e_2 : 1+1\cdot x; \end{aligned}$$

$k=1$:

$$\begin{aligned} & q_2 : quoziente(1-(1+x)(1-x),x^2)\cdot 1 \\ & \quad = quoziente(x^2,x^2)\cdot 1 = 1, \\ & c_2 : 1, \\ & e_2 : 1+x+x^2; \end{aligned}$$

ecc.

2. Sviluppiamo la funzione:

$$\frac{1}{1-x-x^2},$$

e facciamo vedere che i coefficienti dello sviluppo sono i numeri di Fibonacci $(f_0=0), f_1=1, f_2=1, f_3=2, \ldots, f_{k+2}=f_k+f_{k+1}$, per $k\geq 2$:

$$\frac{1}{1-x-x^2} = 1+x+2x^2+3x^3+\cdots = \sum_{k\geq 0} f_{k+1}x^k.$$

Si ha, dalla (2.12), $c_0=\frac{1}{1}=1$,

$$\begin{aligned} c_1 &= \frac{1-(1-x-x^2)}{x} = \frac{x+x^2}{x} = 1+x \equiv 1 \bmod x; \\ c_2 &= \frac{1-(1-x-x^2)(1+x)}{x^2} = \frac{2x^2+x^3}{x^2} = 2+x \equiv 2 \bmod x, \end{aligned}$$

per cui $c_0=f_1$, $c_1=f_2$, $c_2=f_3$. Sia, per induzione, $c_k=f_{k+1}=f_k+f_{k-1}$. Dalla (2.12) si ha:

$$c_n = \frac{1-(1-x-x^2)\sum_{k=0}^{n-1} f_{k+1}x^k}{x^n} \bmod x.$$

Il numeratore della precedente frazione vale:

$$\begin{aligned} & 1-\sum_{k=0}^{n-1} f_{k+1}x^k + \sum_{k=0}^{n-1} f_{k+1}x^{k+1} + \sum_{k=0}^{n-1} f_{k+1}x^{k+2} = \\ = \; & (1-f_1)+(f_1-f_2)x+(f_1+f_2-f_3)x^2+\cdots+(f_{n-2}+f_{n-1}-f_n)x^{n-1} \\ + \; & (f_n+f_{n-1})x^n + f_n x^{n+1}. \end{aligned}$$

Per induzione, $f_{k+1} = f_k + f_{k-1}$ per $k < n$, e dunque i coefficienti delle potenze x^k, $k < n$, sono tutti zero. Si ha allora:

$$c_n = \frac{(f_{n-1} + f_n)x^n + f_n x^{n+1}}{x^n} \bmod x,$$

da cui $c_n = f_n + f_{n-1}$ e dunque $c_n = f_{n+1}$.

Sviluppiamo ora la stessa funzione applicando direttamente il Teorema 2.10. Si ha:

$$(1 - x - x^2) \cdot 1 + x(1 + x) = 1, \tag{2.13}$$

e dunque:

$$\frac{1}{1 - x - x^2} = 1 + \frac{1 + x}{1 - x - x^2} x. \tag{2.14}$$

Moltiplicando la (2.13) per $1 + x$,

$$(1 - x - x^2)(1 + x) + x(1 + x)^2 = 1 + x.$$

Qui $c_0(x) = 1 + x$. Dividendo per x otteniamo quoziente 1 e resto 1. Dunque $c_1 = 1$ e $d_1(x) = (1 + x)^2 + 1 \cdot (1 - x - x^2) = 1 + 2x + x^2 + 1 - x - x^2 = 2 + x$. Allora:

$$\frac{1 + x}{1 - x - x^2} = 1 + \frac{2 + x}{1 - x - x^2} x.$$

e, sostituendo nella (2.14),

$$\frac{1}{1 - x - x^2} = 1 + x + \frac{2 + x}{1 - x - x^2} x^2.$$

Analogamente:

$$(1 - x - x^2)(2 + x) + x(1 + x)(2 + x) = 2 + x,$$

e col solito procedimento si trova $c_2 = 2$ e $d_2(x) = 3 + 2x$. Dunque:

$$\frac{1}{1 - x - x^2} = 1 + x + 2x^2 + \frac{3 + 2x}{1 - x - x^2} x^3.$$

Nota. Come si vede da quest'ultimo sviluppo, i coefficienti c_i coincidono con quelli del quoziente della divisione di $f(x)$ per $g(x)$ ordinando i due polinomi secondo le potenze *crescenti* di x; la divisione si effettua allora dividendo i due monomi di grado più basso. Si ha infatti, nel nostro caso, che il primo quoziente è 1, e il primo resto $x + x^2 = (1 + x)x = d(x) \cdot x$. Il secondo quoziente è ancora 1, e il secondo resto $2x^2 + x^3 = (2 + x)x^2 = d_1(x) \cdot x^2$, ecc. E' facile vedere che si tratta di un fatto generale.

L'algoritmo suggerito dal metodo di Newton si applica anche al caso di una funzione razionale $f(x)/g(x)$. Come nel caso di un numero razionale questa può infatti essere vista come soluzione dell'equazione in y:

$$g(x)y - f(x) = 0$$

a coefficienti polinomi. (Il polinomio a primo membro è un polinomio a coefficienti nel campo delle funzioni razionali $Q(x)$). Il numero primo p dell'algoritmo visto in precedenza è qui sostituito dalla variabile x. A partire da una soluzione mod x, e cioè $y = f(0)/g(0) = c_0$ (ci limitiamo allo sviluppo in potenze di x, e dunque supponiamo che $g(0) \neq 0$), il seguente algoritmo fornisce i coefficienti $c_1, c_2, \ldots$. Nell'algoritmo, d è l'inverso della derivata del polinomio $F(y) = g(x)y - f(x)$ rispetto a y presa mod x, cioè calcolata in $x = 0$: $d = 1/g(0)$.

input: *f(x),g(x)*,
$F(y) = g(x)y - f(x)$, $d : \frac{1}{g(0)}$, $c_0 : d$, $e_1 : d$,
per $k : 1$ a $n - 1$ fare:
$(q_k : quoziente(-F(e_k), x^k) \cdot d$,
$c_k : resto(q_k, x)$,
$e_{k+1} : e_k + c_k \cdot x^k)$,
output: $c_0, c_1, \ldots, c_n$ (oppure: $e_1, e_2, \ldots, e_n$).

Esempio. Sviluppiamo:

$$\frac{1+x}{(1-x)^2}.$$

Qui $F(y) = (1-x)^2 y - (1+x)$, $F'(y) = (1-x)^2$, $F'(1) = 1$,
$d : 1$, $c_0 : 1$ $e_1 : 1$.

Facendo girare l'algoritmo abbiamo:

$k = 1$:

$$\begin{aligned} q_1 &: quoziente(-F(1), x) \\ &= quoziente((1-x)^2 - (1+x), x) = -x + 3, \\ c_1 &: resto(q_1, x) = 3, \\ e_2 &: 1 + 3x; \end{aligned}$$

$k = 2$:

$$\begin{aligned} q_2 &: quoziente((1-x)^2(1+3x) - (1+x), x^2) \\ &= quoziente(-3x^3 + 5x^2, x^2) = -3x + 5, \\ c_2 &: resto(q_2, x) = 5, \\ e_3 &: 1 + 3x + 5x^2, \end{aligned}$$

ecc. Si ottiene in questo modo la serie generatrice dei numeri dispari:

$$1 + 3x + 5x^2 + 7x^3 + \cdots$$

(una serie di potenze $\sum_{k\geq 0} c_k x^k$ prende anche il nome di *serie generatrice* dei numeri c_k).

Esercizi

10. Dimostrare che se $F(x) = a_0 + a_1 x + \cdots$, e se $b_k = a_0 + a_1 + \cdots + a_k$, allora:

$$\frac{F(x)}{1-x} = b_0 + b_1 x + \cdots.$$

11. Determinare le prime cifre dello sviluppo delle due radici quadrate di 5 mod 11 e verificare che la somma termine a termine è 0 mod 11.

12. Come nell'esercizio precedente con le radici di $x^2 - 2$ mod 47.

2.5 Relazioni di ricorrenza lineari

Sappiamo che lo sviluppo in serie di un numero razionale è periodico: la successione delle cifre è tale che esiste d per il quale, a partire da un certo n,

$$c_{n+d} = c_n.$$

Sia ora $u_1, u_2, \ldots$ una successione di numeri. Una relazione del tipo:

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_{k-1} u_{n+1} + a_k u_n \tag{2.15}$$

si chiama *relazione di ricorrenza lineare di ordine (o periodo) k* tra gli elementi della successione. A partire da un certo n, i valori di $n+k$ sono determinati dai k valori precedenti. La $c_{n+d} = c_n$ è una relazione di ordine d, con i coefficienti $a_{d-1} = \ldots = a_1 = 0$ e $a_0 = 1$. I coefficienti di uno sviluppo in serie di una funzione razionale soddisfano una relazione di questo tipo, come vedremo tra un momento. E' questa dunque la nozione, più generale, che corrisponde alla periodicità nel caso dei numeri razionali. Diamo qualche esempio. I coefficienti della $\frac{1}{1-x}$ sono tutti uguali (e uguali a 1) e soddisfano perciò la relazione $u_{n+1} = u_n$, $n \geq 0$, di ordine 1. La serie dei numeri naturali, cioè i coefficienti della $\frac{1}{(1-x)^2}$, soddisfano la $u_{n+2} = 2u_{n+1} - u_n$, $n \geq 0$, di ordine 2, come pure una qualunque altra serie di numeri in progressione aritmetica (se la differenza tra due termini consecutivi è costante, $u_{n+2} - u_{n+1} = u_{n+1} - u_n$, allora $u_{n+2} = 2u_{n+1} - u_n$). I numeri di Fibonacci, come sappiamo, soddisfano la $u_{n+2} = u_{n+1} + u_n$, per $n \geq 2$, anch'essa di ordine 2.

Teorema 2.11. *Sia data la funzione razionale $f(x)/g(x)$, $\partial f(x) < \partial g(x)$, $g(0) \neq 0$, e sia $\partial g(x) = k$. Allora i coefficienti dello sviluppo:*

$$\frac{f(x)}{g(x)} = c_0 + c_1 x + c_2 x^2 + \cdots$$

soddisfano una relazione di ricorrenza lineare di ordine k.

Dim. Sia $f(x) = a_0 + a_1 x + \cdots + a_m x^m$, $g(x) = b_0 + b_1 x + \cdots + b_k x^k$. Sia $n \geq m - k + 1$, e fermiamoci, nello sviluppo, al termine x^{n+k}. Abbiamo:

$$a_0 + a_1 x + \cdots + a_m x^m = (b_0 + b_1 x + \cdots + b_k x^k)(c_0 + c_1 x + \cdots + c_{n+k} x^{n+k}) + R(x).$$

Il resto $R(x)$ contiene potenze di x superiori a $n + k$, e il polinomio a primo membro potenze di x inferiori a $n+k$, in quanto $m \leq n+k-1$; il coefficiente di questa potenza di x a secondo membro è dunque zero. Ma questo coefficiente è

$$c_{n+k} b_0 + c_{n+k-1} b_1 + \cdots + c_n b_k = 0,$$

da cui, essendo $b_0 = g(0) \neq 0$,

$$c_{n+k} = -\frac{b_1}{b_0} c_{n+k-1} - \cdots - \frac{b_k}{b_0} c_n,$$

ciò che dimostra l'asserto. $\diamondsuit$

Nota. Se $m = \partial f(x) \geq \partial g(x)$ si prenda $n \geq m - k + 1$.

Esempio. Con $f(x) = 1$ e $g(x) = 1 - x - x^2$ (Fibonacci), si ha $b_0 = 1$, $b_1 = -1$, $b_2 = -1$, ed essendo $k = 2$,

$$c_{n+2} = 1 \cdot c_{n+1} + 1 \cdot c_n.$$

Sussiste anche il viceversa del Teorema 2.11. In altri termini, quello visto nel Teorema 2.11 è l'unico modo in cui possono nascere relazioni di ricorrenza lineari.

Teorema 2.12. *Sia $u_1, u_2, \ldots$ una successione che soddisfa la relazione di ricorrenza lineare:*

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_n u_n,$$

$n \geq m \geq 1$. Allora esistono due polinomi $f(x)$ e $g(x)$ tali che

$$\frac{f(x)}{g(x)} = u_1 + u_2 x + \cdots.$$

Dim. Sia $g(x) = 1 - a_1 x - \cdots - a_k x^k$, e moltiplichiamo $g(x)$ per $u_1 + u_2 x + \cdots + u_{n+1} x^n$; se m è un intero, $n \geq m \geq 1$, si ha:

$$\begin{aligned}
u_1 + (u_2 - a_1 u_1) x \quad &+ \quad \cdots + (u_{k+m-1} - a_1 u_{k+m-2} - \cdots - a_k u_{m-1}) x^{k+m-2} \\
&+ \quad (u_{k+m} - a_1 u_{k+m-1} - \cdots - a_k u_m) x^{k+m-1} + \\
&\vdots \\
&+ \quad (u_{n+1} - a_1 u_n - \cdots - a_k u_{n-k+1}) x^n - \\
&- \quad (a_1 u_{n+1} + \cdots + a_k u_{n-k+2}) x^{n+1} + \cdots + a_k u_{n+1} x^{n+k}.
\end{aligned}$$

I coefficienti delle potenze di x che compaiono nelle righe dalla seconda alla penultima sono zero per l'ipotesi di ricorrenza lineare della successione degli u_i. Chiamiamo $f(x)$ il polinomio che compare nella prima riga, e $-R(x)$ quello che compare nell'ultima. Allora:

$$f(x) = (1 - a_1x - \cdots - a_kx^k)(u_1 + u_2x + \cdots + u_{n+1}x^n) + R(x),$$

per cui gli u_i sono effettivamente i coefficienti del quoziente

$$\frac{f(x)}{1 - a_1x - \cdots - a_kx^k}$$

nella divisione effettuata una volta ordinati i due polinomi secondo le potenze crescenti di x. $\diamondsuit$

Nota. L'*equazione caratteristica* della relazione (2.15) è l'equazione:

$$x^k = a_1x^{k-1} + a_2x^{k-2} + \cdots + a_{k-1}x + a_k.$$

Le radici di questa equazione permettono di esprimere il termine generico u_n della successione. Si ha infatti il seguente risultato (che non dimostriamo): se $\lambda_1, \lambda_2, \ldots, \lambda_t$ sono le dette radici, di molteplicità $n_1, n_2, \ldots, n_t$, allora esistono t polinomi:

$$p_1(x), p_2(x), \ldots, p_t(x),$$

tali che:

$$u_n = p_1(n)\lambda_1^{n_1-1} + p_2(n)\lambda_2^{n_2-1} + \cdots + p_t(n)\lambda_t^{n_t-1}.$$

Inoltre, se le radici λ_i sono tutte semplici, i polinomi $p_i(x)$ sono costanti.

Esercizi

13. Dimostrare che la successione dei numeri naturali $u_n = n$ soddisfa la relazione di ordine 2:

$$u_{n+2} = 2u_{n+1} - u_n$$

e che la stessa relazione è soddisfatta da ogni successione i cui termini sono dati da un polinomio di primo grado in n : $u_n = an + b$.

Dimostrare inoltre che la successione dei quadrati dei naturali $u_n = n^2$ soddisfa la relazione di ordine 3:

$$u_{n+3} = 3u_{n+2} - 3u_{n+1} + u_n,$$

e che la stessa relazione è soddisfatta da ogni successione i cui termini sono dati da un polinomio quadratico in n : $u_n = an^2 + bn + c$.

Denotiamo con s_k la somma dei primi k termini di una successione $\{u_i\}$, $i = 1, 2, \ldots$.

14. Dimostrare che se $\{u_i\}$ è la successione di Fibonacci, allora gli s_k relativi soddisfano la relazione di ordine 3:

$$s_{n+3} = 2s_{n+2} - s_n.$$

15. Quale relazione soddisfano i termini di una progressione geometrica di ragione q? E gli s_k relativi?

Nota bibliografica

[**C**] I-5. Per le relazioni di ricorrenza lineari si veda [**CMP**].

Capitolo 3

Il Risultante

3.1 Il risultante

Siano $f = f(x)$ e $g = g(x)$ due polinomi di grado n e m, rispettivamente. Se f e g hanno un fattore non costante $d = d(x)$ in comune, allora:

$$\begin{aligned} f &= dk, \qquad \partial k < n, \\ g &= dh, \qquad \partial h < m, \end{aligned}$$

per certi polinomi k e h. Ne segue:

$$d = \frac{f}{k} = \frac{g}{h}$$

e

$$fh = gk. \tag{3.1}$$

Viceversa, supponiamo che esistano polinomi k e h, con $\partial k < n$ e $\partial h < m$, tali che la (3.1) sia soddisfatta. Dividendo h e k per (h, k) la (3.1) diventa $fh_1 = gk_1$, con $(h_1, k_1) = 1$. Allora k_1 divide f, $f = k_1 w$ e dunque $gk_1 = fh_1 = k_1 wh_1$, per cui $g = h_1 w$. Inoltre, $\partial w = \partial f - \partial k_1$ e $\partial k_1 \leq \partial k < \partial f$, per cui $\partial w > 0$. Cambiando k in $-k$, la (3.1) si può scrivere:

$$fh + gk = 0. \tag{3.2}$$

Abbiamo così:

Teorema 3.1. *Condizione necessaria e sufficiente affinchè due polinomi f e g abbiano un fattore non banale in comune è che esistano due polinomi k e h, con $\partial k < n$ e $\partial h < m$ tali che sussista la* (3.2). ♢

Vediamo ora quand'è che due polinomi come k e h esistono. Dati f e g,

$$\begin{aligned} f &= a_0x^n + a_1x^{n-1} + \cdots + a_n, \\ g &= b_0x^m + b_1x^{m-1} + \cdots + b_m, \end{aligned}$$

di grado effettivo n e m (cioè con a_0 e b_0 diversi da zero), due polinomi k e h:

$$\begin{aligned} k &= c_0x^{n-1} + c_1x^{n-2} + \cdots + c_{n-1}, \\ h &= d_0x^{m-1} + d_1x^{m-2} + \cdots + d_{m-1}, \end{aligned}$$

tali che sussista la (3.2) esistono se e solo se tutti i coefficienti del polinomio $fh+gk$ sono uguali a zero. Ciò conduce al seguente sistema omogeneo di $n+m$ equazioni nelle $n+m$ incognite $d_0, d_1, \ldots, d_{m-1}, c_0, c_1, \ldots, c_{n-1}$:

$$\begin{cases} a_0d_0 + b_0c_0 & = 0 \\ a_1d_0 + a_0d_1 + b_1c_0 + b_0c_1 & = 0 \\ a_2d_0 + a_1d_1 + a_0d_2 + b_2c_0 + b_1c_1 + b_0c_2 & = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_nd_{m-1} + b_mc_{n-1} & = 0. \end{cases}$$

Questo sistema ha una soluzione non tutta nulla se e solo se la sua matrice ha determinante 0, e ogni soluzione non tutta nulla dà luogo a due polinomi k e h che soddisfano la (3.2). Si osservi che a causa della forma del sistema se uno dei due polinomi k e h è il polinomio nullo, anche l'altro lo è. In altre parole, una soluzione non tutta nulla del sistema deve avere almeno uno dei d e uno dei c diversi da 0. Trasponendo la matrice del sistema abbiamo la *matrice di Sylvester* $S(f,g)$ dei due polinomi dati:

$$S(f,g) = \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & 0 & 0 & 0 \\ 0 & a_0 & a_1 & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & a_0 & \ldots & a_{n-1} & a_n \\ b_0 & b_1 & b_2 & \ldots & 0 & 0 & 0 \\ 0 & b_0 & b_1 & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & b_0 & \ldots & b_{m-1} & b_m \end{pmatrix}.$$

Il *risultante* $R(f,g)$ dei due polinomi f e g è il determinante della matrice di Sylvester $S(f,g)$.

Se in f e g compaiono più variabili, poichè il risultante è definito per polinomi in una variabile, si può calcolare il risultante considerando f e g come polinomi in una sola di esse, e le altre come costanti. Se x è la variabile prescelta, scriviamo $R_x(f,g)$, e questo risultante sarà un polinomio nelle restanti variabili.

Dalla discussione precedente si ha allora:

Teorema 3.2. *Due polinomi f e g hanno un fattore non costante in comune se e solo se $R(f,g)=0$.* ♢

Vediamo ora alcune proprietà del risultante.

Se uno dei due polinomi è costante, diciamo $g=a$, si pone per definizione:

$$R(f,a)=R(a,f)=a^{\partial f}.$$

Se entrambi sono costanti, $f{=}a$ e $g{=}b$, allora, ancora per definizione,

$$R(f,g)=\begin{cases} 0, & \text{se } a=b=0;\\ 1, & \text{altrimenti.}\end{cases}$$

Inoltre

$$R(g,f)=(-1)^{mn}R(f,g),$$

e questo perchè $S(g,f)$ si ottiene da $S(f,g)$ permutandone le righe 1,2,...,$m-1, m, m+1,\dots,m+n$ fino a raggiungere la permutazione $m+1, m+2,\dots,m+n, 1, 2,\dots,m$, e questo si può fare spostando m in fondo mediante n trasposizioni, e analogamente per $m-1, m-2,\dots,1$. Il numero totale di trasposizioni necessarie per far ciò è mn.

Per il Teorema 3.2, $\mathrm{MCD}(f,g)\neq 1$ se e solo se $R(f,g)=0$. La relazione tra il massimo comun divisore di f e g e la loro matrice di Sylvester $S(f,g)$ si spiega col fatto che *l'eliminazione di Gauss sulla matrice $S(f,g)$ corrisponde all'algoritmo della divisione per il calcolo di* $\mathrm{MCD}(f,g)$. Più precisamente sia $\partial f\leq\partial g$; nella divisione di g per f si moltiplica f per $\frac{b_0}{a_0}x^{m-n}$ e si sottrae il risultato da g. Si ottiene così il primo resto parziale ρ_1 della divisione:

$$\rho_1=(b_1-\frac{b_0a_1}{a_0})x^{m-1}+(b_2-\frac{b_0a_2}{a_0})x^{m-2}+\cdots+b_m.$$

Consideriamo ora l'eliminazione di Gauss su $S(f,g)$. Sottraiamo dalla $(m+1)-$esima riga (cioè dalla prima riga dei b) la prima moltiplicata per b_0/a_0; il risultato è:

$$\begin{pmatrix} a_0 & a_1 & a_2 & \dots & 0\\ 0 & a_0 & a_1 & \dots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \dots & a_n\\ 0 & b_1-b_0a_1/a_0 & b_2-a_2b_0/a_0 & \dots & 0\\ 0 & b_0 & b_1 & \dots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \dots & b_m \end{pmatrix}.$$

Nel blocco ottenuto sopprimendo la prima riga e la prima colonna di questa matrice gli elementi della prima riga dei b sono i coefficienti di ρ_1 (più alcuni zeri). Cerchiamo ora di eliminare il b_0 che si trova sulla prima colonna. Sottraiamo dalla riga dove si trova questo b_0 la prima moltiplicata per b_0/a_0; gli elementi della seconda riga dei b sono ora i coefficienti di ρ_1. Continuiamo l'operazione finchè il b_0 dell'ultima riga non è stato eliminato: il risultato è una matrice che ha un certo numero k_1 di a_0 sulla diagonale principale, e sotto la quale vi sono solo zeri, più un blocco quadrato. Quest'ultimo blocco è $S_1 = S(f, \rho_1)$, la *matrice di Sylvester di f e del primo resto ρ_1*. A questo punto,

$$R(f, g) = a_0^{k_1} R(f, \rho_1),$$

per un certo k_1. Se $\partial f \leq \partial \rho_1$, si continua la divisione e si trova un altro resto parziale ρ_2. L'eliminazione di Gauss sulla matrice $S(f, \rho_1)$ dà $R(f, \rho_1) = a_0^{k_2} R(f, \rho_2)$, e pertanto:

$$R(f, g) = a_0^{k_1+k_2} R(f, \rho_2).$$

Si continua la divisione finchè non si trova un resto r di grado inferiore al grado di f (questo r è allora *il* resto della divisione di g per f). La matrice corrispondente $S(f, r)$ è di dimensione $n+\partial r$, e poichè la dimensione di $S(f, g)$ è $n+m$, il numero degli a_0 che precedono il blocco (f, r) è $n+m-(n+\partial r) = m-\partial r$, e si ha:

$$R(f, g) = a_0^{m-\partial r} R(f, r). \tag{3.3}$$

Come si vede, le operazioni dell'eliminazione sulla matrice fino a questo punto corrispondono alle operazioni che si compiono per trovare il resto r. Arrivati a questo resto r abbiamo fatto il primo passo dell'algoritmo di Euclide della divisione di g per f, primo passo che corrisponde al passaggio da $S(f, g)$ a $S(f, r)$. Avendosi $\partial f > \partial r$, consideriamo $S(r, f)$ e applichiamo l'argomento precedente; troviamo:

$$R(f, g) = a_0^{m-\partial r_1} (-1)^{n \cdot \partial r_1} R(r_1, r_2),$$

dove si è posto $r = r_1$ e dove r_2 è il resto (finale) della divisione di f per r_1. Infine, se l'algoritmo di Euclide ha k passi,

$$R(f, g) = h \cdot R(r_{k-1}, r_{k-2}),$$

dove h è una costante. Se f e g sono relativamente primi, $r_{k-1} = c$, una costante, per definizione si ha $R(c, r_{k-2}) = c^{\partial r_{k-2}}$. In questo caso $R(f, g) \neq 0$. Se f e g hanno un fattore non costante in comune allora $\partial r_{k-1} \geq 1$. Abbiamo $R(r_{k-1}, r_{k-2}) = h \cdot R(r_{k-1}, \rho)$, dove ρ è il penultimo resto della divisione di

r_{k-2} per r_{k-1}. Ma il resto di questa divisione è zero, e ciò implica che ρ e r_{k-1} sono proporzionali. Quindi, la prima riga di $S(r_{k-1}, \rho)$ è proporzionale alla $(\partial r_{k-1} + 1)-$esima (e la seconda alla $(\partial r_{k-1} + 2)-$esima, ecc.), per cui il determinante è zero. In questo caso $R(f, g) = 0$. Abbiamo così una nuova dimostrazione del Teorema 3.2.

Esempio. Siano:

$$\begin{aligned} f &= 2x^2 + 1, \\ g &= 2x^5 - x^3 - 2x^2 - 2. \end{aligned}$$

La divisione $g = fq + r$ dà come primo resto:

$$\rho_1 = -2x^3 - 2x^2 - 2,$$

come secondo:

$$\rho_2 = -2x^2 + x - 2,$$

e infine:

$$\rho_3 = r = x - 1.$$

La matrice $S(f, g)$ è

$$\begin{pmatrix} 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 1 \\ 2 & 0 & -1 & -2 & 0 & -2 & 0 \\ 0 & 2 & 0 & -1 & -2 & 0 & -2 \end{pmatrix}.$$

Procediamo con l'eliminazione di Gauss. Aggiungiamo alla sesta riga la prima moltiplicata per -1, e nella matrice così ottenuta sottraiamo la seconda riga dall'ultima. Il risultato è:

$$\begin{pmatrix} 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & -2 & -2 & 0 & -2 & 0 \\ 0 & 0 & 0 & -2 & -2 & 0 & -2 \end{pmatrix}.$$

Il blocco 5×5 in basso a destra è $S_1 = S(f, \rho_1)$. A questo punto, $R(f,g) = 2^2 \cdot R(f, \rho_1)$. L'eliminazione di Gauss continua ora nella matrice S_1. Aggiungiamo in S_1 la prima riga alla quarta e nella matrice così ottenuta aggiungiamo la seconda riga all'ultima. Si ha:

$$\begin{pmatrix} 2 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & -2 & 1 & -2 & 0 \\ 0 & 0 & -2 & 1 & -2 \end{pmatrix}.$$

Il blocco 4×4 in basso a destra è $S_2 = S(f, \rho_2)$. Qui $R(f,g) = 2^3 \cdot R(f, \rho_2)$. In S_2, aggiungiamo la terza riga alla prima; la nuova matrice è:

$$\begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix},$$

e il blocco 3×3 in basso a destra è $S_3 = S(f, \rho_3)$. Così,

$$R(f,g) = 2^4 \cdot R(f,r).$$

(Si osservi che l'esponente 4 è uguale a $\partial f - \partial r = 5 - 1$).

Il primo passo dell'algoritmo di Euclide corrisponde all'eliminazione in $S(f,g)$, e ci porta qui a $S_3 = S(f,r)$. Continuiamo con l'algoritmo e dividiamo f per r, ottenendo un primo resto parziale $\rho_4 = 2x + 1$ e un secondo (e ultimo) $\rho_5 = 3$. Poichè $\partial f > \partial r$ consideriamo la matrice $S_3' = S(r,f)$, ottenuta dalla S_3 trasponendo la prima e la seconda riga, e quindi la seconda e la terza (in tal modo il determinante non cambia):

$$\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 2 & 0 & 1 \end{pmatrix}.$$

Aggiungiamo all'ultima riga la prima moltiplicata per -2; si ha

$$\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 2 & 1 \end{pmatrix},$$

da cui:

$$S_4 = \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix},$$

che è la Sr, ρ_4), e il cui determinante è uguale a 3. Per definizione, 3 è il risultante $R(x-1,3) = R(r,\rho_5)$.

Riassumendo:

$$\begin{aligned} R(f,g) &= 2^2 \cdot R(f,\rho_1), \\ R(f,\rho_1) &= 2 \cdot R(f,\rho_2), \\ R(f,\rho_2) &= 2 \cdot R(f,r) = R(r,f), \\ R(r,f) &= R(r,\rho_4) = R(r,\rho_5), \end{aligned}$$

e dunque $R(f,g) = 2^4 \cdot 3 = 48$. Se ne conclude che f e g sono relativamente primi.

Nota. Il numero di passi necessari per passare da S_i a S_{i+1} nel processo di eliminazione è uguale al più piccolo dei gradi dei due polinomi di cui S_{i+1} è la matrice di Sylvester.

La (3.3) suggerisce un modo per calcolare ricorsivamente il risultante, e dunque il seguente algoritmo:

input: f, g,
$n = \partial f$, $m = \partial g$,
se $n > m$ allora $R : (-1)^{mn} R(g,f)$, altrimenti fare:
$(a_n : coeffprinc(f)$,
se $n = 0$ allora $R : a_n^m$, altrimenti fare:
$(r : resto(g,f)$,
se $r = 0$ allora $R : 0$, altrimenti fare:
$p : \partial r$,
$R : a_n^{m-p} R(f,r)))$
output: R.

Il teorema che segue dà un'espressione del risultante in termini delle radici dei due polinomi. Prima un lemma.

Lemma 3.3. *Siano $\alpha_1, \alpha_2, \ldots, \alpha_n$ e $\beta_1, \beta_2, \ldots, \beta_m$ le radici di $f(x)$ e $g(x)$, rispettivamente, in un ampliamento del campo dei coefficienti. Allora valgono le seguenti uguaglianze:*

$$a_0^m \prod_{f(x)=0} g(x) = (-1)^{mn} b_0^n \prod_{g(x)=0} f(x) = a_0^m b_0^n \prod_{i,j} (\alpha_i - \beta_j). \tag{3.4}$$

Dim. (L'espressione $\prod_{f(x)=0} g(x)$ sta per $\prod_{i=1}^n g(\alpha_i)$, cioè il prodotto dei valori che $g(x)$ assume sulle radici di $f(x)$). Dimostriamo che la prima e la seconda quantità sono uguali alla terza. Per la prima abbiamo

$$g(x) = b_0(x-\beta_1)(x-\beta_2)\cdots(x-\beta_m),$$

per cui:

$$g(\alpha_i) = b_0(\alpha_i-\beta_1)(\alpha_i-\beta_2)\cdots(\alpha_i-\beta_m).$$

Il prodotto di tutte queste espressioni per $i = 1, 2, \ldots, n$ è

$$\prod_{f(x)=0} g(x) = b_0^n \prod_{i,j} (\alpha_i - \beta_j).$$

Per la seconda,

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

e dunque:

$$f(\beta_j) = a_0(\beta_j - \alpha_1)(\beta_j - \alpha_2) \cdots (\beta_j - \alpha_n)$$

ovvero:

$$(-1)^n f(\beta_j) = a_0(\alpha_1 - \beta_j)(\alpha_2 - \beta_j) \cdots (\alpha_n - \beta_j).$$

Il prodotto di tutte queste espressioni per $j = 1, 2, \ldots, m$ è

$$(-1)^{mn} \prod_{g(x)=0} f(x) = a_0^m \prod_{i,j} (\alpha_i - \beta_j),$$

da cui il risultato. ♢

Teorema 3.4. *Sussiste la seguente uguaglianza, dove $m = \partial g$:*

$$R(f, g) = a_0^m \prod_{f(x)=0} g(x).$$

Dim. Sia $\partial f \leq \partial g$. Per induzione su ∂f, il grado del primo polinomio della coppia f, g. Se $\partial f = 0$, allora $f = a_0$, una costante, e per definizione $R(a_0, g) = a_0^m$. Sia $\partial f > 0$. Se $g = fq + r$ abbiamo:

$$R(f, g) = a_0^{m - \partial r} R(f, r).$$

Essendo $\partial f > \partial r$, consideriamo $R(r, f)$. Per ipotesi induttiva:

$$R(r, f) = r_0^n \prod_{r(x)=0} f(x) = (-1)^{n\partial r} a_0^{\partial r} \prod_{f(x)=0} r(x),$$

dove la seconda uguaglianza segue dalla prima delle (3.4). Ma se calcoliamo $g = fq + r$ in una radice α di f abbiamo $g(\alpha) = r(\alpha)$, e quindi $\prod_{f(x)=0} r(x) = \prod_{f(x)=0} g(x)$. Allora:

$$\begin{aligned} R(f, g) &= a_0^{m-\partial r} R(f, r) = a_0^{m-\partial r} (-1)^{n\partial r} R(r, f) \\ &= a_0^{m-\partial r} (-1)^{n\partial r} (-1)^{n\partial r} a_0^{\partial r} \prod_{f(x)=0} g(x) \\ &= a_0^m \prod_{f(x)=0} g(x). \end{aligned}$$

Se $\partial f > \partial g$, consideriamo $R(f,g) = (-1)^{mn} R(g,f)$. L'argomento precedente fornisce $R(g,f) = b_0^n \prod_{g(x)=0} f(x)$, e il risultato segue dalla prima uguaglianza delle (3.4). ♢

Esempio. Sia $z = a + bi$ un numero complesso, $\overline{z} = a - bi$ il suo coniugato. Questi due numeri sono i valori del polinomio $a + bx$ nei punti i e $-i$, rispettivamente, vale a dire nelle radici di $x^2 + 1$. Il loro prodotto è $a^2 + b^2$, la *norma* di z. Dunque,

$$N = R(x^2 + 1, a + bx).$$

Ciò si può verificare calcolando il determinante della matrice:

$$\begin{pmatrix} b & a & 0 \\ 0 & b & a \\ 1 & 0 & 1 \end{pmatrix}$$

che vale appunto $a^2 + b^2$. La norma del numero complesso $a + bi$ si può anche definire come norma del polinomio $a + bx$ rispetto alle radici di $x^2 + 1$. Più in generale, si può definire la *norma di un polinomio g rispetto alle radici di un altro polinomio f* come il risultante $R(f,g)$.

Corollario 3.5. *Siano f, g e h tre polinomi. Allora:*

$$R(fg,h) = R(f,h)R(g,h).$$

Dim. Per il teorema,

$$R(fg,h) = (a_0 b_0)^{\partial h} \prod_{fg=0} h(x).$$

Ma $fg(x) = f(x)g(x) = 0$ se e solo se $f(x) = 0$ oppure $g(x) = 0$. Dunque:

$$\prod_{fg(x)=0} h(x) = \prod_{f(x)=0} h(x) \cdot \prod_{g(x)=0} h(x),$$

e si ha il risultato. ♢

Esercizi

1. Dimostrare che, con $m = \partial g$,

$$R(ax + b, g) = a^m g(-\frac{b}{a}).$$

In particolare, $R(x - a, g) = g(a)$.

2. Dimostrare il Teorema 3.4 usando l'esercizio precedente e il Corollario 3.5. (*Sugg.:* induzione su ∂f, il primo polinomio).

3. Sia y una variabile. Dimostrare che:

$$R_x(f, g - y) = a_0^m \prod_{f(x)=0} (g(x) - y).$$

(Per $y = 0$ si ottiene il Teorema 3.4. $R(f, g)$ è il termine noto di $R_x(f, g - y)$, che è un polinomio in y).

4. Siano $f(x), g(x)$ e $h(y)$ tre polinomi. Dimostrare che

$$R_y(f(h), g(h)) = (h_0^{nm} R_x(f, g))^{\partial h},$$

escluso il caso in cui $h(y)$ è una costante tale che $f(h) = g(h) = 0$.

5. (Caratterizzazione del risultante). Sia F una funzione che associa ad ogni coppia di polinomi su un campo K un elemento di K e tale che:
a) $F(f, 0) = 0$, se f non è costante;
b) $F(g, f) = (-1)^{mn} F(f, g)$;
c) se $\partial f \leq \partial g$ e $g = fq + r$, allora $F(f, g) = a_0^{m-\partial r} F(f, r)$,
dove a_0 è il coefficiente principale di f. Dimostrare che $F(f, g)$ è il risultante $R(f, g)$. (*Sugg.:* induzione su $\min(\partial f, \partial g)$).

6. Sia P_i lo spazio vettoriale dei polinomi di grado al più i, e siano f e g due polinomi di gradi n e m, rispettivamente. Sia $P_m \times P_n$ lo spazio vettoriale delle coppie di polinomi (p, q) e consideriamo l'applicazione lineare:

$$\phi : \ P_m \times P_n \to P_{m+n}$$

data da:

$$(p, q) \to fp + gq.$$

Dimostrare che la matrice di ϕ è la matrice di Sylvester $S(f, g)$.

7. Sia A una matrice e sia $f = f(x)$ un polinomio arbitrario. Dimostrare che

$$det\, f(A) = R(f, p),$$

dove $p = p(x)$ è il polinomio caratteristico di A.

8. Dimostrare che esistono due polinomi $a(x)$ e $b(x)$ tali che:

$$R(f, g) = a(x)f(x) + b(x)g(x),$$

e che se f e g sono a coefficienti interi anche a e b lo sono.

9. Sia R_i il determinante ottenuto da $R(f, g)$ sopprimendo le prime e le ultime i colonne, le prime i righe del gruppo corrispondente a f, e le prime i righe di quello corrispondente a g. Dimostrare che condizione necessaria e sufficiente affinchè f e g abbiano un MCD di grado d è che si abbia $R = 0$, $R_1 = 0, \ldots, R_{d-1} = 0$, $R_d \neq 0$.

3.2 Applicazioni

Il risultante permette di risolvere il seguente problema: *dato un polinomio f, trovare un polinomio g le cui radici sono una data funzione razionale delle radici di f.* Va da sè che questo problema ha interesse solo nel caso in cui le radici di f non siano note.

Intanto, un polinomio f si può esprimere come risultante di due polinomi. Siano infatti $\alpha_1, \alpha_2, \ldots, \alpha_n$ le radici di f (in un ampliamento del campo); allora:

$$f(x) = a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) = a_0 \prod_{f(y)=0} (x-y),$$

e dunque:

$$f(x) = R_y(f(y), -y+x),$$

che è l'espressione richiesta. Il problema sopra menzionato è qui risolto nel caso in cui la funzione razionale è la funzione identica. Supponiamo ora che la funzione razionale sia un polinomio $p(x)$. Il polinomio $\prod_{f(y)=0}(x-p(y))$ ha come radici $p(\alpha_i)$ e quindi è una soluzione del nostro problema; prendiamo allora:

$$g(x) = R_y(f(y), x-p(y)).$$

Sia ora $p(x)/q(x)$ una qualunque funzione razionale. Intanto, perchè il nostro problema abbia soluzione è evidentemente necessario che $q(x)$ non si annulli su una radice di $f(x)$, e perciò q e f non debbono avere radici in comune. Sia:

$$g_1(x) = \prod_{f(y)=0} (x - \frac{p(y)}{q(y)}) = \prod_{f(y)=0} (q(y)x - p(y)) \cdot \frac{1}{\prod_{f(y)=0} q(y)}.$$

Allora $g_1(x)$ è una soluzione, e così pure $\prod_{f(y)=0}(q(y)x-p(y))$ e dunque anche:

$$g(x) = R_y(f(y), q(y)x - p(y)).$$

Si osservi come per $q(y) = 1$ si ottenga la formula precedente per il caso di un polinomio.

Nota. Una funzione razionale delle radici può sempre ridursi ad una funzione polinomiale. In altri termini, se $p(\alpha)/q(\alpha)$ è una funzione razionale della radice α di $f(x)$, allora esiste un polinomio $r(x)$ tale che $p(\alpha)/q(\alpha) = r(\alpha)$ (il polinomio $r(x)$ essendo lo stesso per tutte le radici di $f(x)$). Infatti, essendo f e q primi tra loro (se hanno un fattore in comune nel campo hanno una radice in comune in un ampliamento del campo), si ha $af + bq = 1$ da cui, moltiplicando per p si ha $a_1 f + rq = p$, per certi a_1 e r. Calcolando in α si ottiene $r(\alpha)q(\alpha) = p(\alpha)$, in quanto $f(\alpha) = 0$, e dunque r è il polinomio cercato. Si osservi che la riduzione a r si effettua mediante operazioni razionali sui coefficienti di p e q, e dunque anche r avrà i coefficienti nello stesso campo di p e q. Inoltre, se $\partial r \geq \partial f$, dividendo si ha $r = fq_1 + r_1$, con $\partial r_1 < \partial f$, e, calcolando

in α, $r(\alpha) = r_1(\alpha)$. Si può cioè ottenere una riduzione della funzione razionale ad un polinomio di grado inferiore a quello di $f(x)$.

Consideriamo ora alcuni casi particolari della funzione $p(x)/q(x)$.

1. *Radici aumentate*

Si richiede che $g(x)$ abbia come radici $\alpha + k$, dove k è un numero e α una radice di $f(x)$. La soluzione è ovviamente $g(x) = f(x-k)$, che espressa in termini di risultante è:

$$g(x) = R_y(f(y), x - y - k). \tag{3.5}$$

Per certi valori di k il polinomio g è più semplice di f, e quindi, a priori, è più facile trovare una radice β di g; una radice di f sarà allora semplicemente $\alpha = \beta - k$. Per esempio, è possibile determinare g in modo che manchi il termine in x^{n-1}: nella (3.5) il coefficiente di x^{n-1} è $a_1 - na_0k$ e dunque basta scegliere $k = a_1/na_0$. (Che il coefficiente di x^{n-1} in g sia $a_1 - na_0k$ si può anche vedere dal fatto che $g(x)$ è uguale a $f(x-k) = a_0(x-k)^n + a_1(x-k)^{n-1} + \cdots + a_n$ e applicando poi il teorema del binomio). Nel caso particolare dell'equazione di secondo grado tutto ciò conduce alla ben nota formula per la soluzione di queste equazioni: sia $f(x) = a_0x^2 + a_1x + a_2$; allora:

$$g(x) = R_y(f(y), -y + x - k) = \begin{vmatrix} a_0 & a_1 & a_2 \\ -1 & x-k & 0 \\ 0 & -1 & x-k \end{vmatrix}$$

e dunque:

$$g(x) = a_0x^2 + (a_1 - 2ka_0)x + a_0k^2 - a_1k + a_2,$$

scegliendo $k = a_1/2a_0$ il termine in x^{n-1}, cioè in questo caso in x, scompare, e si ha:

$$\begin{aligned} g(x) &= a_0x^2 + \frac{a_1^2}{4a_0} - \frac{a_1^2}{2a_0} + a_2 \\ &= a_0x^2 - \frac{a_1^2 - 4a_0a_2}{4a_0}. \end{aligned}$$

Le radici di $g(x)$ si ottengono semplicemente con una estrazione di radice quadrata: $\beta = \pm\sqrt{(a_1^2 - 4a_0a_2)/4a_0^2}$, e quelle di $f(x)$ sono:

$$\begin{aligned} \alpha &= \beta - k = \frac{\pm\sqrt{a_1^2 - 4a_0a_2}}{2a_0} - \frac{a_1}{2a_0} \\ &= \frac{-a_1 \pm \sqrt{a_2^2 - 4a_0a_2}}{2a_0}. \end{aligned}$$

Nello stesso modo si ottiene la riduzione di un polinomio di terzo grado alla forma di Cardano $x^3 + px + q$.

2. *Multipli di radici*

Se $g(x)$ deve avere come radici $k\alpha_i$, per un certo k, allora:

$$g(x) = R_y(f(y), x - ky)$$

e

$$g(x) = a_0 x^n + a_1 k x^{n-1} + a_{n-2} k^2 x^{n-2} + \cdots + a_n x^n.$$

(Così $g(k\alpha) = k^n f(\alpha) = 0$). In particolare, per $k = -1$ si ha:

$$g(x) = \sum_{i=0}^{n} a_{n-i} (-1)^i x^{n-i},$$

cosa che si ottiene cambiando alternativamente di segno ai coefficienti di $f(x)$.

3. *Radici reciproche*

Se α_i sono le radici di $f(x)$, $g(x)$ deve avere come radici $1/\alpha_i$. Allora $p(x)/q(x) = 1/x$ e

$$g(x) = R_y(f(y), xy - 1).$$

La matrice di Sylvester è:

$$\begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} & a_n \\ x & -1 & 0 & \dots & 0 & 0 \\ 0 & x & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & x & -1 \end{pmatrix},$$

il cui determinante, a meno del fattore $(-1)^n$, è $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$, che è il polinomio g cercato. I suoi coefficienti sono gli stessi di quelli di f ma nell'ordine inverso, e $g(x) = x^n f(1/x)$.

4. *Trasformazioni lineari fratte*

La funzione razionale abbia la forma:

$$\frac{p(x)}{q(x)} = \frac{ax + b}{cx + d}.$$

I tre casi $x+k$, kx e $1/x$ sono casi particolari di questo. Tuttavia, una trasformazione lineare fratta si può sempre ridurre ad una successione di trasformazioni dei tre tipi particolari detti. Infatti, se $c \neq 0$,

$$x \to x + \frac{d}{c} = u \to \frac{1}{u} = v \to \frac{bc - ad}{c^2} v = w \to w + \frac{a}{c} = \frac{ax + b}{cx + d}.$$

Ciò significa calcolare quattro risultanti:

$$\begin{aligned} g_1(x) &= R_y(f(y), x - y - \frac{d}{c}), \\ g_2(x) &= R_y(g_1(y), xy - 1), \\ g_3(x) &= R_y(g_2(y), x - \frac{bc - ad}{c^2}y), \\ g(x) &= R_y(g_3(y), x - y - \frac{a}{c}), \end{aligned}$$

e l'ultimo, $g(x)$, è il polinomio le cui radici sono $(a\alpha + b)/(c\alpha + d)$. Se invece $c = 0$, allora la successione di trasformazioni si riduce a due sole:

$$x \to \frac{a}{d}x = u \to u + \frac{b}{d} = \frac{ax + b}{d},$$

e così pure quella dei risultanti:

$$\begin{aligned} g_1(x) &= R_y(f(y), x - \frac{a}{d}y), \\ g(x) &= R_y(g_1(y), x - y - \frac{b}{d}). \end{aligned}$$

5. *Invarianza per trasformazioni*

In quale caso g, ottenuto da f con una trasformazione razionale, ha le stesse radici di f? Perchè ciò accada è ovviamente necessario e sufficiente che g sia un multiplo scalare di f. Consideriamo due casi:

1. Sia $k = -1$ in **2.**; vogliamo cioè che g abbia le radici $-\alpha_i$ (radici *opposte*). Allora g è equivalente a f se e solo se $a_1 = a_3 = \ldots = 0$. Se n è pari, $n = 2m$, abbiamo $g(x) = a_0x^{2m} + a_2x^{2m-2} + \cdots + a_{2m}$; se n è dispari, $n = 2m+1$, allora $g(x) = a_0x^{2m+1} + a_2x^{2m-2} + \cdots + a_{2m}x$. Questa si riduce alla prima se si tiene conto della radice $\alpha = 0$ (che è uguale alla sua opposta $-\alpha$), e posto $y = x^2$ abbiamo un polinomio il cui grado è la metà del grado di f.

2. Consideriamo la trasformazione reciproca vista in 3.; i coefficienti di g sono quelli di f ma nell'ordine inverso. Si deve quindi avere $\rho a_i = a_{n-i}$, $i = 1, 2, \ldots, n$, per un certo ρ, e da $\rho a_0 = a_n$ e $\rho a_n = a_0$ segue $\rho^2 = 1$ e $\rho = \pm 1$. Allora, per ogni i, o $a_i = a_{n-i}$ oppure $a_i = -a_{n-i}$.

6. *Eliminazione di una indeterminata*

Siano f e g due polinomi in x e y:

$$\begin{aligned} f(x, y) &= a_0(y)x^n + a_1(y)x^{n-1} + \cdots + a_n(y), \\ g(x, y) &= b_0(y)x^m + b_1(y)x^{m-1} + \cdots + b_m(y), \end{aligned}$$

scritti come polinomi in x a coefficienti polinomi in y. Cerchiamo una radice comune di f e g. Consideriamo il risultante $R_x(f, g)$; questo è un polinomio

in y, diciamo $r(y)$. Se $x = \alpha$ e $y = \beta$ è una radice comune di f e g, i due polinomi in x, $f(x,\beta)$ e $g(x,\beta)$ hanno la radice comune α, e dunque il loro risultante, che è $r(\beta)$, deve annullarsi. Ne segue che β è una radice di $r(y)$. Viceversa, se $r(\beta) = 0$ per qualche β, allora il risultante $r(y)$ ha la radice β, e dunque i due polinomi $f(x,\beta)$ e $g(x,\beta)$ hanno una radice in comune (oppure i loro coefficienti principali sono zero: $a_0(\beta) = b_0(\beta) = 0$). Il problema di trovare una radice comune a due polinomi in due indeterminate f e g è ridotto a quello di trovare una radice del polinomio $r(y)$ nella singola indeterminata y: *l'indeterminata x è stata eliminata.*

Nota. Osserva G. Ascoli[1] che nel linguaggio corrente, l'espressione "eliminare una variabile x" tra due equazioni $f = 0$ e $g = 0$ viene spesso usata nel senso vago di "dedurre dalle due equazioni una terza che non contenga la x". Il senso preciso dell'espressione è invece "trovare la condizione necessaria e sufficiente alla quale debbono soddisfare le altre variabili affinchè i polinomi f e g, considerati come polinomi in x abbiano una radice comune". E questa condizione è, per quanto visto sopra, l'annullarsi del risultante $R_x(f,g)$.

Esempi. 1. Trovare le radici comuni dei polinomi[2]:

$$\begin{aligned} f(x,y) &= x^2y + 3xy + 2y + 3, \\ g(x,y) &= 2xy - 2x + 2y + 3. \end{aligned}$$

Eliminiamo x. Scriviamo le due equazioni secondo le potenze decrescenti di x:

$$\begin{aligned} f(x,y) &= y \cdot x^2 + 3y \cdot x + (2y+3), \\ g(x,y) &= (2y-2) \cdot x + (2y+3). \end{aligned}$$

Allora:

$$R_x(f,g) = \begin{vmatrix} y & 3y & 2y+3 \\ 2y-2 & 2y+3 & 0 \\ 0 & 2y-2 & 2y+3 \end{vmatrix} = 2y^2 + 11y + 12.$$

Le radici del risultante sono $\beta_1 = -4$ e $\beta_2 = -\frac{3}{2}$, e per questi valori i coefficienti principali di f e g non si annullano. Dunque, ciascuno di questi valori, assieme ad un valore corrispondente di x, dà una radice comune di f e g. Si ha:

$$\begin{aligned} f(x,-4) &= -4x^2 - 12x - 5, \\ g(x,-4) &= -10x - 5, \end{aligned}$$

[1] [A], p. 276, nota.

[2] Questo esempio e il seguente sono tratti da [Ku], p. 319.

che hanno la radice comune $\alpha_1 = -\frac{1}{2}$. Per l'altro valore,

$$\begin{aligned} f(x, -\frac{3}{2}) &= -\frac{3}{2}x^2 - \frac{9}{2}x, \\ g(x, -\frac{3}{2}) &= -5x, \end{aligned}$$

e $\alpha_2 = 0$ è una radice comune. Concludendo, $(-\frac{1}{2}, -4)$ e $(0, -\frac{3}{2})$ sono le soluzioni del nostro problema.

L'esempio che segue mostra che le cose non sono sempre così semplici.

2. Sia:

$$\begin{aligned} f(x, y) &= 2x^3y - xy^2 + x + 5, \\ g(x, y) &= x^2y^2 + 2xy^2 - 5y + 1, \end{aligned}$$

che scriviamo come polinomi in y, la variabile che vogliamo eliminare (perchè f e g sono di grado 2 in y, e f è di grado 3 in x):

$$\begin{aligned} f(x, y) &= (-x) \cdot y^2 + (2x^3) \cdot y + (x + 5), \\ g(x, y) &= (x^2 + 2x) \cdot y^2 - 5y + 1. \end{aligned}$$

Il risultante è:

$$R_y(f, g) = 4x^8 + 8x^7 + 11x^6 + 84x^5 + 161x^4 + 154x^3 + 96x^2 - 125x,$$

che ha la radice $x = 0$. Per questo valore, i coefficienti principali di f e g si annullano. Inoltre, $f(0, y)$ e $g(0, y)$ non hanno radici in comune. Le altre radici del risultante non sono facili da calcolare. In ogni caso, per nessuna di loro i coefficienti principali di f e g si annullano contemporaneamente, e pertanto ciascuna radice non nulla del risultante, assieme al corrispondente valore di x, dà una radice comune di f e g.

7. *Il discriminante*

Consideriamo ora le radici multiple di un polinomio f. Sappiamo che α è radice multipla di f se e solo se α è anche radice di $f'(x)$, la derivata di f. Allora, $R(f, f') = 0$ *è condizione necessaria e sufficiente affinchè* f *abbia una radice multipla.* Per il Lemma 3.3,

$$R(f, f') = a_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i),$$

e derivando l'uguaglianza $f(x) = a_0 \prod_{k=1}^{n}(x - \alpha_k)$ abbiamo:

$$f'(x) = a_0 \sum_{k=1}^{n} \prod_{j \neq k} (x - \alpha_j).$$

Per $x = \alpha_i$, tutti i termini della somma si annullano, eccetto l'$i-$esimo; dunque:

$$f'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j),$$

e

$$R(f, f') = a_0^{n-1} a_0^n \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j).$$

Ad ogni coppia di indici (i, j), $i > j$ corrispondono due fattori $\alpha_i - \alpha_j$ e $\alpha_j - \alpha_i$, il cui prodotto è $-(\alpha_i - \alpha_j)^2$. Poichè vi sono $n(n-1)/2$ coppie di questo tipo, abbiamo:

$$\begin{aligned} R(f, f') &= (-1)^{\frac{n(n-1)}{2}} a_0^{2n-1} \prod_{i<j} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} a_0 D, \end{aligned}$$

dove

$$D = a_0^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

è il *discriminante* di f. Dunque, a meno del segno, il discriminante di f è il risultante $R(f, f')$ diviso per il coefficiente direttore di f. **Esempio.** Consideriamo un polinomio di secondo grado, $f = ax^2 + bx + c$. Poichè $f' = 2ax + b$, abbiamo:

$$R(f, f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = a(-b^2 + 4ac).$$

Qui $n(n-1)/2 = 1$ e dunque $D = -a^{-1} R(f, f') = b^2 - 4ac$, come è ben noto dall'algebra elementare. In modo analogo si dimostra che il discriminante dell'equazione ridotta di terzo grado $x^3 + px + q$ è $D = -4p^3 - 27q^2$.

Esercizi

10. Dimostrare la seguente proprietà del discriminante:

$$D(fg) = D(f) D(g) [R(f, g)]^2.$$

11. Determinare il discriminante dei polinomi $x^{n-1} + x^{n-2} + \cdots + x + 1$ e $x^n + a$.

8. *Polinomi di Hurwitz*

Siano α_i, $i = 1, \ldots, n$ le radici del polinomio $f(x)$, e sia y una indeterminata. I polinomi $f(y - x)$ e $f(y + x)$ nella variabile x hanno le radici $y - \alpha_i$ e $-y + \alpha_i$,

rispettivamente. Se questi due polinomi hanno una radice in comune, allora $y - \alpha_i = -y + \alpha_j$, per certi i e j, da cui:

$$y = \frac{\alpha_j + \alpha_i}{2}.$$

Viceversa, se y ha questa forma, allora $y - \alpha_i = -y + \alpha_j$ è una radice comune di $f(y - x)$ e $f(y + x)$. Ne segue che il polinomio in y:

$$r(y) = R_x(f(y - x), f(y + x)) \tag{3.6}$$

di grado n^2, dove n è il grado di f, ha come radici le semisomme delle radici di $f(x)$. L'equazione $r(y) = 0$ prende il nome di *equazione alle semisomme.*

Un polinomio f a coefficienti reali è un *polinomio di Hurwitz* se le sue radici reali sono negative e quelle complesse hanno la parte reale negativa. I fattori irriducibili di un polinomio a coefficienti reali o sono lineari, della forma $x - \alpha$, nel caso di una radice reale α, o quadratici, della forma $x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$, nel caso di α complessa. Se α è reale negativa, $x - \alpha$ è a coefficienti positivi; se α ècomplessa a parte reale negativa, la somma $\alpha + \overline{\alpha}$ è negativa. e dunque il coefficiente $-(\alpha + \overline{\alpha})$ è positivo, come pure $\alpha\overline{\alpha}$, che è una somma di quadrati. I coefficienti dei fattori irriducibili di $f(x)$ sono dunque tutti positivi, e dunque f, come prodotto di fattori con coefficienti positivi, è un polinomio i cui coefficienti hanno tutti lo stesso segno, e cioè il segno del coefficiente principale. Abbiamo il seguente teorema.

Teorema 3.6. *Sia f un polinomio a coefficienti reali aventi tutti lo stesso segno. Allora f è un polinomio di Hurwitz se e solo se i coefficienti di $r(y)$ hanno tutti lo stesso segno.*

Dim. Se f è di Hurwitz, una radice ha la parte reale negativa, e lo stesso accade per la semisomma di due radici. Allora per quanto visto sopra anche $r(y)$ è di Hurwitz, e i suoi coefficienti hanno tutti lo stesso segno. Viceversa, se $r(y)$ ha i coefficienti tutti dello stesso segno le radici reali sono necessariamente negative. Ma queste radici reali sono semisomme di coppie di radici coniugate di $f(x)$, cioè sono le parti reali delle radici complesse di $f(x)$. Dunque le radici complesse di $f(x)$ hanno parte reale negativa. ♢

Nota. Un polinomio di Hurwitz si dice anche *stabile.* Questa terminologia proviene dalla teoria delle equazioni differenziali. Affinché un sistema fisico sia asintoticamente stabile nell'intorno di un punto di equilibrio deve aversi $\lim_{t\to\infty} e^{\lambda t} = 0$, dove λ è una qualunque radice del polinomio di grado n associato all'equazione differenziale di ordine n a coefficienti costanti che descrive il fenomeno fisico. Se $\lambda = \alpha + i\beta$, allora $e^{\lambda t} = e^{\alpha t}e^{i\beta t} = e^{\alpha t}(\cos(\beta t) + i\sin(\beta t))$. Il termine dominante è dunque $e^{\alpha t}$, e la condizione che il limite sia 0 è equivalente alla condizione $\alpha < 0$.

9. *Quadrati di radici*

Un polinomio $g(x)$ le cui radici sono i quadrati delle radici di $f(x)$ è

$$g(x) = R_y(f(y), x - y^2).$$

Vediamo due applicazioni.

9*a. Maggiorazione per il numero di radici reali*

Per la regola dei segni di Cartesio il numero di radici reali positive di un polinomio $f(x)$ a coefficienti reali è minore o uguale al numero N di cambiamenti di segno in $f(x)$ (è uguale a N meno un numero pari). Ora, il quadrato di un numero reale è positivo; dunque, il numero di radici reali di $f(x)$ non può superare il numero delle radici positive di $g(x)$.

Esempio. Sia $f(x) = x^5 + x^3 + x^2 + 2x + 3$. Qui $g(x) = x^5 + 2x^4 + 5x^3 + 3x^2 - 2x - 9$, e dunque $N = 1$. Se ne conclude che $f(x)$ ha quattro radici complesse.

9*b. Il metodo di Graeffe*

Questo metodo si usa per calcolare radici approssimate di polinomi. L'osservazione fondamentale è la seguente. Siano $\alpha_1, \alpha_2, \ldots, \alpha_n$ le radici di $f(x)$, e supponiamo che sia noto il valore di

$$s_k = \alpha_1^k + \alpha_2^k + \cdots + \alpha_n^k$$

per un certo k. Scriviamo s_k nella forma:

$$s_k = \alpha_1^k (1 + \frac{\alpha_2^k}{\alpha_1^k} + \cdots + \frac{\alpha_n^k}{\alpha_1^k}).$$

Sia α_1 la radice che in modulo è più grande di tutte le altre. Allora, per un k sufficientemente grande, le quantità α_i^k/α_1^k sono trascurabili e dunque $s_k \approx \alpha_1^k$, cioè:

$$\lim_{n\to\infty} s_k^{1/k} = \alpha_1.$$

Consideriamo ora la trasformazione 9; applicandola più volte otteniamo un polinomio di grado $n = \partial f$ le cui radici sono $\alpha_1^{2^m}, \alpha_2^{2^m}, \ldots, \alpha_n^{2^m}$:

$$g(x) = R_y(f(x), x - y^{2^m}).$$

Sia:

$$g(x) = a_0^{(m)} x^n + a_1^{(m)} x^{n-1} + \cdots + a_n^{(m)};$$

ora,

$$-\frac{a_1^{(m)}}{a_0^{(m)}} = \sum_{i=1}^{n} {\alpha_i}^{2^m}.$$

Se le radici sono tutte distinte e $|\alpha_1| > |\alpha_i|$, $i = 1, 2, \ldots, n$ si ha, per m sufficientemente grande,

$$-\frac{a_1^{(m)}}{a_0^{(m)}} \approx \alpha_1^{2^m}.$$

Analogamente:

$$\frac{a_2^{(m)}}{a_0^{(m)}} = \sum_{i,j} (\alpha_i \alpha_j)^{2^m},$$

e se $|\alpha_2| > |\alpha_i|$, $i = 3, 4, \ldots, n$,

$$\frac{a_2^{(m)}}{a_0^{(m)}} \approx (\alpha_1 \alpha_2)^{2^m}.$$

La divisione per ${\alpha_1}^{2^m} \approx -{a_1}^{(m)}/{a_0}^{(m)}$ dà:

$$\frac{a_2^{(m)}}{a_1^{(m)}} \approx -\alpha_2^{2^m},$$

e così via. Se f ha solo radici reali semplici, le formule viste valgono per m sufficientemente grande. Il segno delle radici non è determinato, ma si può ottenere per sostituzione o con altri metodi. Tuttavia, se f ha coefficienti reali e radici complesse allora queste radici sono a due a due coniugate e dunque hanno a due a due lo stesso valore assoluto. Per esempio, tutte le radici di $f = x^n - 1$ hanno modulo 1, e in questo caso il metodo non funziona.

Esempio.[3] Sia $f = x^3 - 6x^2 + 11x - 6$ (le radici sono 3, 2 e 1). Si ha:

$$R(f(y), x - y^2) = x^3 - 14x^2 + 49x - 36.$$

Qui $m = 1$ e $\sqrt{14} = 3.741657\ldots$, $\sqrt{49/14} = 1.870828\ldots$ e $\sqrt{36/49} = 0,857142\ldots$, che approssimano 3, 2 e 1, rispettivamente. Una migliore approssimazione si ottiene al passo successivo, per $m = 2$:

$$R(f(y), x - y^4) = x^3 - 98x^2 + 1393x - 1296.$$

(Si osservi come il rapporto tra i due ultimi coefficienti sia già prossimo a 1). Ora, $98^{1/4} = 3,146346\ldots$, $(1393/98)^{1/4} = 1,941696\ldots$ e $(1296/1393)^{1/4} = 0,982117\ldots$. Già per $m = 4$ si ha, fermandosi a sei decimali: 3,000285; 1,999811; 0,999999. Come si vede da questo esempio, il metodo converge rapidamente (la convergenza è quadratica). Tuttavia, i coefficienti dei risultanti corrispondenti diventano subito estremamente grandi (nel nostro esempio, per

[3] I calcoli sono stati eseguiti con il sistema Maxima.

$m = 3$ vi sono coefficienti che hanno 13 cifre), per cui in pratica l'uso dei risultanti non è molto utile per problemi come questo.

10. *Ampliamenti algebrici*

Sia $f(x)$ il polinomio minimo di un elemento θ su un campo K. Gli elementi $1, \theta, \theta^2, \ldots, \theta^{n-1}$ formano una base dello spazio vettoriale $K(\theta)$ dei polinomi in θ di grado $< \partial f$ su K. Sia $\alpha \in K(\theta)$; allora α è un polinomio in θ di grado al più $n-1$, $\alpha = p(\theta) = c_0 + c_1\theta + \ldots + c_{n-1}\theta^{n-1}$. Come tutti gli elementi di $K(\theta)$, α è algebrico su K: gli elementi $1, \alpha, \alpha^2, \ldots, \alpha^n$ sono in numero di $n+1$, e dunque sono dipendenti su K; una loro combinazione lineare è allora uguale a 0, e i coefficienti di questa combinazione sono i coefficienti di un polinomio che si annulla su α. Vediamo allora come trovare un polinomio che si annulla su α. Consideriamo la moltiplicazione della base $\{\theta^i\}$ per α; questa moltiplicazione è una trasformazione lineare dello spazio vettoriale $K(\theta)$. Si ha:

$$\begin{aligned} 1 \cdot \alpha &= c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}, \\ \theta \cdot \alpha &= c_{0,1} + c_{1,1}\theta + \cdots + c_{n-1,1}\theta^{n-1}, \\ &\vdots \\ \theta^{n-1}\alpha &= c_{0,n-1} + c_{1,n-1}\theta + \cdots + c_{n-1,n-1}\theta^{n-1}, \end{aligned}$$

dopo riduzione mod $f(x)$. Il seguente sistema di equazioni lineari omogenee:

$$\left\{ \begin{array}{lcl} (c_0 - \alpha)x_0 + c_1x_1 + \cdots + c_{n-1}x_{n-1} & = & 0, \\ c_{0,1}x_0 + (c_{1,1} - \alpha)x_1 + \cdots + c_{n-1,1}x_{n-1} & = & 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \\ c_{0,n-1}x_0 + c_{1,n-1}x_1 + \cdots + (c_{n-1,n-1} - \alpha)x_{n-1} & = & 0, \end{array} \right.$$

ammette allora la soluzione non nulla $1, \theta, \ldots, \theta^{n-1}$. Quindi il suo determinante è zero. Questo determinante è un polinomio g in α, di grado n a coefficienti in K; scrivendolo come un polinomio in x si ha $g(\alpha) = 0$, ed è dunque il polinomio che cerchiamo. E' il polinomio caratteristico della trasformazione lineare indotta da α nel modo che abbiamo visto. (Si vede facilmente che cambiando la base in $K(\theta)$ il polinomio $g(x)$ non cambia; si può quindi parlare di polinomio caratteristico dell'elemento α).

Vediamo ora come ottenere $g(x)$ sotto forma di risultante. Poniamo $\alpha = \alpha_1$, $\theta = \theta_1$, $\alpha_2 = p(\theta_2), \ldots, \alpha_n = p(\theta_n)$, dove i θ_i, $i > 1$ sono le altre radici di $f(x)$ nel suo campo di spezzamento[4]. Le α_i sono radici dello stesso polinomio $g(x)$, come si può vedere sostituendo nel sistema di sopra α con α_i e θ con il θ_i corrispondente. Il polinomio $\prod_{i=1}^{n}(x - p(\theta_i))$ ha le radici α_i, e dunque, a meno di una costante, è uguale a g. Dunque, a meno di una costante,

$$g(x) = R_y(f(y), x - p(y)).$$

[4]L'esistenza di questo campo verrà dimostrata nel Teorema 4.14.

Esempio. Sia $K = Q$, il campo razionale, e sia $\theta = \sqrt{2} + \sqrt{3}$. Il polinomio $f(x) = x^4 - 10x^2 + 1$ ammette θ come radice (come subito si vede da $\theta^2 = 5 + 2\sqrt{6}$ e $(\theta^2 - 5)^2 = \theta^4 - 10\theta^2 + 25 = (2\sqrt{6})^2 = 24$). Questo polinomio è irriducibile su Q, per cui si tratta del polinomio minimo di θ. In termini di θ, $\sqrt{2} = (\theta^3 - 9\theta)/2$ (e $\sqrt{3} = (11\theta - \theta^3)/2$). Con $f(y) = y^4 - 10y^2 + 1$ e $p(y) = \frac{1}{2}y^3 - \frac{9}{2}y$, si ha, calcolando:

$$g(x) = R_y(f(y), x - p(y)) = 16(x^4 - 4x^2 + 4) = (4(x^2 - 2))^2.$$

Si ha effettivamente $g(\alpha) = g(\sqrt{2}) = 0$. Il fatto che $g(x)$ sia riducibile corrisponde al fatto che $\alpha = \sqrt{2}$ non è un elemento primitivo dell'ampliamento, cioè $Q(\sqrt{2})$ non è tutto $Q(\theta)$ (in quanto, ad esempio, non è possibile esprimere $\sqrt{3}$ come un polinomio in $\sqrt{2}$ a coefficienti in Q).

Nota bibliografica

[**A**], p. 242 e seguenti.

Capitolo 4

Fattorizzazione di polinomi

4.1 Il metodo di Kronecker

In questo primo paragrafo consideriamo un classico metodo di fattorizzazione di un polinomio a coefficienti interi, dovuto a Kronecker. Diciamo subito che l'interesse del metodo non sta tanto nella sua applicabilità pratica (già per polinomi di grado superiore o uguale al quinto esso è molto poco efficiente), quanto nella sua esistenza: esso fornisce infatti un algoritmo che in un numero finito di passi permette di stabilire se un polinomio è riducibile o meno, e in caso affermativo fornisce la fattorizzazione in fattori irriducibili. In altri termini, esso permette di affermare che *il problema della fattorizzazione di un polinomio a coefficienti interi è decidibile*.

Cominciamo con il lemma di Gauss. Un polinomio a coefficienti interi si dice *primitivo* se il MCD dei suoi coefficienti è uguale a 1.

Lemma 4.1 (Gauss) *Il prodotto di due polinomi primitivi è primitivo.*

Dim. Siano g e h primitivi, e supponiamo che il loro prodotto f non lo sia. Esiste allora un primo p che divide tutti i coefficienti di f. Sia a_s il primo coefficiente di g e b_t quello di h non divisi da p. Ora, il coefficiente di x^{s+t} in gh è:

$$\begin{aligned} c_{s+t} = \sum_{i+j=s+t} a_i b_j &= (a_0 b_{s+t} + a_1 b_{t+s-1} + \cdots + a_{s-1} b_{t+1}) \\ &+ (a_{s+t} b_0 + a_{s+t-1} b_1 + \cdots + a_{s+1} b_{t-1}) + a_s b_t, \end{aligned}$$

e p divide le due quantità in parentesi per via della minimalità di s e t. Per ipotesi, p divide c_{s+t}; ne segue che p divide a_s o b_t, contro l'ipotesi. $\diamondsuit$

Questo lemma ci permette ora di dimostrare il seguente teorema, anch'esso dovuto a Gauss.

Teorema 4.2. *Se un polinomio a coefficienti interi si spezza nel prodotto di due polinomi a coefficienti razionali, allora esso si spezza anche nel prodotto di due polinomi a coefficienti interi.*

Dim. Sia $f = gh$ con g e h a coefficienti razionali. Riduciamo i coefficienti di g e h allo stesso denominatore e mettiamo in evidenza il MCD dei coefficienti dei numeratori:

$$f = af_1,\ g = \frac{b}{m}g_1,\ h = \frac{c}{n}h_1.$$

Ne segue:

$$amnf_1 = bcg_1h_1,$$

con g_1 e h_1 primitivi. Il MCD dei coefficienti è, a sinistra, amn, e a destra bc in quanto g_1h_1, per il lemma, è primitivo. Ne segue $a = \frac{bc}{mn}$, e dunque $\frac{bc}{mn}$ è un intero. Allora:

$$f = (ag_1)h_1,$$

dove ag_1 e h_1 sono a coefficienti interi. $\diamondsuit$

Nota. La versione originale di Gauss del lemma suona così:

Siano g e h polinomi monici a coefficienti razionali. Se questi coefficienti non sono tutti interi, allora i coefficienti di $f = gh$ non possono essere tutti interi.

La versione moderna da noi data implica questa, come si vede facilmente (il viceversa è anche vero, ma non immediato). Ma quella di Gauss ha il vantaggio di prestarsi ad una generalizzazione molto profonda:

Siano g e h polinomi monici a coefficienti numeri algebrici. Se questi coefficienti non sono tutti interi algebrici, allora i coefficienti di $f = gh$ non possono essere tutti interi algebrici.

La versione moderna non ammette una tale generalizzazione perchè non c'è una nozione di MCD per numeri algebrici; esiste però una sua formulazione, dovuta a Dedekind, che si generalizza a numeri algebrici:

Siano g e h polinomi a coefficienti razionali. Se tutti i coefficienti di $f = gh$ sono interi, allora il prodotto di ogni coefficiente di g e ogni coefficiente di h è un intero.

La generalizzazione a numeri algebrici è il "teorema di Praga" dello stesso Dedekind:

Siano g e h polinomi a coefficienti numeri algebrici. Se tutti i coefficienti di $f = gh$ sono interi algebrici, allora il prodotto di ogni coefficiente di g e ogni coefficiente di h è un intero algebrico.

Se cerchiamo una fattorizzazione di un polinomio f a coefficienti interi, è sufficiente, per il teorema, cercarne una $f = gh$ con g e h a coefficienti interi. Il *metodo di Kronecker* che ora illustriamo permette di determinare, se esiste, una tale fattorizzazione, oppure di dimostrare che il polinomio è irriducibile. Esso consiste in quanto segue. In una eventuale fattorizzazione $f = gh$, con $\partial f = n$, il grado di uno dei due fattori, diciamo g è al più $[\frac{n}{2}] = m$, e dunque g è determinato quando se ne conoscano i valori su $m + 1$ punti distinti. Siano $x_0, x_1, \ldots, x_m$ numeri *interi*; avendosi:

$$f(x_i) = g(x_i)h(x_i),$$

i valori possibili per $g(x_i)$ devono trovarsi tra i divisori del numero intero $f(x_i)$. Si procede allora in questo modo:

1. Si calcolano gli $f(x_i)$, $i = 0, 1, \ldots, m$.

2. Per ogni i si trovano i divisori di $f(x_i)$.

3. Per ogni $(m+1)-$pla $d_0, d_1, \ldots, d_m$ di divisori d_i di $f(x_i)$ si pone $g(x_i) = d_i$.

4. Ciascuna di queste scelte dà i valori di g negli $m+1$ punti x_i.

5. Il metodo di Lagrange permette ora di determinare univocamente un polinomio $g = g(x) = d_0 L_0(x) + d_1 L_1(x) + \cdots + d_m L_m(x)$.

6. Se questo polinomio non è a coefficienti interi, o lo è ma non divide f, lo si scarta e si passa ad un'altra $(m+1)-$pla di divisori.

7. Poichè $f(x_i)$ è un intero, esso ha solo un numero finito di divisori; vi sono perciò solo un numero finito di $(m+1)-$ple e dunque di polinomi g.

8. Se nessun g così trovato divide f, il polinomio f è irriducibile su Z, e dunque, per il Lemma di Gauss, anche su Q.

Come si vede, questo metodo riconduce la ricerca dei divisori di un polinomio a quella dei divisori di numeri interi.

Esempio. Sia $f(x) = x^5 + x - 1$. Poichè uno degli eventuali fattori $g(x)$ ha grado al più 2, prendiamo tre punti: $x_0 = 0$, $x_1 = 1$ e $x_2 = -1$. Si ha:

$$\begin{array}{rcrcl} f(0) & = & -1, & g(0) & = & d_0 = 1, -1, \\ f(1) & = & 1, & g(1) & = & d_1 = 1, -1, \\ f(-1) & = & -3, & g(-1) & = & d_2 = 1, -1, 3, -3, \end{array}$$

e i polinomi di Lagrange per i punti 0, 1 e -1 sono:

$$L_0(x) = -x^2 + 1,\ L_1(x) = \frac{x^2 + x}{2},\ L_2(x) = \frac{x^2 - x}{2}.$$

Il valore $d_0 = -1$ si può scartare (basta cambiare g in $-g$). La terna $d_0 = 1$, $d_1 = 1$ $d_2 = 1$ fornisce $g = 1$. Restano allora 7 terne. A questo punto, prima di procedere con altre terne di divisori, si può prendere un $\overline{x}$ diverso da tutti gli x_i, e vedere per quali terne d_0, d_1, d_2 il numero:

$$s = d_0 L_0(\overline{x}) + d_1 L_1(\overline{x}) + d_2 L_2(\overline{x})$$

(che dà il valore di $g(\overline{x})$) è un intero e divide $f(\overline{x})$. Se questo non è il caso, la terna si scarta. Nel nostro caso sia $\overline{x} = 2$; la precedente diventa:

$$s = -3d_0 + 3d_1 + d_2.$$

Allora sono da prendere in considerazione solo quelle terne per le quali s è un intero che divide $f(2) = 33$. Ad esempio, la terna $1, -1, 1$ fornisce $s = -5$, e

dunque si scarta. La terna 1,1,3 dà $s = 3$. Con questi valori dei d_i si trova $g = x^2 - x + 1$, che divide effettivamente f:

$$x^5 + x - 1 = (x^2 - x + 1)(x^3 - x^2 + 1).$$

Per vedere se questi fattori sono irriducibili, si continua il procedimento. Ad esempio, con la terna $1, -1, 3$ si ha $s = -3$ e $g = -2x + 1$, che non divide f perchè f non ha la radice $\frac{1}{2}$. Con la $1, 1, -3$ si trova $g = -x^2 + x + 2$, che non è un fattore di f perchè il suo termine noto non divide quello di f. In modo analogo si scartano le terne restanti. Quella trovata è dunque la fattorizzazione di f in fattori irriducibili.

Oltre a considerare il *valore di controllo* $\overline{x}$ come fatto nell'esempio, vi sono altri accorgimenti per semplificare i calcoli:
1. calcolare $f(x_i)$ per più di $m + 1$ punti x_i in modo da scegliere poi quelli tra gli $f(x_i)$ che hanno il minor numero di divisori;
2. se q è un intero, il polinomio $g(x) - g(q)$ ha la radice q, e dunque è divisibile per $x - q$, e il quoziente è a coefficienti interi. In particolare, per $x = p$, $g(p) - g(q)$ è divisibile per $p - q$. Dunque, $g(x_i) - g(x_k)$ è divisibile per $x_i - x_k$, ovvero $x_i - x_k$ divide $d_i - d_k$. Si possono dunque eliminare i gruppi di divisori d_i per i quali questa condizione non è soddisfatta. (Questa osservazione è dovuta a Runge).

Come già detto, questo metodo è poco efficiente. Metodi moderni, più efficienti, consistono nel fattorizzare il polinomio modulo un numero primo p e poi "sollevare" questa fattorizzazione ad una sugli interi. E' quanto vedremo nei prossimi paragrafi. Vediamo intanto se è possibile scoprire se il polinomio è irriducible.

4.2 Criteri di irriducibilità

Per vedere se un dato polinomio è irriducibile si può utilizzare il "passaggio modulo p", che si basa sul fatto seguente. Se f è un polinomio primitivo, prendendo i coefficienti modulo p si ottiene un polinomio $\overline{f}$ su Z_p, e se p non divide il coefficiente direttore di f, allora f e $\overline{f}$ hanno lo stesso grado. Se f si riduce su Z, $f = gh$ con g e h primitivi, allora $\overline{f} = \overline{g}\overline{h}$. Dunque, se per un certo p si trova che $\overline{f}$ è irriducibile, allora f è irriducibile sugli interi. Abbiamo così una condizione necessaria per l'irriducibilità.

Esempio. Sia $f = x^2 + x + 1$. Se f si riduce modulo qualche primo p allora si riduce in due polinomi di primo grado, e dunque ha due radici nel campo Z_p. Ma per $p = 2$ f non ha radici, e quindi è irriducibile mod 2, e dunque anche su Z.

Si può poi provare con più numeri primi, e usare anche il fatto che Z_p è un campo, e dunque la fattorizzazione in fattori irriducibili è unica.

Esempio. Sia $f = x^4 + 3x^3 + 3x^2 - 5$. Modulo 2 questo polinomio è $x^4 + x^3 + x^2 + 1$, e ammette la radice 1. Dividendo per $x - 1$ si trova:

$$f = (x + 1)(x^3 + x + 1),$$

ed essendo i due fattori irriducibili, quella scritta è *la* fattorizzazione di f su Z_2. Se f si fattorizza su Z, ciò non può avvenire con un fattore irriducibile di grado 2. Un tale fattore infatti, o resta irriducibile su Z_2, ma ciò darebbe una diversa fattorizzazione su Z_2, oppure si decompone in due fattori lineari, che mod 2 darebbero ancora un'altra fattorizzazione. La sola possibilità allora è che su Z si abbia:

$$f = (ax + b)q(x),$$

per cui f ha un fattore lineare, e perciò una radice, modulo p per ogni p. Ma per $p = 3$ è $f = x^4 + 1$, e $f(0) = 1$, $f(1) = 2$ e $f(2) = 2$, e dunque non vi sono radici in Z_3. Ne segue che f è irriducibile su Z.

Una condizione sufficiente per l'irriducibilità di un polinomio, è data dal seguente teorema.

Teorema 4.3. (Criterio di Eisenstein). *Sia:*

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \tag{4.1}$$

un polinomio a coefficienti interi. Se esiste un numero primo p tale che $p \not| a_n$, $p|a_i$ per $i < n$, e $p^2 \not| a_0$, allora f è irriducibile su Z.

Dim. Sia $f = gh$ su Z. Prendendo i coefficienti mod p si ha:

$$\overline{g}\overline{h} \equiv \overline{a}_n x^n.$$

Poichè la fattorizzazione su Z_p è unica, i fattori irriducibili di $\overline{g}$ devono trovarsi tra quelli di $\overline{a}_n x^n$, e dunque sono polinomi con termine noto 0. Lo stesso per $\overline{h}$. Dunque, se b_0, c_0 e a_0 sono i termini noti di g, h e f, rispettivamente, si ha $p|b_0$, $p|c_0$ e dunque $p^2|b_0 c_0 = a_0$, contro l'ipotesi. $\diamondsuit$

Questo criterio può applicarsi direttamente, ad esempio nel caso del polinomio $f = x^4 + 3x^3 + 6x^2 - 15$, con $p = 3$, oppure dopo un'opportuna trasformazione del polinomio, come mostra il seguente esempio.

Esempio. Sia $f = x^4 + 1$. Così com'è, il polinomio non si presenta nella forma richiesta per l'applicabilità del criterio. Ma osservando che se $f(x)$ è riducibile anche $f(x + 1)$ lo è, sostituiamo x con $x + 1$, ottenendo:

$$f(x + 1) = (x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2.$$

Ora il criterio è applicabile con $p = 2$, e si conclude che f è irriducibile su Z.

Lemma 4.4. *Se p è un numero primo, il coefficiente binomiale $\binom{p}{k}$ è divisibile per p se $0 < k < p$.*

Dim. Si ha:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!},$$

e se $k \neq p$, il denominatore non è divisibile per p. $\diamondsuit$

Esempio. Sia, con p primo,

$$f = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Anche qui sostituiamo x con $x + 1$:

$$\frac{(x+1)^p - 1}{(x+1) - 1} = \frac{1}{x}(\sum_{k=0}^{p} \binom{p}{k} x^k - 1).$$

Ora, il coefficiente binomiale $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ per $0 < k < p$ è divisibile per p perchè p non divide il denominatore. Si ha allora:

$$f(x+1) = \frac{1}{x}(1 + px + \cdots + x^p - 1) = x^{p-1} + \cdots + p,$$

dove i termini indicati con i puntini sono tutti divisibili per p. Possiamo allora applicare il criterio e dedurre che il polinomio dato f è irriducibile su Z.

Nota. I polinomi dei due esempi precedenti sono esempi di polinomi *ciclotomici* (o della divisione del cerchio). Si tratta rispettivamente di $\varphi_8(x)$ e $\varphi_p(x)$. Torneremo su questo in seguito.

Il criterio di Eisenstein ammette la seguente generalizzazione (che diamo senza dimostrazione): *Sia f il polinomio* (4.1)*; se esistono un primo p e un intero i tale che $(i, n) = 1$ e $p^i \not| a_n$, $p^i | a_k$ per $k < n$, e $p^{i+1} \not| a_0$, allora f è irriducibile.*

Esempio. $f = x^5 + 4x^3 + 8x^2 + 8x + 4$. Con $p = 2$ il criterio di Eisenstein non è applicabile, ma quello generalizzato sì, con $i = 2$. Va notato che la condizione che i sia primo col grado, $(i, n) = 1$, è necessaria. Il polinomio precedente con x^4 invece di x^5 si riduce come $(x^2 + 2x + 2)^2$.

Possiamo ora concludere in questo modo. Prima di applicare il metodo di Kronecker, rischiando di scoprire che il polinomio è irriducibile, si cerca con i criteri visti o passando modulo uno o più primi di sapere in anticipo se il polinomio è irriducibile. Tuttavia, la ricerca di un primo per il quale il polinomio sia irriducibile può essere vana: esistono infatti polinomi che si spezzano modulo

ogni numero primo ma che sono irriducibili sugli interi (ne vedremo degli esempi nel prossimo paragrafo). Se questi o altri tentativi falliscono, si può passare all'applicazione del metodo di Kronecker. Questa era più o meno la situazione ancora negli anni '60 di questo secolo. Da allora, metodi molto più efficaci sono a nostra disposizione come ora vedremo. Prima però abbiamo bisogno di alcune proprietà dei campi finiti e dei polinomi a coefficienti in questi campi.

4.3 Campi finiti e polinomi

Sia Z_p il campo delle classi resto mod p, $Z_p = \{0, 1, \ldots, p-1\}$, elementi che scriveremo anche nella forma:

$$-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-3}{2}, \frac{p-1}{2}$$

(rappresentazione *bilanciata*). In ogni campo, una uguaglianza $a^2 = b^2$ è possibile solo se $a = \pm b$, come si vede dalla $0 = a^2 - b^2 = (a-b)(a+b)$ e dall'assenza di divisori dello zero. Denotiamo con Z_p^* l'insieme (il gruppo) degli elementi non nulli di Z_p. Per quanto appena visto, i quadrati degli elementi $0, 1, \ldots, \frac{p-1}{2}$ sono tutti distinti, e sono uguali a quelli ottenuti quadrando i restanti elementi. I seguenti corollari discendono da questo fatto.

Corollario 4.5. *Sia $p > 2$. Allora esattamente la metà degli elementi di Z_p^* sono quadrati.* $\diamondsuit$

Esempio. I quadrati di Z_{13}^* sono $1, 4, -4, 3, -1, -3$.

E' chiaro che il prodotto di due quadrati è ancora un quadrato. Se $Q = \{a_1, a_2, \ldots, a_r\}$ è l'insieme dei quadrati di Z_p^*, e b è un non-quadrato, allora l'insieme $Qb = \{a_1 b, a_2 b, \ldots, a_r b\}$ consta di elementi distinti ed è disgiunto da Q, in quanto se $a_i b = a_k$, allora $b = a_i^{-1} a_k$ sarebbe un quadrato. Dunque $Z_p^* = Q \cup Qb$. Se c e d sono non quadrati si ha allora $c = a_i b$ e $d = a_k b$, da cui $cd = a_i b a_k b = a_i a_k b^2$, prodotto di due quadrati, e dunque cd è un quadrato.

Corollario 4.6. *In Z_p^* il prodotto di due quadrati è un quadrato, e il prodotto di due non-quadrati è un quadrato.* $\diamondsuit$

Corollario 4.7. *Siano -1, a e $-a$ tre elementi di Z_p^*. Allora uno dei tre è un quadrato.*

Dim. Se -1 e a non sono quadrati, per il corollario precedente il loro prodotto $-1 \cdot a = -a$ è un quadrato. $\diamondsuit$

Il Corollario 4.7 è particolarmente utile quando si vuole dimostrare che esistono polinomi irriducibili sugli interi ma che si riducono modulo ogni numero primo.

Esempi. 1. Abbiamo visto con il criterio di Eisenstein che x^4+1 è irriducibile su Z. Dimostriamo ora che esso si riduce su Z_p per ogni primo p.

i) Se -1 è un quadrato, $-1=a^2$, si ha:

$$x^4+1=x^4-(-1)=x^4-a^2=(x^2-a)(x^2+a).$$

ii) Se 2 è un quadrato, $2=a^2$:

$$\begin{aligned} x^4+1 &= (x^2+1)^2-2x^2=(x^2+1)^2-(a^2x^2)=(x^2+1)^2-(ax)^2 \\ &= (x^2+1-ax)(x^2+1+ax). \end{aligned}$$

iii) Se -2 è un quadrato, $-2=a^2$:

$$\begin{aligned} x^4+1 &= (x^2-1)^2+2x^2=(x^2-1)^2-(-2x^2)=(x^2-1)^2-(ax)^2 \\ &= (x^2-1-ax)(x^2-1+ax). \end{aligned}$$

(Come si vede, la tecnica è quella del *completamento del quadrato*). Così, per $p=5$, -1 è un quadrato: $-1=4=2^2$; siamo allora nel caso *i*):

$$x^4+1=(x^2-2)(x^2+2).$$

Per $p=23$, $2=5^2$, e da *ii*) si ha:

$$(x^2-5x+1)(x^2+5x+1).$$

Per $p=11$, $-2=3^2$, e da *iii*) abbiamo:

$$x^4+1=(x^2-3x-1)(x^2+3x-1).$$

Nel caso *ii*), il discriminante dei due fattori è a^2-4, cioè -2. Dunque, se anche -2 è un quadrato, $-2=b^2$, i due fattori hanno le radici $(a\pm b)/2$ e $(-a\pm b)/2$ (qui la divisione per 2 significa moltiplicazione per l'inverso di 2, che esiste sempre se $p>2$). Ne segue:

$$x^4+1=(x-\frac{a+b}{2})(x-\frac{a-b}{2})(x-\frac{-a+b}{2})(x-\frac{-a-b}{2}),$$

e dunque il polinomio si spezza in fattori lineari. Ciò accade per esempio per $p=17$, dove $2=6^2$ e $-2=7^2$; inoltre, l'inverso di 2 è 9. Si ha:

$$\begin{aligned} x^4+1 &= (x-(6+7)\cdot 9)(x-(-1)\cdot 9)(x-1\cdot 9)(x-(-6-7)\cdot 9) \\ &= (x-117)(x+9)(x-9)(x+117) \\ &= (x-2)(x+9)(x-9)(x+2). \end{aligned}$$

2. Un altro polinomio irriducibile su Z che si spezza per ogni p è $x^4 - 2x^2 + 9$: *i*) se $-1 = a^2$,

$$\begin{aligned} x^4 - 2x^2 + 9 &= (x^2-3)^2 + 4x^2 = (x^2-3)^2 - (-4x^2) = (x^2-3)^2 - (2ax)^2 \\ &= (x^2 - 3 - 2ax)(x^2 - 3 + 2ax). \end{aligned}$$

Con $p = 5$ si ha $-1 = 4 = 2^2$, $a = 2$:

$$x^4 - 2x^2 + 9 = (x^2 - 3 - 4x)(x^2 - 3 + 4x).$$

ii) Se $2 = a^2$,

$$\begin{aligned} x^4 - 2x^2 + 9 &= (x^2+3)^2 - 8x^2 = (x^2+3)^2 - 2 \cdot 4x^2 \\ &= (x^2+3)^2 - (a \cdot 2 \cdot x)^2 = (x^2 + 3 - 2ax)(x^2 + 3 + 2ax). \end{aligned}$$

Con $p = 17$, $2 = 6^2$, $a = 6$ e dunque:

$$x^4 - 2x^2 + 9 = (x^2 + 3 - 12x)(x^2 + 3 + 12x).$$

iii) Se $-2 = a^2$,

$$\begin{aligned} x^4 - 2x^2 + 9 &= (x^2-1)^2 + 8 = (x^2-1)^2 - (-2 \cdot 4) = (x^2-1)^2 - (2a)^2 \\ &= (x^2 - 1 - 2a)(x^2 - 1 + 2a). \end{aligned}$$

Con $p = 11$, $-2 = 3^2$, $a = 3$ e

$$x^4 - 2x^2 + 9 = (x^2 - 7)(x^2 + 5).$$

Nel caso *i*) il discriminante dei due fattori è $a^2 + 3 = -1 + 3 = 2$. Dunque, se anche 2 è un quadrato, $2 = b^2$, il polinomio si spezza in fattori lineari:

$$x^4 - 2x^2 + 9 = (x + a - b)(x + a + b)(x - a - b)(x - a + b).$$

Ciò si verifica ad esempio per $p = 17$, dove $-1 = 4^2$ e $2 = 6^2$. Allora con $a = 4$ e $b = 6$ si ha:

$$x^4 - 2x^2 + 9 = (x - 2)(x + 10)(x - 10)(x + 2).$$

Un'analoga discussione si può fare negli altri casi.

Il polinomio visto in quest'ultimo esempio ha le radici complesse $\pm i \pm \sqrt{2}$. Più in generale (risultato che non dimostriamo) se $p_1, p_2, \ldots, p_{n-1}$ sono i primi $n-1$ numeri primi, il polinomio le cui radici sono:

$$\pm i \pm \sqrt{2} \pm \sqrt{3} \pm \cdots \pm \sqrt{p_{n-1}}$$

è un polinomio di grado 2^n irriducibile su Z ma che si spezza per ogni p. Tale è ad esempio:

$$x^8 - 16x^6 + 88x^4 + 192x^2 + 144,$$

che ha le radici $\pm i \pm \sqrt{2} \pm \sqrt{3}$.

3. Sia $x^4 + 1$ che $x^4 - 2x^2 + 9$ sono casi particolari di:

$$f(x) = x^4 + ax^2 + b^2.$$

Dimostriamo che, qualunque siano a e b, questo polinomio si fattorizza per ogni p. Se $p = 2$, allora $a, b = 0, 1$, e il polinomio si spezza in $(x^2 + ax + b)^2$. Se $p > 2$, allora esiste $s = \frac{a}{2}$ e $f(x) = x^4 + 2sx + b^2$ si può scrivere in tre modi:

$$\begin{aligned} (x^2 + s)^2 &- (s^2 - b^2), \\ (x^2 + b)^2 &- (2b - 2s)x^2, \\ (x^2 - b)^2 &- (-2b - 2s)x^2. \end{aligned}$$

Se né $2b - 2s$ né $-2b - 2s$ sono dei quadrati, il loro prodotto lo è, e vale $4(s^2 - b^2) = c^2$, da cui $s^2 - b^2 = \frac{c^2}{4} = (\frac{c}{2})^2$. In ogni caso quindi $f(x)$ è una differenza di due quadrati.

Lemma 4.8. *Siano a e b due interi. Allora:*

$$(a + b)^p \equiv a^p + b^p \bmod p \tag{4.2}$$

e, per ogni n,

$$(a + b)^{p^n} \equiv a^{p^n} + b^{p^n} \bmod p. \tag{4.3}$$

Più in generale:

$$(a_1 + a_2 + \cdots + a_k)^{p^n} \equiv a_1^{p^n} + a_2^{p^n} + \cdots + a_k^{p^n} \bmod p.$$

Dim.

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}. \tag{4.4}$$

Per $k \neq 0, p$ il coefficiente binomiale $\binom{p}{k}$ è divisibile per p, per il Lemma 4.4, e dunque è 0 mod p. Per $k = 0$ abbiamo b^p, e per $k = p$ abbiamo a^p. Se $n = 1$, la (4.3) non è che la (4.2). Se $n > 1$,

$$(a + b)^{p^n} \equiv ((a + b)^{p^{n-1}})^p \equiv (a^{p^{n-1}} + b^{p^{n-1}})^p \equiv a^{p^n} + b^{p^n} \bmod p,$$

dove la seconda equivalenza segue per induzione e la terza dalla (4.2). La (4.3) si ottiene per induzione. $\diamondsuit$

Nota. Questo lemma sussiste, con la stessa dimostrazione, per ogni anello commutativo di caratteristica p.

Teorema 4.9. (PICCOLO TEOREMA DI FERMAT). *Per ogni intero a e ogni primo p:*

$$a^p \equiv a \bmod p, \tag{4.5}$$

e più in generale:

$$a^{p^n} \equiv a \bmod p. \tag{4.6}$$

Dim. Se $a = 0$ non c'è niente da dimostrare. Distinguiamo i due casi $a > 0$ e $a < 0$.
i) $a > 0$. Per induzione su a. Dalla $a = (a-1)+1$ si ha, per il lemma precedente,

$$a^p = (a-1)^p + 1^p.$$

Per induzione, $(a-1)^p \equiv a - 1 \bmod p$, e dunque:

$$a^p \equiv a - 1 + 1 = a \bmod p.$$

Se $a < 0$, $-a > 0$ e dunque, per quanto appena visto, $(-a)^p \equiv -a \bmod p$. Se $p = 2$, $-a \equiv a \bmod 2$; se $p > 2$, p è dispari, e dunque $(-a)^p = -(a^p)$, da cui $-(a^p) = (-a)^p \equiv -a \bmod p$, dove l'ultima congruenza segue dal caso precedente. La (4.6) si ottiene per induzione dalla (4.5). $\diamondsuit$

Corollario 4.10. *Se $a \not\equiv 0 \bmod p$, allora:*

$$a^{p-1} \equiv 1 \bmod p.$$

Dim. Se $a \not\equiv 0 \bmod p$, a ammette un inverso mod p. Moltiplicando i due membri della (4.5) per questo inverso si ha il risultato. $\diamondsuit$

Corollario 4.11. *Si ha:*

$$x^p - x \equiv (x-0)(x-1)\cdots(x-(p-1)) \bmod p,$$

e più in generale, per ogni polinomio $f(x)$ a coefficienti interi:

$$f(x)^p - f(x) \equiv (f(x)-0)(f(x)-1)\cdots(f(x)-(p-1)) \bmod p.$$

Dim. Per il teorema di Fermat, ogni intero mod p è radice di $x^p - x$, e pertanto questo polinomio è divisibile per $x - i$, $i \in Z_p$. L'altra uguaglianza segue subito dalla prima. $\diamondsuit$

Teorema 4.12. *Siano K un campo e f un polinomio irriducibile a coefficienti in K. Allora i polinomi su K di grado $< \partial f$ formano un campo F rispetto alla somma usuale e al prodotto modulo f.*

Dim. F è chiuso rispetto alle due operazioni dette. Per l'esistenza dell'inverso di un polinomio $g \in F$ si osservi che $(f, g) = 1$, essendo f irriducibile e $\partial g < \partial f$, e dunque $af + bg = 1$, per certi polinomi a e b. Modulo f questa uguaglianza diventa $bg \equiv 1 \bmod f$, per cui g ha come inverso $b \bmod f$. F è dunque un campo. Si osservi che F contiene K come insieme dei polinomi di grado zero (costanti). $\diamondsuit$

Corollario 4.13. *Siano K e f come nel teorema precedente. Allora esiste un ampliamento F di K che contiene una radice di f.*

Dim. Sia F il campo ottenuto nel teorema precedente; poichè $f(x) \equiv 0 \bmod f(x)$, il polinomio $p(x) = x$ è una radice di f. $\diamondsuit$

Teorema 4.14. *Se $f(x)$ è un polinomio a coefficienti in K esiste un ampliamento di K nel quale $f(x)$ si spezza in fattori lineari.*

Dim. Se $\partial f = 1$, allora l'ampliamento richiesto è K stesso. Altrimenti, $f(x) = g(x)q(x)$ con $g(x)$ irriducibile. Per il teorema precedente esiste $F \supseteq K$ nel quale g ha una radice, e sia α, e nel quale dunque $g(x) = (x - \alpha)h(x)$. Allora in F si ha $f(x) = (x-\alpha)h(x)q(x)$, ed essendo il grado di $h(x)q(x)$ uguale a $\partial f - 1$, per induzione sul grado di f esiste un ampliamento di F nel quale $h(x)q(x)$, e dunque f, si spezza in fattori lineari. $\diamondsuit$

Il più piccolo campo K' contenente K e nel quale f si spezza in fattori lineari si chiama *campo di spezzamento* di f. E' il più piccolo nel senso che f non si spezza in fattori lineari in alcun sottocampo di K'.

Teorema 4.15. *L'insieme delle radici del polinomio $x^{p^n} - x$ su Z_p è un campo.*

Dim. Intanto 0 e 1, sono radici, come pure, per il Teorema 4.9, tutti gli altri elementi di Z_p. Se poi α e β sono radici in un ampliamento di Z_p, anche $\alpha + \beta$ e $\alpha\beta$ lo sono:

$$\begin{aligned}(\alpha+\beta)^{p^n} - (\alpha+\beta) &= \alpha^{p^n} + \beta^{p^n} - \alpha - \beta \\ &= (\alpha^{p^n} - \alpha) + (\beta^{p^n} - \beta) = 0 + 0 = 0\end{aligned}$$

(Lemma 4.8), e:

$$\begin{aligned}(\alpha\beta)^{p^n} - \alpha\beta &= \alpha^{p^n}\beta^{p^n} - \alpha\beta \\ &= \alpha\beta - \alpha\beta = 0.\end{aligned}$$

Per l'inverso si ha:

$$(\alpha^{-1})^{p^n} - \alpha^{-1} = (\alpha^{p^n})^{-1} - \alpha^{-1} = \alpha^{-1} - \alpha^{-1} = 0,$$

e per l'opposto:

$$(-\alpha)^{p^n} - (-\alpha) = (-1)^{p^n}\alpha^{p^n} + \alpha = (-1)^{p^n}\alpha + \alpha;$$

se p è dispari, l'ultima quantità è $-\alpha + \alpha = 0$ mentre se $p = 2$ si ha $\alpha + \alpha = 2\alpha = 0$. $\diamondsuit$

L'insieme delle radici costituisce dunque esso stesso il campo di spezzamento del polinomio $x^{p^n} - x$. (Nel Corollario 4.11 abbiamo visto che Z_p è il campo di spezzamento di $x^p - x$). Questo campo ha dunque al più p^n elementi; vedremo tra un momento (Corollario 4.20) che ne ha esattamente p^n.

Un campo finito ha un numero di elementi che è una potenza di un primo p. Infatti, esso contiene intanto Z_p, come insieme dei multipli dell'unità; inoltre, è uno spazio vettoriale su Z_p di dimensione finita, diciamo m. I suoi elementi sono allora tutte le combinazioni lineari degli elementi di una base, e sono dunque p^m.

Se $q = p^n$, denotiamo con F_q un campo con q elementi (vedremo che esso è unico, a meno di isomorfismi). Continueremo tuttavia a denotare con Z_p il campo con p elementi.

Sia F un campo finito. Esiste allora un elemento $a \in F^* = F \setminus \{0\}$ tale che ogni altro elemento di F^* è una potenza di a. (In altre parole, il gruppo moltiplicativo di un campo finito è ciclico). Un tale elemento si chiama *elemento primitivo* di F. Se F ha ordine q, il numero degli elementi primitivi di F è $\varphi(q-1)$, dove φ è la funzione di Eulero.

Esistenza di un elemento primitivo in un campo finito F. Sia $a \in F^*$; non tutte le sue potenze possono essere distinte per via della finitezza di F. Se $a^h = a^k$ con $h > k$ allora $a^{h-k} = 1$, e dunque c'è un m minimo per cui $a^m = 1$; m è l'*ordine* $o(a)$ di a. E' chiaro che se $a^k = 1$ per un certo k, allora $o(a)$ divide k.

Sia $o(a) = h$ e $o(b) = k$, con $(h,k) = 1$; allora $o(ab) = hk$. Intanto, per la commutatività, $(ab)^{hk} = 1$. Se $o(ab) < hk$ allora $o(ab)|hk$ e dunque $o(ab) = h'k'$, con $h'|h$ e $k'|k$, e perciò $(h',k') = 1$. Si ha $(ab)^{h'k} = 1$, e dunque $a^{h'k}b^{h'k} = 1$, da cui $a^{h'k} = 1$. Allora $o(a) = h|h'k$, ed essendo $(h,k) = 1$ deve aversi $h|h'$, e perciò $h' = h$. Ragionando analogamente con hk' si ha il risultato.

Sia allora a un elemento di ordine massimo M. Facciamo vedere che ogni altro $b \in F^*$ ha un ordine che divide M. Se questo non è il caso, esiste un primo r tale che $o(b) = r^h u$ e $M = r^k v$, dove $(r,u) = (r,v) = 1$ e $h > k$. Allora $o(a^{r^k}) = v$ e $o(b^u) = r^h$, ed essendo $(r,v) = 1$ l'elemento $a^{r^k}b^u$ ha per ordine il prodotto degli ordini vr^h, che è maggiore di M.

Le M potenze $1, a, a^2, \ldots, a^{M-1}$ di a sono tutte distinte, e sono tutte radici di $x^M - 1$ che dunque, avendo grado M, non può averne altre. Ma $b \in F^*$, è radice di questo polinomio in quanto $o(b)|M$ per quanto appena visto, e dunque $b^M = 1$, cioè $b^M - 1 = 0$. Ne segue che b è una delle potenze di a.

Se $a \in F^*$ ha ordine m, allora a^k ha anch'esso ordine m se e solo se $(k,m) = 1$. Se a^k ha ordine m, e $d = (k,m) > 1$, allora $(a^k)^{\frac{m}{d}} = (a^{\frac{k}{d}})^m = 1$, contro la minimalità di m. Viceversa, se $(k,m) = 1$ e $(a^k)^h = a^{kh} = 1$, allora $m|kh$, ed essendo $(k,m) = 1$ si ha $m|h$, e dunque essendo m l'ordine massimo possibile per una potenza di a, è $h = m$.

Ne segue che gli elementi di F^* di ordine massimo, sono in numero di $\varphi(q-1)$.

Polinomio minimo di un elemento. Se $F \supseteq K$, e α è un elemento di F algebrico su K, cioè radice di un polinomio a coefficienti in K, tra tutti i polinomi di cui α è radice sia $p(x)$ uno di grado minimo m. Intanto $p(x)$ è irriducibile, in quanto se $p(x) = h(x)q(x)$, con $\partial h < m$ e $\partial q < m$, allora $0 = p(\alpha) = h(\alpha)q(\alpha)$, e dunque $h(\alpha) = 0$ o $q(\alpha) = 0$;

in entrambi i casi α sarebbe radice di un polinomio di grado inferiore al grado di $p(x)$. Inoltre, $p(x)$ divide tutti i polinomi di cui α è radice. Se infatti $g(\alpha) = 0$, allora dalla $g(x) = p(x)q(x) + r(x)$, $\partial r < m$, si ha $0 = g(\alpha) = p(\alpha)q(\alpha) + r(\alpha)$ e $r(\alpha) = 0$, per cui, per la minimalità di m abbiamo $r(x) = 0$. Dividendo ora i coefficienti di $p(x)$ per il coefficiente direttore possiamo supporre $p(x)$ monico. Allora $p(x)$ è unico, in quanto se $p_1(x)$ è un altro polinomio di cui α è radice, di grado minimo m e monico, la differenza $p(x) - p_1(x)$ ammette ancora α come radice ed è di grado al più $m-1$. Possiamo allora parlare de *il* polinomio minimo di α.

I polinomi di un dato grado k su F_q sono numero di $(q-1)q^k$ ($q-1$ scelte per il coefficiente direttore, che non deve essere 0 altrimenti il grado è minore di k, e q scelte per ciascuno degli altri k). I polinomi di grado $< m$ (contando anche il polinomio nullo) sono allora in numero di:

$$\begin{aligned} 1 + \sum_{k=0}^{m-1} (q-1)q^k &= 1 + (q-1)\sum_{k=0}^{m-1} q^k = 1 + (q-1)(1 + q + q^2 + \cdots + q^{m-1}) \\ &= 1 + (q-1)\frac{q^m - 1}{q-1} = 1 + q^m - 1 = q^m. \end{aligned}$$

Sottocampi. Il campo F_q, $q = p^n$, contiene uno e un solo sottocampo di ordine p^d per ogni divisore d di n. Infatti, sia $|L| = p^d$, e dimostriamo che $d|n$. Ogni elemento di L è radice del polinomio $x^{p^d} - x$, ma come elemento di F_q è anche radice di $x^{p^n} - x$; ne segue che $x^{p^d} - x$ divide $x^{p^n} - x$; p er l'*es.* 11, $d|n$. Viceversa, se $d|n$ allora $x^{p^d} - x$ divide $x^{p^n} - x = \prod_{\alpha \in F_q}(x - \alpha)$, e perciò $x^{p^d} - x$ ha p^d radici in F_q. Queste, per l'argomento del Teorema 4.15, costituiscono un campo. Il sottocampo di ordine p^d consta degli elementi di F_q che sono radici di $x^{p^d} - x$. Se L_1 e L_2 sono due sottocampi di F_q di ordini p^r e p^s, rispettivamente, allora $L_1 \cap L_2| = p^{(r,s)}$. Infatti, per quanto appena visto, L_1 e L_2 contengono il sottocampo L' di ordine $p^{(r,s)}$ perché (r,s) divide r e s. Viceversa, ogni sottocampo comune a L_1 e L_2 ha ordine che divide r e s, e dunque anche (r,s), ed è perciò contenuto in L'.

Teorema 4.16. *i) La corrispondenza $\phi : F_q \longrightarrow F_q$ data da :*

$$x \to x^p$$

è un automorfismo (automorfismo di Frobenius) di ordine m, dove $q = p^m$.
ii) I punti fissi della ϕ sono tutti e soli gli elementi di $Z_p \subseteq F_q$.

Dim. i) In ogni campo, $(xy)^p = x^p y^p$. Inoltre, per il Lemma 4.8, $(x+y)^p = x^p + y^p$, e dunque la ϕ è un omomorfismo di campi, il cui nucleo è ridotto al solo 0 in quanto $x^p = 0$ implica $x = 0$. La ϕ è dunque iniettiva, ed essendo F_q finito, anche surgettiva. Inoltre, $\phi^m(x) = x^{p^m} = x^q = x$, e dunque $\phi^m = id$, e non può essere $\phi^t = id$ con $t < m$ perchè altrimenti $x^{p^t} = x$ anche per un elemento primitivo x, per cui $x^{p^t - 1} = 1$ con $p^t - 1 < q - 1$.
ii) Un punto fisso a è tale che $a^p = a$, e dunque è radice di $x^p - x$. I p elementi di Z_p sono radici di questo polinomio, che avendo grado p non può avere più di p radici. $\diamondsuit$

Teorema 4.17. *Un polinomio in x^p su F_q è la potenza $p-$esima di un polinomio in x:*

$$f(x^p) = g(x)^p,$$

per un certo $g(x)$. Se inoltre $F_q = Z_p$ allora $g(x) = f(x)$.

Dim. Sia:

$$f(x^p) = a_0 + a_1 x^p + a_2 (x^p)^2 + \cdots + a_t (x^p)^t.$$

Per il Teorema 4.16 *i*), per ogni i si ha $a_i = b_i^p$, per certi b_i, e dunque, per il Lemma 4.8:

$$\begin{aligned} f(x^p) &= b_0^p + (b_1 x)^p + (b_2 x^2)^p + \cdots + (b_t x^t)^p \\ &= (b_0 + b_1 x + b_2 x^2 + \cdots + b_t x^t)^p, \end{aligned}$$

e con $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_t x^t$ si ha il risultato. Se $F_q = Z_p$, allora per il piccolo teorema di Fermat $b_i = b_i^p$, e dunque $b_i = a_i$ e $g(x) = f(x)$. $\diamondsuit$

Teorema 4.18. *Se su F_q la derivata $f'(x)$ di $f(x)$ è zero, allora $f(x)$ è un polinomio in x^p:*

$$f(x) = h(x^p) = g(x)^p, \tag{4.7}$$

dove l'ultima uguaglianza segue dal teorema precedente. Viceversa, se vale la (4.7)*, allora $f'(x) = 0$.*

Dim. Sia $f(x) = \sum_{k=0}^{n} a_k x^k$; allora $f'(x) = \sum_{k=1}^{n} k a_k x^{k-1}$, e se questo polinomio è zero allora p divide tutti i coefficienti ka_k, e dunque $p|a_k$ o $p|k$. Se $p|a_k$, allora $a_k \equiv 0 \bmod p$, e quindi il monomio $a_k x^k$ non è presente in $f(x)$. Ne segue che i monomi $a_k x^k$ presenti sono, al più, quelli per cui $p|k$, cioè quelli in cui x^k è della forma $x^{pt} = (x^p)^t$. Allora $f(x)$ è un polinomio in x^p: $f(x) = a_0 + a_p x^p + a_{2p} (x^p)^2 + \cdots + a_{tp} (x^p)^t = h(x^p)$, dove qualcuno degli a_{kp} può essere zero. Ne segue, per il Teorema 4.17, che $f(x) = g(x)^p$. Viceversa, se vale questa uguaglianza, allora $f'(x) = p g(x)^{p-1} g'(x) = 0$. $\diamondsuit$

Nota. $f(x)$ è un polinomio in x di grado pt; posto $y = x^p$ si ha $h(y) = b_0 + b_1 y + \cdots + b_t y^t$, con $b_k = a_{kp}$, per cui $h(y)$ è di grado t.

Teorema 4.19. *Sia $f(x)$ un polinomio su un campo K, e sia $p(x)$ un suo fattore di molteplicità $\geq t > 1$. Allora $p(x)$ è un fattore della derivata $f'(x)$ di molteplicità $\geq t - 1$. In particolare, $f(x)$ non ha fattori multipli se e solo se $(f(x), f'(x)) = 1$.*

Dim. Sia $f(x) = p(x)^t q(x)$, $\partial p(x) \geq 1$, $t > 1$. Allora:

$$\begin{aligned} f'(x) &= t p(x)^{t-1} p'(x) q(x) + p(x)^t q'(x) \\ &= p(x)^{t-1} (t p'(x) q(x) + p(x) q'(x)), \end{aligned}$$

e dunque $p^{t-1}(x)$ è un polinomio di grado almeno 1 che divide sia $f(x)$ che $f'(x)$. In questo caso allora $(f(x), f'(x)) \neq 1$. Viceversa, sia $p(x)$ un polinomio irriducibile non costante che divide sia $f(x)$ che $f'(x)$. Allora $f(x) = p(x)q(x)$ da cui $f'(x) = p(x)q'(x) + p'(x)q(x)$, e $p(x)$, dividendo $f'(x)$ deve dividere anche il prodotto $p'(x)q(x)$, ed essendo irriducibile uno dei due fattori. Se $q(x) = p(x)q_1(x)$, si ha $f(x) = p^2(x)q_1(x)$, e $f(x)$ ha un fattore multiplo. Se $p(x)$ divide $p'(x)$, allora $p'(x) = 0$, il polinomio nullo, in quanto se non fosse nullo avrebbe un grado d e si avrebbe $d < \partial p(x)$, e perciò non potrebbe essere $p(x)|p'(x)$. (Nel caso della caratteristica 0 questo caso non può darsi in quanto $p(x) = ax^m + \cdots$ con $m > 0$, e dunque $p'(x) = max^{m-1} + \cdots \neq 0$). Se la caratteristica è p è possibile che $p'(x) = 0$, ma allora per il teorema precedente $p(x)$ è della forma $g(x)^p$, per un certo $g(x)$, e dunque non può essere irriducibile. $\diamondsuit$

Un polinomio che non ha fattori multipli si dice *privo di quadrati.*

Corollario 4.20. *Il campo di spezzamento di $x^{p^n} - x$ su Z_p ha esattamente p^n elementi.*

Dim. Il polinomio è primo con la sua derivata $p^n x^{p^n-1} - 1 = -1$, e dunque si spezza nel prodotto di fattori lineari distinti. $\diamondsuit$

Corollario 4.21. *Per ogni p e n, p primo, esiste un campo con p^n elementi.* $\diamondsuit$

Teorema 4.22. *Per ogni p e n, p primo, esistono polinomi irriducibili su Z_p di grado n.*

Dim. Sia a un elemento primitivo del campo di spezzamento F di $x^{p^n} - x$. Poichè a è radice di $x^{p^n-1} - 1$, il polinomio minimo $p(x)$ di a su Z_p è di grado $m \leq p^n - 1$. Sappiamo che l'insieme dei polinomi su Z_p di grado $< m$ è un campo F_1 che ha p^m elementi. Consideriamo l'applicazione $\psi : F_1 \to F$ che associa a $f(x) \in F_1$ l'elemento $f(a)$ ($f(a)$ è una combinazione lineare a coefficienti in Z_p di potenze di a, e dunque sta in F). E' chiaro che si tratta di un omomorfismo. Poichè $\partial f < m$, se $f(a) = 0$ allora f è il polinomio nullo. Dunque la ψ è iniettiva. Se $b \in F$, allora $b = a^k$, per un certo k. Se $k < m$, allora b proviene dal polinomio x^k di F_1. Se $k \geq m$, dividendo x^k per $p(x)$ otteniamo $x^k = p(x)q(x) + r(x)$, con $\partial r(x) < \partial p(x)$, e dunque $r(x) \in F_1$. Allora, essendo $p(a) = 0$, è $a^k = r(a)$, e b proviene da $r(x)$. La ψ è dunque anche surgettiva, e perciò è un isomorfismo. Allora $p^m = |F_1| = |F| = p^n$, e perciò $m = n$. Il polinomio $p(x)$, che è irriducibile, ha dunque il grado n richiesto. $\diamondsuit$

Corollario 4.23. *Due campi finiti dello stesso ordine sono isomorfi.*

Dim. Sia F finito, $|F| = p^n$. Se a è un elemento primitivo di F, allora, con

la stessa dimostrazione del Teorema 4.22, il polinomio minimo di a è di grado n e F è isomorfo al campo dei polinomi su Z_p di grado $< n$. $\diamondsuit$

Teorema 4.24. *Il polinomio $x^{p^n} - x$ su Z_p è il prodotto di tutti i polinomi monici irriducibili $f_d(x)$ su Z_p di grado d che divide n:*

$$x^{p^n} - x = \prod_{d|n} f_d(x). \tag{4.8}$$

Dim. Sia $d|n$, $n = dk$. Il campo di spezzamento di f_d ha p^d elementi per cui se α è una radice di f_d allora $\alpha^{p^d-1} = 1$, ovvero $\alpha^{p^d} = \alpha$. Ma

$$\begin{aligned} \alpha^{p^n} &= \alpha^{p^{dk}} = (\alpha^{p^d})^{p^{d(k-1)}} \\ &= \alpha^{p^{d(k-1)}} = (\alpha^{p^d})^{p^{d(k-2)}} = \dots \\ &= \alpha, \end{aligned}$$

e dunque α è radice di $x^{p^n} - x$. Allora $x^{p^n} - x$ è divisibile per tutti i fattori $x - \alpha$ di f_d, e dunque è divisibile per f_d. Viceversa, se f_d divide $x^{p^n} - x$, una radice di f_d è anche radice di $x^{p^n} - x$, e dunque il campo di spezzamento F' di f_d è un sottocampo di F, il campo di spezzamento di $x^{p^n} - x$. Allora F è uno spazio vettoriale su F', e come tale ha $(p^d)^k$ elementi, per un certo k. Ne segue $p^n = |F| = (p^d)^k$, e dunque $n = dk$, cioè d è un divisore di n. Infine $x^{p^n} - x$ non ha fattori multipli.$\diamondsuit$

Esempio. $x^8 - x$. Qui $p^n = 2^3$, e dunque $d = 1$ o 3. I polinomi di primo grado su Z_2 sono x e $x + 1$, quelli di grado 3 irriducibili sono $x^3 + x + 1$ e $x^3 + x^2 + 1$. Si verifica facilmente che il prodotto di questi quattro polinomi è $x^8 - x$.

Corollario 4.25. *Se I_d è il numero dei polinomi monici irriducibili di grado $d|n$ su Z_p allora:*

$$p^n = \sum_{d|n} dI_d. \tag{4.9}$$

Dim. Segue prendendo i gradi dei due membri della (4.8). $\diamondsuit$

4.4 Il polinomio ciclotomico

Sia K un campo, di caratteristica zero o $p > 0$, e consideriamo il polinomio $x^n - 1$ a coefficienti in K. Le sue radici sono le radici $n-$esime dell'unità di K, che, se p non divide n sono tutte distinte. L'insieme di queste radici è un sottogruppo finito U del campo di spezzamento di $x^n - 1$, di ordine n se $p \not| n$ (se $p|n$, sia $n = p^k r$, $p \not| r$; allora $x^n - 1 = (x^r - 1)^{p^k}$, e il gruppo ha ordine r). Per l'argomento del paragrafo precedente U è ciclico, generato da una radice

primitiva $n-$esima α dell'unità, e queste radici primitive sono in numero di $\varphi(n)$ (se $p|n$, radici primitive $n-$esime non ce ne sono). Il polinomio $x^n - 1$ si spezza allora in fattori lineari:

$$x^n - 1 = \prod_{i=1}^{n}(x - \alpha^i).$$

Raccogliendo le α_i che sono primitive abbiamo il polinomio di grado $\varphi(n)$, che denotiamo con $\varphi_n(x)$:

$$\varphi_n(x) = \prod_{\substack{k \\ (k,n)=1}} (x - \alpha^k).$$

Questo polinomio va sotto il nome di *$n-$esimo polinomio ciclotomico*. Se d è un divisore di n, $\alpha^{\frac{n}{d}}$ è una radice primitiva $d-$esima di 1. Definiamo allora analogamente $\varphi_d(x)$ come il prodotto dei fattori lineari corrispondenti alle radici $d-$esime. Ne segue:

$$x^n - 1 = \prod_{d|n} \varphi_d(x). \tag{4.10}$$

Esempi. 1. Se $K = Q$, il campo razionale, allora:

$$x^4 - 1 = (x - 1)(x + 1)(x - i)(x + i).$$

Le radici primitive quarte di 1 sono i e $-i$; dunque:

$$\varphi_4(x) = (x - i)(x + i) = x^2 + 1.$$

L'unica radice primitiva seconda di 1 è -1, e perciò:

$$\varphi_2(x) = x + 1,$$

e l'unica radice $1-$esima è 1, e dunque:

$$\varphi_1(x) = x - 1.$$

In generale, una radice primitiva $n-$esima dell'unità su Q è il numero complesso $e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$. Le altre sono i numeri $e^{\frac{2\pi i}{n}k}$, per $k = 2, \ldots, n$, e quelle primitive si hanno per $(k, n) = 1$.

2. Se $K = Z_p$ e $n = p - 1$ tutti gli elementi non nulli sono radici $(p-1)-$esime dell'unità (Corollario 4.11). Per $p = 11$, le radici primitive decime dell'unità sono: 2, $8 = 2^3$, $7 = 2^7$ e $6 = 2^9$, il tutto modulo 11, e dunque:

$$x^{10} - 1 = \prod_{k=1}^{10}(x - k),$$

$$\begin{aligned}
\varphi_{10}(x) &= (x-2)(x-8)(x-7)(x-6) = x^4 - x^3 + x^2 - x + 1, \\
\varphi_5(x) &= (x-4)(x-5)(x-9)(x-3) = x^4 + x^3 + x^2 + x + 1, \\
\varphi_2(x) &= x - 10 = x + 1, \\
\varphi_1(x) &= x - 1.
\end{aligned}$$

3. Sia $K = F_9$ il campo con $3^2 = 9$ elementi; i suoi elementi si possono rappresentare con i polinomi su Z_3 di grado 0 o 1. Scelto un polinomio irriducibile di secondo grado $p(x)$ su Z_3, il prodotto in F_9 è il prodotto usuale seguito dalla riduzione modulo $p(x)$. Consideriamo ad esempio $p(x) = x^2 + 1$; allora tutti gli elementi di F_9 si ottengono come potenze di $x + 1$:

$$(x+1)^2 = x^2 + 1 + 2x \equiv 2x,\ (x+1)^3 \equiv 2x + 1,\ (x+1)^4 \equiv 2,\ \ldots,\ (x+1)^8 \equiv 1,$$

dove le congruenze sono mod $x^2 + 1$. Dunque $x + 1$ è un elemento primitivo il cui polinomio minimo è $x^2 + x + 2$; gli altri sono $2x + 1, 2x + 2$ e $x + 2$. Allora:

$$\varphi_8(y) = (y - x - 1)(y - 2x - 1)(y - 2x - 2)(y - x - 2) = y^4 + (x^2+1)y^2 + x^4 + x^2 + 1,$$

che modulo $x^2 + 1$ è $y^4 + 1$.

Nota. Se K è un ampliamento di un campo F di dimensione finita, il *teorema dell'elemento primitivo* afferma che esiste un elemento α in K tale che $K = F(\alpha)$, cioè tale che gli elementi di K sono tutti funzioni razionali di α a coefficienti in F. L'elemento α si dice *primitivo*. Se K è un campo finito, abbiamo definito 'primitivo' un elemento $\alpha \in K$ che genera il gruppo moltiplicativo di K; α è dunque anche primitivo nel nuovo senso perché le potenze di α sono funzioni razionali di α. Il viceversa non è vero: nell'esempio **3.** qui sopra, il polinomio $f(x) = x$ è primitivo nel nuovo senso (ogni elemento di F_9 è un polinomio in x, e dunque una funzione razionale di x) ma non ogni elemento di F_9è una potenza di x (le potenze di x sono $x, -1, -x, 1$, e costituiscono un gruppo ciclico di ordine 4).

Consideriamo ora il caso del campo Q dei razionali.

Teorema 4.26. *Il polinomio ciclotomico $\varphi_n(x)$ su Q è a coefficienti interi.*

Dim. Induzione su n. Se $n = 1$, $\varphi_1(x) = x - 1$, che è a coefficienti interi. Supponiamo il teorema vero per $\varphi_m(x)$, per $m < n$. Dalla (4.10) abbiamo:

$$x^n - 1 = \prod_{\substack{d|n \\ d<n}} \varphi_d(x) \cdot \varphi_n(x).$$

I $\varphi_d(x)$ per $d < n$ sono, per induzione, a coefficienti interi, e dunque il loro prodotto lo è; inoltre poichè i coefficienti direttori dei $\varphi_d(x)$ sono tutti 1, anche quello del prodotto lo è. Ne segue che il quoziente di $x^n - 1$ per questo prodotto è a coefficienti interi. Ma questo quoziente è proprio $\varphi_n(x)$. $\diamondsuit$

Nota. In un campo a caratteristica $p > 0$, questo teorema è ancora vero quando si considerino interi gli elementi del campo base Z_p, cioè i multipli di 1. In particolare, la fattorizzazione (4.10) sussiste anche per ogni campo finito.

La (4.10) si può considerare come una formula che permette di calcolare in modo ricorsivo i polinomi $\varphi_n(x)$. Noti infatti i $\varphi_d(x)$ con $d|n$ e $d < n$, $\varphi_n(x)$

si ottiene come quoziente tra $x^n - 1$ e il prodotto dei $\varphi_d(x)$. Abbiamo cosí: $\varphi_1(x) = x - 1$, e, per $n = p$, primo:

$$\varphi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Diamo qualche altra espressione di $\varphi_n(x)$:

$$\begin{aligned}
\varphi_4(x) &= \frac{x^4 - 1}{(x-1)(x+1)} = x^2 + 1, \\
\varphi_6(x) &= \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1, \\
\varphi_8(x) &= x^4 + 1, \\
\varphi_9(x) &= x^6 + x^3 + 1, \\
\varphi_{10}(x) &= x^4 - x^3 + x^2 - x + 1, \\
\varphi_{12}(x) &= x^4 - x^2 + 1.
\end{aligned}$$

Teorema 4.27. *Il polinomio ciclotomico $\varphi_n(x)$ è irriducibile su Q.*

Dim. Dimostriamo che il polinomio ciclotomico è il polinomio minimo di una radice primitiva $n-$esima dell'unità w (e dunque è irriducibile). Sia $f(x)$ il polinomio minimo di w; $f(x)$ è monico, e divide $\varphi_n(x)$: $\varphi_n(x) = f(x)h(x)$. Facciamo vedere che tutte le radici primitive $n-$esime dell'unità sono radici di $f(x)$; allora sarà $\partial f(x) \geq \varphi(n)$, e dunque $f(x) = \varphi_n(x)$. Per il lemma di Gauss, $f(x)$ e $h(x)$ sono a coefficienti interi. Sia p un primo, $p \not| n$. Se w^p non è radice di $f(x)$ deve esserlo di $h(x)$: $h(w^p) = 0$, e dunque w è radice di $h(x^p)$. Dunque $h(x^p) = f(x)g(x)$ per un certo $g(x)$, anch'esso a coefficienti interi. Passando modulo p abbiamo (Teorema 4.17):

$$h(x)^p = h(x^p) = f(x)g(x) \mod p.$$

Se $f_1(x)$ è un fattore irriducibile di $f(x)$ in $Z_p(x)$, allora $f_1(x)$ divide $h(x)$ mod p e dunque, sempre mod p, $x^n - 1 = f(x)h(x))k(x) = f_1^p(x)h_1(x)$ per un certo $h_1(x)$. Ma allora $x^n - 1$ ha un fattore multiplo, il che è assurdo perchè la sua derivata è nx^{n-1}, che è diversa da zero in quanto $p \not| n$ e dunque $x^n - 1$ è primo con la propria derivata. Ne segue che w^p è radice di $f(x)$. Una radice primitiva è della forma w^r, con $(r, n) = 1$, e dunque r è prodotto di primi p che non dividono n. Si può allora ripetere il ragionamento per ciascuno di questi primi. $\diamondsuit$

Nota. Questo teorema si può dimostrare facendo uso del teorema di Dirichlet secondo il quale se r e n sono due interi relativamente primi nella successione $r + kn$, $k = 1, 2, \ldots$ compaiono infiniti numeri primi. Facciamo vedere che se w è una radice primitiva $n-$esima dell'unità, ogni altra radice primitiva è radice di ogni polinomio a coefficienti

razionali (interi) di cui è radice w. Per ogni primo p della progressione si ha $w^p = w^{r+kn} = w^r \cdot w^{kn} = w^r$. Se ora $f(x)$ è un polinomio che ammette w come radice, da $f(w) = 0$ si ha $0 = f(w)^p \equiv f(w^p) = f(w^r) \bmod p$. Il numero $f(w^r)$ è dunque divisibile per infiniti primi, e perciò è zero, cioè w^r è radice di $f(x)$. Poiché, essendo $(r, n) = 1$, w^r è primitiva, abbiamo quanto richiesto. Se ora $f(x)$ è il polinomio minimo irriducibile su $\mathcal{Q}$ che ammette la radice w esso divide $\Phi_n(x)$; dunque ammette tutte le radici di $\Phi_n(x)$ e perció lo uguaglia. Sia $p = r + kn$ per un certo k. Intanto, essendo $w^n = 1$, si ha $w^p = w^{r+kn} = w^r \cdot w^{kn} = w^r$; inoltre, con $f(x)$ come nella dimostrazione precedente abbiamo, per Fermat, $f(w)^p \equiv f(w^p) \bmod p$. Ne segue:

$$0 = f(w)^p \equiv f(w^p) = f(w^r) \mod p,$$

e ciò vale per tutti i p della successione detta. In altri termini, il numero $f(w^r)$ è zero mod p per infiniti primi p, è cioè divisibile per infiniti primi, e dunque è zero: $f(w^r) = 0$. Ma w^r è primitiva, e dunque il polinomio $f(x)$ ha come radici tutte le radici primitive dell'unità e dunque ha lo stesso grado di $\varphi_n(x)$, e perciò lo eguaglia.

Il polinomio ciclotomico si può però spezzare su un campo finito. Abbiamo visto che $\varphi_8(x) = x^4 + 1$ si spezza su Z_p addirittura per ogni p. Sussiste a tale proposito il seguente teorema generale (che non dimostriamo): *se $p \nmid n$, e $q = p^n$, il polinomio $\varphi_n(x)$ si spezza nel prodotto di $\varphi(n)/m$ fattori irriducibili di grado m, dove m è l'ordine di q* mod n. Concludiamo questo paragrafo osservando che, prendendo i gradi dei due membri della (4.10) otteniamo:

$$n = \sum_{d|n} \varphi(d). \tag{4.11}$$

Ciò si può anche vedere dal fatto che le radici $n-$esime dell'unità, che sono in numero di n, si ripartiscono in radici primitive $d-$esime, per ogni d che divide n. (Si veda anche la discussione che precede il Teorema 4.22).

Come nel caso dei polinomi ciclotomici, la (4.11) si può considerare come una formula che permette di calcolare $\varphi(n)$ in modo ricorsivo. Conoscendo infatti $\varphi(d)$ per $d|n$ e $d < n$ possiamo calcolare $\varphi(n)$ come:

$$\varphi(n) = n - \sum_{\substack{d|n \\ d<n}} \varphi(d).$$

Esempio. $n = 15$. Allora per la (4.11):

$$15 = \varphi(1) + \varphi(3) + \varphi(5) + \varphi(15) = 1 + 2 + 4 + \varphi(15),$$

e dunque $\varphi(15) = 15 - 7 = 8$. I numeri minori di 15 e primi con 15 sono in effetti gli otto interi 1,2,4,7,8,11,13 e 14.

4.5 Massimo comun divisore modulare

Nel calcolo del MCD d di due polinomi f e g a coefficienti interi può ben accadere che d abbia coefficienti che sono più grandi in modulo di quelli di f o g, come mostra il seguente esempio[1]:

$$\begin{aligned} f &= x^3 + x^2 - x - 1 = (x+1)^2(x-1), \\ g &= x^4 + x^3 + x + 1 = (x+1)^2(x^2 - x - 1), \\ d &= x^2 + 2x + 1 = (x+1)^2. \end{aligned}$$

Cosí, per due polinomi con MCD uguale a 1, il calcolo con l'algoritmo di Euclide dà per risultato un intero, che però può essere molto più grande di 1. E ciò complica inutilmente il procedimento. Tutto ciò non accade se si prendono i coefficienti modulo un numero primo p, perchè allora i numeri che intervengono sono limitati da $p-1$ (o da $(p-1)/2$, se si opera con la rappresentazione bilanciata). Può tuttavia accadere che il MCD mod p non sia uguale a quello sugli interi. In questo paragrafo ci proponiamo di discutere brevemente questo problema.

Siano f e g due polinomi a coefficienti interi, p un numero primo e siano f_p e g_p i polinomi ottenuti prendendo i coefficienti modulo p. Vediamo che relazione c'è tra i due massimi comun divisori:

$$(f,g)_p \text{ e } (f_p, g_p).$$

Si tratta in generale di due polinomi distinti. Ad esempio, se $f = x+1$ e $g = x-1$ si ha $(f,g) = 1$ in $Z[x]$ e dunque anche $(f,g)_2 = 1$, mentre i due polinomi sono uguali in $Z_2[x]$ e perciò $(f_2, g_2) = x+1$. In generale, per i gradi dei due MCD si ha:

Teorema 4.28. $\partial(f_p, g_p) \geq \partial((f,g)_p)$.

Dim. Sia $f = (f,g)q, g = (f,g)q'$, da cui $f_p = (f,g)_p q_p$ e $g_p = (f,g)_p q'_p$. Ne segue che $(f,g)_p$ divide sia f_p che g_p, e dunque anche (f_p, g_p), da cui la tesi. $\diamondsuit$

Se p non divide i coefficienti direttori di f e g, allora $\partial((f,g)_p) = \partial(f,g)$ e dunque, per il teorema appena visto $\partial(f_p, g_p) \geq \partial(f,g)$. Così se f_p e g_p sono primi tra loro, cioè $\partial(f_p, g_p) = 0$, lo stesso accade per f e g in $Z[x]$.

Il teorema che segue mostra che la disuguaglianza $\partial(f_p, g_p) > \partial((f,g)_p)$ può aver luogo solo per un numero finito di primi p.

Teorema 4.29. *Sia $d = (f,g)$. Se p non divide entrambi i coefficienti direttori di f e g e non divide il risultante $R(f/d, g/d)$, allora:*

$$\partial(f_p, g_p) = \partial((f,g)_p) = \partial(f,g).$$

[1] Dovuto a Davenport e Trager, e citato in **[DST]**, p. 131.

Dim. Sia $f = dq$, $g = dq'$. Allora $f_p = d_p q_p$ e $g_p = d_p q'_p$; inoltre,

$$\begin{aligned}(f_p, g_p) &= (d_p q_p, d_p q'_p) = d_p(q_p, q'_p) \\ &= d_p(\frac{f_p}{d_p}, \frac{g_p}{d_p}) = d_p((\frac{f}{d})_p, (\frac{g}{d})_p)\end{aligned}$$

(in quanto $f_p/d_p = q_p = (f/d)_p$). Si ha allora che $(f_p, g_p) \neq d_p$ se e solo se il massimo comun divisore $((f/d)_p, (g/d)_p)$ non è costante, e dunque se e solo se

$$R((\frac{f}{d})_p, (\frac{g}{d})_p) = 0.$$

Ma questo risultante è uguale a $R((f/d), (g/d))_p$ (il risultante non è che un determinante, e questo è una somma di prodotti dei propri coefficienti). Dunque $R = 0$ se e solo se p divide $R((f/d), (g/d))$. $\diamondsuit$

Poichè f/d e g/d sono primi tra loro, $R(f/d, g/d)$ è diverso da zero, e dunque ha un numero finito di divisori. La disuguaglianza $\partial(f_p, g_p) > \partial((f, g)_p)$ può dunque aver luogo solo per un numero finito di primi p, e cioè quelli che dividono $R(f/d, g/d)$.

4.6 Forma priva di quadrati di un polinomio

Sia $u = u(x)$ un polinomio di grado $n > 0$, e sia u_i il prodotto di tutti i fattori di molteplicità i di u, $i = 1, 2, \ldots, n$ (se per qualche i non vi sono fattori di questo tipo porremo $u_i = 1$). Si ha allora:

$$u = u_1 u_2^2 u_3^3 \cdots u_r^r, \tag{4.12}$$

dove r è la molteplicità massima per un fattore di u (e dunque $u_{r+1} = \ldots = u_n = 1$). La (4.12) si chiama *forma priva di quadrati* di u; si osservi che il polinomio $u_1 u_2 u_3 \cdots u_r$ (ed è questo che propriamente è privo di quadrati) ha le stesse radici di u ma semplici. Descriviamo ora un algoritmo che ci permette di determinare il numero r e i polinomi u_i. Supponiamo per il momento che la caratteristica del campo sia 0. Per u nella forma (4.12) abbiamo:

$$u' = u'_1 u_2^2 \cdots u_r^r + 2u'_2 u_1 u_2 u_3^3 \cdots u_r^r + \cdots + r u'_r u_1 u_2^2 \cdots u_{r-1}^{r-1} u_r^{r-1},$$

$$d = (u, u') = u_2 u_3^2 \cdots u_r^{r-1}, \ \frac{u}{d} = u_1 u_2 u_3 \cdots u_r,$$

$$\begin{aligned}\frac{u'}{d} = u'_1 u_2 u_3 \cdots u_r &+ 2u'_2 u_1 u_3 \cdots u_r + \cdots + i u'_i u_1 u_2 \cdots \hat{u}_i \cdots u_r + \cdots \\ &+ r u'_r u_1 u_2 u_3 \cdots u_{r-1}\end{aligned}$$

$$(\frac{u}{d})' = u_1' u_2 u_3 \cdots u_r + u_2' u_1 u_3 \cdots u_r + \cdots + u_i' u_1 u_2 \cdots \hat{u}_i \cdots u_r + \cdots + u_r' u_1 u_2 u_3 \cdots u_{r-1},$$

(l'apice denota derivazione e $\hat{u}_i$ significa che il termine u_i manca). Moltiplicando l'ultima uguaglianza per i e sottraendo dalla penultima abbiamo:

$$\begin{aligned} \frac{u'}{d} - i(\frac{u}{d})' &= (1-i)u_1' u_2 u_3 \cdots u_i \cdots u_r \\ &+ (2-i)u_2' u_1 u_3 \cdots u_i \cdots u_r + \cdots \\ &- u_{i-1}' u_1 u_2 \cdots u_i \cdots u_r + u_{i+1}' u_1 u_2 \cdots u_i \cdots u_r \\ &+ \cdots + (r-i)u_r' u_1 u_2 \cdots u_i \cdots u_{r-1}. \end{aligned} \tag{4.13}$$

Se ora un polinomio irriducibile $p(x)$ divide u/d, allora divide uno degli u_k, e uno solo perchè $(u_k, u_j) = 1$ se $k \neq j$. Se $k \neq i$, allora $p(x)$ divide tutti gli addendi della somma (4.13) meno l'addendo $(k-i)u_k' u_1 u_2 \cdots \hat{u}_k \cdots u_r$, e dunque non può dividere la somma. I soli polinomi irriducibili che dividono u/d e (4.13) sono quelli che dividono u_i, e poichè u_i divide u/d e (4.13) si tratta del loro massimo comun divisore:

$$u_i = (\frac{u}{d}, \frac{u'}{d} - i(\frac{u}{d})').$$

Abbiamo allora il seguente algoritmo per determinare gli u_i:

input: $u,\ n = \partial u$,
$d : (u, u'),\ v : \frac{u}{d}, w : (\frac{u}{d})'\ , z : \frac{u'}{d}$,
per $i : 1$ a n fare:
$(u_i : (v, z - iw))$,
output: $u_1, u_2, \ldots, u_n$.

Il numero dei fattori multipli di ordine massimo è dato dall'intero r per il quale $u_r \neq 1$ e $u_i = 1$ per $i = r+1, \ldots, n$.

Esempio. Sia $u = x^4 + 2x^3 - 2x - 1$. Allora:

$$d = (u, u') = (x+1)^2,\ \frac{u}{d} = x^2 - 1,\ \frac{u'}{d} = 4x - 2,\ (\frac{u}{d})' = 2x.$$

Ne segue:

$$\begin{aligned} u_1 &= (x^2 - 1, 4x - 2 - 1 \cdot 2x) = (x^2 - 1, 2(x-1)) = x - 1, \\ u_2 &= (x^2 - 1, 4x - 2 - 2 \cdot 2x) = (x^2 - 1, -2) = 1, \\ u_3 &= (x^2 - 1, 4x - 2 - 3 \cdot 2x) = (x^2 - 1, -2(x+1)) = x + 1, \\ u_4 &= (x^2 - 1, 4x - 2 - 4 \cdot 2x) = (x^2 - 1, -2(2x-1)) = 1, \end{aligned}$$

e dunque:

$$u = (x-1)\cdot 1\cdot (x+1)^3.$$

Nota. Poichè u può avere più fattori con la stessa molteplicità gli u_i sono in generale riducibili, e dunque la (4.12) non è in generale lo spezzamento in fattori irriducibili. Lo è se e solo se gli u_i sono irriducibili.

Se la caratteristica del campo è $p > 0$ l'algoritmo ora visto può non funzionare. Ad esempio, con $u = x^p + 1$ si ha $u' = 0, d = u, v = 1, w = z = 0$ e l'algoritmo fornisce $u_i = 1$ per ogni i, mentre essendo $x^p + 1 = (x+1)^p$ si ha $r = p$ e

$$x^p + 1 = 1\cdot 1\cdots 1\cdot (x+1)^p.$$

La cosa si può allora affrontare come segue. Sappiamo che se $u' = 0$ allora $u = g^p$ per un certo g. Si può allora applicare l'algoritmo a g e poi elevare gli u_i che si ottengono alla p. (Se anche $g' = 0$, si procede per g come per u). Nel caso di $u = x^p + 1$ si ha $u = g^p$ con $g = x + 1$. L'algoritmo fornisce ovviamente l'unico fattore $x + 1$ che elevato alla p dà la decomposizione di sopra.

Se non interessa raccogliere i fattori con la stessa molteplicità, ma si vuole semplicemente una fattorizzazione in fattori privi di quadrati si può procedere in questo modo:

1. Se $(u, u') = 1$, u è privo di quadrati.

2. Sia $d = (u, u')$ con $\partial d > 0$.

   2a. Se $d = u$, allora $u' = 0$ e siamo in caratteristica p. Dunque $u = g^p$. Si ricomincia allora con g al posto di u.

   2b. Se $d \neq u$, d è un fattore non banale di u, e u/d non ha fattori multipli. Allora:

$$u = d\cdot \frac{u}{d},$$

e se d ha fattori multipli si procede come sopra con d al posto di u. Ci si riduce così a

$$u = v_1 v_2 \cdots v_s,$$

con i v_i privi di quadrati.

Per il polinomio dell'esempio precedente, questo metodo fornisce la fattorizzazione $u = v_1 \cdot v_2 \cdot v_3 = (x+1)(x+1)(x^2-1)$.

Osserviamo infine che per un polinomio a coefficienti interi e privo di quadrati si ha, dal Teorema 4.19, che il risultante $R(f, f')$ è diverso da zero, e anzi questa condizione è anche sufficiente. Lo stesso polinomio può però non essere più privo di quadrati se preso modulo un certo primo p (ad esempio, $x^2 + 1$ è privo di quadrati sugli interi ma non lo è modulo 2, dove è uguale a $(x+1)^2$). Perchè resti privo di quadrati il risultante $R(f, f')$ sugli interi deve restare diverso da zero quando viene preso mod p, e cioè non deve essere divisibile per p. (Nel caso dell'esempio il risultante è 4).

Il risultato di questo paragrafo ci permette, quando vogliamo fattorizzare un polinomio, di limitarci al caso di un polinomio privo di quadrati.

Esercizi

1. Dimostrare che i polinomi

$$x^4 + 2(1-a)x^2 + (1+a)^2,$$

dove $a \neq 1, -1$ è un intero privo di quadrati, sono irriducibili sugli interi ma si spezzano mod p per ogni p.

2. Dimostrare che i polinomi

$$(x^2 + x + 1)(x^3 - a)$$

con a intero che non è un cubo, hanno un fattore lineare mod p per ogni p, ma non ne hanno sugli interi.

3. Sia K un campo a caratteristica 0 e sia

$$f = \prod_{i=1}^{n} (x - \alpha_i)^{k_i}$$

la sua fattorizzazione in un ampliamento $K' \supseteq K$. Dimostrare che:

$$(f, f') = \prod_{i=1}^{n} (x - \alpha_i)^{k_i - 1}.$$

4. Dimostrare che il numero dei polinomi irriducibili monici di secondo grado su F_q è $q(q-1)/2$.

5. Sia $p > 2$. Dimostrare che -1 è un quadrato mod p se e solo se $p \equiv 1 \bmod 4$.

6. Usare il Corollario 4.11 per dimostrare il Teorema di Wilson:

$$(p-1)! \equiv -1 \bmod p.$$

7. Dimostrare che 2 è un elemento primitivo di Z_{13}. (Si sa che se $p = 4q + 1$ con q primo, allora 2 è primitivo in Z_p).

8. Dimostrare che 10 è primitivo in Z_{17}.

9. Siano n, m e t interi. Dimostrare che:

$$(t^n - 1, t^m - 1) = t^{(n,m)} - 1.$$

(*Sugg.*: osservare che $(t^n-1)-t^{n-m}(t^m-1)=t^{n-m}-1$, e procedere per induzione sul massimo tra n e m, ricordando che per ogni terna di interi h,k e s si ha $(h,k)=(h,k-hs)$).

10. Dimostrare che:
a) 2^n-1 e 2^m-1 sono primi tra loro se e solo se n e m lo sono.
b) $2^n \equiv 2^m \bmod\ 2^k-1$ se e solo se $n \equiv m \bmod\ k$.

11. Dimostrare che:

$$(x^{p^n}-x, x^{p^m}-x) = x^{p^{(n,m)}}-x.$$

12. Dimostrare che:

$$\varphi(n) = n\sum_{d|n}\frac{\mu(d)}{d} = n\cdot \prod_{\substack{p|n\\ p\ distinti}}(1-\frac{1}{p}) = \prod_{i=1}^{k} p_i^{h_i-1}(p_i-1),$$

se $n=p_1^{h_1}p_2^{h_2}\cdots p_k^{h_k}$.

13. Dimostrare che $\varphi_{12}(x)$ si spezza su Z_p per ogni p.

14. Dimostrare che per un polinomio $u=u(x)$ di grado n, i polinomi q_i dati ricorsivamente da:

$$\begin{aligned} q_1 &= u, \\ q_{k+1} &= (q_k, q_k'), \end{aligned}$$

$k=1,2,\ldots,n-1$, forniscono la forma priva di quadrati di u quando si ponga:

$$u_i = \frac{q_i q_{i+2}}{q_{i+1}^2},$$

$i=1,2,\ldots,r-1$, dove r è il più piccolo intero tale che $q_{r+1}=1$.

15. Sia $f=x^2+ax+b$ un polinomio di secondo grado. Dimostrare che per ogni $n\geq 2$ esiste ed è unico un polinomio della forma x^n+cx+d che lo ammette come fattore. Generalizzare al caso in cui f è di grado m.

16. Dimostrare che per p primo si ha $x^p-x\equiv 0 \bmod 2p$.

4.7 La funzione di Möbius

Le formule (4.11), (4.8) e (4.9) esprimono, la prima il numero intero n in termini della funzione di Eulero $\varphi(d)$ dei suoi divisori d, la seconda il polinomio $x^{p^n}-x$ come prodotto di tutti i polinomi irriducibili $f_d(x)$ di grado d che divide n, e la terza il grado p^n in termini del numero I_d di questi polinomi. Ci poniamo

ora il problema di "invertire" queste formule, e altre dello stesso tipo, cioè di determinare $\varphi(d)$, $f_d(x)$ e I_d a partire dai primi membri.

Nei casi ora menzionati interviene la relazione di divisibilità tra naturali, che è una relazione di *ordine parziale*, cioè riflessiva, antisimmetrica e transitiva. Consideriamo allora il caso più generale di un qualunque insieme parzialmente ordinato $\mathcal{P}$, con relazione d'ordine che indicheremo con "$\leq$" ($\mathcal{P}$ può essere l'insieme dei reali rispetto all'ordine usuale, l'insieme delle parti di un insieme rispetto all'inclusione, ecc.). Se $x, y \in \mathcal{P}$, il *segmento* di estremi x e y è l'insieme degli elementi $a \in \mathcal{P}$ tali che $x \leq a \leq y$; $\mathcal{P}$ è *localmente finito* se ogni segmento è un insieme finito. Ad esempio, l'insieme $\mathcal{N}$ dei naturali ordinato con la divisione è localmente finito perchè ogni intero ha un numero finito di divisori. Inoltre $\mathcal{N}$ ha un primo elemento, e cioè 1, per cui il segmento $1 \leq a \leq y$ è l'insieme $\{a \in \mathcal{N} | a \leq y\}$.

Sia ora F un campo, $\mathcal{P}$ localmente finito, e consideriamo l'insieme delle funzioni f da $\mathcal{P} \times \mathcal{P}$ a valori in F e tali che $f(x, y) = 0$ se $x \not\leq y$. La somma tra due tali funzioni e il prodotto per uno scalare si definiscono in modo ovvio, per cui queste funzioni costituiscono uno spazio vettoriale su F. Il prodotto $f * g$ di due funzioni si definisce come

$$(f * g)(x, y) = \sum_{x \leq u \leq y} f(x, u) g(u, y),$$

(la somma ha senso perchè $\mathcal{P}$ è localmente finito). Siamo così in presenza di un'algebra, l'*algebra d'incidenza* $\mathcal{A}(\mathcal{P})$ di $\mathcal{P}$. Tra le funzioni dette c'è la funzione δ di Kronecker:

$$\delta(x, y) = \begin{cases} 1, & \text{se } x = y; \\ 0, & \text{altrimenti.} \end{cases}$$

Sia f una qualunque altra funzione; allora:

$$(f * \delta)(x, y) = \sum_{x \leq u \leq y} f(x, u) \delta(u, y),$$

ed essendo $\delta(u, y) = 0$ se $u \neq y$ resta solo il termine $f(x, u)$ con $u = y$, cioè $f(x, y)$. Dunque $f * \delta = f$, cioè δ è l' *elemento unità* di quest'algebra. Se una f ammette un'inversa g, deve essere:

$$\sum_{x \leq u \leq y} f(x, u) g(u, y) = \delta(x, y); \tag{4.14}$$

in particolare, $f(x, x) g(x, x) = 1$, e dunque $f(x, x) \neq 0$. Questa condizione è anche sufficiente. Infatti, definiamo g per induzione sulla cardinalità del segmento $x \leq u \leq y$. Se esso ha cardinalità 1 (è formato dal solo x) poniamo

$g(x,x) = 1/f(x,x)$. Supponiamo la g definita per segmenti di cardinalità n, e sia il segmento $x \leq u \leq y$ di cardinalità $n+1$; poniamo allora

$$g(x,y) = -\frac{1}{f(x,x)} \sum_{x<u\leq y} f(x,u)g(u,y),$$

(che ha senso in quanto il segmento $u \leq z \leq y$ ha cardinalità al più n e quindi la g è ivi definita). Abbiamo dunque dimostrato che *condizione necessaria e sufficiente affinchè una f sia invertibile è che si abbia $f(x,x) \neq 0$ per ogni $x \in \mathcal{P}$.*

Consideriamo ora la *funzione zeta*, così definita:

$$\zeta(x,y) = \begin{cases} 1, & \text{se } x \leq y; \\ 0, & \text{altrimenti.} \end{cases}$$

Poichè $\zeta(x,x) = 1 \neq 0$ questa funzione ha un'inversa, che prende il nome di *funzione di Möbius*, e si denota con μ. Essa si determina per induzione, esattamente come visto sopra, a partire da $\mu(x,x) = 1$. Inoltre, essendo

$$\sum_{x\leq u\leq y} \zeta(x,u)\mu(u,y) = \delta(x,y),$$

si ha, per $x = y$, $\zeta(x,x)\mu(x,x) = \delta(x,x) = 1 \cdot \mu(x,x) = 1$, e per $x \neq y$, $\zeta(x,u) = 1$ e dunque $\sum_{x\leq u\leq y} \mu(u,y) = 0$. La funzione di Möbius è dunque caratterizzata dalle proprietà:

$$\mu(x,x) = 1,$$

e una delle seguenti:

$$\begin{array}{l} \sum_{x\leq u\leq y} \mu(u,y) = 0, \\ \sum_{x\leq u\leq y} \mu(x,u) = 0, \\ \mu(x,y) = -\sum_{x<u\leq y} \mu(u,y), \\ \mu(x,y) = -\sum_{x\leq u<y} \mu(x,u) \end{array} \tag{4.15}$$

($x < y$ significa $x \leq y$ e $x \neq y$). Facciamo ora vedere che nel caso dei naturali la μ è la funzione definita come segue:

$$\mu(x,y) = \begin{cases} 1, & \text{se } \frac{y}{x} = 1; \\ (-1)^k, & \text{se } \frac{y}{x} = p_1 p_2 \cdots p_k \text{ primi } \textit{distinti}; \\ 0, & \text{altrimenti.} \end{cases}$$

La μ è allora una funzione della sola variabile y/x; la denoteremo con $\overline{\mu}$. Si ha $\mu(x,x) = 1$ e dunque la prima condizione di sopra è soddisfatta. Se poi $x|y$, $x \neq y$ e $y/x = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}$, allora:

$$\sum_{x|u|y} \mu(x,u) = \sum_{1|\frac{u}{x}|\frac{y}{x}} \overline{\mu}(\frac{u}{x}) = \sum_{1|h|\frac{y}{x}} \overline{\mu}(h);$$

gli h che dividono y/x e per i quali $\overline{\mu}(h) \neq 0$ sono prodotti di primi distinti tra quelli che dividono y/x; sono dunque i p_i, i prodotti p_ip_j, $p_ip_jp_t$, ecc. I primi sono in numero di k, e su questi la $\overline{\mu}$ vale -1, i secondi in numero di $\binom{k}{2}$, e la $\overline{\mu}$ vale 1, ecc. In definitiva la somma precedente vale:

$$\sum_{j=0}^{k}(-1)^j\binom{k}{j} = 0$$

(si ricordi la formula del binomio $(x+y)^k = \sum_{j=0}^{k}\binom{k}{j}x^jy^{k-j}$ e si ponga $x = -1$ e $y = 1$). La $\mu(x,y)$ soddisfa dunque la seconda delle (4.16) ed è quindi effettivamente la funzione di Möbius sui naturali.

L'interesse della funzione μ risiede principalmente nel fatto che essa permette di "invertire" funzioni f definite su $\mathcal{P}$ a valori in F. E' quanto ci siamo proposti all'inizio di questo paragrafo. Sia f definita a partire da una funzione g in questo modo: $f(x) = \sum_{y\leq x} g(y)$. Vogliamo dimostrare che allora la g è determinata dalla f. Per dare un'idea di questo fatto, consideriamo il caso dei naturali con la relazione di divisibilità. Allora $g(1) = f(1), g(2) = f(2) - f(1), g(3) = f(3) - f(1), \ldots, g(6) = f(6) - f(3) - f(2) + f(1)$, ecc.

Teorema 4.30. (FORMULA D'INVERSIONE DI MÖBIUS) *Se f e g sono funzioni a valori in F definite su $\mathcal{P}$ e*

$$f(x) = \sum_{y\leq x} g(y),$$

allora:

$$g(n) = \sum_{y\leq x} f(y)\mu(y,x).$$

Dim. Sostituiamo l'espressione di f data dalla prima uguaglianza nella seconda. Si ha:

$$\sum_{y\leq x} f(y)\mu(y,x) = \sum_{y\leq x}\sum_{u\leq y} g(u)\mu(y,x) = \sum_{y\leq x}\sum_{u} g(u)\zeta(u,y)\mu(y,x),$$

dove si è usata l'uguaglianza $\sum_{u\leq y} g(u) = \sum_u g(u)\zeta(u,y)$. Scambiando l'ordine di sommazione, e ricordando che la μ è l'inversa della ζ, abbiamo:

$$\sum_u g(u)\sum_{y\leq x}\zeta(u,y)\mu(y,x) = \sum_u g(u)\delta(u,x) = g(x),$$

che è quanto si voleva. $\diamondsuit$

Nel caso dei naturali l'inversione di Möbius prende la forma (scriviamo semplicemente μ invece di $\overline{\mu}$):

$$f(n) = \sum_{d|n} g(d) \Longrightarrow g(n) = \sum_{d|n} f(d)\mu(\frac{n}{d});$$

$g(n)$ è dunque la differenza tra la somma dei termini per i quali $\mu(\frac{n}{d})$ vale 1 e quella per i quali vale -1.

In forma moltiplicativa:

$$f(n) = \prod_{d|n} g(d) \Longrightarrow g(x) = \prod_{d|n} f(d)^{\mu(\frac{n}{d})}.$$

Esempi. 1. Con $f(n) = n$ e $g(d) = \varphi(d)$ abbiamo dalla (4.11):

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}.$$

2. Invertendo la (4.9) possiamo sapere qual è il numero dei polinomi irriducibili monici su Z_p. Con $f(n) = p^n$ e $g(d) = dI_d$ abbiamo:

$$I_n = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

Così ad esempio, per $p = 2$ e $n = 4$,

$$I_4 = \frac{1}{4}(\mu(1)2^4 + \mu(2)2^2 + \mu(4)2) = \frac{1}{4}(2^4 - 2^2) = 3,$$

(i tre polinomi irriducibili di quarto grado su Z_2 sono $(x^4 + x + 1)$, $(x^4 + x^3 + 1)$ e $(x^4 + x^3 + x^2 + x + 1)$).

3. Usando l'inversione di Möbius moltiplicativa, con $f(n) = x^{p^n} - x$ e $g(d) = f_d(x)$ abbiamo dalla (4.8):

$$f_d(x) = \prod_{d|n} (x^{p^d} - x)^{\mu(\frac{n}{d})}.$$

Ad esempio, per $p = 2$ e $n = 4$,

$$1 \cdot (x^4 - x)^{-1}(x^{16} - x) = \frac{(x^{16} - x)}{x^4 - x} = x^{12} + x^9 + x^3 + 1$$

che è il prodotto dei tre polinomi irriducibili di grado 4 su Z_2 visti sopra.
Per il polinomio ciclotomico si ha dalla (4.10):

$$\varphi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}.$$

Calcoliamo ad esempio $\varphi_{12}(x)$. Si ha:

$$\varphi_{12}(x) = \frac{(x^2 - 1)(x^{12} - 1)}{(x^4 - 1)(x^6 - 1)} = x^4 - x^2 + 1,$$

in quanto $\mu(12) = \mu(4) = 0, \mu(6) = 1, \mu(3) = \mu(2) = -1$. Il calcolo di questo polinomio fatto direttamente implica una divisione di un polinomio di grado 14 per uno di grado 10. Per evitare una tale divisione, che è piuttosto lunga, si può procedere in questo modo. Sappiamo che il risultato sarà un polinomio di grado $14 - 10 = 4$ (lo sappiamo anche perchè $\varphi(12) = 4$), e quindi, prendendo i polinomi che compaiono nel quoziente modulo x^k, con $k > 4$, il risultato sarà lo stesso. Prendiamo $k = 5$; abbiamo allora $x^{12} - 1 = x^5 \cdot x^7 - 1 \equiv -1 \bmod x^5$. Analogamente, $x^6 - 1 \equiv -1 \bmod x^5$, e dunque:

$$\varphi_{12}(x) = \frac{1 - x^2}{1 - x^4} = \frac{1}{1 + x^2} \bmod x^5.$$

Sappiamo (Cap. 2) che $\frac{1}{1+x^2} = 1 - x^2 + x^4 - x^6 + \cdots$, e questa serie modulo x^5 è proprio il polinomio $x^4 - x^2 + 1$.

4.8 Il metodo di Berlekamp

Vediamo ora un metodo generale di fattorizzazione di un polinomio $u(x)$ su Z_p. Possiamo limitarci al caso in cui il polinomio sia privo di quadrati, sia considerando la forma priva di quadrati vista nel paragrafo 4.6 e fattorizzando i singoli u_i, sia fattorizzando $u/(u, u')$. Inoltre, ci si può sempre ridurre al caso di un polinomio monico: basta infatti sostituire x con x/a, dove a è il coefficiente direttore di $u(x)$, e moltiplicare per a^{n-1}, dove n è il grado di $u(x)$. Si fattorizzerà allora il polinomio monico $g(x) = a^{n-1}u(x/a)$.

Esempio. Sia $u(x) = 3x^2 + 4x + 1$. Procedendo come detto si ha:

$$g(x) = 3(3(\frac{x}{3})^2 + 4(\frac{x}{3}) + 1) = x^2 + 4x + 3 = (x + 1)(x + 3).$$

Tornando indietro, se sostituiamo x con $3x$ e dividiamo per 3 otteniamo $\frac{1}{3}(3x + 1)(3x + 3) = u(x)$.

Quello che ora illustriamo è il *metodo di Berlekamp*, e permette di trovare tutti i fattori irriducibili di $u(x)$. Sia

$$u(x) = p_1(x)p_2(x) \cdots p_r(x)$$

la fattorizzazione $u(x)$ che cerchiamo. Poichè $u(x)$ è privo di quadrati, i $p_i(x)$ sono a due a due primi tra loro. Vediamo dapprima di trovare fattori di $u(x)$ non necessariamente irriducibili; ciò si può fare per mezzo di polinomi che si trovano come segue.

Per ogni polinomio $f(x)$, e $s \neq t$ due elementi di Z_p, i polinomi $f(x) - s$ e $f(x) - t$ sono relativamente primi (se un polinomio li divide entrambi allora divide la loro differenza $t - s$, che è una costante), e dunque, a fortiori, lo sono

$$\mathrm{MCD}(u(x), f(x) - s) \text{ e } \mathrm{MCD}(u(x), f(x) - t)$$

e poichè entrambi dividono $u(x)$ anche il loro prodotto divide $u(x)$. Ne segue che

$$\prod_{s \in Z_p} \mathrm{MCD}(u(x), f(x) - s) \text{ divide } u(x). \tag{4.16}$$

Vediamo ora per quali polinomi $f(x)$, se ce ne sono, si ha che viceversa $u(x)$ divide $\prod_{s \in Z_p} \mathrm{MCD}(u(x), f(x) - s)$. Ciò accade se e solo se per ogni fattore irriducibile $p_i(x)$ di $u(x)$ esiste un s tale che $p_i(x)$ divide $f(x) - s$. Ora, data comunque una $r-$pla $s_1, s_2, \ldots, s_r$ di elementi di Z_p, non necessariamente distinti, poichè i $p_i(x)$ sono a due a due relativamente primi, esiste per il teorema cinese un polinomio $v(x)$ tale che

$$v(x) \equiv s_i \bmod p_i(x),\ i = 1, 2, \ldots, r, \tag{4.17}$$

e $v(x)$ è unico modulo il prodotto $\prod_{i=1}^{r} p_i(x)$, e cioè modulo $u(x)$. Per questo $v(x)$, allora, per ogni $p_i(x)$ esiste un s_i tale che $p_i(x)$ divide $v(x) - s_i$, e dunque $\mathrm{MCD}(u(x), v(x) - s_i)$. Assieme a quanto visto sopra possiamo allora concludere con il seguente teorema.

Teorema 4.31. *Sia $v(x)$ un polinomio che soddisfa la* (4.17)*. Allora:*

$$u(x) = \prod_{s \in Z_p} \mathrm{MCD}(u(x), v(x) - s). \tag{4.18}$$

Se dunque $u(x)$ è riducibile e $\partial v(x) \geq 1$, la (4.18) è una fattorizzazione non banale di $u(x)$. Il grado di ciascuno dei MCD è infatti inferiore a quello di $u(x)$ in quanto $\partial v(x) < \partial u(x)$, e non tutti possono essere di grado 0, cioè costanti, perchè il loro prodotto è $u(x)$, che non è costante.

Chiameremo *polinomio che riduce* $u(x)$ un polinomio $v(x)$ di grado ≥ 1 per cui vale la (4.18).

Dimostriamo ora che una soluzione del sistema di congruenze (4.17), che dipende dai polinomi incogniti $p_i(x)$, è equivalente alla soluzione di una sola congruenza, che dipende dal prodotto dei $p_i(x)$, cioè dal polinomio (noto) $u(x)$. Per il piccolo teorema di Fermat $s_i^p \equiv s_i \bmod p$; ne segue:

$$v(x)^p \equiv s_i^p \equiv s_i \equiv v(x) \bmod p_i(x),$$

da cui $v(x)^p \equiv v(x) \bmod p_i(x)$, per ogni i, e dunque

$$v(x)^p \equiv v(x) \bmod u(x). \tag{4.19}$$

La (4.19) è dunque una condizione necessaria perchè valga la (4.17). Ma è anche sufficiente: infatti, se $v(x)$ soddisfa la (4.19), allora $u(x)$ divide $v(x)^p - v(x)$, che dunque è diviso anche da tutti i $p_i(x)$. Avendosi

$$v(x)^p - v(x) = (v(x) - 0)(v(x) - 1) \cdots (v(x) - (p - 1))$$

ciascun $p_i(x)$ deve dividere uno dei fattori a secondo membro, diciamo $v(x) - s_i$. In questo modo ogni fattore di $p_i(x)$ determina un elemento s_i di Z_p tale che sussiste la (4.17). Abbiamo dimostrato:

Teorema 4.32. *Se r è il numero dei fattori irriducibili di $u(x)$, ogni $r-$pla $s_1, s_2, \ldots, s_r$ di elementi di Z_p determina un polinomio $v(x)$ che soddisfa la* (4.19)*, e viceversa ogni tale polinomio determina una $r-$pla che soddisfa la* (4.17)*. Poichè il numero di queste $r-$ple è p^r, vi sono esattamente p^r soluzioni della* (4.17) *e dunque della* (4.19)*.* $\diamondsuit$

Esempio. Sia $p = 5$, $u(x) = x^4 + 1$; si ha $(u(x), u'(x)) = 1$, e dunque $u(x)$ privo di quadrati. Come polinomio $v(x)$ prendiamo $v(x) = x^2$. Si ha $v(x)^5 - v(x) = x^{10} - x^2 = (x^4 + 1)(x^6 - x^2) \equiv 0 \bmod x^4 + 1$, e dunque $v(x)^5 \equiv v(x) \bmod u(x)$, cioé $v(x)$ soddisfa la (4.19). I MCD$(x^4 + 1, x^2 - s)$, $s = 0, 1, 4$ sono uguali a 1; MCD$(x^4 + 1, x^2 - 2) = x^2 - 2$ e MCD$(x^4 + 1, x^2 - 3) = x^2 - 3$. Si ha dunque: $u(x) = x^4 + 1 = 1 \cdot 1 \cdot (x^2 - 2) \cdot (x^2 - 3) \cdot 1$.

Il Teorema 4.32 ci suggerisce allora di trovare polinomi che soddisfano la (4.19). Noi li determineremo come *punti fissi* di una certa trasformazione lineare dello spazio vettoriale dei polinomi di grado inferiore al grado n di $u(x)$ su Z_p. Questo spazio ha dimensione n, una base essendo data dai monomi $1, x, x^2, \ldots, x^{n-1}$, e dunque contiene p^n polinomi.

L'applicazione:

$$\varphi : f(x) \to f(x)^p \bmod u(x)$$

è una trasformazione lineare dello spazio; si ha infatti:

$$\begin{aligned} \varphi(af(x) + bg(x)) &= (af(x) + bg(x))^p = a^p f(x)^p + b^p g(x)^p \\ &= af(x)^p + bg(x)^p \\ &= a\varphi(f(x)) + b\varphi(g(x)), \end{aligned}$$

ricordando che $a^p \equiv a \bmod p$, e lo stesso per b. *I polinomi che soddisfano la* (4.19) *sono i punti fissi di questa trasformazione lineare.* L'argomento usato sopra per mostrare che la φ è lineare mostra anche che i polinomi che soddisfano la (4.19) formano un sottospazio.

Nella base $1, x, x^2, \ldots, x^{n-1}$ la φ si rappresenta con una matrice i cui elementi nella $k-$esima riga sono i coefficienti del polinomio, preso modulo $u(x)$, che è l'immagine secondo φ del monomio x^k. Questi elementi sono dunque i coefficienti del resto della divisione di x^{pk} per $u(x)$:

$$Q = \begin{pmatrix} q_{0,0} & q_{0,1} & \cdots & q_{0,n-1} \\ q_{1,0} & q_{1,1} & \cdots & q_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ q_{k,0} & q_{k,1} & \cdots & q_{k,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ q_{n-1,0} & q_{n-1,1} & \cdots & q_{n-1,n-1} \end{pmatrix},$$

dove:

$$\varphi(x^k) = x^{pk} \equiv q_{k,0} + q_{k,1}x + \cdots + q_{k,n-1}x^{n-1} \bmod u(x),$$

per $k = 0, 1, \ldots, n-1$. (Si osservi che la prima riga di una tale matrice, riga che corrisponde a $x^0 \bmod u(x)$, è sempre $1, 0, \ldots, 0$).
Se $f(x) = \sum_{k=0}^{n} a_k x^k$ è un polinomio dello spazio che stiamo considerando, la sua immagine secondo φ è

$$\begin{aligned} \varphi(f(x)) &= \varphi(\sum_{k=0}^{n-1} a_k x^k) = \sum_{k=0}^{n-1} a_k \varphi(x^k) = \sum_{k=0}^{n-1} a_k (x^{pk} \bmod u(x)) \\ &= \sum_{k=0}^{n-1} a_k \sum_{i=0}^{n-1} q_{k,i} x^i = \sum_{k,i=0}^{n-1} a_k q_{k,i} x^i. \end{aligned}$$

Ciò mostra che i coefficienti di $\varphi(f(x))$ si ottengono come prodotto del vettore le cui componenti sono i coefficienti di $f(x)$ per la matrice Q. I polinomi $v(x)$ che soddisfano la (4.19) sono quelli fissati da φ; se $v_0, v_1, \ldots, v_{n-1}$ sono i coefficienti di un tale polinomio, allora:

$$(v_0, v_1, \ldots, v_{n-1})Q = (v_0, v_1, \ldots, v_{n-1}). \tag{4.20}$$

Viceversa, se un vettore soddisfa questa uguaglianza, le sue componenti sono i coefficienti di un polinomio fissato da φ. Riassumiamo questa discussione nel seguente teorema.

Teorema 4.33. *Un polinomio a coefficienti in Z_p soddisfa la* (4.19) *se e solo se i suoi coefficienti sono, nell'ordine delle potenze crescenti di x, le componenti di un autovettore della matrice Q relativo all'autovalore* 1. *Inoltre, il numero di questi autovettori è p^r (perchè questo è il numero dei polinomi che soddisfano la* (4.19)). $\diamondsuit$

Si ha così che il numero r dei fattori irriducibili di $u(x)$ è uguale alla molteplicità geometrica dell'autovalore 1 della matrice Q. Siamo ora in grado di determinare il numero r. Sia $v = (v_0, v_1, \ldots, v_{n-1})$; se per questo v vale la (4.20), allora $v(Q - I) = 0$, dove I è la matrice identità $n \times n$. Abbiamo così che r è la dimensione del nucleo di $Q - I$. Se ρ è il rango di $Q - I$, allora $n = r + \rho$.

Teorema 4.34. *Il numero r dei fattori irriducibili di $u(x)$ è uguale alla dimensione del nucleo di $Q - I$, e dunque è uguale a*

$$r = n - \rho.$$

dove ρ è il rango di $Q - I$. $\diamondsuit$

Nota. Non può mai essere $\rho = n$ perché la prima riga di Q è $1, 0, \ldots, 0$, e dunque la prima riga di $Q - I$ ha solo zeri per cui il suo rango ρ è al più $n - 1$.

La matrice Q ammette sempre l'autovettore $(1, 0, \ldots, 0)$ e tutti i suoi multipli $(a, 0, \ldots, 0)$, $a \in Z_p$. Questi vettori sono i coefficienti dei polinomi di grado 0, e ciò corrisponde al fatto che gli elementi di Z_p, visti come polinomi di grado zero, soddisfano la (4.19) per il teorema di Fermat. Se questi sono i soli autovettori di Q allora $r = 1$, e il polinomio $u(x)$ è irriducibile, e viceversa. Abbiamo così il seguente corollario.

Corollario 4.35. *Il polinomio $u(x)$ è irriducibile se e solo se i soli polinomi che soddisfano la* (4.19) *sono le costanti.* $\diamondsuit$

Questo corollario si può anche dimostrare usando (4.17) e (4.18). Infatti, se esiste una soluzione $v(x)$ non costante di (4.17), allora nessuno dei MCD che compaiono nella (4.18) può essere uguale a $u(x)$, in quanto $\partial v(x) < \partial u(x)$. In questo caso almeno due MCD sono non banali, e pertanto $u(x)$ è riducibile. Se tutte le soluzioni sono costanti, allora per ognuna di queste $v(x)$ il sistema (4.17) si riduce ad una sola congruenza, quella nella quale s_i è uguale alla costante $v(x)$, e dunque $u(x)$ coincide con il proprio fattore irriducibile $p_i(x)$.

Osserviamo infine che se $v(x)$ è costante, $v(x) = t$, allora $\mathrm{MCD}(u(x), t - s)$ è uguale a 1 se $s \neq t$ ed a $u(x)$ se $s = t$. La fattorizzazione è allora quella banale $u(x) = 1 \cdot 1 \cdots 1 \cdot u(x) \cdot 1 \cdots 1$.

Corollario 4.36. *Il polinomio $u(x)$ si spezza in fattori lineari su Z_p se e solo se Q è la matrice identità, $Q = I$, e dunque se e solo se tutti i polinomi di grado inferiore a n sono dei $v(x)$ che riducono $u(x)$.*

Dim. $u(x)$ si spezza in fattori lineari se e solo se $r = n$, e ciò accade se e solo se $\rho = 0$, cioè $Q = I$. Inoltre $r = n$ significa che $Ker(Q - I)$ contiene p^n vettori, cioè tutti i polinomi di grado inferiore a n. $\diamondsuit$

Il corollario seguente fa vedere che se $v(x) = x$ è un polinomio che riduce $u(x)$, allora tutti i polinomi riducono $u(x)$.

Corollario 4.37. *Il polinomio $u(x)$ si spezza in fattori lineari su Z_p se e solo se $v(x) = x$ è un polinomio che riduce $u(x)$.*

Dim. Per la (4.17) si ha $x \equiv s_i \bmod p_i(x)$ per cui $p_i(x) = x - s_i$, e gli s_i sono distinti perchè i $p_i(x)$ lo sono. Viceversa, se $u(x)$ si spezza in fattori

lineari, allora $u(x) = \prod_{i=1}^{r}(x - s_i)$ e dunque $u(x)$ divide $x^p - x = \prod_{s \in Z_p}(x - s)$, e perciò $x^p - x \equiv 0 \bmod u(x)$. Per la (4.19) $v(x) = x$ è un polinomio che riduce $u(x)$. $\diamondsuit$

Esempi. 1. Sia $u(x) = x^4 - x^2 + 1$ e $p = 5$. Si vede subito che $(u(x), u'(x)) = 1$. Poichè i calcoli si fanno modulo $u(x)$, poniamo $u(x) = 0$, cioè $x^4 = x^2 - 1$. Ora,
$x^0 = 1 = 1 + 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3$;
$x^5 = x^4 \cdot x = (x^2 - 1)x = x^3 - x = 0 - 1 \cdot x + 0 \cdot x^2 + 1 \cdot x^3$;
$x^{10} = x^5 \cdot x^5 = (x^3 - x)(x^3 - x) = x^6 - 2x^4 + x^2$. Ma $x^6 = x^4 \cdot x^2 = (x^2 - 1)x^2 = x^4 - x^2 = x^2 - 1 - x^2 = -1$, e dunque $x^{10} = -1 - 2x^2 + 2 + x^2 = 1 - x^2 = 1 + 0 \cdot x - 1 \cdot x^2 + 0 \cdot x^3$;
$x^{15} = x^{10} \cdot x^5 = (1 - x^2)x^5 = x^5 - x^7$. Ma $x^7 = x^5 \cdot x^2 = (x^3 - x)x^2 = x^5 - x^3 = (x^3 - x) - x^3 = -x$, e dunque $x^{15} = x^3 - x + x = x^3 = 0 + 0 \cdot x + 0 \cdot x^2 + 1 \cdot x^3$.

Abbiamo così la matrice:

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

da cui:

$$Q - I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 1 \\ 1 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Cerchiamo i vettori annullati da $Q - I$:

$$(v_0, v_1, v_2, v_3)(Q - I) = (0, 0, 0, 0);$$

si ha

$$(v_2, -2v_1, -2v_2, v_1) = (0, 0, 0, 0),$$

da cui $v_1 = v_2 = 0$; le altre due componenti sono arbitrarie. I vettori annullati da $Q - I$ sono allora, tutti e soli, quelli del tipo $(a, 0, 0, b)$, con a e b qualunque in Z_5. Ve ne sono dunque $5^2 = 25$, e una base del sottospazio che essi formano (cioè il nucleo di $Q - I$), è $(1, 0, 0, 0), (0, 0, 0, 1)$. Dunque dim $Ker(Q - I) = 2$, $r = n - 2 = 4 - 2 = 2$, e perciò $x^4 - x^2 + 1$ si spezza in due fattori irriducibili su Z_5. Per trovare questi due fattori prendiamo un qualunque polinomio di $Ker(Q - I)$, ad esempio $v(x) = x^3$. Calcolando i MCD$(x^4 - x^2 + 1, x^3 - s)$, con $s = 0, 1, 2, 3, 4$, ne abbiamo due diversi da 1, quelli per $s = 2$ e $s = 3$, e gli altri uguali a 1. Dunque:

$$u(x) = 1 \cdot 1 \cdot (2x^2 + x - 2) \cdot (3x^2 + x + 2) \cdot 1.$$

Dividendo il primo fattore per 2 e il secondo per 3 (il che equivale a dividere $u(x)$ pr 6, cioè per 1), abbiamo i due fattori monici $x^2 + 3x - 1$ e $x^2 + 2x - 1$.

2. Consideriamo il polinomio $u(x) = x^{p-1} + 1$ su Z_p, $p > 2$. Poichè $u'(x) = (p-1)x^{p-2}$ abbiamo $(u(x), u'(x)) = 1$. Inoltre,

$$x^{pk} = (x^{p-1})^k \cdot x^k \equiv (-1)^k \cdot x^k,$$

per cui la matrice è la matrice diagonale:

$$Q = diag(1, -1, 1, \ldots, 1, -1).$$

Ne segue $Q - I = diag(0, -2, 0, \ldots, 0, -2)$, per cui il rango di $Q - I$, che in questo caso è il numero di elementi non nulli sulla diagonale, è $\rho = \frac{p-1}{2}$. Essendo $n = p - 1$, il numero dei fattori irriducibili del polinomio è $r = n - \rho = \frac{p-1}{2}$.

Per un vettore del nucleo di $Q - I$ si ha $(0, -2v_1, 0, -2v_3, \ldots, 0, -2v_{p-2}) = (0, 0, \ldots, 0)$, e dunque $v_1 = v_3 = \ldots = v_{p-2} = 0$, e le altre componenti arbitrarie. Una base del nucleo di $Q - I$ è data dai vettori che hanno rispettivamente 1 nei posti $0, 2, \ldots, p-2$ e 0 altrove, e che corrispondono dunque ai polinomi $v(x) = 1, x^2, x^4, \ldots, x^{p-3}$.

Così, ad esempio, con $p = 5$ e $v(x) = x^2$ si ha $\mathrm{MCD}(x^4 + 1, x^2 - s) = 1$ per $s = 0, 1, 4$, e uguale a $x^2 - 2$ e $x^2 - 3$ per $s = 2$ e 3, rispettivamente, e questi sono i due fattori irriducibili. Si osservi che il polinomio $v(x) = x^2$ corrisponde alla coppia di elementi di Z_5 formata da 2 e 3; si ha infatti $x^2 \equiv 2 \mod (x^2 - 2)$ e $x^2 \equiv 3 \mod (x^2 - 3)$.

2. Se $u(x)$ non è privo di quadrati può accadere che $r \neq n - \rho$. Ad esempio, con $u(x) = x^2 + 1$ e $p = 2$ abbiamo $Q = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ e $Q - I = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$, e $\rho(Q - I) = 1$. Dunque $n - \rho = 2 - 1 = 1$ e $u(x)$ sarebbe irriducibile, mentre $u(x) = (x + 1)^2$.

La fattorizzazione (4.18) per un certo $v(x)$ può non essere completa. Se infatti per questo $v(x)$ due degli s_i della (4.17) sono uguali, $s_i = s_j = s$, allora $\mathrm{MCD}(u(x), v(x) - s)$ sarà un polinomio $w(x)$ divisibile per $p_i(x)$ e $p_j(x)$ (ed eventualmente altri $p_k(x)$), ma nel quale questi due fattori non sono evidenti perchè $w(x)$ compare come prodotto dei propri fattori. Diremo allora in questo caso che il polinomio $v(x)$ *non separa* i fattori $p_i(x)$ e $p_j(x)$ di $u(x)$. La (4.18) avrà in tal caso la forma $u(x) = w_1(x) \cdot w_2(x) \cdots w_t(x)$, con $t < r$ con uno dei $w_i(x)$ uguale a $w(x)$.

Corollario 4.38. *La fattorizzazione di $u(x)$ data dalla* (4.18) *è completa se e solo se $v(x)$ soddisfa la* (4.17) *con gli s_i tutti distinti.* $\diamondsuit$

Esempio. Vediamo ora un esempio di polinomio $v(x)$ che non separa tutti i fattori di $u(x)$. Sia $u(x) = x^3 - x^2 + x - 1$ con $p = 5$. Questo polinomio si spezza in fattori lineari su Z_5; è uguale infatti a $(x-1)(x-2)(x-3)$, come subito si verifica, per cui la matrice Q è l'identità. Tutti i polinomi di grado 2 fanno allora

parte del nucleo, cioè sono tutti dei $v(x)$ per i quali vale la (4.20). Prendiamo $v(x) = 3x^2 + x + 2$; allora i MCD valgono 1 per $s = 0, 3, 4$, e $x^2 - 2x + 2$ e $x - 3$, per $s = 1$ e 2, rispettivamente. I due fattori $x - 1$ e $x - 2$ si trovano uniti nel prodotto $x^2 - 2x + 2$, e ciò accade perchè $v(x)$ è congruo modulo $x - 1$ e modulo $x - 2$ allo stesso elemento di Z_5, e cioè 1.

Se la fattorizzazione non è completa, si prenda uno dei fattori $w(x)$ ottenuti, un altro $v(x)$ e si proceda come prima. Che in questo modo si arrivi ad ottenere tutti i fattori $p_i(x)$ si vedrà nel teorema seguente. Inoltre, nella scelta dei $v(x)$ ci si può limitare ad un insieme particolare di polinomi.

Sia $v^{(k)} = (a_{k_0}, a_{k_1}, \ldots, a_{k_{n-1}})$, $k = 1, 2, \ldots, r$ una base per il nucleo di $Q - I$, e sia $v_k(x) = a_{k_0} + a_{k_1}x + \cdots + a_{k_{n-1}}x^{n-1}$, cioè il polinomio avente come coefficienti le componenti di $v^{(k)}$.

Teorema 4.39. *Dati due fattori irriducibili $p_i(x)$ e $p_j(x)$ di $u(x)$ esiste uno dei polinomi $v_k(x)$ definiti qui sopra che li separa.*

Dim. Se nessuno dei $v_k(x)$ separa i due fattori, allora ognuno di essi è congruo allo stesso elemento di Z_p modulo entrambi i fattori. Per ogni k esiste cioè s_k tale che:

$$\begin{aligned} v_k(x) &\equiv s_k \bmod p_i(x), \\ v_k(x) &\equiv s_k \bmod p_j(x). \end{aligned}$$

Ora, ogni v del nucleo di $Q - I$ è combinazione lineare dei $v^{(k)}$, e dunque ogni $v(x)$ che soddisfa la (4.17) è combinazione lineare dei polinomi $v_k(x)$: $v(x) = \sum_{k=1}^{r} c_k v_k(x)$. Ne segue:

$$v(x) = \sum_{k=1}^{r} c_k v_k(x) \equiv \sum_{k=1}^{r} c_k s_k = s \bmod p_i(x),$$

e analogamente:

$$v(x) \equiv s \bmod p_j(x).$$

Ogni $v(x)$ che soddisfa la (4.17) è allora congruo modulo $p_i(x)$ e $p_j(x)$ ad uno stesso s di Z_p. Ma abbiamo visto (Teorema 4.32) che ogni $r-$pla $\{s_i\}$ dà luogo ad un polinomio $v(x)$ che soddisfa la (4.17), ed una $r-$pla nella quale $s_i \neq s_j$ è tale che il corrispondente $v(x)$ è congruo a due distinti elementi (s_i e s_j, appunto) di Z_p. $\diamondsuit$

Vediamo ora qual è la probabilità che scegliendo a caso un polinomio $v(x)$ che soddisfa la (4.19) questo separi tutti i fattori. Per il Corollario 4.38 è la probabilità che scegliendo r elementi a caso di Z_p questi siano tutti distinti. Le $r-$ple di elementi distinti di Z_p, con $r < p$ sono in numero di

$$p(p-1)\cdots(p-(p-(r+1))) = \frac{p!}{(p-r)!},$$

(e questo è il numero dei casi favorevoli), e poichè vi sono in tutto p^r $r-$ple (casi possibili) la probabilità cercata è

$$P = \frac{p!}{(p-r)!p^r}.$$

Ora, se $r << p$, questa probabilità è circa 1. Ad esempio, con $r = 2$, si ha: per $p = 7$, $P = 6/7 \sim 0,86$; per $p = 11$, $P = 10/11 \sim 0,9$; per $p = 17$, $P = 16/17 \sim 0,94$.

4.8.1 Riduzione del calcolo dei MCD: metodo di Zassenhaus-Cantor

Quando p è molto grande rispetto a n, il numero dei MCD da calcolare è molto grande. Vediamo come ridurlo. Osserviamo che:

$$v(x)^p - v(x) = v(x)(v(x)^{\frac{p-1}{2}} + 1)(v(x)^{\frac{p-1}{2}} - 1).$$

Se $u(x)$ divide il primo membro, è probabile che qualche fattore di $u(x)$ sia anche fattore di $(v(x)^{\frac{p-1}{2}} - 1)$. Invece di MCD$(u(x), v(x) - s)$, calcoliamo allora MCD$(u(x), v(x)^{\frac{p-1}{2}} - 1)$: questo sarà un fattore non banale di $u(x)$ con una certa probabilità, che ora calcoliamo. Vediamo dapprima la probabilità che si tratti di un fattore banale: MCD=$u(x)$ o MCD=1.

1. MCD $=u(x)$. Ciò accade se e solo se tutti i $p_i(x)$ dividono $v(x)^{\frac{p-1}{2}} - 1$. Ora dalla (4.17) si ha $v(x)^{\frac{p-1}{2}} \equiv s_i^{\frac{p-1}{2}}$, e dunque $p_i(x)$ divide $v(x)^{\frac{p-1}{2}} - 1$ se e solo se $s_i^{\frac{p-1}{2}} \equiv 1 \bmod p$, cioè se s_i è soluzione della $x^{\frac{p-1}{2}} - 1 = 0$ in Z_p. Questa equazione ha esattamente $\frac{p-1}{2}$ soluzioni in Z_p. Infatti, dalla $x^p - x = \prod_{i=0}^{p-1}(x - i)$ si ha, dividendo per x, $x^{p-1} - 1 = \prod_{i=1}^{p-1}(x - i)$. D'altra parte, $x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1)$, e dunque $x - i$ divide uno dei due fattori, per ogni $i \neq 0$. Ma esattamente la metà degli $x - i$ divide $x^{\frac{p-1}{2}} - 1$: non possono essere di più perchè altrimenti il polinomio $x^{\frac{p-1}{2}} - 1$, che è di grado $\frac{p-1}{2}$ avrebbe più di $\frac{p-1}{2}$ radici, e non possono essere di meno altrimenti l'altro fattore avrebbe più di $\frac{p-1}{2}$ radici. Dunque, i casi favorevoli perchè un dato $p_i(x)$ divida $v(x)^{\frac{p-1}{2}} - 1$ sono in numero di $\frac{p-1}{2}$, e perchè tutti i $p_i(x)$ dividano sono in numero di $(\frac{p-1}{2})^r$. Poichè vi sono p^r scelte per $v(x)$, la probabilità che sia abbia MCD $=u(x)$ è

$$\frac{(\frac{p-1}{2})^r}{p^r} = (\frac{p-1}{2p})^r.$$

2. MCD=1. La probabilità che uno di $p_i(x)$ non divida $v(x)^{\frac{p-1}{2}} - 1$ è, per

quanto visto sopra, $p - \frac{p-1}{2} = \frac{p+1}{2}$; quella che nessuno divida è allora:

$$\frac{(\frac{p+1}{2})^r}{p^r} = (\frac{p+1}{2p})^r.$$

La probabilità che $\mathrm{MCD}(u(x), v(x)^{\frac{p-1}{2}} - 1)$ sia un fattore non banale di $u(x)$ è allora:

$$1 - (\frac{p-1}{2p})^r - (\frac{p+1}{2p})^r.$$

Questa, per $r \geq 2$ e $p \geq 3$ è maggiore o uguale a $4/9$.

4.8.2 Riduzione del calcolo dei MCD: metodo del risultante

Dato $v(x)$, molti dei $\mathrm{MCD}(u(x), v(x) - s)$ sono uguali a 1, e dunque è inutile calcolarli, e ciò accade certamente se $p >> n = \partial u(x)$ in quanto il numero dei fattori di $u(x)$ è al massimo n. Come si possono scoprire gli s di Z_p per i quali il MCD è 1? Qui ci viene in aiuto la teoria del risultante. Infatti MCD$\neq 1$ se e solo se il risultante $R(u(x), v(x) - s)$ è uguale a 0, cioè se e solo se s è radice del polinomio:

$$r(y) = R_y(u(x), v(x) - y)$$

(che è di grado n). Se $s \in Z_p$ è una tale radice, allora $y - s$ divide $r(y)$; ma $y - s$ divide anche $y^p - y$, che è il prodotto di tutti gli $y - i$, al variare di i in Z_p. Ne segue che $y - s$ divide $\mathrm{MCD}(r(y), y^p - y)$, che è un certo polinomio $g(y)$. Viceversa, se $y - s$ divide $g(y)$ allora s è radice di $r(y)$. Dunque, *le radici di* $r(y)$ *in* Z_p *sono quelle di* $g(y)$ (che le ha tutte in Z_p).

Qual è il grado di $g(y)$? Questo polinomio ha solo radici semplici, perchè questo è il caso di $y^p - y$ e dunque il suo grado è uguale al numero di radici che possiede. Inoltre, se $s_1, s_2, \ldots, s_t$ sono queste radici, allora queste sono anche le radici di $r(y)$ in Z_p, e come tali danno luogo a fattori $u_i(x)$=MCD$(u(x), v(x) - s_i)$ di $u(x)$ non banali (e distinti). E poichè, viceversa, un MCD non banale corrisponde ad uno degli s_i, si ha in conclusione che *il grado di* $g(y)$ *è uguale al numero di fattori in cui si spezza* $u(x)$ *mediante* $v(x)$. In particolare, questo grado è $\leq r$.

Il grado t di $g(y)$ ci dice dunque se la fattorizzazione ottenuta mediante $v(x)$ è quella completa: è questo il caso se e solo se $t = r$.

Nota. Può ben accadere che i tre polinomi u, r e g siano uguali. Perchè ciò accada è necessario e sufficiente che u si spezzi in fattori lineari su Z_p. Infatti, $\partial r = \partial u$ significa, per quanto visto sopra, che $v(x)$ spezza u in $t = n$ fattori. Viceversa, se $u(x)$ si spezza in fattori lineari, per il Corollario 4.33 $v(x) = x$ è un polinomio che riduce u, e con questo polinomio $r(y) = R_y(u(x), x - y) = u(y)$. Inoltre, poichè tutte le radici di u, e dunque di r, stanno ora in Z_p, $g(y)$=MCD$(r(y), y^p - y) = r(y)$.

Esempio.[2] Sia $p = 13$ e

$$u = x^8 + x^6 + 10x^4 + 10x^3 + 8x^2 + 2x + 8.$$

Con il polinomio:

$$v = x^6 + 5x^5 + 9x^4 + 5x^2 + 5x,$$

si ha:

$$r(y) = R(u, v - y) = y^8 - 6y^7 - y^6 + 5y^5 = (y-2)^3 y^5.$$

Poichè siamo interessati alle radici di $r(y)$, consideriamo il polinomio ottenuto eliminando i fattori multipli, cioè dividendo per $\mathrm{MCD}(r, r') = y^6 - 4y^5 + 4y^4$; si ottiene:

$$r_1 = y^2 - y.$$

Inoltre,

$$\prod_{s \in Z_{13}} \mathrm{MCD}(u, v - s) = (x^5 + 5x^4 - 4x^3 + 5x + 5)(x^3 - 5x^2 + 4x - 1)$$

dove i due fattori corrispondono rispettivamente a $s = 0$ e $s = 2$. Il polinomio $g(y)$ avrà dunque grado 2; infatti:

$$g(y) = \mathrm{MCD}(r_1, y^{13} - y) = y^2 - 2y,$$

e le radici sono 0 e 2, in corrispondenza ai due fattori già trovati.

Per il calcolo dei coefficienti delle potenze di x prese mod $u(x)$ che servono per formare la matrice Q si può far uso della seguente relazione. Sia:

$$u(x) = x^n + u_{n-1}x^{n-1} + \cdots + u_1 x + u_0,$$

e sia:

$$x^k = a_{k,0} + a_{k,1}x + \cdots + a_{k,n-1}x^{n-1}.$$

Allora, moltiplicando per x,

$$x^{k+1} = a_{k,0}x + a_{k,1}x^2 + \cdots + a_{k,n-1}x^n.$$

Ora

$$x^n \equiv -u_{n-1}x^{n-1} - \cdots - u_1 x - u_0 \bmod u(x),$$

che sostituita nella precedente dà:

$$x^{k+1} = a_{k+1,0} + a_{k+1,1}x + \cdots + a_{k+1,n-1}x^{n-1},$$

[2] I calcoli sono stati eseguiti con il sistema Maxima.

dove, e questa è la relazione annunciata,

$$a_{k+1,j} = a_{k,j-1} - a_{k,n-1}u_j,$$

$(a_{k,-1} = 0)$.

Nota. Un'applicazione molto interessante della fattorizzazione modulo un primo p si ha in teoria di Galois. Sussiste infatti il seguente teorema di Dedekind: *se p non divide il discriminante di un polinomio $u(x)$ e in Z_p il polinomio si spezza in fattori di gradi $n_1, n_2, \ldots, n_k$, allora nel gruppo di Galois di $u(x)$ esiste una permutazione i cui cicli hanno lunghezza $n_1, n_2, \ldots, n_k$.* Consideriamo ad esempio il polinomio $u(x) = x^7 + 2x + 2$; il suo discriminante vale -1, e dunque ogni primo va bene. Sia $p = 3$; allora il metodo di Berlekamp ci dice che $u(x)$ ha due fattori in Z_3, e poichè non ha radici in Z_3, i due fattori sono di gradi $n_1 = 2, n_2 = 5$ oppure $n_1 = 3, n_2 = 4$ (si può poi vedere che è il primo caso che ha luogo). Per il teorema di Dedekind allora, nel gruppo di Galois di $u(x)$ vi è una permutazione che ha un ciclo di lunghezza 2 e uno di lunghezza 5, oppure una permutazione che ha un ciclo di lunghezza 3 e uno di lunghezza 4. Ma l'unico sottogruppo transitivo di S_7 che contiene una permutazione di uno dei due tipi è tutto il gruppo S_7, che dunque è il gruppo di Galois di $u(x)$. In particolare, l'equazione $u(x) = 0$ non è risolubile per radicali.

4.8.3 Il polinomio caratteristico di Q

Come abbiamo visto nel primo capitolo, un polinomio $f(x)$ di grado inferiore al grado di $u(x)$ si scrive in modo unico come:

$$f(x) \equiv f_1(x)L_1(x) + f_2(x)L_2(x) + \cdots + f_r(x)L_r(x) \bmod u(x),$$

dove $L_1(x), L_2(x), \ldots, L_r(x)$ sono i polinomi di Lagrange relativi ai polinomi $p_i(x)$, e dove $f_i(x)$ è il resto della divisione di $f(x)$ per $p_i(x)$. L'algebra A dei polinomi di grado $< n$ si decompone allora nella somma diretta di sottoalgebre:

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_n,$$

con $A_k = \{f_k(x)L_k\} \simeq Z_p[x]/(p_k(x))$. Essendo $p_k(x)$ irriducibile, A_k è un campo, che, se $\partial p_k(x) = n_k$, ha p^{n_k} elementi. Le sottoalgebre A_k sono invarianti per l'automorfismo $\varphi : f(x) \to f(x)^p$ di $Z_p[x]/(u(x))$. Infatti:

$$f(x)^p \equiv f_1(x)^p L_1(x)^p + f_2(x)^p L_2(x)^p + \cdots + f_r(x)^p L_r(x)^p \bmod u(x),$$

e prendendo il resto $r_k(x)$ della divisione di $f_k(x)^p$ per $p_k(x)$ l'elemento $r_k(x)L_k(x)^p$ appartiene ancora ad A_k in quanto, essendo $L_k(x)$ idempotente, $L_k(x)^p \equiv L_k(x) \bmod u(x)$.

Lo studio della trasformazione lineare φ può dunque farsi su ciascuna delle componenti A_k. In altri termini, possiamo supporre $u(x)$ irriducibile e $A_k = A$

di ordine $q = p^n$. Se $\alpha \in A$, allora $\varphi^n(\alpha) = \alpha^q = \alpha$, e dunque $\varphi^n(\alpha) = id$. Allora la matrice Q di φ nella base $1, x, \ldots, x^{n-1}$ è tale che $Q^n = I$, e dunque Q soddisfa il polinomio $\lambda^n - 1$. Dico che questo è il polinomio minimo di Q. Se infatti Q soddisfa un polinomio di grado minore $\sum_{i=1}^{n-1} a_i \lambda^i$, allora $\sum_{i=1}^{n-1} a_i Q^i = 0$, e applicando questa uguaglianza alla base degli x^i si ha il sistema omogeneo:

$$\begin{cases} a_0 + a_1 + \cdots + a_{n-1} = 0, \\ a_0 x + a_1 x^p + \cdots + a_{n-1} x^{p^{n-1}} = 0, \\ a_0 x^2 + a_1 x^{2p} + \cdots + a_{n-1} x^{2p^{n-1}} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 x^{n-1} + a_1 x^{(n-1)p} + \cdots + a_{n-1} x^{(n-1)p^{n-1}} = 0. \end{cases}$$

Posto $x_i = x^{p^i}$, il determinante di questo sistema è il determinante di Vandermonde degli x_i. Essendo questi tutti distinti, il determinante è diverso da 0, e dunque il sistema ha la sola soluzione nulla. Ciò dimostra che $\lambda^n - 1$ è il polinomio minimo di Q, e dunque, a meno eventualmente del segno, anche il polinomio caratteristico:

$$det(Q - \lambda I) = (-1)^n(\lambda^n - 1).$$

Possiamo ora tornare al caso generale. Poichè gli A_k sono invarianti per φ, la matrice di Q su A è diagonale a blocchi:

$$Q = diag(C_1, C_2, \ldots, C_r)$$

ciascun blocco C_k essendo di dimensione $n_k = \partial p_k(x)$. Il polinomio caratteristico di Q è allora il prodotto dei polinomi caratteristici dei blocchi C_k, e dunque:

$$det(Q - \lambda I) = (-1)^n(\lambda^{n_1} - 1)(\lambda^{n_2} - 1)\cdots(\lambda^{n_r} - 1),$$

dove $n_1 + n_2 + \cdots + n_r = n = \partial u(x)$. In particolare, $det(Q) = \pm 1$.

4.9 Il lemma di Hensel

In questo paragrafo ci poniamo il problema di vedere se è possibile, a partire da una fattorizzazione mod p di un polinomio a coefficienti interi, ottenerne una mod p^k, per ogni k. Vedremo che la risposta è positiva. Abbiamo già risolto parzialmente questo problema quando abbiamo visto lo sviluppo $p-$adico di un numero algebrico. Ad esempio, 3 è una radice quadrata di 2 mod 7, cioè una radice di $u(x) = x^2 - 2$; sviluppandola si ottengono i valori approssimati 3,10,108, ecc., modulo, rispettivamente, 7, 7^2, 7^3, ecc. Analogamente, per l'altra radice 4 si ottiene 4, 39, 235, ecc., rispetto agli stessi moduli. Questi sviluppi

danno allora le fattorizzazioni:

$$\begin{aligned} u(x) &\equiv (x-3)(x+3) \bmod 7, \\ u(x) &\equiv (x-10)(x+10) \bmod 7^2, \\ u(x) &\equiv (x-108)(x+108) \bmod 7^3, \\ &\vdots \end{aligned}$$

tenuto conto che $4 \equiv -3, 39 \equiv -10$, $235 \equiv -108$, ecc. In questo modo, la fattorizzazione mod 7 (l'esistenza di una radice equivale infatti ad una fattorizzazione) si "solleva" ad una mod 7^k per ogni k.

Il lemma che segue fornisce un metodo per costruire le fattorizzazioni mod p^k, che, come suggerito dall'esempio appena visto, è analogo a quello che permette di ottenere lo sviluppo $p-$adico di un numero: una volta nota e_n, cioè l'approssimazione mod p^n, si trova l'approssimazione mod p^{n+1} nella forma $e_{n+1} = e_n + cp^n$.

Lemma 4.40. (Lemma di Hensel). *Sia, per un dato $k \geq 1$ e un primo p,*

$$u(x) \equiv f(x)g(x) \bmod p^k,$$

con $u(x), f(x)$ e $g(x)$ a coefficienti interi, monici e $f(x)$ e $g(x)$ relativamente primi mod p. *Allora esistono e sono univocamente determinati due polinomi $f_1(x)$ e $g_1(x)$, anch'essi monici e relativamente primi* mod$p$ *e tali che*:

$$u(x) \equiv f_1(x)g_1(x) \bmod p^{k+1},$$

e inoltre:

$$\begin{aligned} f_1(x) &\equiv f(x) \bmod p^k, \\ g_1(x) &\equiv g(x) \bmod p^k. \end{aligned}$$

Dim. (Scriviamo f per $f(x)$). Cerchiamo f_1 e g_1 nella forma:

$$\begin{aligned} f_1 &= f + p^k v, \\ g_1 &= g + p^k w, \end{aligned} \tag{4.21}$$

per certi polinomi v e w da determinare. I polinomi f_1 e g_1 dovranno allora essere tali che:

$$u \equiv f_1 g_1 = fg + (wf + vg)p^k + vwp^{2k} \bmod p^{k+1},$$

cioè:

$$u \equiv fg + (wf + vg)p^k \bmod p^{k+1}.$$

Per ipotesi, $u - fg$ è divisibile per p^k; dunque il nostro problema è ridotto a quello della determinazione di due polinomi v e w tali che:

$$c = \frac{u - fg}{p^k} \equiv wf + vg \bmod p. \tag{4.22}$$

Il fatto che $(f, g) \equiv 1 \bmod p$ ci permette di trovare v e w. Infatti, siano a e b tali che $af + bg \equiv 1 \bmod p$; allora:

$$caf + cbg \equiv c \bmod p.$$

Inoltre, u e fg sono entrambi monici e dello stesso grado; nella differenza $u - fg$ i loro termini di grado massimo si annullano, per cui il grado di c è inferiore a quello di fg. Sappiamo allora che esiste una soluzione $c \equiv wf + vg \bmod p$, con $\partial v < \partial f$ e $\partial w < \partial g$, e la coppia v, w univocamente determinata dalla coppia f, g. Con questi u e v gli f_1 e g_1 di (4.21) risolvono il problema. Infatti:
1. la coppia f_1, g_1 è univocamente determinata dalla coppia f, g perchè la coppia v, w lo è;
2. f_1 e g_1 sono monici perchè essendo $\partial v < \partial f$ e $\partial w < \partial g$ i monomi di grado massimo di f_1 e g_1 sono quelli di f e g.
3. f_1 e g_1 sono relativamente primi mod p: dalla $af + bg \equiv 1 \bmod p$ segue $af_1 + bg_1 \equiv af + bg + (av + bw)p^k \equiv af + bg \equiv 1 \bmod p$.
Il lemma è così completamente dimostrato. $\diamondsuit$

Nota. Poichè il MCD di due polinomi è definito a meno di una costante, è possibile che il calcolo dei coefficienti di Bézout dia un valore d di $af + bg$ diverso da 1. Per il funzionamento dell'algoritmo occorre invece che il MCD sia proprio 1; occorre allora dividere a e b per d prima di proseguire.

Con le notazioni del lemma abbiamo il seguente algoritmo, che fornisce la fattorizzazione mod p^{n+1} nota quella mod p.

input: u, f, g, a, b, p, k
per k : 1 a n fare:
($c : quoziente(u - fg, p^k) \bmod p$,
$q : quoziente(cb, f) \bmod p$,
$v : resto(cb, f) \bmod p$,
$w : ca + qg \bmod p$,
$f : f + vp^k \bmod p^{k+1}$,
$g := g + wp^k \bmod p^{k+1}$),
output: f, g.

Nota. Poichè per ogni intero s, $s \cdot p^k \bmod p^{k+1} = (s \bmod p) \cdot p^k$, prendiamo i valori di v e w modulo p prima di moltiplicare per p^k.

Vediamo ora su un esempio il funzionamento di questo algoritmo.

Esempio. Consideriamo il polinomio $u = x^4 - 2x^2 + 9$, con $p = 5$, $n = 4$. Fattorizziamo u modulo 5 (con Berlekamp, per esempio); troviamo:

$$u \equiv (x^2 + x + 2)(x^2 - x + 2) \bmod 5.$$

Questi due fattori sono i dati f e g dell'input. Inoltre, $a = x - 1$ e $b = -x - 1$. Con questi dati,

$k = 1$:

$$c = \frac{u - fg}{5} = \frac{-5x^2 + 5}{5} = 1 - x^2.$$

Ora, $cb = x^3 + x^2 - x - 1$; dividendo per f abbiamo quoziente x e resto $2x - 1$:

$$\begin{aligned} q &= x, \\ v &= 2x - 1, \\ w &= (1 - x^2)(x - 1) + x(x^2 - x + 2) = 3x - 1, \end{aligned}$$

e

$$\begin{aligned} f_1 &= f - 10x - 5 \equiv x^2 + 11x - 3 \bmod 5^2, \\ g_1 &= g + 15x - 5 \equiv x^2 - 11x - 3 \bmod 5^2. \end{aligned}$$

$k = 2$:
con i nuovi valori di f e g abbiamo $fg = x^4 - 127x^2 + 9$:

$$c = \frac{u - fg}{5^2} = \frac{125x^2}{5^2} = 5x^2 \equiv 0 \bmod 5.$$

In questo caso $v = w = 0$ per cui i valori di f e g sono quelli precedenti.

$k = 3$:

$u - fg = 125x^2$, $c = \frac{125x^2}{5^3} = x^2$, $cb = x^2(-x - 1) = -x^3 - x^2$ che diviso per f dà quoziente $-x$ e resto $-3x$. Allora $v = -3x$, $w = x^2(x - 1) - x(x^2 - 11x - 3) = 10x^2 + 3x \equiv 3x \bmod 5$, e

$$\begin{aligned} f &= x^2 + 11x - 3 - 3 \cdot 125x = x^2 - 364x - 3 \equiv x^2 + 261x - 3 \bmod 5^4 \\ g &= x^2 - 11x - 3 + 3 \cdot 125x = x^2 + 364x - 3 \equiv x^2 - 261x - 3 \bmod 5^4. \end{aligned}$$

4.9.1 Il lemma di Hensel per più fattori

Il metodo per il sollevamento di una fattorizzazione mod p^k a una mod p^{k+1}, visto nella dimostrazione del lemma di Hensel si può estendere al caso di più fattori, come ora vedremo.

Lemma 4.41. (LEMMA DI HENSEL, CASO GENERALE). *Siano*:

$$u, u_1, u_2, \ldots, u_n \tag{4.23}$$

polinomi a coefficienti interi e monici, tali che:

$$\mathrm{MCD}(u_i, u_j) \equiv 1 \bmod p,\ i \neq j, \tag{4.24}$$

e inoltre:

$$u \equiv u_1 u_2 \cdots u_n \mod p^k. \tag{4.25}$$

Allora esistono polinomi monici a coefficienti interi $\overline{u}_1, \overline{u}_2, \ldots, \overline{u}_n$ *tali che*

$$\partial \overline{u}_i = \partial u_i,\ \overline{u}_i \equiv u_i \mod p^k,\ \mathrm{MCD}(\overline{u}_i, \overline{u}_j) \equiv 1 \bmod p,$$

e inoltre:

$$u \equiv \overline{u}_1 \overline{u}_2 \cdots \overline{u}_n \mod p^{k+1}. \tag{4.26}$$

Dim. Come nel caso di due fattori cerchiamo gli $\overline{u}_i$ nella forma:

$$\overline{u}_i = u_i + p^k v_i,\ i = 1, 2, \ldots, r, \tag{4.27}$$

per certi v_i da determinare. Sostituendo i valori (4.27) nella (4.26) si ottiene:

$$u \equiv u_1 u_2 \cdots u_n + p^k (u_1 v_2 u_3 \cdots u_n + v_1 u_2 u_3 \cdots u_n + \cdots + u_1 u_2 u_3 \cdots v_n)$$

mod p^{k+1}. Per la (4.25),

$$c = \frac{u - u_1 u_2 \cdots u_n}{p^k}$$

è un polinomio a coefficienti interi, ed è di grado inferiore al grado di u, che è poi il grado di $u_1 u_2 \cdots u_n$: quest'ultimo è un polinomio monico, perchè tali sono gli u_i, e dunque nella differenza con u il monomio di grado massimo scompare. Dobbiamo dunque risolvere rispetto ai v_i la congruenza:

$$c \equiv u_1 v_2 u_3 \cdots u_n + v_1 u_2 u_3 \cdots u_n + \cdots + u_1 u_2 u_3 \cdots v_n \mod p. \tag{4.28}$$

Per l'ipotesi (4.24), esistono polinomi $a_1, a_2, \ldots, a_n$ tali che

$$a_1 u_2 u_3 \cdots u_n + a_2 u_1 u_3 \cdots u_n + \cdots + a_n u_1 u_2 \cdots u_{n-1} \equiv 1 \mod p. \tag{4.29}$$

Moltiplicando questa congruenza per c e dividendo ca_i per u_i, $ca_i = q_i u_i + r_i$, $0 \leq \partial r_i < \partial u_i$, si ottiene, sostituendo e raccogliendo,

$$\begin{aligned} u_1 u_2 \cdots u_n (q_1 + q_2 + \cdots + q_n) \quad &+ \quad r_1 u_2 u_3 \cdots u_n + r_2 u_1 u_3 \cdots u_n + \cdots \\ &+ \quad r_n u_1 u_2 \cdots u_{n-1} \equiv c \mod p. \end{aligned}$$

Ora, gli addendi $r_i u_1 u_2 \cdots u_{i-1} u_{i+1} \cdots u_n$ e il polinomio c sono di grado inferiore al grado di $u_1 u_2 \cdots u_n$ per cui se $q_1 + q_2 + \cdots + q_n$ non è il polinomio nullo si ha una contraddizione. Posto allora $v_i = r_i$ abbiamo la soluzione richiesta[3] . Si ha infatti, come nel caso di due fattori:

1. la $n-$pla degli $\overline{u}_i$ è univocamente determinata da quella degli u_i perchè la $n-$pla dei $v_i = r_i$ lo è: se si avesse un'altra soluzione r_i', sottraendo dalla precedente si otterrebbe:

$$\sum_{i=1}^{n}((r_i - r_i') \prod_{j \neq i} u_j) \equiv 0 \bmod p.$$

Ora u_j divide tutti i prodotti $(r_i - r_i')u_1 u_2 \cdots u_{i-1} u_{i+1} \cdots u_n$ per $i \neq j$, e dunque anche $(r_j - r_j')u_1 u_2 \cdots u_{j-1} u_{j+1} \cdots u_n$, ed essendo primo con gli u_i, $i \neq j$, deve dividere $r_j' - r_j$. Ma essendo quest'ultimo di grado inferiore al grado di u_j deve aversi $r_j' - r_j = 0$, e dunque $r_j' = r_j$, e ciò per ogni $j = 1, 2, \ldots, n$.

2. $\partial \overline{u}_i = \partial u_i$ in quanto $\partial v_i < \partial u_i$. Questa disuguaglianza implica anche che il monomio di grado massimo di $\overline{u}_i$ è quello di u_i, e perciò $\overline{u}_i$ è monico.

3. $\mathrm{MCD}(\overline{u}_i, \overline{u}_j) = 1$: se $au_i + bu_j \equiv 1 \bmod p$, allora $a\overline{u}_i + b\overline{u}_j = au_i + bu_j + p^k(av_i + bv_j) \equiv 1 \bmod p$. $\diamondsuit$

Esempio. Sia $u = x^4 - x^3 - 2x + 1$. Fattorizzando $u \bmod 5$ (ad esempio con il metodo di Berlekamp) si ha:

$$u(x) \equiv (x-2)(x+1)(x^2+2) \bmod 5.$$

Ora, $u - u_1 u_2 u_3 = 5$ e dunque $c = \frac{5}{5} = 1$. Risolvendo la:

$$a_1(x+1)(x^2+2) + a_2(x-2)(x^2+2) + a_3(x-2)(x+1) \equiv 1 \bmod p,$$

si trova $a_1 = 2$, $a_2 = 1$, $a_3 = 2x + 2$, ed essendo $\partial c a_i = \partial a_i < \partial u_i$, abbiamo direttamente, senza bisogno di dividere per u_i, $v_i = a_i$ e dunque:

$$\begin{aligned}
\overline{u}_1 &= u_1 + 5v_1 = x - 2 + 5 \cdot 2 = x + 8, \\
\overline{u}_2 &= u_2 + 5v_2 = x + 1 + 5 \cdot 1 = x + 6, \\
\overline{u}_3 &= u_3 + 5v_3 = x^2 + 2 + 5(2x + 2) = x^2 + 10x + 12.
\end{aligned}$$

Ne segue:

$$x^4 - x^3 - 2x + 1 = (x+8)(x+6)(x^2 + 10x + 12) \bmod 25.$$

[3] Si osservi come gli r_i siano i polinomi che danno la decomposizione in frazioni semplici:

$$\frac{c}{u} = \frac{r_1}{u_1} + \frac{r_2}{u_2} + \cdots + \frac{r_n}{u_n}.$$

4.10 Fattorizzazioni su Z

Vogliamo ora utilizzare i risultati dei due precedenti paragrafi per trovare fattorizzazioni di polinomi a coefficienti interi. Cominciamo con la seguente osservazione.

Sia:

$$u(x) = F(x)G(x)$$

una fattorizzazione su Z del polinomio $u(x)$. Passando modulo un intero M abbiamo:

$$u(x) \equiv f(x)g(x) \bmod M,$$

con

$$\begin{aligned} F(x) &\equiv f(x) \bmod M, \\ G(x) &\equiv g(x) \bmod M. \end{aligned} \tag{4.30}$$

Supponiamo di sapere che i coefficienti di ogni possibile fattore di $u(x)$ non superano, in modulo, un certo intero B (vedremo come fare nel prossimo paragrafo). Allora, se $M > 2B$, scegliendo i coefficienti di $f(x)$ nell'intervallo $(-M/2, M/2]$ (scegliendo cioè la rappresentazione bilanciata delle classi resto mod M), le (4.30) non sono più solo congruenze, ma addirittura uguaglianze. Infatti, se $F(x) \neq f(x)$, esiste un coefficiente a di $F(x)$ che differisce dal coefficiente b del monomio dello stesso grado di $f(x)$ per un multiplo di M: $a - b = hM$. Dunque, $a = b + hM$, e con i possibili valori per b si ha $|a| \geq M/2 > B$, contro l'ipotesi.

Supponiamo ora che per un primo $p > 2B$ un polinomio si spezzi mod p nel prodotto di due fattori:

$$u(x) \equiv f(x)g(x) \bmod p. \tag{4.31}$$

Possiamo allora sapere se questa fattorizzazione proviene da una fattorizzazione:

$$u(x) = F(x)G(x) \tag{4.32}$$

sugli interi. Scegliendo infatti i coefficienti di $f(x)$ tra $-(p-1)/2$ e $(p-1)/2$, se la (4.31) proviene dalla (4.32) si ha $f(x) = F(x)$, e dunque $f(x)$ deve dividere $u(x)$ su Z.

Per trovare dei fattori di $u(x)$ si può allora procedere come segue.

1. Fattorizzare $u(x)$ mod p, con $p > 2B$, in fattori irriducibili, ad esempio con il metodo di Berlekamp.

2. Per ciascun fattore $p_i(x)$, considerato come polinomio a coefficienti interi e compresi nell'intervallo $[-(p-1)/2, (p-1)/2]$, vedere se divide $u(x)$ su Z.

Ogni $p_i(x)$ che divide $u(x)$ è un fattore irriducibile di $u(x)$ (se si riduce, si riduce anche mod p).

3. Se vi sono dei $p_i(x)$ che non dividono $u(x)$, formare con questi i prodotti $p_i(x)p_j(x)$, ridurre i coefficienti all'intervallo detto, e vedere se questi polinomi prodotto dividono $u(x)$. Ogni polinomio così costruito che divide $u(x)$ è un fattore irriducibile di $u(x)$ (se si riduce, ciò avviene necessariamente nel prodotto di $p_i(x)$ e $p_j(x)$, che dunque dividerebbero $u(x)$); eliminare i $p_i(x)$ che entrano in un fattore di $u(x)$.

4. Con i $p_i(x)$ che restano, formare i prodotti $p_i(x)p_j(x)p_k(x)$ e sempre dopo riduzione dei coefficienti all'intervallo $[-(p-1)/2, (p-1)/2]$, vedere se dividono $u(x)$.

5. Continuare fino a che tutte le combinazioni sono state provate.

6. Se restano dei $p_i(x)$, il loro prodotto è un fattore irriducibile di $u(x)$.

Invece di considerare un primo $p > 2B$ (il numero B può essere molto grande), si può prendere un primo qualunque, fattorizzare modulo p, e poi sollevare la fattorizzazione a p^n, dove n è un intero tale che $p^n > 2B$.

4.10.1 Maggiorazioni per i coefficienti di un fattore

Vediamo ora come determinare l'intero B del paragrafo precedente. Che esso esista dipende dal fatto che è possibile maggiorare il modulo delle radici di un polinomio, come dimostra il seguente teorema.

Teorema 4.42. *Sia:*

$$u(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

un polinomio a coefficienti complessi. Allora per una radice z di $u(x)$ si ha:

$$|z| < 1 + \frac{M}{|a_0|}, \tag{4.33}$$

dove $M = \max\{|a_0|, |a_1|, \ldots, |a_n|\}$.

Dim. Se $|z| \leq 1$ non c'è niente da dimostrare. Sia allora $|z| \geq 1$. Essendo $u(z) = 0$ si ha:

$$a_0 z^n = -a_1 z^{n-1} - a_2 z^{n-2} - \cdots - a_n.$$

Ne segue:

$$\begin{aligned} |a_0||z|^n &\leq |a_1||z|^{n-1} + |a_2||z|^{n-2} + \cdots + |a_n| \\ &\leq M(|z|^{n-1} + |z|^{n-2} + \cdots + 1) = M\frac{|z|^n - 1}{|z| - 1} \\ &< M\frac{|z|^n}{|z| - 1}, \end{aligned}$$

da cui:

$$|z| < 1 + \frac{M}{|a_0|},$$

che è quanto si voleva. $\diamondsuit$

Sia ora $f(x)$ un polinomio monico, di radici z_i:

$$f(x) = x^m + b_1 x^{m-1} + \cdots + b_m = (x - z_1)(x - z_2)\cdots + (x - z_m).$$

Allora i coefficienti b_i sono dati dalle funzioni simmetriche elementari degli z_i:

$$\begin{aligned} b_1 &= -(z_1 + z_2 + \cdots + z_m), b_2 = z_1 z_2 + z_1 z_3 + \cdots + z_{m-1} z_m, \ldots, \\ b_k &= (-1)^k \sum z_{i_1} z_{i_2} \cdots z_{i_k}, \ldots, b_m = (-1)^m z_1 z_2 \cdots z_m. \end{aligned}$$

Se $|z_i| \leq B$, allora:

$$\begin{aligned} |b_1| &= |\sum z_i| \leq \sum |z_i| \leq mB, \\ |b_2| &= |\sum_{i,j} z_i z_j| \leq \sum_{i,j} |z_i||z_j| \leq \binom{m}{2} B^2, \\ &\vdots \\ |b_m| &= |z_1||z_2|\cdots|z_m| \leq B^m, \end{aligned}$$

da cui

$$|b_i| \leq \max\{\binom{m}{k} B^k,\ k = 1, 2, \ldots, m\}.$$

Se $f(x)$ è un fattore di un polinomio $u(x)$ una radice di $f(x)$ è anche radice di $u(x)$, e dunque una maggiorazione per i coefficienti di $f(x)$ si può ottenere a partire da quella per le radici di $u(x)$ data dalla (4.33).

Un'altra maggiorazione (che non dimostriamo) per il modulo dei coefficienti di un fattore si ottiene in questo modo. Dato il polinomio:

$$u(x) = u_n x^n + u_{n-1} x^{n-1} + \cdots + u_0,$$

definiamo:

$$||u|| = (|u_n|^2 + |u_{n-1}|^2 + \cdots + |u_0|^2)^{\frac{1}{2}}.$$

Sia $f(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$ un fattore di $u(x)$. Allora:

$$|b_j| = \binom{m-1}{j} ||u|| + \binom{m-1}{j-1} |u_n|.$$

Esempio. Sia

$$u(x) = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5.$$

Se $u(x)$ si riduce deve avere un fattore di grado al più 4. Sia:

$$f(x) = b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0.$$

Si ha:

$$||u|| = \sqrt{113} \sim 10,6,$$

da cui:

$$\begin{aligned} |b_0| &\leq \binom{3}{0}||u|| + 0 \sim 10,6;\ |b_1| \leq \binom{3}{1}||u|| + \binom{3}{0} \sim 31,9; \\ |b_2| &\leq \binom{3}{2}||u|| + \binom{3}{1} \sim 34,9;\ |b_3| \leq \binom{3}{3}||u|| + \binom{3}{2} \sim 13,6. \end{aligned}$$

Dunque, un coefficiente di $f(x)$ non supera in modulo 34.

Possiamo allora vedere se $u(x)$ si fattorizza su Z con il metodo visto in precedenza. Scegliamo un primo $p > 2 \cdot 34 = 68$, e sia $p = 71$. Il metodo di Berlekamp fornisce:

$$u(x) \equiv (x+12)(x+25)(x^2 - 13x - 7)(x^4 - 24x^3 - 16x^2 + 31x - 12) \bmod 71.$$

Nessuno di questi fattori divide $u(x)$ su Z (perchè nessuno dei termini noti divide 5). Raggruppando due a due i fattori si hanno i termini noti $12 \cdot 25 = 300, 12 \cdot (-7) = -84, 12 \cdot (-12) = -144$, e nessuno di questi è congruo a ± 1 o a ± 5 mod 71. Se ne conclude che $u(x)$ è irriducibile sugli interi.

Il procedimento che abbiamo visto per fattorizzare su Z (metodo di Berlekamp seguito o no da un sollevamento alla Hensel), presenta l'inconveniente di essere di complessità algoritmica[4] esponenziale, cioè di richiedere un numero di prove che è esponenziale nel grado n del polinomio $u(x)$. Quando i fattori del polinomio mod p sono tutti lineari e $u(x)$ è irriducibile su Z, prima di accorgersi dell'irriducibilità occorre fare 2^n divisioni, tante cioè quante sono in totale le combinazioni a uno a uno, a due a due, ecc. degli n fattori. Esiste tuttavia un metodo, detto "L^3",[5] che permette la fattorizzazione in tempo polinomiale. In esso vengono in sostanza eliminate le prove di cui sopra.

4.11 Fattorizzazioni in un ampliamento

Sia K il campo di spezzamento di un polinomio irriducibile monico $p(x)$ di grado m a coefficienti nel campo Q dei razionali, e siano $\alpha_1, \alpha_2, \ldots, \alpha_m$ le sue radici (che sono tutte distinte perchè $p(x)$ è irriducibile e Q è a caratteristica

[4] Per una breve discussione sul problema della complessità algoritmica si veda il capitolo seguente.

[5] Dalle iniziali di A.K. Lenstra, H.W. Lenstra e L. Lovász, autori dell'articolo [**LLL**].

zero). Consideriamo il sottocampo $Q(\alpha)$ di K, che consta dei polinomi in α a coefficienti in Q di grado al più $n-1$. Se $\beta \in Q(\alpha)$ è $\beta = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}$ con $a_i \in Q$. La *norma* di β si definisce come:

$$N(\beta) = \prod_{i=1}^{m}(a_0 + a_1\alpha_i + \cdots + a_{m-1}\alpha_i^{m-1}).$$

Se $g(x)$ è il polinomio $a_0 + a_1x + \cdots + a_{m-1}x^{m-1}$ si ha allora:

$$N(\beta) = \prod_{p(x)=0} g(x) = R(p,g),$$

il risultante dei polinomi p e g. In particolare, *la norma di un elemento di $Q(\alpha)$ appartiene a Q*, è cioè un numero razionale. Sia ora $f = f(x)$ un polinomio a coefficienti in $Q(\alpha)$, $f(x) \in Q(\alpha)[x]$. Esso si può considerare come un polinomio $f(\alpha, x)$ nelle due variabili α e x, a coefficienti in Q. Definiamo allora la *norma del polinomio f* come:

$$N(f) = \prod_{i=1}^{n} f(\alpha_i, x) = \prod_{p(y)=0} f(y,x) = R_y(p(y), f(y,x)).$$

La norma di $f \in Q(\alpha)[x]$ è allora un polinomio a coefficienti razionali, $N(f) \in Q[x]$, di grado $\partial f \cdot \partial p$, il prodotto dei gradi di f e del polinomio p di cui α è radice. Se $f \in Q[x]$, allora $N(f) = f$ (in questo caso α è semplicemente uno dei coefficienti di f; la cosa si può vedere anche dal risultante, in quanto ora $p(y) = y - \alpha$, e $R_y(y-\alpha, f(y,x)) = f(\alpha, x) = f(x)$). Inoltre, per una proprietà del risultante, la norma è moltiplicativa: $N(fg) = N(f)N(g)$.

Ci proponiamo ora di dimostrare che la fattorizzazione di un polinomio a coefficienti in $Q(x)$ si riduce a quella della sua norma.

Sia $p(x)$ un polinomio irriducibile su un campo F e sia K il suo campo di spezzamento. Il *gruppo di Galois* di K su F, che si denota con $G(K/F)$, è il gruppo degli automorfismi di K che lasciano fisso F elemento per elemento. Poichè K è il campo di spezzamento di un polinomio, non vi sono altri elementi di K fissati da elementi di $G(K/F)$. Se $\sigma \in G(K/F)$, allora σ si estende in modo naturale ai polinomi su K: se $f(x) = a_0 + a_1x + \cdots + a_nx^n$, allora $\overline{\sigma}(f(x)) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n$. In particolare, se $f(x)$ è a coefficienti in F, allora $\overline{\sigma}(f(x)) = f(x)$. Se α è una radice del nostro polinomio $p(x) \in F[x]$, l'elemento $\sigma(\alpha)$, $\sigma \in G(K/F)$, è ancora radice di $p(x)$. Il gruppo di Galois induce allora un gruppo di permutazioni delle radici, e si può dimostrare, in virtù del fatto che K è il campo di spezzamento di un polinomio irriducibile $p(x)$, che date due radici di $p(x)$ esiste un elemento di $G(K/F)$ che porta una sull'altra.

Lemma 4.43. *Sia $f \in Q(\alpha)[x]$ irriducibile. Allora $N(f)$ è una potenza di un polinomio irriducibile.*

Dim. Sia $N(f(x)) = h(x)g(x)$, con $h(x), g(x) \in Q[x]$ e $(h(x), g(x)) = 1$. Per definizione, $N(f(x)) = \prod_{i=1}^{n} f(\alpha_i, x)$, e dunque $f(\alpha, x)$ deve dividere h o g in $Q(\alpha)[x]$. Sia $h(x) = f(\alpha, x)h_1(\alpha, x)$. Per ogni α_i esiste $\sigma_i \in G(K/Q)$ tale che $\sigma(\alpha) = \alpha_i$, e dunque:

$$\overline{\sigma}(h(x)) = h(x) = \overline{\sigma}(f(\alpha, x))\overline{\sigma}(h_1(\alpha, x)) = f(\alpha_i, x)h_1(\alpha_i, x).$$

Tutti i polinomi $f(\alpha_i, x)$ dividono quindi h, e pertanto nessuno divide g in quanto $(h, g) = 1$. Allora $N(f) = h$, e h o è irriducibile, o è potenza di un polinomio irriducibile. $\diamondsuit$

Teorema 4.44. *Sia $f \in Q(\alpha)[x]$ con $N(f)$ priva di quadrati. Se:*

$$N(f) = \prod_i G_i(x)$$

è la fattorizzazione della norma di f in prodotto di fattori irriducibili in $Q(x)$, allora:

$$f = \prod_i \mathrm{MCD}(f(x), G_i(x))$$

è la fattorizzazione di f in prodotto di fattori irriducibili in $Q(\alpha)[x]$.

Dim. Dimostriamo intanto che i massimi comun divisori $g_i = (f, G_i)$ sono irriducibili. Se $h_i \in Q(\alpha)[x]$ è un fattore non banale di g_i, allora lo è anche di G_i e dunque $G_i = h_i k_i$, per un certo k_i. Passando alle norme, $G_i = N(G_i) = N(h_i)N(k_i)$, e per l'irriducibilità di G_i, una delle due norme deve essere una costante, e dunque uno dei due polinomi, e perciò anche l'altro, appartiene a $Q(x)$; ma ciò contraddice l'irriducibilità di G_i in $Q[x]$. Inoltre i g_i sono distinti perchè tali sono i G_i.

Se $f = \prod_j h_j$ è la fattorizzazione di f in fattori irriducibili in $Q(\alpha)[x]$ abbiamo:

$$N(f) = \prod_j N(h_j) = \prod_i G_i.$$

Per il Lemma 4.43 $N(h_j)$ è una potenza di un polinomio irriducibile, e ogni $N(h_j)$ deve dividere $N(f)$. Ma $N(f)$ è priva di quadrati, e pertanto $N(h_j)$ è uno dei fattori irriducibili di $N(f)$, e dunque eguaglia uno dei G_i. Inoltre, $(N(h_i), N(h_j)) = 1$ se $i \neq j$, sempre per il fatto che $N(f)$ è priva di quadrati. Per l'unicità della fattorizzazione segue allora che a meno dell'ordine gli h_j e i g_i sono uguali. $\diamondsuit$

Se $N(f)$ ha radici multiple possiamo utilizzare il seguente risultato.

Teorema 4.45 *Sia $f(x) \in Q(\alpha)[x]$ un polinomio di grado n privo di quadrati. Allora esistono al più $\frac{(nm)^2}{2} - 1$ interi s tali che $N(f(x - s\alpha))$ ha radici multiple.*

Dim. Se $\beta_1, \beta_2, \ldots, \beta_n$ sono le radici di $f(x)$, allora $\beta_i + s\alpha_j$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$ sono le radici di $N(f(x - s\alpha))$. Le radici multiple sono quelle per cui $\beta_i + s\alpha_j = \beta_k + s\alpha_t$, con $i \neq k$ e $j \neq t$, ovvero quelle per cui $s = \frac{\beta_k - \beta_i}{\alpha_j - \alpha_t}$. Le coppie (ordinate) dei β sono in numero di $n(n-1)$, quelle degli α in numero di $m(m-1)$, e due coppie (β_k, β_i) e (α_j, α_t) danno per s lo stesso valore delle coppie (β_i, β_k) e (α_t, α_j). L'intero s può allora assumere al massimo $\frac{n(n-1)m(m-1)}{2} < \frac{(nm)^2}{2}$ valori. $\diamondsuit$

Per fattorizzare $f(x)$ si procede allora come segue.

1. Se f non è privo di quadrati, sostituiamo f con f/d, dove $d = (f, f')$.

2. Cerchiamo un intero s tale che $N(f(x - s\alpha))$ sia priva di quadrati.

3. Fattorizziamo $N(f(x - s\alpha))$ in $Q[x]$:
$$N(f(x - s\alpha)) = \prod_i H_i(x).$$

4. Per il Teorema 4.44,
$$f(x - s\alpha) = \prod_i \mathrm{MCD}(H_i(x) f(x - s\alpha))$$
è la fattorizzazione completa di $f(x - s\alpha)$ in $Q(\alpha)[x]$.

5. Con la sostituzione $x \to x + s\alpha$ abbiamo infine la fattorizzazione completa di $f(x)$:
$$f(x) = \prod_i \mathrm{MCD}(H_i(x + s\alpha), f(x)).$$

Esempio. Sia $K = Q(\sqrt{2})$, e sia:
$$f(x) = x^3 - (1 + \sqrt{2})x^2 + \sqrt{2}x - \sqrt{2} - 2.$$
Il polinomio minimo di $\sqrt{2}$ è $p(y) = y^2 - 2$, e la norma di $f(x)$ è
$$\begin{aligned} N(f) &= R_y(p(y), f(x, y)) \\ &= x^6 - 2x^5 - x^4 - 2x^2 + 4x + 2 \\ &= (x^2 - 2x - 1)(x^4 - 2), \end{aligned}$$
e dunque $N(f)$ è priva di quadrati. Posto:
$$G_1(x) = x^2 - 2x - 1,\ G_2(x) = x^4 - 2,$$
abbiamo:
$$(f(x), G_1(x)) = x - 1 - \sqrt{2},\ (f(x), G_2(x)) = x^2 + \sqrt{2},$$
da cui la fattorizzazione:
$$f(x) = (x - 1 - \sqrt{2})(x^2 + \sqrt{2}).$$

Nota bibliografica

Per il metodo di Kronecker si veda [**A**], p. 159. Campi finiti e metodo di Berlekamp sono trattati un po' dovunque, in particolare in [**C**] II-12, [**McE**] Cap. 6 e 7, [**LN**] Cap IV e [**DST**], §4.2; in quest'ultimo volume viene anche discusso il lemma di Hensel, come pure in [**Kn**], p. 439, es. 22. Per il §4.5 ci siamo basati su [**DST**], §4.1; da qui (p. 131) è preso anche l'esempio dei due polinomi visto all'inizio del paragrafo. Per le maggiorazioni dei coefficienti di un fattore, [**CA**] p. 259 e [**Kn**], p. 438, es. 20.

Capitolo 5

La trasformata di Fourier discreta

5.1 Radici dell'unità

Le radici $n-$esime dell'unità sono le radici del polinomio $x^n - 1$ nel campo complesso; sappiamo che queste sono tutte distinte in quanto il polinomio è primo con la propria derivata, e che si ottengono tutte come potenze di una di esse, una radice primitiva $w = e^{2\pi i/n}$. Queste radici sono dunque:

$$1, w, w^2, \ldots, w^{n-1},$$

con $w^n = 1$. (Ricordiamo che le w^k primitive sono quelle per cui $(k, n) = 1$, e sono perciò in numero di $\varphi(n)$, dove φ è la funzione di Eulero). Avendo la radice 1, il polinomio $x^n - 1$ è divisibile per $x - 1$, con quoziente $1 + x + x^2 + \cdots + x^{n-1}$, e dunque tutte le w^k, con $k \neq 0$ (o meglio $k \not\equiv 0 \mod n$) soddisfano l'equazione:

$$1 + x + x^2 + \cdots + x^{n-1} = 0. \tag{5.1}$$

In particolare, per $x = w$ vediamo che la somma di tutte le radici $n-$esime dell'unità è uguale a zero: $1 + w + w^2 + \cdots + w^{n-1} = 0$. Inoltre, essendo $|w| = 1$ è $w^k = 1$, e perciò $w^k \overline{w}^k = |w^k|^2 = 1$, da cui

$$\overline{w}^k = \frac{1}{w^k} = w^{-k}. \tag{5.2}$$

Facciamo uso delle (5.1) e (5.2) per dimostrare il seguente teorema, che malgrado la sua semplicità sarà di fondamentale importanza in tutta la nostra discussione.

Teorema 5.1. *Si ha:*

$$\sum_{j=0}^{n-1} w^{hj} \overline{w}^{kj} = \begin{cases} n, & \text{se } h \equiv k \mod n; \\ 0, & \text{altrimenti.} \end{cases} \tag{5.3}$$

Dim. Tenuto conto della (5.2), la somma della (5.3), scritta per esteso, vale

$$1 + w^{h-k} + w^{2(h-k)} + \cdots + w^{(n-1)(h-k)}.$$

Se $h \equiv k \bmod n$, questa è una somma di n volte 1, e dunque vale n. Altrimenti, w^{h-k} è una radice $n-$esima dell'unità diversa da 1 e dunque soddisfa la (5.1); la somma vale perciò 0. $\diamondsuit$

Le (5.3) si chiamano *relazioni di ortogonalità.*

5.1.1 Interpolazione nelle radici dell'unità

Un polinomio $u(x) = u_0 + u_1 x + \cdots + u_{n-1}x^{n-1}$ di grado inferiore ad n è univocamente determinato quando si conoscono i valori $z_0, z_1, \ldots, z_{n-1}$ che esso assume su n punti distinti $x_0, x_1, \ldots, x_{n-1}$. Il polinomio si può dunque rappresentare in due modi:
i) mediante la $n-$pla dei suoi coefficienti:

$$u = (u_0, u_1, \ldots, u_{n-1});$$

ii) mediante la $n-$pla dei valori assunti sugli n punti x_i:

$$z = (z_0, z_1, \ldots, z_{n-1}).$$

Noti gli z_i possiamo risalire agli u_i risolvendo il sistema:

$$u_0 + u_1 x_i + u_2 x_i^2 \cdots + u_{n-1}x_i^{n-1} = z_i, \tag{5.4}$$

nelle incognite u_i, $i = 0, 1, \ldots, n-1$, che ammette una ed una sola soluzione in quanto il suo determinante è il Vandermonde degli x_i, ed è quindi non nullo perchè gli x_i sono distinti. La soluzione si può dunque trovare con la regola di Cramer. Nel caso in cui gli x_i sono le radici dell'unità possiamo però risolvere il sistema diversamente, facendo uso delle relazioni di ortogonalità (5.3). Consideriamo gli z_i come coefficienti di un nuovo polinomio $v(x) = z_0 + z_1 x + \cdots + z_{n-1}x^{n-1}$; allora la $k-$esima incognita u_k è il valore del polinomio $\frac{1}{n}v(x)$ nel punto $\overline{w}^k$, come dimostra il teorema seguente.

Teorema 5.2 *Sia $u(x)$ un polinomio del quale si conoscono i valori nei punti w^i, $i = 0, 1, \ldots, n-1$. Allora i coefficienti $u_0, u_1, \ldots, u_{n-1}$ di $u(x)$ sono dati da:*

$$u_k = \frac{1}{n}(z_0 + z_1\overline{w}^k + z_2\overline{w}^{2k} + \cdots + z_{n-1}\overline{w}^{(n-1)k}), \tag{5.5}$$

$k = 0, 1, \ldots, n-1$.

Dim. Consideriamo il sistema (5.4) con $x_i = w^i$:

$$u_0 + u_1 w^i + u_2 w^{2i} + \cdots + u_{n-1}w^{(n-1)i} = z_i, \tag{5.6}$$

moltiplichiamo l'equazione numero 0 per $1 = \overline{w}^0$, la numero 1 per $\overline{w}^k$, la numero 2 per $\overline{w}^{2k}$, ecc., e sommiamo le equazioni cosí ottenute; otteniamo:

$$\sum_{i=0}^{n-1} z_i \overline{w}^{ik} = \sum_{i=0}^{n-1} \sum_{h=0}^{n-1} u_h w^{ih} \overline{w}^{ik} = \sum_{h=0}^{n-1} u_h \sum_{i=0}^{n-1} w^{ih} \overline{w}^{ik}.$$

Per le relazioni di ortogonalità (5.3) l'ultima somma vale zero per $h \neq k$. Resta allora solo il termine $u_k \sum_{i=0}^{n-1} w^{ik} \overline{w}^{ik}$, nel quale, sempre per la (5.3), la somma vale n. Il risultato segue. $\diamondsuit$

Nota. Si osservi che il termine costante u_0 di $u(x)$ è la media dei valori z_i.

Il passaggio dalla $n-$pla z alla u dato dalla (5.5) si chiama *trasformata di Fourier* della z, e i coefficienti u_k si chiamano *coefficienti di Fourier* della z [1]. Per sottolineare la differenza con il caso classico, la (5.5) si chiama trasformata di Fourier *discreta* (DFT)[2].

La matrice del sistema (5.6) è la

$$F = F_n = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & \dots & w^{n-1} \\ 1 & w^2 & w^4 & \dots & w^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{n-1} & w^{2(n-1)} & \dots & w^{(n-1)(n-1)} \end{pmatrix}$$

che prende il nome di *matrice di Fourier*. E' la matrice di Vandermonde delle radici $n-$esime dell'unità, che in questo caso è una matrice simmetrica. Per la (5.3) le colonne v_k, $k = 0, 1, \dots, n-1$, di questa matrice sono vettori (dello spazio $\mathcal{C}^n$ delle $n-$ple di numeri complessi) ortogonali rispetto al prodotto scalare hermitiano $(x, y) = \sum_{i=0}^{n-1} x_i \overline{y}_i$ (ortonormali se si divide per $\sqrt{n}$); sono poi indipendenti (sia per l'ortogonalità, sia perchè si tratta di una matrice di Vandermonde). Per gli u_k della (5.5) si può allora scrivere:

$$u_k = \frac{(z, v_k)}{(v_k, v_k)},$$

e dunque il vettore $u_k v_k$ è la proiezione del vettore z sulla retta del vettore v_k. Nella base $\{v_k\}$ il vettore z si scrive:

$$z = u_0 + u_1 v_1 + \dots + u_{n-1} v_{n-1}.$$

[1] Più precisamente il passaggio dalla z alla u si dovrebbe chiamare *trasformazione* di Fourier, riservando alla u il nome di *trasformata*. Ma quella da noi usata è la terminologia stabilita dall'uso.

[2] Acronimo dell'inglese Discrete Fourier Transform.

L'inversa F^{-1} della F esprime il passaggio dagli z_i agli u_i, ed è la matrice del sistema (5.5). Basta allora prendere i coefficienti della F e cambiarli nei loro coniugati (cioè, per la (5.2), nei loro inversi) dividendo poi per n:

$$F^{-1} = \frac{1}{n}\overline{F}.$$

La DFT della $n-$pla z si esprime allora come[3]:

$$F^{-1}z = u.$$

La matrice U ottenuta dalla F dividendo ogni elemento per la propria norma $\sqrt{n}$ è unitaria[4], cioè la coniugata della trasposta è uguale all'inversa: $\overline{U}^t = U^{-1}$; infatti, per le relazioni di ortogonalità (5.3):

$$U\overline{U}^t = \frac{1}{\sqrt{n}}F \cdot \frac{1}{\sqrt{n}}\overline{F}^t = F \cdot \frac{1}{n}\overline{F} = F \cdot F^{-1} = I.$$

Ancora in virtù delle (5.3) si ha che U^2 è la matrice:

$$\tau = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 \end{pmatrix},$$

e poichè $\tau^2 = I$ è $U^4 = 1$. In particolare, gli autovalori di U sono le radici quarte dell'unità $1, i, -1, -i$ con le opportune molteplicità, e dunque *gli autovalori della F sono, a meno del fattore $\sqrt{n}$, le radici quarte dell'unità.*

In uno spazio vettoriale reale di dimensione finita la lunghezza di un vettore è definita come la radice quadrata della *norma*, cioè della somma dei quadrati delle componenti del vettore. Nel caso della dimensione infinita consideriamo il sottospazio costituito dai vettori per i quali la serie dei quadrati delle componenti converge ad un numero finito (*spazio di Hilbert*); la radice quadrata di questo numero sarà allora per definizione la lunghezza del vettore. Se ora consideriamo lo spazio delle funzioni reali definite in un intervallo $[a, b]$, una funzione $f = f(x)$ di questo spazio si può pensare come un vettore ad una infinità continua di componenti (i valori della f nei punti dell'intervallo), e la serie di cui sopra viene sostituita da un integrale. Lo spazio di Hilbert sarà allora costituito dalle f per le quali esiste finito l'integrale $\int_a^b f(x)^2 dx$ (funzioni a *quadrato sommabile*). Ci interessiamo ora all'intervallo $[0, 2\pi]$, e alle funzioni:

$$1, \cos(kx), \sin(kx),$$

[3] Per non appesantire la notazione, denotiamo ancora con z il vettore colonna formato dagli elementi della $n-$pla z, e non con z^t (dove t indica la trasposta), come sarebbe più opportuno fare. Ci atterremo a questa notazione anche nel seguito.

[4] Alcuni autori chiamano matrice di Fourier questa U, altri la $\overline{U}$, e trasformata di Fourier la (5.6), cioè quella data dalla F.

per $k = 1, 2, \ldots$. Per queste funzioni si ha:

$$\int_0^{2\pi} 1^2 dx = 2\pi, \int_0^{2\pi} \cos^2(kx)dx = \int_0^{2\pi} \sin^2(kx)dx = \pi,$$

per ogni k, e dunque si tratta di vettori di lunghezza $\sqrt{2\pi}$, $\sqrt{\pi}$ e $\sqrt{\pi}$, rispettivamente. L'integrale del quadrato è il caso particolare per $g = f$ del *prodotto scalare*:

$$(f, g) = \int_0^{2\pi} f(x)g(x)dx.$$

Rispetto a questo prodotto le funzioni precedenti sono *ortogonali*:

$$(1, \cos(kx)) = 0, (1, \sin(kx)) = 0, (\cos(kx), \sin(kx)) = 0,$$

per le note proprietà degli integrali delle funzioni trigonometriche.

Sotto opportune ipotesi, una funzione f periodica di periodo 2π si può sviluppare in *serie di Fourier* nell'intervallo $[0, 2\pi]$:

$$f(x) = \frac{a_0}{2} + a_1 \cos x + b_1 \sin x + \cdots + a_k \cos kx + b_k \sin kx + \cdots.$$

I coefficienti a_k e b_k sono i *coefficienti di Fourier* della f. Per ottenere uno di questi coefficienti a_k (b_k) si moltiplicano i due membri dell'uguaglianza per il coseno (seno) corrispondente e si integra poi da 0 a 2π. Per l'ortogonalità, tutti i termini nella serie vanno a zero, meno quello che contiene il coefficiente cercato, termine che vale $a_k \int_0^{2\pi} \cos^2(kx)$, e analogamente per b_k. Ad esempio,

$$b_1 = \frac{\int_0^{2\pi} f(x)\sin(x)dx}{\int_0^{2\pi} \sin^2(x)} = \frac{1}{\pi}\int_0^{2\pi} f(x)\sin(x)dx,$$

ovvero, in termini di prodotto scalare e più in generale:

$$a_k = \frac{(f, \cos(kx))}{(\cos(kx), \cos(kx))}, \; b_k = \frac{(f, \sin(kx))}{(\sin(kx), \sin(kx))}.$$

Come nel caso finito, gli addendi della serie di Fourier della f sono allora le proiezioni della f, pensata come vettore dello spazio di Hilbert, sulle rette sostegno degli infiniti vettori $1, \cos(kx)$ e $\sin(kx)$. (Si osservi che un coefficiente come a_k è il valore di r che minimizza la differenza $f(x) - r\cos(kx)$; infatti $f(x) - a_k \cos(kx)$ è la lunghezza del segmento di perpendicolare che proietta la f sulla retta per $\cos(kx)$).

Per l'identità di Eulero $e^{ijx} = \cos(jx) + i\sin(jx)$, dove i è l'unità immaginaria, lo sviluppo in seni e coseni equivale allo sviluppo:

$$f(x) = \sum_{j=-\infty}^{+\infty} c_j e^{ijx};$$

si ha infatti, da quest'ultima uguaglianza,

$$f(x) = \sum_{j=0}^{\infty}(c_j e^{ijx} + c_{-j}e^{-ijx}) = 2c_0 + \sum_{j=1}^{\infty}(c_j + c_{-j})\cos(jx) + i(c_j - c_{-j})\sin(jx),$$

e i due sviluppi sono uguali per $a_j = c_j + c_j$ e $b_j = i(c_j - c_{-j})$. I c_j sono i coefficienti di Fourier della f in questo nuovo sviluppo. Nel caso di uno spazio complesso di dimensione finita n il prodotto scalare è il prodotto hermitiano:

$$(u, v) = \sum_{i=0}^{n} x_i \overline{y}_i$$

(dove x_i e y_i sono le coordinate di u e v, rispettivamente). Nel nostro caso:

$$(f, g) = \int_0^{2\pi} f(x)\overline{g(x)}dx.$$

Rispetto a questo prodotto le funzioni $1, e^{ikx}$ sono ortogonali:

$$\int_0^{2\pi} 1 \cdot e^{ikx}dx = 0, \int_0^{2\pi} e^{ikx}e^{-ijx}dx = \begin{cases} 2\pi, & \text{se } k = j; \\ 0, & \text{se } k \neq j. \end{cases}$$

(si ricordi che $\overline{e^{ijx}} = e^{-ijx}$). Queste relazioni di ortogonalità, e le analoghe per seni e coseni viste prima, corrispondono alle (5.3) del caso discreto.

Per determinare un coefficiente c_k si procede analogamente a quanto già visto moltiplicando $f(x)$ e il suo sviluppo per e^{-ikx} e integrando poi da 0 a 2π. Tenendo conto delle relazioni di ortogonalità si ottiene:

$$c_k = \frac{1}{2\pi} \int_0^{2\pi} f(x)e^{-ikx}dx,$$

ovvero:

$$c_k = \frac{(f(x), e^{ikx})}{(e^{ikx}, e^{ikx})},$$

e l'addendo $c_k e^{ikx}$ della serie risulta essere la proiezione sull' "asse" e^{ikx} della funzione (del vettore) $f(x)$.

Quanto visto con la DFT è la versione discreta del caso classico che abbiamo ora discusso. La serie del caso discreto è una serie finita, cioè un polinomio, e la moltiplicazione per e^{-ikx} seguita dall'integrazione da 0 a 2π diventa moltiplicazione per $\overline{w}^k$, cioè per w^{-k}, seguita dalla somma da 0 a n. Più precisamente, la versione discreta è l'usuale approssimazione, col metodo del trapezio, dell'integrale che dà c_k quando si prendono un numero finito di valori della $f(x)$ su punti opportunamente scelti. Ricordiamo che nel metodo del trapezio si suddivide l'intervallo $[a, b]$ in parti uguali mediante i punti $a = x_0, x_1, \ldots, x_n = b$, e l'area $\int_a^b g(x)dx$ sottesa dalla curva $y = g(x)$ si approssima con la somma delle aree dei trapezi di vertici $(x_k, 0), (x_k, g(x_k)), (x_{k+1}, g(x_{k+1})), (x_{k+1}, 0)$. Questa somma vale:

$$\frac{b-a}{n}(\frac{1}{2}(g(a) + g(b)) + \sum_{i=1}^{n-1} g(x_i)).$$

Nel nostro caso per l'integrale che dà c_k abbiamo $g(x) = f(x)e^{-ikx}$, con $a = 0$ e $b = 2\pi$. Prendiamo $x_j = \frac{2\pi j}{n}$; poichè la $f(x)$ è periodica di periodo 2π, è $f(2\pi) = f(0)$, e dunque

con $z_j = f(\frac{2\pi j}{n})$ abbiamo il seguente valore approssimato di c_k:

$$\begin{aligned}\hat{c}_k &= \frac{1}{2\pi}\cdot\frac{2\pi}{n}(\frac{1}{2}\cdot 2z_0 + \sum_{j=1}^{n-1} z_j e^{-ik\frac{2\pi j}{n}}) \\ &= \frac{1}{n}(z_0 + \sum_{j=0}^{n} z_j \overline{w}^{jk}),\end{aligned}$$

dove $w = e^{\frac{2\pi i}{n}}$. I $\hat{c}_k$ così ottenuti sono proprio gli u_k della (5.5).

5.2 Convoluzione

Siano $u = (u_0, u_1, \ldots, u_{n-1})$ e $v = (v_0, v_1, \ldots, v_{n-1})$ due $n-$ple di numeri complessi. Il *prodotto di convoluzione* o semplicemente la *convoluzione* delle due $n-$ple, e che si denota con $u * v$ è la $n-$pla che ha come coefficienti

$$c_k = \sum_{i+j\equiv k \bmod n} u_i v_j, \tag{5.7}$$

$k = 0, 1, \ldots, n-1$. In forma esplicita:

$$\begin{aligned} c_0 &= u_0v_0 + u_1v_{n-1} + u_2v_{n-2} + \cdots + u_{n-1}v_1, \\ c_1 &= u_0v_1 + u_1v_0 + u_2v_{n-1} + \cdots + u_{n-1}v_2, \\ &\vdots \\ c_{n-1} &= u_0v_{n-1} + u_1v_{n-2} + u_2v_{n-3} + \cdots + u_{n-1}v_0, \end{aligned} \tag{5.8}$$

ovvero:

$$u * v = Mu,$$

dove M è la matrice dei v_i. La (5.7) si può anche scrivere:

$$c_k = \sum_{i=0}^{n-1} u_i v_{k-i}, \tag{5.9}$$

prendendo gli indici modulo n. Siano ora $z = Fu$ e $x = Fv$; il $k-$esimo coefficiente di z e di x è, rispettivamente,

$$z_k = \sum_{s=0}^{n-1} u_s w^{ks},\ x_k = \sum_{t=0}^{n-1} v_t w^{kt}. \tag{5.10}$$

Consideriamo la convoluzione $z * x$; per il $k-$esimo coefficiente di questo prodotto si ha:

$$\begin{aligned} y_k &= \sum_{i=0}^{n-1} z_i x_{k-i} = \sum_{i=0}^{n-1}(\sum_{s=0}^{n-1} u_s w^{is}\cdot\sum_{t=0}^{n-1} v_t w^{(k-i)t}) \\ &= \sum_{s,t=0}^{n-1} u_s v_t w^{kt}.\sum_{i=0}^{n-1} w^{is}w^{-it} = n\sum_{s=0}^{n-1} u_s v_s w^{ks}, \end{aligned} \tag{5.11}$$

dove l'ultima uguaglianza segue dalle relazioni di ortogonalità. Vediamo allora che il $k-$esimo elemento della $n-$pla $z*x$ è uguale a n volte il $k-$esimo elemento della $n-$pla $F(u \cdot v)$, dove il prodotto $u \cdot v$ è la $n-$pla $(u_0 v_0, u_1 v_1, \ldots, u_{n-1} v_{n-1})$, cioè la $n-$pla dei prodotti termine a termine. Dunque,

$$F(u) * F(v) = nF(u \cdot v). \tag{5.12}$$

Da questa uguaglianza si deduce una regola per il calcolo della convoluzione. Si ha infatti, dalla $u = F(F^{-1}u)$, e analogamente per v,

$$u * v = F(F^{-1}u) * F(F^{-1}v) = nF[(F^{-1}u) \cdot (F^{-1}v)], \tag{5.13}$$

ovvero, *il calcolo di una convoluzione si ottiene mediante due trasformate di Fourier più una trasformata inversa.* Dalla stessa formula, o direttamente dalla (5.9), si ha anche che $u * v = v * u$, cioè che *il prodotto di convoluzione tra due $n-$ple di numeri complessi è commutativo.* La (5.13) si può anche scrivere:

$$F^{-1}(u * v) = nF^{-1}(u) \cdot F^{-1}(v),$$

ovvero, a meno del fattore n, *la trasformata di Fourier del prodotto di convoluzione è il prodotto componente per componente delle trasformate dei fattori.*

Il prodotto di convoluzione di due $n-$ple u e v nasce nel modo seguente. Consideriamo le due $n-$ple come le $n-$ple dei coefficienti di due polinomi u e v in w di grado $n-1$:

$$\begin{aligned} u &= u_0 + u_1 w + \cdots + u_{n-1} w^{n-1}, \\ v &= v_0 + v_1 w + \cdots + v_{n-1} w^{n-1}. \end{aligned}$$

Tenuto conto del fatto che $w^n = 1$, il prodotto uv dei due polinomi è il polinomio in w che ha ancora grado $n-1$ e che ha come coefficienti i c_k della (5.9).

Anche il prodotto di due polinomi in una indeterminata x si può ottenere come una convoluzione. La cosa non si può tuttavia fare direttamente: se g e h sono due polinomi di grado $n-1$, la convoluzione delle $n-$ple dei loro coefficienti è ancora una $n-$pla, mentre il prodotto gh è un polinomio di grado $2n-2$, e dunque i suoi coefficienti formano una $(2n-1)-$pla. Si ricorre allora ad un artificio: si considerano g ed h come polinomi di grado apparente $2n-2$, aggiungendo gli $n-1$ monomi $0 \cdot x^n$, $0 \cdot x^{n+1}$, $\ldots$, $0 \cdot x^{2n-2}$:

$$\begin{aligned} u &= (u_0, u_1, \ldots, u_{n-1}, u_n, u_{n+1}, \ldots, u_{2n-2}), \\ v &= (v_0, v_1, \ldots, v_{n-1}, v_n, v_{n+1}, \ldots, v_{2n-2}), \end{aligned}$$

con $u_i = v_i = 0$, per $i \geq n$. Dalla (5.7), con $2n-1$ al posto di n si ha che i termini $u_i v_j$ con $i + j \geq 2n-1$ sono tutti zero, in quanto uno almeno tra i e j deve essere $\geq n$ (altrimenti $i + j < 2n-2$) e dunque il corrispondente

u_i o v_j è zero. La (5.7) diventa allora $c_k = \sum_{i+j=k} u_i v_j$, che è la formula che dà il coefficiente $k-$esimo del polinomio prodotto di g e h. In questo modo, il prodotto di due polinomi si ottiene per convoluzione dei loro coefficienti.

Vediamo ora come i coefficienti y_k del prodotto di convoluzione $z * x$ dati dalla (5.11) si possono ottenere operando un'opportuna trasformazione lineare su z. Essendo i v_s i coefficienti di Fourier della $x = Fv$ abbiamo:

$$nv_s = x_0 + x_1\overline{w}^s + x_2\overline{w}^{2s} \cdots + \cdots + x_{n-1}\overline{w}^{(n-1)s},$$

o, in forma equivalente,

$$nv_s = x_0 + x_{n-1}w^s + x_{n-2}w^{2s} + \cdots + x_1 w^{(n-1)s}.$$

Poniamo $x_0 = a_0$, $x_{n-i} = a_i$; si ha:

$$nv_s = a_0 + a_1 w^s + a_2 w^{2s} + \cdots + a_{n-1}w^{(n-1)s}.$$

Se:

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}, \tag{5.14}$$

allora:

$$\begin{aligned} y_k &= n\sum_{s=0}^{n-1} u_s v_s w^{ks} = \sum_{s=0}^{n-1} nv_s \cdot u_s w^{ks} \\ &= \sum_{s=0}^{n-1} f(w^s)u_s \cdot w^{ks}. \end{aligned}$$

I termini $f(w^s)u_s$ sono le componenti del vettore Az ottenuto trasformando z mediante la matrice:

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{pmatrix}. \tag{5.15}$$

Il risultato contenuto nella (5.11) si può allora esprimere nel modo che segue:

Teorema 5.3. *Se $u_0, u_1, \dots, u_{n-1}$ sono i coefficienti di Fourier di z, e se $z' = Az$, dove A è la matrice* 5.15*, allora i coefficienti di Fourier di z' sono:*

$$u_0 f(1), u_1 f(w), \dots, u_s f(w^s), \dots, u_{n-1} f(w^{n-1}),$$

dove $f(x)$ è il polinomio (5.14).

5.3 Matrici circolanti

Una matrice come la (5.15) si chiama *circolante*: le sue righe si ottengono permutando circolarmente la prima. Si scrive:

$$A = circ(a_0, a_1, \ldots, a_{n-1}).$$

Si osservi che una matrice $A = (a_{i,j})$ è circolante se e solo se $a_{i,j} = a_{i+1,j+1}$ (indici mod n). Il Teorema 5.3 dice che se A è una tale matrice, allora $u' = F^{-1}z' = F^{-1}Az = F^{-1}AF(u) = \{u_s f(w^s)\}$, cioè:

$$F^{-1}AF \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{bmatrix} = \begin{pmatrix} f(1) & & & \\ & f(w) & & \\ & & \ddots & \\ & & & f(w^{n-1}) \end{pmatrix} \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{bmatrix},$$

e poichè ciò vale per ogni $n-$pla u e ogni matrice circolante A, il Teorema 5.3 si può enunciare in questo modo:

Teorema 5.4. *La matrice di Fourier $F = F_n$ diagonalizza tutte le matrici circolanti $n \times n$:*

$$F^{-1}AF = \begin{pmatrix} f(1) & & & \\ & f(w) & & \\ & & \ddots & \\ & & & f(w^{n-1}) \end{pmatrix}, \tag{5.16}$$

dove $A = circ(a_0, a_1, \ldots, a_{n-1})$ e $f(x)$ è il polinomio (5.14). $\diamondsuit$

Abbiamo visto che le colonne $v_0, v_1, \ldots, v_{n-1}$ della matrice F formano una base dello spazio vettoriale di dimensione n sui complessi C^n; la F è dunque la matrice che fa passare dalla base $(1, 0, \ldots, 0)$,$(0, 1, 0, \ldots, 0)$, $\ldots$,$(0, 0, \ldots, 0, 1)$ dello spazio C^n alla base $\{v_i\}$. Il Teorema 5.4 dice allora che se ϕ è la trasformazione lineare che nella base standard è rappresentata dalla matrice A, allora nella base $\{v_i\}$ la ϕ è rappresentata dalla matrice diagonale (5.16). In altri termini, $\phi(v_i) = f(w^i)v_i$, ovvero *gli autovettori di una qualunque matrice circolante A sono le colonne v_j della matrice di Fourier (essi non dipendono cioè da A), e gli autovalori corrispondenti a $v_0, v_1, \ldots, v_{n-1}$ sono, rispettivamente, $f(1), f(w), \ldots, f(w^{n-1})$, dove $f(x)$ è il polinomio* (5.14).

Nota. 1. I numeri $f(w^i)$ possono non essere tutti distinti.

2. La matrice M dei v_i della (5.8) è circolante.

Sussiste anche il viceversa del Teorema 5.4.

Teorema 5.5. *Sia $D = diag\{\lambda_0, \lambda_1, \ldots, \lambda_{n-1}\}$ una matrice diagonale (con i λ_i non necessariamente tutti distinti). Allora la matrice $A = FDF^{-1}$ è circolante.*

Dim. Esiste ed è unico il polinomio $f(x)$ di grado al più $n-1$ che vale λ_i su w^i. Per il Teorema 5.4, la matrice circolante $A = \text{circ}(a_0, a_1, \ldots, a_{n-1})$, dove gli a_i sono i coefficienti di $f(x)$, è tale che:

$$F^{-1}AF = diag\{f(1), f(w), \ldots, f(w^{n-1})\}.$$

Ma questa matrice diagonale è proprio la matrice D, e il risultato segue. $\diamondsuit$

Dalla (5.16) si ha $\det A = \prod_{i=0}^{n-1} f(w^i)$ e poichè i numeri w^i sono le radici di $x^n - 1$ si ha:

Teorema 5.6. *Il determinante di una matrice circolante è il risultante*:

$$\det A = R(x^n - 1, f(x)) = a_{n-1}^n \prod_{i=0}^{n-1} ({\alpha_i}^n - 1),$$

dove $f(x)$ è il polinomio (5.14) *e α_i le sue radici.* $\diamondsuit$

Siano ora $A = circ(a_0, a_1, \ldots, a_{n-1})$ e $B = circ(b_0, b_1, \ldots, b_{n-1})$ due matrici circolanti. La prima riga del prodotto AB è la $n-$pla $(c_0, c_1, \ldots, c_{n-1})$, dove:

$$\begin{aligned}
c_0 &= a_0b_0 + a_1b_{n-1} + a_2b_{n-2} + \cdots + a_{n-1}b_1, \\
c_1 &= a_0b_1 + a_1b_0 + a_2b_{n-1} + \cdots + a_{n-1}b_2, \\
&\vdots \\
c_{n-1} &= a_0b_{n-1} + a_1b_{n-2} + a_2b_{n-3} + \cdots + a_{n-1}b_0.
\end{aligned}$$

Ricordando la (5.8) si riconosce qui la convoluzione $a * b$. La seconda riga di AB ha come elementi:

$$\begin{aligned}
c'_0 &= a_{n-1}b_0 + a_0b_{n-1} + a_1b_{n-2} + \cdots + a_{n-2}b_1, \\
c'_1 &= a_{n-1}b_1 + a_0b_0 + a_1b_{n-1} + \cdots + a_{n-2}b_2, \\
&\vdots \\
c'_{n-1} &= a_{n-1}b_{n-1} + a_0b_{n-2} + a_1b_{n-3} + \cdots + a_{n-2}b_0,
\end{aligned}$$

e quindi $c'_0 = c_{n-1}, c'_1 = c_0, c'_2 = c_1, \ldots, c'_{n-1} = c_{n-2}$. Le prime due righe di AB sono allora:

$$AB = \begin{pmatrix} c_0 & c_1 & c_2 & \ldots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \ldots & c_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

Analogamente, $c''_0 = c_{n-2}, c''_1 = c_{n-1}, \ldots, c''_{n-1} = c_{n-3}$, ecc. Si vede così che AB è la matrice circolante $circ(c_0, c_1, \ldots, c_{n-1})$. Dunque:

Teorema 5.7. *Il prodotto di due matrici circolanti di numeri complessi è ancora circolante. Inoltre, questo prodotto è commutativo perchè tale è la convoluzione.* $\diamondsuit$

Tra le matrici circolanti gioca un ruolo particolare la matrice:

$$\sigma = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

Se $u = (u_0, u_1, \ldots, u_{n-1})$ è un vettore, si ha $\sigma u = (u_1, u_2, \ldots, u_{n-1}, u_0)$; la σ determina dunque sui coefficienti la permutazione circolare (che indichiamo con lo stesso simbolo σ usato per la matrice):

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & \ldots & n-2 & n-1 \\ 1 & 2 & 3 & \ldots & n-1 & 0 \end{pmatrix},$$

che scriviamo anche come $\sigma = (0, 1, 2, \ldots, n-1)$. Si osservi che $\sigma^{-1} = \sigma^{n-1}$, sia per la matrice che per la permutazione, e che per la matrice $\sigma^{-1} = \sigma^t$. Inoltre, per ogni matrice $A = (a_{i,j})$ si ha $\sigma^{-1} A \sigma = (a_{i+1,j+1})$ (indici mod n), in quanto $A\sigma$ si ottiene da A permutando le colonne secondo la permutazione σ (la prima prende il posto della seconda, la seconda della terza,..., l'ultima della prima): dunque, l'elemento $a_{i,j}$ va nell'elemento $a_{i,j+1}$. La moltiplicazione a sinistra per σ^{-1} permuta le righe secondo lo stesso principio. Dunque, $a_{i,j}$ va in $a_{i+1,j+1}$ con $\sigma^{-1} A \sigma$.

Poichè σ è circolante, anche le sue potenze lo sono (Teorema 5.7). Ora, se A è una matrice circolante qualunque si ha $A\sigma = \sigma A$, in quanto due matrici circolanti permutano. Viceversa, sia A una matrice che permuta con σ; allora, $\sigma^{-1} A \sigma = A$, e pertanto, per quanto visto sopra, $a_{i,j} = a_{i+1,j+1}$. In altre parole, *A è circolante se e solo se permuta con σ*. Questo fatto si può vedere come caso particolare del seguente. Poichè le potenze di σ si ottengono da σ spostando verso l'alto la diagonale degli 1, si vede facilmente che se $A = circ(a_0, a_1, \ldots, a_{n-1})$, allora A è un polinomio in σ:

$$A = a_0 + a_1\sigma + a_2\sigma^2 + \cdots + a_{n-1}\sigma^{n-1},$$

e viceversa, se A è di questa forma, poichè ogni addendo è circolante è chiaro che anche A lo è. Dunque, *A è circolante se e solo se è un polinomio in σ.*

Per la matrice σ, il polinomio (5.14) è $f(x) = x$, e dunque dalla (5.16) si ha che *gli autovalori di σ sono le radici $n-$esime dell'unità* $1, w, \ldots, w^{n-1}$.

5.4 La trasformata di Fourier rapida (FFT)

Il calcolo di un polinomio in un punto richiede, col metodo di Horner (Cap. 1, §1.3) n moltiplicazioni; se si vogliono i valori del polinomio in n punti sono allora necessarie con questo metodo n^2 moltiplicazioni. L'interpolazione in n punti richiede anch'essa un numero di moltiplicazioni dell'ordine di n^2, come pure, come si vede dalla (5.8), la convoluzione. Se gli n punti sono le radici $n-$esime dell'unità $1, w, \ldots, w^{n-1}$, l'interpolazione si riduce, come visto nel Teorema 5.2, al calcolo di un polinomio negli n punti $1, \overline{w}, \ldots, \overline{w}^{n-1}$, e così pure, per via della (5.13), la convoluzione, in quanto la trasformata di Fourier è il calcolo di un polinomio nelle $\overline{w}^k$. Se ora n è una potenza di 2, $n = 2^l$, questo calcolo si può organizzare in modo da ridurre il numero di operazioni[5] da n^2 a $n \log n$. Per questo motivo, al procedimento che ora illustreremo viene dato il nome di *trasformata di Fourier rapida* (FFT).[6] Osserviamo che la $n-$pla $1, \overline{w}, \ldots, \overline{w}^{n-1}$ coincide con la $n-$pla $1, w^{n-1}, \ldots, w$, e dunque il calcolo nelle $\overline{w}^k$ coincide con quello nelle w^k a meno dell'ordine.

Si vogliono dunque il valori di un polinomio di grado $n-1$:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$$

nei punti $1, w, w^2, \ldots, w^{n-1}$, con $n = 2^l$. L'osservazione da fare è che essendo n pari, il quadrato di una radice $n-$esima dell'unità è una radice $\frac{n}{2}-$esima, in quanto:

$$((w^k)^2)^{\frac{n}{2}} = w^{kn} = 1.$$

Per sfruttare quasto fatto, scriviamo il polinomio separando le potenze pari da quelle dispari:

$$\begin{aligned} f(x) &= (a_0 + a_2 x^2 + \cdots + a_{n-2} x^{2\frac{n-2}{2}}) + x(a_1 + a_3 x^2 + \cdots + a_{n-1} x^{2\frac{n-2}{2}}) \\ &= f_1(x^2) + x f_2(x^2) = f_1(y) + x f_2(y), \end{aligned}$$

riducendo così il calcolo di $f(x)$ nelle radici $n-$esime dell'unità a quello di due polinomi $f_1(y)$ e $f_2(y)$ di grado $\frac{n}{2} - 1$, nelle radici $\frac{n}{2}-$esime dell'unità, più n moltiplicazioni (quelle di x per $f_2(y)$).

Essendo n una potenza di 2, il procedimento si può ripetere su f_1 e f_2, ottenendo:

$$f(x) = f_{11}(z) + y f_{12}(z) + x(f_{21}(z) + y f_{22}(z)),$$

e così di seguito. Arriviamo in questo modo a 2^{l-1} polinomi di primo grado, e infine a $n = 2^l$ polinomi di grado 0, cioè le costanti a_i coefficienti del polinomio di partenza $f(x)$, da calcolare nelle radici $1-$esime dell'unità, cioè in 1. Ma

[5] Per "operazioni" intendiamo d'ora in poi le moltiplicazioni.

[6] Acronimo dell'inglese Fast Fourier Transform.

trattandosi di costanti, il valore è sempre a_i, cioè non vi sono operazioni da fare.

Esempio. $n = 8$.

$$\begin{aligned} f(x) &= a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_7x^7 \\ &= (a_0 + a_2x^2 + a_4x^4 + a_6x^6) + x(a_1 + a_3x^2 + a_5x^4 + a_7x^6) \\ &= a_0 + a_4x^4 + x^2(a_2 + a_6x^4) + x(a_1 + a_5x^4 + x^2(a_3 + a_7x^4)) \\ &= a_0 + x^4(a_4) + x^2(a_2 + x^4(a_6)) + x(a_1 + x^4(a_5) + x^2(a_3 + x^4(a_7))). \end{aligned}$$

Abbiamo così due polinomi di grado $3 = \frac{8}{2} - 1$ in x^2; posto $x^2 = y$ si ha:

$$f_1(y) = a_0 + a_2y + a_4y^2 + a_6y^3, \quad f_2(y) = a_1 + a_3y + a_5y^2 + a_7y^3.$$

Ognuno dei due si spezza in due polinomi di grado $1 = \frac{8}{4} - 1$ in y^2, (e dunque in x^4); posto $z = y^2$ si ha:

$$f_{11}(z) = a_0 + a_4z, \ f_{12}(z) = a_2 + a_6z, \ f_{21}(z) = a_1 + a_5z, \ f_{22} = a_3 + a_7z,$$

e ognuno di questi in due polinomi di grado $0 = \frac{8}{8} - 1$, in tutto otto, che sono gli otto coefficienti del polinomio. Scriviamo allora:

$$f(x) = a_0 + a_4z + y(a_2 + a_6z) + x(a_1 + a_5z + y(a_3 + a_7z)).$$

Per ogni valore di $x = 1, w, \ldots, w^{n-1}$, $z = x^4$ è una radice quadrata dell'unità, e dunque $z = \pm 1$ (ed entrambi i valori sono assunti: per $x = w^k$ è $z = \pm 1$ a seconda che k sia pari o dispari). Vi sono dunque da fare 4 prodotti per -1 e 1, e dunque 8 prodotti (ma vedi oltre). Analogamente, y è una radice quarta, e dunque $y = 1, -1, i, -i$. Per ognuno di questi valori di y abbiamo un valore di $z = y^2$ e quindi un solo prodotto $y(a_2 + a_6z)$; analogamente per $y(a_3 + a_7z)$, e perciò in tutto 8 prodotti. Resta il prodotto per x, da fare 8 volte, una per ogni radice dell'unità. In totale dunque $8 \cdot 3 = 24$ prodotti, cioè 8 prodotti per ciascuno dei 3 livelli in cui si è suddiviso il calcolo.

In generale, per passare da un polinomio di grado $n - 1$, cioè con n coefficienti, a n polinomi di grado 0, cioè con un coefficiente, dividendo ogni volta per 2, il numero di passi che si compiono è $\log n$. Come visto nell'esempio, occorre fare n operazioni per ciascun passo, e dunque il costo sarà di $n \log n$ operazioni. Torneremo nel prossimo paragrafo su questo problema.

Va osservato che il costo ora considerato riguarda lo schema di calcolo, più che il calcolo effettivo. Nell'esempio precedente, il numero di operazioni è molto inferiore a 24. Intanto, i prodotti per le radici quadrate dell'unità 1 e -1 non sono da effettuare; basta infatti prendere semplicemente il coefficiente a da moltiplicare o il suo opposto $-a$. Nel computo precedente questi prodotti

contribuivano per un numero di 14 operazioni: 1 e -1 sono infatti radici quadrate, quarte e ottave dell'unità, e dunque intervenivano 2 volte per z (e perciò 8 volte in tutto), 2 volte per y (4 volte) e 2 volte per x. Da 24 si scende cosí a 10 operazioni. Il prodotto per $-i$ compare 3 volte (2 come radice quarta e 1 come radice ottava) e poichè lo z corrispondente è lo stesso di quello per i, basta prendere l'opposto del prodotto per i risparmiando 3 operazioni. Analogamente, si possono evitare i prodotti per $w^5 = -w$ e $w^7 = -w^3$. Restiamo infine con le 5 operazioni:

$$w(a_1 - a_5), w^3(a_1 - a_5), i(a_2 - a_6), i(a_3 - a_7), i(a_1 + a_5).$$

Riassumiamo il calcolo per $n = 8$:

$$\begin{aligned}
f(1) &= a_0 + a_4 + a_2 + a_6 + a_1 + a_5 + a_3 + a_7, \\
f(w) &= a_0 - a_4 + i \cdot (a_2 - a_6) + w \cdot ((a_1 - a_5) + i \cdot (a_3 - a_7)), \\
f(w^2) &= a_0 + a_4 - 1 \cdot (a_2 + a_6) + i \cdot ((a_1 + a_5) - 1 \cdot (a_3 + a_7)), \\
f(w^3) &= a_0 - a_4 - i \cdot (a_2 - a_6) + w^3 \cdot ((a_1 - a_5) - i \cdot (a_3 - a_7)),
\end{aligned}$$

e a partire da $f(w^4)$ ritroviamo valori già noti, ricordando che $w^4 = -1$, $w^5 = w^4 w = -w$, $w^6 = w^4 w^2 = -i$ e $w^7 = -w^3$:

$$\begin{aligned}
f(w^4) &= a_0 + a_4 + a_2 + a_6 - 1 \cdot (a_1 + a_5 + a_3 + a_7), \\
f(w^5) &= a_0 - a_4 + i \cdot (a_2 - a_6) - w \cdot ((a_1 - a_5) + i \cdot (a_3 - a_7)), \\
f(w^6) &= a_0 + a_4 - 1 \cdot (a_2 + a_6) - i \cdot ((a_1 + a_5) - 1 \cdot (a_3 + a_7)), \\
f(w^7) &= a_0 - a_4 - i \cdot (a_2 - a_6) - w^3 \cdot ((a_1 - a_5) - i \cdot (a_3 - a_7)).
\end{aligned}$$

L'ordine in cui compaiono i coefficienti del polinomio alla fine del processo è quello che si ottiene dall'ordine iniziale operando sugli indici di $a_0, a_1, \ldots, a_{n-1}$ quella che si chiama la *bit reversing permutation*. Essa si ottiene in questo modo. Si scrivono i numeri 0,1,...,$n-1$ in base 2, usando quindi solo le cifre 0 e 1 (i *bit*), e si legge poi ciascun numero nell'ordine inverso. Ad esempio, per $n = 8$ i numeri:

$$0, 1, 2, 3, 4, 5, 6, 7,$$

si scrivono:

$$000, 001, 010, 011, 100, 101, 110, 111.$$

Invertendo i bit si ha:

$$000, 100, 010, 110, 001, 101, 011, 111,$$

cioè la successione:

$$0, 4, 2, 6, 1, 5, 3, 7,$$

come appunto visto nell'esempio.

La bit reversing permutation, che denotiamo per n numeri con P_n, si può ottenere ricorsivamente in questo modo (*algoritmo di Buneman*): ottenuta la P_n, la P_{2n} si ottiene raddoppiando i numeri nell'ordine dato dalla P_n (ottenendo così i primi n numeri, i pari) e aggiungendo 1 a ciascuno di questi (ottenendo i restanti numeri, i dispari). Così, partendo da $n = 2$,

$$\begin{array}{l} \underbrace{0\ 1} \\ \quad \downarrow \times 2 \\ \underbrace{0\ 2} \overset{+1}{\rightarrow} 1\ 3 \\ \qquad \downarrow \times 2 \\ \underbrace{0\ 4\ 2\ 6} \overset{+1}{\rightarrow} 1\ 5\ 3\ 7 \\ \qquad\qquad \downarrow \times 2 \\ \underbrace{0\ 8\ 4\ 12\ 2\ 10\ 6\ 14} \overset{+1}{\rightarrow} 1\ 9\ 5\ 13\ 3\ 11\ 7\ 15 \end{array}$$

ecc. Che l'algoritmo funzioni si vede facilmente in questo modo. Sia m un intero, $m \in \{0, 1, \ldots, n-1\}$, e sia:

$$m = a_1 a_2 \cdots a_r$$

la scrittura binaria di m ($a_i = 0, 1$). Allora:

$$P(m) = a_r \cdots a_2 a_1,$$

e raddoppiando:

$$2P(m) = a_r \cdots a_2 a_1 0,$$

che è l'inversa di

$$m = 0 a_1 a_2 \cdots a_r, \tag{5.17}$$

considerando m come elemento di $\{0, 1, \ldots, 2n-1\}$. Si noti che, poichè cominciano con 0, i numeri (5.17) descrivono i primi n numeri di $\{0, 1, \ldots, 2n-1\}$. Inoltre:

$$2P(m) + 1 = a_r \cdots a_2 a_1 1,$$

che è l'inversa di:

$$m = 1 a_1 a_2 \cdots a_r,$$

descrive gli ultimi n numeri di $\{0, 1, \ldots, 2n-1\}$.

Gli a_i che compaiono nell'output dell'algoritmo sono i coefficienti delle potenze x^i (con lo stesso i). Per ridursi alla forma che contiene solo le potenze $\frac{n}{2}, \frac{n}{4}, \ldots, 1$ di x si scrive il polinomio nell'ordine dato dall'algoritmo e si mette in

evidenza una potenza x^k nella somma dei monomi $a_h x^h$ con $h > k$ che seguono $a_k x^k$. Ad esempio, con $n = 16$, abbiamo:

$$a_0 + a_8 x^8 + a_4 x^4 + \cdots + a_{15} x^{15},$$

e mettendo in evidenza come detto si ha:

$$\begin{array}{rcl} a_0 & + & a_8 x^8 + x^4(a_4 + a_{12} x^8) + x^2(a_2 + a_{10} x^8 + a_6 x^4 + a_{14} x^{12}) \\ & + & x(\ldots), \end{array}$$

dove i puntini indicano la somma della riga precedente con gli indici aumentati di 1. Si ripete poi l'operazione, ove necessario, all'interno delle parentesi (ora i monomi non sono più $a_h x^h$ bensí $a_h x^{h-k}$); cosí per la parentesi che moltiplica x^2 abbiamo:

$$a_2 + a_{10} x^8 + x^4(a_6 + a_{14} x^8).$$

5.5 La complessità $n \log n$

Per misurare l'efficacia di un algoritmo si studia il *caso peggiore*, quello cioè per il quale il tempo di esecuzione è massimo ("tempo" significa qui numero di operazioni da eseguire). Con questo approccio si cerca di stabilire *la dipendenza funzionale* $g(n)$ dell'algoritmo dal numero degli input, senza tener conto di costanti che possono provenire dalle proprietà di particolari input, dal tipo di esecuzione (caratteristiche del computer, ad esempio), o dal programma che può essere più o meno intelligente. L'ordine di grandezza della funzione $g(n)$ è la *complessità di calcolo* dell'algoritmo.

Lo schema di calcolo di un polinomio nella radici dell'unità visto sopra è di quelli che consistono nel suddividere un problema in problemi più piccoli, indipendenti l'uno dall'altro, ripetendo poi la suddivisione per ciascuno di questi fino ad arrivare ad un certo numero di problemi la cui soluzione è banale[7]. Per trovare la soluzione del problema dato si combinano poi le soluzioni parziali con un costo che, ad ogni passo, è lineare (ad ogni passo si visitano i dati una volta sola).

Così nel nostro caso, C_n, la complessità di calcolo per un input di grandezza $n = 2^l$ (gli n coefficienti del polinomio da calcolare nelle n radici dell'unità), è uguale a 2 volte quella del calcolo di 1 polinomio con $n/2$ coefficienti (i polinomi f_1 e f_2) più n moltiplicazioni (quelle per le n radici dell'unità):

$$C_n = 2C_{\frac{n}{2}} + n,$$

[7] La tecnica di suddividere il problema in problemi più piccoli e indipendenti va sotto il nome di "divide et impera" ("divide and conquer" in inglese).

con $C_1 = 0$ (calcolo di costanti in 1). Ripetendo l'operazione con f_1 e f_2 si ha la stessa uguaglianza con $n/2$ al posto di n: $C_{\frac{n}{2}} = 2C_{\frac{n}{4}} + \frac{n}{2}$, che sostituita nella precedente dà $C_n = 4C_{\frac{n}{4}} + 2n$, e in generale $C_n = kC_{\frac{n}{2^k}} + kn$. Ora, $n = 2^l$, e con $k = l$ si ha:

$$C_n = kC_1 + l \cdot 2^l = l \cdot 2^l,$$

in quanto $C_1 = 0$. Ne segue:

$$C_n = 2^l l = n \log n.$$

In un problema in cui ad ogni passo occorra visitare solo la metà degli input, come nel caso del calcolo di un polinomio nelle radici dell'unità, il calcolo ora visto fornisce il valore $\frac{1}{2} n \log n$.

Come abbiamo visto, il numero di operazioni in un caso concreto può essere inferiore a $n \log n$. Dicendo che un dato problema si può risolvere effettuando $n \log n$ operazioni, che si tratta cioè di un problema di *complessità* $n \log n$, si intende affermare che esso appartiene alla classe di problemi per la cui soluzione si applica lo schema visto sopra, schema che richiede appunto $n \log n$ operazioni. La trasformata di Fourier è uno di questi problemi.

Nota bibliografica

[**AHU**] Cap. 7, [**BCLR**] Cap. 4, [**Se**] Cap. 41, [**St**] §4.2 e 5.5, [**Da**] e [**VL**] (quest'ultimo contiene una ricchissima bibliografia). Per le questioni di complessità algoritmica [**Se**] e [**BCLR**].

5.6 Appendice

La trasformata di Fourier discreta si inserisce in modo naturale nella teoria dei gruppi abeliani (finiti) e delle loro algebre (che definiremo qui sotto). La *teoria delle rappresentazioni* di questi gruppi è essenzialmente un modo di interpretare questa trasformata, come ora vedremo.

5.6.1 L'algebra di un gruppo

Sia $G = \{g_0 = 1, g_1, \ldots, g_{n-1}\}$ un gruppo finito (non necessariamente abeliano) di ordine n, $\mathcal{C}$ il campo complesso, e sia $\mathcal{C}[G]$ l'insieme di tutte le funzioni:

$$u : G \longrightarrow \mathcal{C}.$$

$\mathcal{C}[G]$ assume struttura di spazio vettoriale definendo:

$$(u+v)(g) = u(g) + v(g),$$
$$(\alpha u)(g) = \alpha(u(g)), \alpha \in \mathcal{C}.$$

Il vettore zero di questo spazio è la funzione u che vale 0 su tutti i $g \in G$. Una base di $\mathcal{C}[G]$ è data dalle n funzioni u_g così definite:

$$u_g(h) = \begin{cases} 1, & \text{se } h = g; \\ 0, & \text{altrimenti.} \end{cases}$$

Ogni $u \in \mathcal{C}[G]$ si può infatti scrivere come:

$$u = \sum_{g \in G} u(g) u_g, \tag{5.18}$$

e se una tale combinazione lineare è il vettore zero, tutti i coefficienti sono zero in quanto $0 = u(h) = \sum_{g \in G} u(g) u_g(h) = u(g)$. Si tratta dunque di uno spazio vettoriale di dimensione l'ordine $|G|$ del gruppo G.

In $\mathcal{C}[G]$ si può poi introdurre un prodotto come segue. Se $u, v \in \mathcal{C}[G]$, allora sia uv l'elemento di $\mathcal{C}[G]$ che su $g \in G$ ha il valore definito in questo modo: per ogni $h \in G$ si consideri $h^{-1}g$ e si ponga:

$$uv(g) = \sum_{h \in G} u(h) v(h^{-1}g). \tag{5.19}$$

E' chiaro che se $\alpha \in \mathcal{C}$ allora $\alpha(uv) = (\alpha u)v = u(\alpha v)$. Inoltre, valgono le proprietà associativa e distributiva, come si verifica facilmente, ed esiste un elemento unità: la funzione che vale 1 sull'unità del gruppo e zero altrove. Si tratta dunque di un'algebra, l'*algebra gruppo* del gruppo G.

Consideriamo ora l'applicazione $G \longrightarrow \mathcal{C}[G]$ definita da $g \to u_g$. Si osservi che

$$u_g u_h(t) = \sum_{s \in G} u_g(s) u_h(s^{-1}t),$$

e poichè se $s \neq g$ o $s^{-1}t \neq h$ i termini della somma valgono zero, resta solo il termine per $s = g$ e $s^{-1}t = h$, cioè $g^{-1}t = h$. In altre parole,

$$u_g u_h(t) = \begin{cases} 1, & \text{se } t = gh; \\ 0, & \text{altrimenti.} \end{cases}$$

e dunque, per definizione, $u_g u_h = u_{gh}$. Gli elementi u_g si combinano dunque come gli elementi g di G, e questo fatto permette di immergere G in $\mathcal{C}[G]$ mediante l'identificazione di g con u_g. $\mathcal{C}[G]$ contiene allora una copia di G, e la (5.18) si può scrivere:

$$u = \sum_{g \in G} u(g) g. \tag{5.20}$$

In questo modo $\mathcal{C}[G]$ diventa l'insieme delle combinazioni lineari formali degli elementi di G, e il prodotto (5.19) estende a queste combinazioni lineari il prodotto di G (*estensione per linearità*). Più precisamente, con u come nella (5.20) e $v = \sum_{h \in G} v(h)h$, si ha $uv = \sum_{g,h \in G} u(g)v(h)gh$. Il coefficiente in uv dell'elemento s di G, quando uv è scritto nella forma (5.20) è quello che si ottiene per $gh = s$, cioè per $h = g^{-1}s$; si tratta quindi di $\sum_{g \in G} u(g)v(g^{-1}s)$, cioè del valore definito più sopra. Si ha perciò:

$$uv = \sum_s (\sum_g u(g)v(g^{-1}s))s. \tag{5.21}$$

Nota. Si osservi che dalla $gh = s$ segue anche $g = sh^{-1}$, e dunque

$$\sum_{g \in G} u(g)v(g^{-1}s) = \sum_{h \in G} u(sh^{-1})v(h).$$

Il prodotto (5.21) è il *prodotto di convoluzione*. Si ritrova quello visto nel §5.3 considerando il caso in cui il gruppo G è ciclico, $G = \{1, g, g^2, \ldots, g^{n-1}\}$. Scrivendo infatti u_k per $u(g^k)$, e $u = \sum_{i=0}^{n-1} u_i g^i$, $v = \sum_{j=0}^{n-1} v_j g^j$, il coefficiente di g^k nel prodotto uv secondo la (5.21) è $\sum_{i=0}^{n-1} u_i v_{k-i}$, come nella (5.11).

5.6.2 Gruppi ciclici

La trasformata di Fourier interpretata nell'algebra gruppo $\mathcal{C}[G]$ di un gruppo ciclico G si riduce ad un cambiamento della base $G = \{1, g, g^2, \ldots, g^{n-1}\}$. Lo scopo di questo cambiamento è che il prodotto di convoluzione di due elementi, scritti nella nuova base, si esegue componente per componente.

Più precisamente, abbiamo, come spazio vettoriale,

$$\mathcal{C}[G] = \mathcal{C} \cdot 1 \oplus \mathcal{C}g \oplus \cdots \oplus \mathcal{C}g^{n-1},$$

e questo spazio assume una struttura di algebra mediante il prodotto di convoluzione (5.21). Scrivendo $u = \alpha_0 \cdot 1 + \alpha_1 g + \cdots + \alpha_{n-1} g^{n-1}$ e $v = \beta_0 \cdot 1 + \beta_1 \cdot g + \cdots + \beta_{n-1} \cdot g^{n-1}$, nel prodotto uv compaiono i termini $\alpha_i \beta_j g^i g^j$, $i \neq j$, cioè prodotti di termini appartenenti a componenti diverse. Cerchiamo ora una nuova base $e_0, e_1, \ldots, e_{n-1}$:

$$\mathcal{C}[G] = \mathcal{C}e_0 \oplus \mathcal{C}e_1 \oplus \cdots \oplus \mathcal{C}e_{n-1}, \tag{5.22}$$

tale che $e_i e_j = 0$ per $i \neq j$, in modo che scrivendo u e v come sopra i termini $\alpha_i \beta_j e_i e_j$, $i \neq j$, si annullino. Il prodotto di convoluzione sarà allora dato semplicemente dai prodotti delle componenti omonime.

Trasformiamo allora la base dei $\{g^i\}$ mediante la matrice $F^{-1} = \frac{1}{n}\overline{F}$, e sia $\{e_i\}$ la base che si ottiene. Allora e_i è l'elemento di $\mathcal{C}[G]$ che scritto nella forma (5.20) ha come coefficiente di g^j il numero complesso $\overline{w}^{ij}/n$:

$$e_i = \sum_{j=0}^{n-1} \frac{\overline{w}^{ij}}{n} g^j.$$

Osserviamo che

$$e_i g = w^i e_i, \tag{5.23}$$

e che da questa uguaglianza segue $e_i e_j = 0$ per $i \neq j$. Infatti, essendo $e_i e_j g = e_i g e_j$, si ha $e_i w^j e_j = w^i e_i e_j$, da cui $(w^i - w^j) e_i e_j = 0$, e per $i \neq j$ è $w^i \neq w^j$ e perciò:

$$e_i e_j = 0, \ i \neq j. \tag{5.24}$$

Inoltre,

$$\sum_{i=0}^{n-1} e_i = \frac{1}{n} \sum_{j=0}^{n-1} (\sum_{i=0}^{n-1} \overline{w}^{ij}) g^j,$$

e poichè la somma interna vale 0 per $j \neq 0$ e n per $j = 0$,

$$e_0 + e_1 + \cdots + e_{n-1} = 1. \tag{5.25}$$

Moltiplicando quest'ultima uguaglianza per e_i e ricordando la (5.24) abbiamo:

$$e_i^2 = e_i, \tag{5.26}$$

per ogni $i = 0, 1, \ldots, n-1$. Gli e_i sono dunque idempotenti ortogonali e a somma 1. Si osservi che sommando su i la (5.23) si ha $(\sum e_i)g = g = \sum w^i e_i$, cioè:

$$g = 1 \cdot e_0 + w \cdot e_1 + \cdots + w^{n-1} e_{n-1},$$

e analogamente:

$$g^k = 1 \cdot e_0 + w^k \cdot e_1 + \cdots + w^{k(n-1)} e_{n-1},$$

come d'altra parte è chiaro essendo la matrice di passaggio dalla base $\{e_i\}$ alla base $\{g^k\}$ la matrice inversa della F^{-1}, cioè la F. In generale, per

$$u = u_0 + u_1 g + \cdots + u_{n-1} g^{n-1}$$

si ha dalla (5.23):

$$u = \sum_{i=0}^{n-1} e_i u = \sum_{i=0}^{n-1} (\sum_{k=0}^{n-1} u_k w^{ik}) e_i = \sum_{i=0}^{n-1} z_i e_i,$$

(v. (5.7)), e se analogamente $v = \sum_{i=0}^{n-1} x_i e_i$ il prodotto (5.21) di u e v è

$$uv = (z_0 x_0) e_0 + (z_1 x_1) e_1 + \cdots + (z_{n-1} x_{n-1}) e_{n-1}.$$

La (5.22) è dunque una decomposizione di $\mathcal{C}[G]$ in somma diretta di anelli (nel senso detto nel Cap. I). Ciascun addendo è isomorfo al campo complesso $\mathcal{C}$ perchè la corrispondenza $\mathcal{C} \longrightarrow \mathcal{C}e_i$, se conserva ovviamente la somma, conserva anche il prodotto in quanto se $\alpha \to \alpha e_i$ e $\beta \to \beta e_i$, allora $\alpha\beta \to \alpha\beta e_i^2 = \alpha\beta e_i$, per via della (5.26). Concludendo, *l'algebra gruppo di un gruppo ciclico è un prodotto diretto di algebre isomorfe al campo complesso.* E' questo un altro modo di esprimere il senso della trasformata di Fourier.

Le matrici circolanti rientrano nel quadro delle questioni considerate in questo paragrafo. Si tratta infatti delle matrici delle trasformazioni lineari dello spazio $\mathcal{C}[G]$ ottenute moltiplicando la base $\{1, g, \ldots, g^{n-1}\}$ per un dato elemento u di $\mathcal{C}[G]$. Se $u = g$ si ottiene la trasformazione che nella base detta ha la matrice σ vista nel §5.3; moltiplicando per le potenze di g si ottengono quelle di σ. Se $u = \sum_{i=0}^{n-1} a_i g^i$ si ottiene la (5.15).

5.6.3 Il gruppo dei caratteri

Vediamo ora di estendere quanto visto nei due paragrafi precedenti al caso di un gruppo abeliano G qualunque, cioè non necessariamente ciclico. Vediamo dapprima una condizione necessaria. Se una scrittura come la (5.22) esiste per l'algebra gruppo $\mathcal{C}[G]$, con gli e_i idempotenti ortogonali, allora se $g = \sum_i \alpha_i(g) e_i$ e $h = \sum_i \alpha_i(h) e_i$, si ha $gh = \sum_i \alpha_i(g)\alpha_i(h) e_i$. Ma l'elemento gh si scrive

come $gh = \sum_i \alpha_i(gh)e_i$, e dunque, essendo gli $\{e_i\}$ una base, per l'unicità della scrittura deve essere:

$$\alpha_i(gh) = \alpha_i(g)\alpha_i(h), \tag{5.27}$$

per ogni i e $g, h \in G$. In altri termini, la corrispondenza che associa ad un elemento g di G il suo $i-$esimo coefficiente nella scrittura $g = \sum_i \alpha_i(g)e_i$ è un omomorfismo $G \longrightarrow \mathcal{C}^*$, il gruppo moltiplicativo del campo complesso $\mathcal{C}$. (Si noti che non può aversi $\alpha_i(g) = 0$ perchè essendo $1 = 1 \cdot e_0 + 1 \cdot e_1 + \cdots + 1 \cdot e_{n-1}$ è $\alpha_i(1) = 1$ per ogni i, e dunque se $\alpha_i(g) = 0$ per un certo i si avrebbe $1 = \alpha_i(1) = \alpha_i(gg^{-1}) = \alpha_i(g)\alpha_i(g^{-1}) = 0 \cdot \alpha_i(g^{-1}) = 0$). Nel caso G ciclico avevamo $\alpha_i(g^k) = w^{ik}$, e la (5.27) è verificata.

Un omomorfismo $\chi : G \longrightarrow \mathcal{C}^*$ si chiama *carattere* del gruppo abeliano G, e l'insieme dei caratteri di G è esso stesso un gruppo, rispetto all'operazione:

$$(\chi\chi')(g) = \chi(g)\chi'(g).$$

E' chiaro che questa operazione è associativa. L'elemento neutro è il carattere χ_1 che vale 1 su ogni elemento di G (carattere *principale* o *banale*), mentre l'inverso di un carattere χ è il carattere che vale su g ciò che χ vale su g^{-1}: $\chi^{-1}(g) = \chi(g^{-1})$. Questo gruppo è il *gruppo dei caratteri* di G; si denota con $\widehat{G}$.

Sussiste il seguente importante risultato, che si basa sul teorema fondamentale dei gruppi abeliani finiti (secondo il quale un gruppo abeliano finito è prodotto diretto di gruppi ciclici).

Teorema 5.8. (TEOREMA DI DUALITÀ) *I gruppi G e $\widehat{G}$ sono isomorfi.*

Dim. Se G è ciclico, $G =< g >$, un omomorfismo è determinato quando si conosce l'immagine di g. Se g è di ordine n, allora $\chi(g)^n = 1$ in quanto $\chi(g)^n = \chi(g^n) = \chi(1) = 1$. $\chi(g)$ è allora una radice $n-$esima dell'unità, e poichè queste sono in numero di n, abbiamo n possibili omomorfismi, cioè n caratteri. Se χ_k è il carattere determinato dalla radice w^k, dove w è una radice primitiva, e cioè $\chi_k : g \to w^k$, la corrispondenza $G \longrightarrow \widehat{G}$ data da

$$g^k \to \chi_k$$

è l'isomorfismo cercato. Nel caso generale, G è un prodotto diretto di gruppi ciclici, $G = G_1 \times G_2 \times \cdots \times G_t$, con $|G_i| = n_i$ e $G_i =< g_i >$. Sia g un fissato elemento di G; esso ammette un'unica scrittura $g = g_1^{k_1} g_2^{k_2} \cdots g_t^{k_t}$. Sia $h = g_1^{h_1} g_2^{h_2} \cdots g_t^{h_t}$ un generico elemento di G e w_i una radice primitiva n_i-esima dell'unità. Definiamo:

$$\chi_g : h \to w_1^{k_1 h_1} w_2^{k_2 h_2} \cdots w_t^{k_t h_t}.$$

E' chiaro che $\chi_{gg'} = \chi_g \chi_{g'}$. Se $g \neq g'$, allora $k_i \neq k'_i$ per almeno un i, e dunque $\chi_g(g_i) = w_i^{k_i} \neq w_i^{k'_i} = \chi_{g'}(g_i)$. I χ_g sono dunque, al variare di g in G, tutti distinti, e la corrispondenza $G \longrightarrow \widehat{G}$ data da:

$$g \to \chi_g$$

è l'isomorfismo cercato. Si noti che $\chi_g(h) = \chi_h(g)$. $\diamondsuit$

Nota. Analogamente, $\widehat{G} \simeq \widehat{\widehat{G}}$. Dunque $G \simeq \widehat{G}$ e $G \simeq \widehat{\widehat{G}}$. Ma mentre il primo isomorfismo non è "naturale", nel senso che per definirlo occorre scegliere una "base" di G (un g_i per ogni fattore G_i) ed esprimere gli elementi in questa base, il secondo si può definire direttamente sugli elementi:

$$g \to \hat{\chi}_g : \chi \to \chi(g),$$

cioè associando a $g \in G$ il carattere di $\widehat{G}$ che manda un carattere χ di G nel valore che esso assume su g.

Vediamo ora alcune proprietà dei caratteri.

Lemma 5.9. *Si ha:*

$$\sum_g \chi(g) = \begin{cases} n, & \text{se } \chi = \chi_1; \\ 0, & \text{altrimenti.} \end{cases}$$

Dim. Se $\chi = \chi_1$ il risultato è chiaro. Altrimenti, esiste g' tale che $\chi(g') \neq 1$. Allora, poichè gg' al variare di g in G percorre tutti gli elementi di G, si ha:

$$\sum_g \chi(g) = \sum_g \chi(gg') = \sum_g \chi(g)\chi(g') = \chi(g') \sum_g \chi(g),$$

da cui $(1 - \chi(g')) \sum_g \chi(g) = 0$, e poichè $\chi(g') \neq 1$ si ha $\sum_g \chi(g) = 0$. $\diamondsuit$

Per dualità si ottiene:

Lemma 5.10. *Si ha:*

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} n, & \text{se } g = 1; \\ 0, & \text{altrimenti.} \end{cases}$$

Dim. Sostituire nel lemma precedente χ con g, χ_1 con 1 e g' con χ'. $\diamondsuit$

Corollario 5.11. *Si ha:*

$$\sum_{\chi \in \widehat{G}} \chi(g)\chi(h^{-1}) = \begin{cases} n, & \text{se } g = h; \\ 0, & \text{altrimenti.} \end{cases}$$

Lemma 5.12. (RELAZIONI DI ORTOGONALITÀ) *Si ha:*

$$\sum_g \chi_i(g)\chi_j(g^{-1}) = \begin{cases} n, & \text{se } i = j; \\ 0, & \text{altrimenti.} \end{cases}$$

Dim. Se $i = j$, $\chi_i(g)\chi_i(g^{-1}) = \chi_i(1) = 1$, e si ha il risultato. Se $i \neq j$ esiste h tale che $\chi_i(h) \neq \chi_j(h)$; allora,

$$\begin{aligned} \sum_g \chi_i(g)\chi_j(g^{-1}) &= \sum_g \chi_i(gh)\chi_j(h^{-1}g^{-1}) \\ &= (\sum_g \chi_i(g)\chi_j(g^{-1}))(\chi_i(h)\chi_j(h^{-1})), \end{aligned}$$

da cui:

$$(1 - \chi_i(h)\chi_j(h^{-1})) \sum_g \chi_i(g)\chi_j(g^{-1}) = 0.$$

Se $\chi_i(h)\chi_j(h^{-1}) = 1$, si ha $\chi_i(h) = \chi_j(h)$, contro la scelta di h. Allora è il secondo fattore che è nullo, come si voleva. $\diamondsuit$

Nota. Se G è ciclico e generato da g, abbiamo $\chi_i(g) = w^i$, dove w è una radice primitiva $n-$esima dell'unità. La somma del lemma precedente si scrive allora $\sum_{k=1}^{n-1} \chi_i(g^k)\chi_j(g^{-k})$, e il lemma si riduce al Teorema 5.1.

Scrivendo gli elementi di G come $g_1, g_2, \ldots, g_n$ e, in corrispondenza, i caratteri come $\chi_1, \chi_2, \ldots, \chi_n$, possiamo considerare la matrice $n \times n$ il cui elemento di posto (i, j) è $\chi_i(g_j)$. Questa matrice prende il nome di *tavola dei caratteri*; la denoteremo con T. Come osservato alla fine della dimostrazione del Teorema 5.1, si ha $\chi_i(g_j) = \chi_j(g_i)$, e pertanto la T è simmetrica. Nel caso di un gruppo ciclico, la tavola dei caratteri è la matrice di Fourier.

Definiamo ora in $\mathcal{C}[G]$ il seguente prodotto scalare:

$$(u, v) = \frac{1}{n} \sum_g u(g)v(g^{-1}).$$

Il fatto che i $\chi(g)$ siano radici dell'unità implica che $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$. Il Lemma 5.12 afferma allora che tra gli elementi di $\mathcal{C}[G]$ i caratteri formano un sistema *ortonormale*:

$$(\chi_i, \chi_j) = 0, \ i \neq j, \ \ (\chi_i, \chi_i) = 1.$$

In particolare, essi sono indipendenti, ed essendo in numero di n, *i caratteri formano una base di* $\mathcal{C}[G]$, e dunque una base ortonormale. Il prodotto definito sopra è allora non degenere, e la tavola dei caratteri T risulta essere una matrice non singolare (il determinante vale ± 1). Inoltre, come nel caso della matrice di Fourier, $T^{-1} = \frac{1}{n}\overline{T}$.

Esempio. Sia $G = \{1, a, b, c\}$ il gruppo di Klein: ogni elemento è di periodo 2, e il prodotto di due elementi diversi da 1 è uguale al terzo. In questo caso essendo $g^2 = 1$ per ogni elemento di G, i $\chi_i(g)$ sono radici seconde dell'unità, e perciò valgono -1 o 1. Vi sono quattro omomorfismi $G \longrightarrow \mathcal{C}$: quello il cui nucleo è tutto G, cioè χ_1, e quelli i cui nuclei sono $\{1, a\}$, $\{1, b\}$ e $\{1, c\}$, che denotiamo rispettivamente con χ_2, χ_3 e χ_4. Si ha dunque la tavola:

$$\begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \chi_3 \\ \chi_4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & a & b & c \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \end{array}.$$

5.6.4 L'algebra di un gruppo abeliano

Abbiamo visto all'inizio del paragrafo precedente che condizione necessaria affinchè per un elemento $g \in G$ esista una scrittura del tipo $g = \sum_i \alpha_i(g) e_i$ come nel caso di un gruppo ciclico è che i coefficienti $\alpha_i(g)$ siano valori di caratteri. Vediamo ora come determinare una tale scrittura, definendo innanzi tutto gli e_i, $i = 1, 2, \ldots, n$.[8] Scelto un ordine $\chi_1, \chi_2, \ldots, \chi_n$ dei caratteri, definiamo, come nel caso ciclico:

$$e_i = \sum_g \frac{\chi_i(g^{-1})}{n} g \quad (= \sum_g \frac{\overline{\chi_i(g)}}{n} g).$$

Gli e_i cosí definiti sono idempotenti ortogonali a somma 1. La dimostrazione è analoga a quella del caso di un gruppo ciclico. Si ha infatti:

$$\sum_{i=1}^{n} e_i = \frac{1}{n} \sum_g (\sum_i \chi_i(g^{-1})) g,$$

e per il Lemma 5.10 la somma interna vale 0 per $g \neq 1$, e vale n se $g = 1$. Dunque:

$$e_1 + e_2 + \cdots + e_n = 1.$$

Inoltre, per ogni $h \in G$,

$$e_i h = \chi_i(h) e_i, \tag{5.28}$$

in quanto:

$$e_i h = \sum_g \frac{\chi_i(g^{-1})}{n} gh = \sum_s \frac{\chi_i(hs^{-1})}{n} s,$$

[8] Seguendo l'uso corrente, abbiamo denotato il carattere principale con χ_1 e non con χ_0; conseguentemente, elenchiamo in questo paragrafo gli e_i a partire da e_1, e non da e_0 come fatto in precedenza.

dove si è posto $gh = s$, e

$$\chi_i(h)e_i = \chi_i(h)\sum_g \frac{\chi_i(g^{-1})}{n}g = \sum_g \frac{\chi_i(hg^{-1})}{n}g.$$

Ne segue allora:

$$e_i e_j = 0,\ i \neq j\ ;$$

infatti $e_i e_j h = \chi_j(h)e_i e_j$, e dunque $e_i h e_j = \chi_i(h)e_i e_j$. I primi membri essendo uguali, sono uguali anche i secondi, e pertanto $(\chi_j(h) - \chi_i(h))e_i e_j = 0$. Ma per almeno un h di G si ha, per $i \neq j$, $\chi_j(h) \neq \chi_i(h)$, e dunque $e_i e_j = 0$. Da questa e dalla $\sum_i e_i = 1$ segue poi la proprietà di idempotenza $e_i^2 = e_i$.

Gli e_i formano dunque una base per l'algebra gruppo, e abbiamo perciò anche in questo caso una decomposizione (5.22). Il passaggio dalla base $\{g_i\}$ alla $\{e_i\}$ è fornito dalla trasformazione lineare che ha come matrice l'inversa della tavola dei caratteri. Un elemento g del gruppo si scrive, sommando la (5.28) su i,

$$g = \chi_1(g)e_1 + \chi_2(g)e_2 + \cdots + \chi_n(g)e_n, \tag{5.29}$$

e un generico elemento $u = \sum_g u(g)g$ di $\mathcal{C}[G]$ come $\sum_i z_i e_i$, dove il numero complesso z_i vale $\sum_g u(g)\chi_i(g)$.

Nota. Poichè vi sono $n!$ modi di ordinare gli n caratteri di G vi sono $n!$ modi di spezzare $\mathcal{C}[G]$ nel modo visto.

La corrispondenza $\sum_i z_i e_i \to (z_1, z_2, \ldots, z_n)$ stabilisce un isomorfismo tra l'algebra gruppo $\mathcal{C}[G]$ e la somma diretta di n copie del campo complesso $\mathcal{C}$:

$$\mathcal{C}[G] \simeq \mathcal{C} \oplus \mathcal{C} \oplus \cdots \oplus \mathcal{C}, \tag{5.30}$$

e vi sono $n!$ modi di stabilire un tale isomorfismo. La decomposizione (5.30) dipende solo da n, cioè solo dall'ordine del gruppo e non dalla sua struttura. In altre parole, *le algebre gruppo di tutti i gruppi abeliani di ordine n sono tra loro isomorfe.* In particolare, dato un gruppo abeliano G, nella sua algebra gruppo si trova una copia di ogni altro gruppo abeliano dello stesso ordine di G. Più precisamente, sia G' un gruppo abeliano di ordine $n = |G|$, $\mathcal{C}[G']$ la sua algebra gruppo, $\chi'_1, \chi'_2, \ldots, \chi'_n$ i caratteri di G' in un certo ordine, h un elemento di G' e

$$(\chi'_1(h), \chi'_2(h), \ldots, \chi'_n(h))$$

la $n-$pla corrispondente alla scrittura (5.29) di h in $\mathcal{C}[G']$, cioè la $n-$pla corrispondente all'elemento h nell'isomorfismo (5.30) per l'algebra $\mathcal{C}[G']$. Facciamo allora corrispondere ad h l'elemento u di $\mathcal{C}[G]$ che ha come componente $i-$esima nella base degli e_i il numero complesso $\chi'_i(h)$:

$$h \to u = \sum_i \chi'_i(h)e_i.$$

E' chiaro che se k è un altro elemento di G', e $v \in \mathcal{C}[G]$ è la sua immagine, allora l'immagine del prodotto hk è il prodotto uv delle immagini. Inoltre, l'applicazione di sopra è iniettiva in quanto nella tavola dei caratteri non vi sono mai due colonne uguali perchè si tratta di una matrice non singolare. L'immagine di G' in $\mathcal{C}[G]$ è dunque un gruppo isomorfo a G'.

Se si vuole la scrittura di u nella forma $\sum_g u(g)g$, cioè sapere qual è l'immagine secondo u di ogni $g \in G$, si può procedere in questo modo. Sappiamo che $u = \sum_i (\sum_g u(g)\chi_i(g))e_i$; dobbiamo allora determinare gli $u(g)$ in modo tale che

$$\sum_g u(g)\chi_i(g) = \chi_i'(h),$$

per $i = 1, 2, \ldots, n$. Abbiamo così un sistema di n equazioni lineari nelle n incognite $u(g)$, $g \in G$, e la matrice di questo sistema è la tavola di caratteri. Gli $u(g)$ si possono allora determinare con la regola di Cramer.

Esempio. Sia G il gruppo di Klein e G' il gruppo ciclico $C_4 = \{1, x, x^2, x^3\}$. La tavola dei caratteri del primo è stata vista nell'esempio precedente; quella del secondo è la matrice di Fourier:

$$\begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \chi_3 \\ \chi_4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & x & x^2 & x^3 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \end{array}.$$

Sia ora x l'elemento h di sopra; la quaterna che ad esso corrisponde è

$$x \to (1, i, -1, -i),$$

e se $x \to u \in \mathcal{C}[G]$, allora gli $u(g)$, $g \in G$, sono determinati dal sistema:

$$\begin{cases} u(1)\chi_1(1) + u(a)\chi_1(a) + u(b)\chi_1(b) + u(c)\chi_1(c) &= 1, \\ u(1)\chi_2(1) + u(a)\chi_2(a) + u(b)\chi_2(b) + u(c)\chi_2(c) &= i, \\ u(1)\chi_3(1) + u(a)\chi_3(a) + u(b)\chi_3(b) + u(c)\chi_3(c) &= -1, \\ u(1)\chi_4(1) + u(a)\chi_4(a) + u(b)\chi_4(b) + u(c)\chi_4(c) &= -i, \end{cases}$$

ovvero:

$$\begin{cases} u(1) + u(a) + u(b) + u(c) &= 1, \\ u(1) + u(a) - u(b) - u(c) &= i, \\ u(1) - u(a) + u(b) - u(c) &= -1, \\ u(1) - u(a) - u(b) + u(c) &= -i. \end{cases}$$

Si vede facilmente che questo sistema ha la soluzione:

$$u(1) = u(b) = 0,\ u(a) = \frac{1+i}{2},\ u(c) = \frac{1-i}{2},$$

che determina u in $\mathcal{C}[G]$. Dunque:

$$u = 0 \cdot 1 + \frac{1+i}{2}a + 0 \cdot b + \frac{1-i}{2}c = \frac{1+i}{2}a + \frac{1-i}{2}c.$$

Analogamente, per x^2 si trova, se $x^2 \to v$,

$$v(1) = v(a) = v(c) = 0,\ v(b) = 1,$$

cioè:

$$v = 0 \cdot 1 + 0 \cdot a + 1 \cdot b + 0 \cdot c = 1 \cdot b,$$

e per x^3, se $x^3 \to z$,

$$z(1) = z(b) = 0,\ z(a) = \frac{1-i}{2},\ z(c) = \frac{1+i}{2},$$

ovvero:

$$z = 0 \cdot 1 + \frac{1-i}{2}a + 0 \cdot b + \frac{1+i}{2}c = \frac{1-i}{2}a + \frac{1+i}{2}c.$$

Verifichiamo, ad esempio, che l'immagine del prodotto $x \cdot x^2$, ovvero l'immagine di x^3, e cioè z, è effettivamente uguale al prodotto delle immagini di x e x^2, e cioè uv. Quest'ultimo, calcolato secondo la (5.21), fornisce:

$$\begin{array}{l} s = 1\text{: } u(1)v(1) + u(a)v(a) + u(b)v(b) + u(c)v(c) = 0, \\ s = a\text{: } u(1)v(a) + u(a)v(1) + u(b)v(c) + u(c)v(b) = \frac{1-i}{2}, \\ s = b\text{: } u(1)v(b) + u(a)v(c) + u(b)v(1) + u(c)v(a) = 0, \\ s = c\text{: } u(1)v(c) + u(a)v(b) + u(b)v(a) + u(c)v(1) = \frac{1+i}{2}. \end{array}$$

Si ha dunque:

$$uv = \frac{1-i}{2}a + \frac{1+i}{2}c,$$

che è proprio z.

Nota. Il fatto che l'algebra gruppo $\mathcal{C}[G]$ contenga una copia di ogni gruppo abeliano di ordine uguale a quello di G è analogo al fatto che una volta immerso un gruppo di ordine n nel gruppo simmetrico S^n (teorema di Cayley) si trovano poi in S^n copie di ogni gruppo di ordine n.

Abbiamo visto che i caratteri χ_i di un gruppo abeliano G costituiscono una base per lo spazio vettoriale $\mathcal{C}[G]$. Ogni $u \in \mathcal{C}[G]$ si scrive dunque, in modo unico, come:

$$u = \sum_i c_i \chi_i. \tag{5.31}$$

Il coefficiente c_j di χ_j si può calcolare prendendo il prodotto scalare di u con χ_j:

$$\begin{aligned}(u,\chi_j) &= \frac{1}{n}\sum_g u(g)\overline{\chi_j(g)} = \frac{1}{n}\sum_g\sum_i c_i(\chi_i,\chi_j)\\ &= \sum_i c_i(\frac{1}{n}\sum_g \chi_i(g)\overline{\chi_j(g)})\\ &= c_j,\end{aligned}$$

dove l'ultima uguaglianza segue dall'ortogonalità dei caratteri. Il coefficiente c_j di χ_j in u è quindi:

$$c_j = \frac{1}{n}\sum_g u(g)\overline{\chi_j(g)}. \tag{5.32}$$

Se $u = u_g$, cioè la funzione che vale 1 su g e zero altrove, e che abbiamo identificato con $g \in G$, la (5.32) diventa:

$$c_j = \frac{\overline{\chi_j(g)}}{n},$$

e la (5.31):

$$g = \sum_i \frac{\overline{\chi_i(g)}}{n}\chi_i.$$

Si osservi che i coefficienti c_i sono gli stessi di quelli che servono per scrivere gli idempotenti della base $\{e_i\}$ nella base $\{g_i\}$, come visto all'inizio di questo paragrafo:

$$e_i = \sum_{g\in G} c_i g,$$

con matrice di passaggio $\{g_i\} \to \{e_i\}$ la $\frac{1}{n}\overline{T} = T^{-1}$. Per la (5.31),

$$g = \sum_{i=1}^{n} c_i\chi_i.$$

Qui la somma è su i, e non, come sopra, su g. C'è dunque uno scambio di righe e colonne nella matrice dei c_i, che perciò risulta essere la trasposta $(T^{-1})^t$ della precedente. Ma poichè la T è simmetrica, anche la T^{-1} lo è, e pertanto la matrice è la stessa.

Bibliografia

[**A**] Guido Ascoli, *Lezioni di Algebra*, Editrice Tirrena, Torino, 1965.

[**AHU**] Aho, Hopkroft, Ulmann, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, 1974.

[**BLCR**] D. Bini, G. Lotti, M. Capovani, F. Romani, *Complessità numerica*, Boringhieri, Torino, 1981.

[**C**] L. Childs, *Algebra, un'introduzione concreta*, ETS Editrice, Pisa, 1989 (traduzione di C. Traverso di *A concrete introduction to higher algebra*, Springer−Verlag, Berlin−New York, 1983).

[**CA**] *Computer Algebra. Symbolic and Algebraic Computation*, edited by Buchberger et al., 2d edition, Springer−Verlag, Wien−N.Y., 1983.

[**CMP**] L. Cerlienco, M. Mignotte e F. Piras *Suites récurrentes linéaires*, L'Enseignement Mathématique, t. 33 (1987), p. 67−108.

[**Da**] P. J. Davis, *Circulant matrices*, Wiley and Sons, Chichester− Brisbane, 1979.

[**DST**] J. Davenport, Y. Siret, E. Tournier, *Calcul formel*, Masson, Paris, 1987. (Traduzione inglese: *Computer algebra: systems and algorithms for algebraic computation*, Academic Press, London, 1988).

[**Kn**] D. Knuth, *The art of computer programming*, II: *Seminumerical algorithms*, 2d edition, Addison−Wesley, Reading, Ma., 1981.

[**Ku**] A. G. Kuroś, *Corso di algebra superiore*, Editori Riuniti, Roma, 1977.

[**Li**] J. D. Lipson, *Chinese remainder and interpolation algorithm*, SYMSAM, 1971, p. 372−391.

[**LLL**] A. K. Lenstra, H. W. Lenstra, L. Lovasz, *Factoring Polynomials with Rational Coefficients,* Math. Ann., 261 (1982), pp. 515−534.

[**LN**] R. Lidl, H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its applications, Addison−Wesley, Reading, Ma., 1983.

[**McE**] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer Acad. Publ., Boston, 1987.

[**Mi**] M. Mignotte, *Mathématiques pour le calcul formel*, PUF, Paris, 1989. (Traduzione inglese: *Mathematics for computer algebra*, Springer−Verlag, Berlin New York, 1992).

[**Se**] R. Sedgewick, *Algorithms*, 2d edition, Addison−Wesley, Reading, Ma., 1988.

[**St**] G. Strang, *Introduction to applied mathematics*, Wellesley−Cambridge Press, 1986.

[**VL**] C. Van Loan, *Computational Frameworks of the Fast Fourier Transform*, SIAM, Philadelphia, 1992.