Cyclotomic Polynomials and Generations of Finite Fields

Prof. Andrea Previtali
Università dell'Insubria-Como, Italy
andrea.previtali@uninsubria.it
http://scienze-como.uninsubria.it/previtali

L'Aquila, September 20 2006

Discrete Logarithm Problem

Several cryptographic protocols are based on the arithmetic of **finite fields** and the complexity of the **Discrete Logarithm Problem, DLP**.

Namely given a field F, $g, h \in F$ determine (if any) $n \in \mathbb{N}$ such that

$$h = g^n.$$

n is called the discrete logarithm of h with respect to g:

$$n := \log_g h.$$

Diffie-Hellman

The paradigm of such protocols if **Diffie-Hellman key exchange** (A)lice and (B)ob make F and g **public**. Alice chooses a random integer a and sends g^a to Bob. Bob chooses a random b and sends g^b to Alice. Thus they both share

$$k = g^{ab} = (g^a)^b = (g^b)^a$$

which might be used as a key for a symmetric protocol (e.g. DES or AES).

The security of the Diffie-Hellman's protocol relies on the difficulty of obtaining a from g^a.

Multiplicative Structure of Finite Fields

Theorem: (Gauss 1805) Let $G = F^*$ be the multiplicative group of a finite field F. Then G is cyclic, that is, G is the set of powers of a suitable element $g \in G$, $G = \langle g \rangle$.

1. Any such g is called a primitive element;

2. If $q := |F|$, there exist $\varphi(q-1)$ such elements;

3. their abbundance makes highly likely to hit by random choices;

Conway polynomials

A deterministic and fast search of one primitive element is to related to the construction of Conway polynomials.

Given a prime p and an integer n, we may realize the (unique) finite field of order $q := p^n$ as the quotient ring $\mathbb{F}_p[x]/I$, where I is the ideal generated by an irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree n.

There are many choices for such an f. To get uniqueness we impose the following conditions:

1. f must be primitive, that is, $f(g) = 0$ for some primitive element g;

2. If d is a divisor of n we require that the polynomial f_1 associated to p^d satisfies

$$f(x)|f_1(x^{\frac{p^n-1}{p^d-1}}),$$

a compatibility conditions that easily allows to embed $\mathbb{F}_{p^d}$ into $\mathbb{F}_{p^n}$;

3. f must be minimal with respect to a lexicographic ordering on its coefficients.

We denote this polynomial with $C_{p,n}$ and call it the Conway polynomial.

Primitive Subgroups

Various cryptographic protocols like LUC and XTR are based on the fact (among others) that the security of $F = \mathbb{F}_q$, $q = p^n$, may be attained in a subgroup $G = \langle g \rangle$ of F^* as long as $F = \mathbb{F}_p[g]$. In this case G is called a primitive subgroup.

The approach of Pohlig-Hellman to the DLP shows that we may assume that $|g|$ be a prime r.

We analyze under which conditions on p, n, and r we have the generation property (GP):

$$\mathbb{F}_{p^n} = \mathbb{F}_p[g].$$

Primitive Prime Divisors

Since F^* is cyclic the generation property is equivalent to $\mathbb{F}_p[g]$ is not a proper subfield of F. Since those have shape $\mathbb{F}_{p^d}$ for some divisor d of n, (GP) holds iff $p^n \equiv_r 1$, but $p^d \not\equiv_r 1$ for any $d|n$, $d < n$.

Namely r must be a primitive prime divisor of $p^n - 1$.

Theorem: (Zsigmondy1892) Let $a, n > 1$ be integers. Then there exists a primitive prime divisor for $a^n - 1$ unless $(a, n) = (2, 6)$ or $n = 2$ and $a = 2^s - 1$.

In force of this result a primitive prime divisor is also called a Zsigmondy prime.

Cyclotomic Polynomials

We would like to characterize primitive prime divisors.

Let ζ_n be a primitive n-th root of unity in $\mathbb{C}$ and set

$$\Phi_n(x) = \prod_{j=1, \gcd(j,n)=1}^{n} (x - \zeta_n^j).$$

We call Φ_n the n-th cyclotomic polynomial.

1. $\Phi_n(x)$ is an irreducible, monic, integer polynomial of degree $\varphi(n)$, the Euler totient function

2. $x^n - 1 = \prod_{d|n} \Phi_d(x)$;

3. $\Phi_n(x) = \prod_{d|n}(x^{\frac{n}{d}} - 1)^{\mu(d)}$, where μ is the Moebius' function;

4. $\Phi_{ab}(x)|\Phi_a(x^b)$;

5. $\Phi_{ab}(x)|\gcd(\Phi_b(x^a), \Phi_a(x^b))$;

6. $\Phi_n(x) = \Phi_{s(n)}(x^{n/s(n)})$, where $s(n)$ is the square-free part of n.;

In particular,

$$\Phi_n(1) = \begin{cases} r & n = r^i, r \text{ prime} \\ 1 & \text{otherwise} \end{cases}$$

and

$$p^n - 1 = \prod_{d|n} \Phi_d(p)$$

and r is a primitive prime divisor (p.p.d.) iff $\Phi_n(p) \equiv_r 0$ and $\Phi_d(p) \not\equiv_r 0$.

Lüneburg's Lemma

Theorem: (Lüneburg 1981) Let r be a prime divisor of $\Phi_n(a)$, $\mathbb{N} \ni a, n > 1$. Let f be the order of a modulo r. Then $n = r^i f$. If $i > 0$, then r is the biggest prime divisor of n. If $i > 0$ and r^2 divides $\Phi_n(a)$, then $r = n = 2$.

Gcd of Values of Cyclotomic Polynomials

Theorem: Let $q, n > 1$, r the biggest prime divisor of n, and $d|n$, $d < n$. If $\gcd(\Phi_n(q), \Phi_d(q)) \neq 1$, then

1. $\gcd(\Phi_n(q), \Phi_d(q)) = r$, in particular $\gcd(q, r) = 1$;

2. $n = fr^i$, $d = fr^j$, $i > j \geq 0$, where $f = \mathrm{ord}_r(q)$.

Conversely let r be a prime not dividing q, $f = \mathrm{ord}_r(q)$, $n = fr^i$ and $d = fr^j$, $i > j \geq 0$. Then r is the biggest prime divisor of n and $\gcd(\Phi_n(q), \Phi_d(q)) = r$.

Cryptographic Applications

Cryptographic protocols like LUC, XTR and XTR-30 are based on field extensions $F/\mathbb{F}_p$ of degree $3, 6$, and 30. Let $g \in F$, $|g| = r$ a prime divisor of $\Phi_n(p)$.

1. $n = 3$: $F = \mathbb{F}_p[g]$ unless $|g| = 3$ and $p \equiv_3 1$;

2. $n = 6$: $F = \mathbb{F}_p[g]$ unless $|g| = 3$ and $p \equiv_3 2$;

3. $n = 30$: $F = \mathbb{F}_p[g]$. In fact, 5 is the biggest prime divisor of n but $f = 6 = \frac{30}{5}$ does not divide 4.