Introduzione
Primi e Composti
Aritmetica

Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici

Cronologia
Fattorizzazione
Primalità

Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare

Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller

Crittografia

Test di primalità di Rabin-Miller

Andrea Previtali

Dipartimento di Fisica e Matematica
Università degli Studi dell'Insubria-Como

Stage Estivo Como 11-22 Giugno 2007

Test di Primalità

1 Introduzione
- Primi e Composti
- Aritmetica

2 Complessità
- Algoritmi
- Esponenziali
- Polinomiali
- Probabilistici

3 Cronologia
- Fattorizzazione
- Primalità

4 Fermat
- Atomi e primi
- Test di Fermat
- Pseudoprimi
- Aritmetica Modulare

5 Carmicheal
- Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Test di Primalità

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

1 Introduzione
Primi e Composti
Aritmetica
2 Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
3 Cronologia
Fattorizzazione
Primalità
4 Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
5 Carmicheal
Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Definizioni

- un intero n si dice primo se:
- $n = ab$ implica $a = n$ o $b = n$.
- Altrimenti n dicesi composto.

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Definizioni

- un intero n si dice primo se:
- $n = ab$ implica $a = n$ o $b = n$.
- Altrimenti n dicesi composto.

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Definizioni

- un intero n si dice primo se:
- $n = ab$ implica $a = n$ o $b = n$.
- Altrimenti n dicesi composto.

Test di Primalità

1 Introduzione
- Primi e Composti
- Aritmetica

2 Complessità
- Algoritmi
- Esponenziali
- Polinomiali
- Probabilistici

3 Cronologia
- Fattorizzazione
- Primalità

4 Fermat
- Atomi e primi
- Test di Fermat
- Pseudoprimi
- Aritmetica Modulare

5 Carmicheal
- Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Teorema Fondamentale dell'Aritmetica

- Ogni intero è prodotto di numeri primi, $15 = 3 \cdot 5$.
- L'unica libertà consiste nel riordinare i fattori, $15 = 5 \cdot 3$.
- Se diamo cittadinanza ai negativi allora le libertà aumentano, $15 = -3 \cdot -5$.

Teorema Fondamentale dell'Aritmetica

- Ogni intero è prodotto di numeri primi, $15 = 3 \cdot 5$.
- L'unica libertà consiste nel riordinare i fattori, $15 = 5 \cdot 3$.
- Se diamo cittadinanza ai negativi allora le libertà aumentano, $15 = -3 \cdot -5$.

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Teorema Fondamentale dell'Aritmetica

- Ogni intero è prodotto di numeri primi, $15 = 3 \cdot 5$.
- L'unica libertà consiste nel riordinare i fattori, $15 = 5 \cdot 3$.
- Se diamo cittadinanza ai negativi allora le libertà aumentano, $15 = -3 \cdot -5$.

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Teorema Fondamentale dell'Aritmetica

Teorema (Teorema Fondamentale dell'Aritmetica, Euclide 300 a.c.)

Ogni intero (relativo) si fattorizza in un solo modo nel prodotto di numeri primi a meno dell'ordine e dei segni.

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Due Problemi

- Problema P: stabilire se un dato intero n è primo.
- Problema F: nel caso n sia composto determinare la sua fattorizzazione in primi

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Due Problemi

- Problema P: stabilire se un dato intero n è primo.
- Problema F: nel caso n sia composto determinare la sua fattorizzazione in primi

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Due Soluzioni in una

- Soluzione contemporanea a P e F:
- Sia m il massimo intero tale che $m^2 \leq n$;
- Controlla se a divide n al variare di $1 < a \leq m$;
- Se ne trovi uno allora n è composto, $n = ab$ e si ripete il processo per a e b;
- altrimenti n è primo.
- Allora che altro resta da discutere?

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Due Soluzioni in una

- Soluzione contemporanea a P e F:
- Sia m il massimo intero tale che $m^2 \leq n$;
- Controlla se a divide n al variare di $1 < a \leq m$;
- Se ne trovi uno allora n è composto, $n = ab$ e si ripete il processo per a e b;
- altrimenti n è primo.
- Allora che altro resta da discutere?

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Due Soluzioni in una

- Soluzione contemporanea a P e F:
- Sia m il massimo intero tale che $m^2 \leq n$;
- Controlla se a divide n al variare di $1 < a \leq m$;
- Se ne trovi uno allora n è composto, $n = ab$ e si ripete il processo per a e b;
- altrimenti n è primo.
- Allora che altro resta da discutere?

Due Soluzioni in una

- Soluzione contemporanea a P e F:
- Sia m il massimo intero tale che $m^2 \leq n$;
- Controlla se a divide n al variare di $1 < a \leq m$;
- Se ne trovi uno allora n è composto, $n = ab$ e si ripete il processo per a e b;
- altrimenti n è primo.
- Allora che altro resta da discutere?

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Due Soluzioni in una

- Soluzione contemporanea a P e F:
- Sia m il massimo intero tale che $m^2 \leq n$;
- Controlla se a divide n al variare di $1 < a \leq m$;
- Se ne trovi uno allora n è composto, $n = ab$ e si ripete il processo per a e b;
- altrimenti n è primo.
- Allora che altro resta da discutere?

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Due Soluzioni in una

- Soluzione contemporanea a P e F:
- Sia m il massimo intero tale che $m^2 \leq n$;
- Controlla se a divide n al variare di $1 < a \leq m$;
- Se ne trovi uno allora n è composto, $n = ab$ e si ripete il processo per a e b;
- altrimenti n è primo.
- Allora che altro resta da discutere?

Test di Primalità

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

1 Introduzione
Primi e Composti
Aritmetica
2 Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
3 Cronologia
Fattorizzazione
Primalità
4 Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
5 Carmicheal
Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi

- Col termine Algoritmo si intende:
- una procedura di calcolo, ossia una serie di istruzioni impartibili ad esempio al nostro calcolatore preferito
- che forniscono una risposta in un tempo finito (possibilmente breve)
- usando una quantità finita di memoria (possibilmente meno di quella in dotazione al nostro computer)
- ...dimenticavo, la risposta deve essere corretta e data in forma tale che ognuno possa controllarne la correttezza sul suo computer.

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi

- Col termine Algoritmo si intende:
- una procedura di calcolo, ossia una serie di istruzioni impartibili ad esempio al nostro calcolatore preferito
- che forniscono una risposta in un tempo finito (possibilmente breve)
- usando una quantità finita di memoria (possibilmente meno di quella in dotazione al nostro computer)
- ...dimenticavo, la risposta deve essere corretta e data in forma tale che ognuno possa controllarne la correttezza sul suo computer.

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi

- Col termine Algoritmo si intende:
- una procedura di calcolo, ossia una serie di istruzioni impartibili ad esempio al nostro calcolatore preferito
- che forniscono una risposta in un tempo finito (possibilmente breve)
- usando una quantità finita di memoria (possibilmente meno di quella in dotazione al nostro computer)
- ...dimenticavo, la risposta deve essere corretta e data in forma tale che ognuno possa controllarne la correttezza sul suo computer.

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi

- Col termine Algoritmo si intende:
- una procedura di calcolo, ossia una serie di istruzioni impartibili ad esempio al nostro calcolatore preferito
- che forniscono una risposta in un tempo finito (possibilmente breve)
- usando una quantità finita di memoria (possibilmente meno di quella in dotazione al nostro computer)
- ...dimenticavo, la risposta deve essere corretta e data in forma tale che ognuno possa controllarne la correttezza sul suo computer.

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi

- Col termine Algoritmo si intende:
- una procedura di calcolo, ossia una serie di istruzioni impartibili ad esempio al nostro calcolatore preferito
- che forniscono una risposta in un tempo finito (possibilmente breve)
- usando una quantità finita di memoria (possibilmente meno di quella in dotazione al nostro computer)
- ...dimenticavo, la risposta deve essere corretta e data in forma tale che ognuno possa controllarne la correttezza sul suo computer.

Test di Primalità

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

1 Introduzione
Primi e Composti
Aritmetica
2 Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
3 Cronologia
Fattorizzazione
Primalità
4 Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
5 Carmicheal
Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Esponenziali

- Un algoritmo si dice esponenziale se:
- il tempo di risposta è circa $\exp(b)$, dove b indica il numero di cifre dell'input (ad esempio l'intero da fattorizzare)
- l'algoritmo visto sopra richiede circa $\sqrt{n} \sim \exp(b/2)$ divisioni
- quindi è un algoritmo esponenziale
- Ad esempio se $n \sim 10^{100}$, devo compiere 10^{50} divisioni.
- un Pentium 4 compie circa 10^{12} operazioni al secondo
- quindi mi servirebbero $10^{38} = 10^{50}/10^{12}$ secondi, che sono piú di 10^{30} anni
- l'Universo esiste da circa 10^{11} anni

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Esponenziali

- Un algoritmo si dice esponenziale se:
- il tempo di risposta è circa $\exp(b)$, dove b indica il numero di cifre dell'input (ad esempio l'intero da fattorizzare)
- l'algoritmo visto sopra richiede circa $\sqrt{n} \sim \exp(b/2)$ divisioni
- quindi è un algoritmo esponenziale
- Ad esempio se $n \sim 10^{100}$, devo compiere 10^{50} divisioni.
- un Pentium 4 compie circa 10^{12} operazioni al secondo
- quindi mi servirebbero $10^{38} = 10^{50}/10^{12}$ secondi, che sono piú di 10^{30} anni
- l'Universo esiste da circa 10^{11} anni

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Esponenziali

- Un algoritmo si dice esponenziale se:
- il tempo di risposta è circa $\exp(b)$, dove b indica il numero di cifre dell'input (ad esempio l'intero da fattorizzare)
- l'algoritmo visto sopra richiede circa $\sqrt{n} \sim \exp(b/2)$ divisioni
- quindi è un algoritmo esponenziale
- Ad esempio se $n \sim 10^{100}$, devo compiere 10^{50} divisioni.
- un Pentium 4 compie circa 10^{12} operazioni al secondo
- quindi mi servirebbero $10^{38} = 10^{50}/10^{12}$ secondi, che sono piú di 10^{30} anni
- l'Universo esiste da circa 10^{11} anni

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Esponenziali

- Un algoritmo si dice esponenziale se:
- il tempo di risposta è circa $\exp(b)$, dove b indica il numero di cifre dell'input (ad esempio l'intero da fattorizzare)
- l'algoritmo visto sopra richiede circa $\sqrt{n} \sim \exp(b/2)$ divisioni
- quindi è un algoritmo esponenziale
- Ad esempio se $n \sim 10^{100}$, devo compiere 10^{50} divisioni.
- un Pentium 4 compie circa 10^{12} operazioni al secondo
- quindi mi servirebbero $10^{38} = 10^{50}/10^{12}$ secondi, che sono piú di 10^{30} anni
- l'Universo esiste da circa 10^{11} anni

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Esponenziali

- Un algoritmo si dice esponenziale se:
- il tempo di risposta è circa $\exp(b)$, dove b indica il numero di cifre dell'input (ad esempio l'intero da fattorizzare)
- l'algoritmo visto sopra richiede circa $\sqrt{n} \sim \exp(b/2)$ divisioni
- quindi è un algoritmo esponenziale
- Ad esempio se $n \sim 10^{100}$, devo compiere 10^{50} divisioni.
- un Pentium 4 compie circa 10^{12} operazioni al secondo
- quindi mi servirebbero $10^{38} = 10^{50}/10^{12}$ secondi, che sono piú di 10^{30} anni
- l'Universo esiste da circa 10^{11} anni

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Esponenziali

- Un algoritmo si dice esponenziale se:
- il tempo di risposta è circa $\exp(b)$, dove b indica il numero di cifre dell'input (ad esempio l'intero da fattorizzare)
- l'algoritmo visto sopra richiede circa $\sqrt{n} \sim \exp(b/2)$ divisioni
- quindi è un algoritmo esponenziale
- Ad esempio se $n \sim 10^{100}$, devo compiere 10^{50} divisioni.
- un Pentium 4 compie circa 10^{12} operazioni al secondo
- quindi mi servirebbero $10^{38} = 10^{50}/10^{12}$ secondi, che sono piú di 10^{30} anni
- l'Universo esiste da circa 10^{11} anni

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Esponenziali

- Un algoritmo si dice esponenziale se:
- il tempo di risposta è circa $\exp(b)$, dove b indica il numero di cifre dell'input (ad esempio l'intero da fattorizzare)
- l'algoritmo visto sopra richiede circa $\sqrt{n} \sim \exp(b/2)$ divisioni
- quindi è un algoritmo esponenziale
- Ad esempio se $n \sim 10^{100}$, devo compiere 10^{50} divisioni.
- un Pentium 4 compie circa 10^{12} operazioni al secondo
- quindi mi servirebbero $10^{38} = 10^{50}/10^{12}$ secondi, che sono piú di 10^{30} anni
- l'Universo esiste da circa 10^{11} anni

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Esponenziali

- Un algoritmo si dice esponenziale se:
- il tempo di risposta è circa $\exp(b)$, dove b indica il numero di cifre dell'input (ad esempio l'intero da fattorizzare)
- l'algoritmo visto sopra richiede circa $\sqrt{n} \sim \exp(b/2)$ divisioni
- quindi è un algoritmo esponenziale
- Ad esempio se $n \sim 10^{100}$, devo compiere 10^{50} divisioni.
- un Pentium 4 compie circa 10^{12} operazioni al secondo
- quindi mi servirebbero $10^{38} = 10^{50}/10^{12}$ secondi, che sono piú di 10^{30} anni
- l'Universo esiste da circa 10^{11} anni

Test di Primalità

1 Introduzione
- Primi e Composti
- Aritmetica

2 Complessità
- Algoritmi
- Esponenziali
- Polinomiali
- Probabilistici

3 Cronologia
- Fattorizzazione
- Primalità

4 Fermat
- Atomi e primi
- Test di Fermat
- Pseudoprimi
- Aritmetica Modulare

5 Carmicheal
- Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Polinomiali

- Un algoritmo si dice polinomiale se:
- il tempo di risposta è della forma $b, b^2, b^3, \ldots$, dove b indica il numero di cifre dell'input
- ad esempio se un mago mi fornisse due interi a, b con 50 cifre dicendo che il prodotto coincide con un dato intero n
- potrei controllare che dice il vero calcolando $a \cdot b$.
- il classico algoritmo di moltiplicazione richede circa 250 moltiplicazioni elementari e alcune somme
- un Pentium 4 impiegherebbe solo pochi milionesimi di secondo per effettuare questo controllo

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Polinomiali

- Un algoritmo si dice polinomiale se:
- il tempo di risposta è della forma $b, b^2, b^3, \ldots$, dove b indica il numero di cifre dell'input
- ad esempio se un mago mi fornisse due interi a, b con 50 cifre dicendo che il prodotto coincide con un dato intero n
- potrei controllare che dice il vero calcolando $a \cdot b$.
- il classico algoritmo di moltiplicazione richede circa 250 moltiplicazioni elementari e alcune somme
- un Pentium 4 impiegherebbe solo pochi milionesimi di secondo per effettuare questo controllo

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Polinomiali

- Un algoritmo si dice polinomiale se:
- il tempo di risposta è della forma $b, b^2, b^3, \ldots$, dove b indica il numero di cifre dell'input
- ad esempio se un mago mi fornisse due interi a, b con 50 cifre dicendo che il prodotto coincide con un dato intero n
- potrei controllare che dice il vero calcolando $a \cdot b$.
- il classico algoritmo di moltiplicazione richede circa 250 moltiplicazioni elementari e alcune somme
- un Pentium 4 impiegherebbe solo pochi milionesimi di secondo per effettuare questo controllo

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Polinomiali

- Un algoritmo si dice polinomiale se:
- il tempo di risposta è della forma $b, b^2, b^3, \ldots$, dove b indica il numero di cifre dell'input
- ad esempio se un mago mi fornisse due interi a, b con 50 cifre dicendo che il prodotto coincide con un dato intero n
- potrei controllare che dice il vero calcolando $a \cdot b$.
- il classico algoritmo di moltiplicazione richede circa 250 moltiplicazioni elementari e alcune somme
- un Pentium 4 impiegherebbe solo pochi milionesimi di secondo per effettuare questo controllo

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Polinomiali

- Un algoritmo si dice polinomiale se:
- il tempo di risposta è della forma $b, b^2, b^3, \ldots$, dove b indica il numero di cifre dell'input
- ad esempio se un mago mi fornisse due interi a, b con 50 cifre dicendo che il prodotto coincide con un dato intero n
- potrei controllare che dice il vero calcolando $a \cdot b$.
- il classico algoritmo di moltiplicazione richede circa 250 moltiplicazioni elementari e alcune somme
- un Pentium 4 impiegherebbe solo pochi milionesimi di secondo per effettuare questo controllo

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Polinomiali

- Un algoritmo si dice polinomiale se:
- il tempo di risposta è della forma $b, b^2, b^3, \ldots$, dove b indica il numero di cifre dell'input
- ad esempio se un mago mi fornisse due interi a, b con 50 cifre dicendo che il prodotto coincide con un dato intero n
- potrei controllare che dice il vero calcolando $a \cdot b$.
- il classico algoritmo di moltiplicazione richede circa 250 moltiplicazioni elementari e alcune somme
- un Pentium 4 impiegherebbe solo pochi milionesimi di secondo per effettuare questo controllo

Test di Primalità

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

1 Introduzione
Primi e Composti
Aritmetica
2 Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
3 Cronologia
Fattorizzazione
Primalità
4 Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
5 Carmicheal
Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Probabilistici

- Esistono procedure di calcolo che richiedono scelte casuali
- Queste vengono detti algoritmi probabilistici mentre viene riservato l'aggettivo deterministico per gli algoritmi definiti prima
- a loro volta gli algoritmi probabilistici si suddividono in due classi:
- Monte Carlo: forniscono una risposta probabilmente giusta
- Las Vegas: probabilmente forniscono una risposta, ma se lo fanno è corretta

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Probabilistici

- Esistono procedure di calcolo che richiedono scelte casuali
- Queste vengono detti algoritmi probabilistici mentre viene riservato l'aggettivo deterministico per gli algoritmi definiti prima
- a loro volta gli algoritmi probabilistici si suddividono in due classi:
- Monte Carlo: forniscono una risposta probabilmente giusta
- Las Vegas: probabilmente forniscono una risposta, ma se lo fanno è corretta

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Probabilistici

- Esistono procedure di calcolo che richiedono scelte casuali
- Queste vengono detti algoritmi probabilistici mentre viene riservato l'aggettivo deterministico per gli algoritmi definiti prima
- a loro volta gli algoritmi probabilistici si suddividono in due classi:
- Monte Carlo: forniscono una risposta probabilmente giusta
- Las Vegas: probabilmente forniscono una risposta, ma se lo fanno è corretta

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Probabilistici

- Esistono procedure di calcolo che richiedono scelte casuali
- Queste vengono detti algoritmi probabilistici mentre viene riservato l'aggettivo deterministico per gli algoritmi definiti prima
- a loro volta gli algoritmi probabilistici si suddividono in due classi:
- Monte Carlo: forniscono una risposta probabilmente giusta
- Las Vegas: probabilmente forniscono una risposta, ma se lo fanno è corretta

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Algoritmi Probabilistici

- Esistono procedure di calcolo che richiedono scelte casuali
- Queste vengono detti algoritmi probabilistici mentre viene riservato l'aggettivo deterministico per gli algoritmi definiti prima
- a loro volta gli algoritmi probabilistici si suddividono in due classi:
- Monte Carlo: forniscono una risposta probabilmente giusta
- Las Vegas: probabilmente forniscono una risposta, ma se lo fanno è corretta

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Las Vegas e divisione per tentativi

- Ad esempio posso scegliere a caso un intero a tra 2 e $\sqrt{n}$
- testare se a divide n
- in caso affermativo ho un fattorizzazione per n
- a priori, però, potrei essere sfortunato e non scegliere mai un divisore di n
- quindi in questo caso non saprei decidere se n è primo o composto

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Las Vegas e divisione per tentativi

- Ad esempio posso scegliere a caso un intero a tra 2 e $\sqrt{n}$
- testare se a divide n
- in caso affermativo ho un fattorizzazione per n
- a priori, però, potrei essere sfortunato e non scegliere mai un divisore di n
- quindi in questo caso non saprei decidere se n è primo o composto

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Las Vegas e divisione per tentativi

- Ad esempio posso scegliere a caso un intero a tra 2 e $\sqrt{n}$
- testare se a divide n
- in caso affermativo ho un fattorizzazione per n
- a priori, però, potrei essere sfortunato e non scegliere mai un divisore di n
- quindi in questo caso non saprei decidere se n è primo o composto

Las Vegas e divisione per tentativi

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

- Ad esempio posso scegliere a caso un intero a tra 2 e $\sqrt{n}$
- testare se a divide n
- in caso affermativo ho un fattorizzazione per n
- a priori, però, potrei essere sfortunato e non scegliere mai un divisore di n
- quindi in questo caso non saprei decidere se n è primo o composto

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Las Vegas e divisione per tentativi

- Ad esempio posso scegliere a caso un intero a tra 2 e $\sqrt{n}$
- testare se a divide n
- in caso affermativo ho un fattorizzazione per n
- a priori, però, potrei essere sfortunato e non scegliere mai un divisore di n
- quindi in questo caso non saprei decidere se n è primo o composto

Test di Primalità

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

1 Introduzione
Primi e Composti
Aritmetica
2 Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
3 Cronologia
Fattorizzazione
Primalità
4 Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
5 Carmicheal
Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Fattorizzazione

- I problemi Primalità e Fattorizzazione sono legati ma si ha l'impressione che si comporitno molto diversamente
- non si conosce ad oggi alcun algoritmo deterministico polinomiale per la Fattorizzazione
- il campione è un algoritmo dovuto a Pomerance (1985)
- ha complessità subesponenziale, ossia a metà strada tra polinomiale ed esponenziale
- inoltre è di tipo probabilistico Las Vegas

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Fattorizzazione

- I problemi Primalità e Fattorizzazione sono legati ma si ha l'impressione che si comporitno molto diversamente
- non si conosce ad oggi alcun algoritmo deterministico polinomiale per la Fattorizzazione
- il campione è un algoritmo dovuto a Pomerance (1985)
- ha complessità subesponenziale, ossia a metà strada tra polinomiale ed esponenziale
- inoltre è di tipo probabilistico Las Vegas

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Fattorizzazione

- I problemi Primalità e Fattorizzazione sono legati ma si ha l'impressione che si comporitno molto diversamente
- non si conosce ad oggi alcun algoritmo deterministico polinomiale per la Fattorizzazione
- il campione è un algoritmo dovuto a Pomerance (1985)
- ha complessità subesponenziale, ossia a metà strada tra polinomiale ed esponenziale
- inoltre è di tipo probabilistico Las Vegas

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Fattorizzazione

- I problemi Primalità e Fattorizzazione sono legati ma si ha l'impressione che si comporitno molto diversamente
- non si conosce ad oggi alcun algoritmo deterministico polinomiale per la Fattorizzazione
- il campione è un algoritmo dovuto a Pomerance (1985)
- ha complessità subesponenziale, ossia a metà strada tra polinomiale ed esponenziale
- inoltre è di tipo probabilistico Las Vegas

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Fattorizzazione

- I problemi Primalità e Fattorizzazione sono legati ma si ha l'impressione che si comporitno molto diversamente
- non si conosce ad oggi alcun algoritmo deterministico polinomiale per la Fattorizzazione
- il campione è un algoritmo dovuto a Pomerance (1985)
- ha complessità subesponenziale, ossia a metà strada tra polinomiale ed esponenziale
- inoltre è di tipo probabilistico Las Vegas

Test di Primalità

1 Introduzione
- Primi e Composti
- Aritmetica

2 Complessità
- Algoritmi
- Esponenziali
- Polinomiali
- Probabilistici

3 Cronologia
- Fattorizzazione
- Primalità

4 Fermat
- Atomi e primi
- Test di Fermat
- Pseudoprimi
- Aritmetica Modulare

5 Carmicheal
- Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Primalità

- Esistono vari test di primalità polinomiali ma probabilistici
- uno di questi diventa deterministico se risultasse vera l'ipotesi di Riemann generalizzata (ERH)
- Tale ipotesi asserisce che una funzione sui numeri complessi si annulla soltanto in $x = 1/2 + ti$
- nel 2004 3 giovani ricercatori indiani Agrawal, Kayal e Saxena hanno trovato un algoritmo polinomiale e deterministico che stabilisce la primalità di un intero

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Primalità

- Esistono vari test di primalità polinomiali ma probabilistici
- uno di questi diventa deterministico se risultasse vera l'ipotesi di Riemann generalizzata (ERH)
- Tale ipotesi asserisce che una funzione sui numeri complessi si annulla soltanto in $x = 1/2 + ti$
- nel 2004 3 giovani ricercatori indiani Agrawal, Kayal e Saxena hanno trovato un algoritmo polinomiale e deterministico che stabilisce la primalità di un intero

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Primalità

- Esistono vari test di primalità polinomiali ma probabilistici
- uno di questi diventa deterministico se risultasse vera l'ipotesi di Riemann generalizzata (ERH)
- Tale ipotesi asserisce che una funzione sui numeri complessi si annulla soltanto in $x = 1/2 + ti$
- nel 2004 3 giovani ricercatori indiani Agrawal, Kayal e Saxena hanno trovato un algoritmo polinomiale e deterministico che stabilisce la primalità di un intero

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Primalità

- Esistono vari test di primalità polinomiali ma probabilistici
- uno di questi diventa deterministico se risultasse vera l'ipotesi di Riemann generalizzata (ERH)
- Tale ipotesi asserisce che una funzione sui numeri complessi si annulla soltanto in $x = 1/2 + ti$
- nel 2004 3 giovani ricercatori indiani Agrawal, Kayal e Saxena hanno trovato un algoritmo polinomiale e deterministico che stabilisce la primalità di un intero

Test di Primalità

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

1 Introduzione
Primi e Composti
Aritmetica
2 Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
3 Cronologia
Fattorizzazione
Primalità
4 Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
5 Carmicheal
Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Atomi e primi

- per spiegare l'idea che ha condotto a risposte così diverse per i due problemi userò un'analogia
- immaginate un fisico che vuole distinguere atomi da molecole ma non ha a disposizione un microscopio abbastanza potente
- allora prova a bombardare il materiale da analizzare con elettroni
- la deviazione degli elettroni gli dice se ha di fronte atomi piuttosto che molecole composte

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Atomi e primi

- per spiegare l'idea che ha condotto a risposte così diverse per i due problemi userò un'analogia
- immaginate un fisico che vuole distinguere atomi da molecole ma non ha a disposizione un microscopio abbastanza potente
- allora prova a bombardare il materiale da analizzare con elettroni
- la deviazione degli elettroni gli dice se ha di fronte atomi piuttosto che molecole composte

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Atomi e primi

- per spiegare l'idea che ha condotto a risposte così diverse per i due problemi userò un'analogia
- immaginate un fisico che vuole distinguere atomi da molecole ma non ha a disposizione un microscopio abbastanza potente
- allora prova a bombardare il materiale da analizzare con elettroni
- la deviazione degli elettroni gli dice se ha di fronte atomi piuttosto che molecole composte

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Atomi e primi

- per spiegare l'idea che ha condotto a risposte così diverse per i due problemi userò un'analogia
- immaginate un fisico che vuole distinguere atomi da molecole ma non ha a disposizione un microscopio abbastanza potente
- allora prova a bombardare il materiale da analizzare con elettroni
- la deviazione degli elettroni gli dice se ha di fronte atomi piuttosto che molecole composte

Test di Primalità

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

1 Introduzione
Primi e Composti
Aritmetica
2 Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
3 Cronologia
Fattorizzazione
Primalità
4 Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
5 Carmicheal
Criterio di Korselt

Atomi e primi

- Gli “elettroni” sono tradotti nel seguente test dovuto all’avvocato francese Pierre de Fermat (prima metà del ’600)

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1}-1$ è un multiplo di p

  - Conviene indicare di quanto si discosti $a^{n-1}-1$ dall’essere divisibile per n col resto r della divisione con n
  - Ad esempio per $a = 2$ si hanno le seguenti coppie $[r, n]$
  - $[0,3], [0,5], [0,7], [3,9], [0,11], [0,13], [3,15], [0,17]$
  - $[0,19], [3,21], [0,23], [15,25], [12,27], [0,29], [0,31]$
  - $[3,33], [8,35], [0,37], [3,39], [0,41]$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Atomi e primi

- Gli "elettroni" sono tradotti nel seguente test dovuto all'avvocato francese Pierre de Fermat (prima metà del '600)

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1}-1$ è un multiplo di p

  - Conviene indicare di quanto si discosti $a^{n-1}-1$ dall'essere divisibile per n col resto r della divisione con n
  - Ad esempio per $a = 2$ si hanno le seguenti coppie $[r, n]$
  - $[0,3], [0,5], [0,7], [3,9], [0,11], [0,13], [3,15], [0,17]$
  - $[0,19], [3,21], [0,23], [15,25], [12,27], [0,29], [0,31]$
  - $[3,33], [8,35], [0,37], [3,39], [0,41]$

Atomi e primi

- Gli "elettroni" sono tradotti nel seguente test dovuto all'avvocato francese Pierre de Fermat (prima metà del '600)

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1}-1$ è un multiplo di p

  - Conviene indicare di quanto si discosti $a^{n-1}-1$ dall'essere divisibile per n col resto r della divisione con n
  - Ad esempio per $a = 2$ si hanno le seguenti coppie $[r, n]$
  - $[0,3], [0,5], [0,7], [3,9], [0,11], [0,13], [3,15], [0,17]$
  - $[0,19], [3,21], [0,23], [15,25], [12,27], [0,29], [0,31]$
  - $[3,33], [8,35], [0,37], [3,39], [0,41]$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Atomi e primi

- Gli "elettroni" sono tradotti nel seguente test dovuto all'avvocato francese Pierre de Fermat (prima metà del '600)

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1}-1$ è un multiplo di p

  - Conviene indicare di quanto si discosti $a^{n-1}-1$ dall'essere divisibile per n col resto r della divisione con n
  - Ad esempio per $a = 2$ si hanno le seguenti coppie $[r, n]$
  - $[0,3], [0,5], [0,7], [3,9], [0,11], [0,13], [3,15], [0,17]$
  - $[0,19], [3,21], [0,23], [15,25], [12,27], [0,29], [0,31]$
  - $[3,33], [8,35], [0,37], [3,39], [0,41]$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Atomi e primi

- Gli "elettroni" sono tradotti nel seguente test dovuto all'avvocato francese Pierre de Fermat (prima metà del '600)

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1}-1$ è un multiplo di p

  - Conviene indicare di quanto si discosti $a^{n-1}-1$ dall'essere divisibile per n col resto r della divisione con n
  - Ad esempio per $a = 2$ si hanno le seguenti coppie $[r, n]$
  - $[0,3], [0,5], [0,7], [3,9], [0,11], [0,13], [3,15], [0,17]$
  - $[0,19], [3,21], [0,23], [15,25], [12,27], [0,29], [0,31]$
  - $[3,33], [8,35], [0,37], [3,39], [0,41]$

Atomi e primi

- Gli "elettroni" sono tradotti nel seguente test dovuto all'avvocato francese Pierre de Fermat (prima metà del '600)

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1}-1$ è un multiplo di p

  - Conviene indicare di quanto si discosti $a^{n-1}-1$ dall'essere divisibile per n col resto r della divisione con n
  - Ad esempio per $a = 2$ si hanno le seguenti coppie $[r, n]$
  - $[0,3], [0,5], [0,7], [3,9], [0,11], [0,13], [3,15], [0,17]$
  - $[0,19], [3,21], [0,23], [15,25], [12,27], [0,29], [0,31]$
  - $[3,33], [8,35], [0,37], [3,39], [0,41]$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Atomi e primi

- Gli "elettroni" sono tradotti nel seguente test dovuto all'avvocato francese Pierre de Fermat (prima metà del '600)

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1}-1$ è un multiplo di p

  - Conviene indicare di quanto si discosti $a^{n-1}-1$ dall'essere divisibile per n col resto r della divisione con n
  - Ad esempio per $a = 2$ si hanno le seguenti coppie $[r, n]$
  - $[0,3], [0,5], [0,7], [3,9], [0,11], [0,13], [3,15], [0,17]$
  - $[0,19], [3,21], [0,23], [15,25], [12,27], [0,29], [0,31]$
  - $[3,33], [8,35], [0,37], [3,39], [0,41]$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Atomi e primi

- Gli "elettroni" sono tradotti nel seguente test dovuto all'avvocato francese Pierre de Fermat (prima metà del '600)

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1}-1$ è un multiplo di p

  - Conviene indicare di quanto si discosti $a^{n-1}-1$ dall'essere divisibile per n col resto r della divisione con n
  - Ad esempio per $a = 2$ si hanno le seguenti coppie $[r, n]$
  - $[0,3], [0,5], [0,7], [3,9], [0,11], [0,13], [3,15], [0,17]$
  - $[0,19], [3,21], [0,23], [15,25], [12,27], [0,29], [0,31]$
  - $[3,33], [8,35], [0,37], [3,39], [0,41]$

Test di Primalità

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

1 Introduzione
Primi e Composti
Aritmetica
2 Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
3 Cronologia
Fattorizzazione
Primalità
4 Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
5 Carmicheal
Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi

- I pochi test precedenti potrebbero aver suggerito a Fermat il suo Teorema
- in più potrebbero suggerire a noi che valga l'inverso di questo teorema con $a = 2$ e n dispari (un numero pari raramente è primo)
- purtroppo esistono numeri composti dispari n tali che $2^{n-1} - 1$ è divisibile per n
- il più piccolo è $341 = 11 \cdot 31$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi

- I pochi test precedenti potrebbero aver suggerito a Fermat il suo Teorema
- in più potrebbero suggerire a noi che valga l'inverso di questo teorema con $a = 2$ e n dispari (un numero pari raramente è primo)
- purtroppo esistono numeri composti dispari n tali che $2^{n-1} - 1$ è divisibile per n
- il più piccolo è $341 = 11 \cdot 31$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi

- I pochi test precedenti potrebbero aver suggerito a Fermat il suo Teorema
- in più potrebbero suggerire a noi che valga l'inverso di questo teorema con $a = 2$ e n dispari (un numero pari raramente è primo)
- purtroppo esistono numeri composti dispari n tali che $2^{n-1} - 1$ è divisibile per n
- il più piccolo è $341 = 11 \cdot 31$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi

- I pochi test precedenti potrebbero aver suggerito a Fermat il suo Teorema
- in più potrebbero suggerire a noi che valga l'inverso di questo teorema con $a = 2$ e n dispari (un numero pari raramente è primo)
- purtroppo esistono numeri composti dispari n tali che $2^{n-1} - 1$ è divisibile per n
- il più piccolo è $341 = 11 \cdot 31$

Test di Primalità

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

1 Introduzione
Primi e Composti
Aritmetica
2 Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
3 Cronologia
Fattorizzazione
Primalità
4 Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
5 Carmicheal
Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Aritmetica Modulare

- Per esprimere questi fatti occore introdurre una nuova aritmetica
- si fissa un intero m, detto modulo, si depositano gli interi $R = \{0, 1, \ldots, m-1\}$ su una circonferenza
- la somma di a, b in R si effettua partendo da a e spostandosi, passando da zero se necessario, di b ore
- per ottenere il prodotto di a con b in R, si parte da zero e si aggiungono ab ore
- si scrive $a + b \equiv_m s$, $ab \equiv_m p$ per distinguere somma e prodotto negli interi e in R
- ad esempio $4 + 2 \equiv_5 1$ e $3 \cdot 2 \equiv_6 0$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Aritmetica Modulare

- Per esprimere questi fatti occore introdurre una nuova aritmetica
- si fissa un intero m, detto modulo, si depositano gli interi $R = \{0, 1, \ldots, m-1\}$ su una circonferenza
- la somma di a, b in R si effettua partendo da a e spostandosi, passando da zero se necessario, di b ore
- per ottenere il prodotto di a con b in R, si parte da zero e si aggiungono ab ore
- si scrive $a + b \equiv_m s$, $ab \equiv_m p$ per distinguere somma e prodotto negli interi e in R
- ad esempio $4 + 2 \equiv_5 1$ e $3 \cdot 2 \equiv_6 0$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Aritmetica Modulare

- Per esprimere questi fatti occore introdurre una nuova aritmetica
- si fissa un intero m, detto modulo, si depositano gli interi $R = \{0, 1, \ldots, m-1\}$ su una circonferenza
- la somma di a, b in R si effettua partendo da a e spostandosi, passando da zero se necessario, di b ore
- per ottenere il prodotto di a con b in R, si parte da zero e si aggiungono ab ore
- si scrive $a + b \equiv_m s$, $ab \equiv_m p$ per distinguere somma e prodotto negli interi e in R
- ad esempio $4 + 2 \equiv_5 1$ e $3 \cdot 2 \equiv_6 0$

Aritmetica Modulare

- Per esprimere questi fatti occore introdurre una nuova aritmetica
- si fissa un intero m, detto modulo, si depositano gli interi $R = \{0, 1, \ldots, m-1\}$ su una circonferenza
- la somma di a, b in R si effettua partendo da a e spostandosi, passando da zero se necessario, di b ore
- per ottenere il prodotto di a con b in R, si parte da zero e si aggiungono ab ore
- si scrive $a + b \equiv_m s$, $ab \equiv_m p$ per distinguere somma e prodotto negli interi e in R
- ad esempio $4 + 2 \equiv_5 1$ e $3 \cdot 2 \equiv_6 0$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Aritmetica Modulare

- Per esprimere questi fatti occore introdurre una nuova aritmetica
- si fissa un intero m, detto modulo, si depositano gli interi $R = \{0, 1, \ldots, m-1\}$ su una circonferenza
- la somma di a, b in R si effettua partendo da a e spostandosi, passando da zero se necessario, di b ore
- per ottenere il prodotto di a con b in R, si parte da zero e si aggiungono ab ore
- si scrive $a + b \equiv_m s$, $ab \equiv_m p$ per distinguere somma e prodotto negli interi e in R
- ad esempio $4 + 2 \equiv_5 1$ e $3 \cdot 2 \equiv_6 0$

Aritmetica Modulare

- Per esprimere questi fatti occore introdurre una nuova aritmetica
- si fissa un intero m, detto modulo, si depositano gli interi $R = \{0, 1, \ldots, m-1\}$ su una circonferenza
- la somma di a, b in R si effettua partendo da a e spostandosi, passando da zero se necessario, di b ore
- per ottenere il prodotto di a con b in R, si parte da zero e si aggiungono ab ore
- si scrive $a + b \equiv_m s$, $ab \equiv_m p$ per distinguere somma e prodotto negli interi e in R
- ad esempio $4 + 2 \equiv_5 1$ e $3 \cdot 2 \equiv_6 0$

Introduzione
Primi e Composti
Aritmetica

Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici

Cronologia
Fattorizzazione
Primalità

Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare

Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller

Crittografia

Aritmetica Modulare

- In questo linguaggio il teorema di Fermat diventa

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1} \equiv_p 1$

  - si dice che n supera il test di Fermat rispetto ad a se $a^{n-1} \equiv_n 1$
  - se n è composto e supera il test di Fermat relativo ad a n viene detto pseudoprimo rispetto alla base a o più brevemente un a-pseudoprimo
  - per cui 341 è il minimo 2-pseudoprimo

Aritmetica Modulare

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

- In questo linguaggio il teorema di Fermat diventa

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1} \equiv_p 1$

  - si dice che n supera il test di Fermat rispetto ad a se $a^{n-1} \equiv_n 1$
  - se n è composto e supera il test di Fermat relativo ad a n viene detto pseudoprimo rispetto alla base a o più brevemente un a-pseudoprimo
  - per cui 341 è il minimo 2-pseudoprimo

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Aritmetica Modulare

- In questo linguaggio il teorema di Fermat diventa

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1} \equiv_p 1$

  - si dice che n supera il test di Fermat rispetto ad a se $a^{n-1} \equiv_n 1$
  - se n è composto e supera il test di Fermat relativo ad a n viene detto pseudoprimo rispetto alla base a o più brevemente un a-pseudoprimo
  - per cui 341 è il minimo 2-pseudoprimo

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Aritmetica Modulare

- In questo linguaggio il teorema di Fermat diventa

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1} \equiv_p 1$

  - si dice che n supera il test di Fermat rispetto ad a se $a^{n-1} \equiv_n 1$
  - se n è composto e supera il test di Fermat relativo ad a n viene detto pseudoprimo rispetto alla base a o più brevemente un a-pseudoprimo
  - per cui 341 è il minimo 2-pseudoprimo

Aritmetica Modulare

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

- In questo linguaggio il teorema di Fermat diventa

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1} \equiv_p 1$

  - si dice che n supera il test di Fermat rispetto ad a se $a^{n-1} \equiv_n 1$
  - se n è composto e supera il test di Fermat relativo ad a n viene detto pseudoprimo rispetto alla base a o più brevemente un a-pseudoprimo
  - per cui 341 è il minimo 2-pseudoprimo

Aritmetica Modulare

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

- In questo linguaggio il teorema di Fermat diventa

- **Teorema (Piccolo Teorema di Fermat)**

  Sia p un primo e $1 \leq a \leq p-1$, allora $a^{p-1} \equiv_p 1$

  - si dice che n supera il test di Fermat rispetto ad a se $a^{n-1} \equiv_n 1$
  - se n è composto e supera il test di Fermat relativo ad a n viene detto pseudoprimo rispetto alla base a o più brevemente un a-pseudoprimo
  - per cui 341 è il minimo 2-pseudoprimo

Numeri di Carmicheal

- Purtroppo esistono infiniti interi composti che si fingono primi rispetto al test di Fermat
- ossia sono a-pseudoprimi rispetto a tutti gli $1 \leq a \leq n$, $\gcd(a, n) = 1$
- tali interi si dicono di Carmicheal
- il più piccolo di essi vale $561 = 3 \cdot 11 \cdot 17$
- esiste un criterio per descrivere tali numeri in generale (purtroppo è necessario conoscere la loro decomposizione in fattori primi per poterlo applicare)

Introduzione
Primi e Composti
Aritmetica

Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici

Cronologia
Fattorizzazione
Primalità

Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare

Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller

Crittografia

Numeri di Carmicheal

- Purtroppo esistono infiniti interi composti che si fingono primi rispetto al test di Fermat
- ossia sono a-pseudoprimi rispetto a tutti gli $1 \leq a \leq n$, $\gcd(a, n) = 1$
- tali interi si dicono di Carmicheal
- il più piccolo di essi vale $561 = 3 \cdot 11 \cdot 17$
- esiste un criterio per descrivere tali numeri in generale (purtroppo è necessario conoscere la loro decomposizione in fattori primi per poterlo applicare)

Numeri di Carmicheal

- Purtroppo esistono infiniti interi composti che si fingono primi rispetto al test di Fermat
- ossia sono a-pseudoprimi rispetto a tutti gli $1 \leq a \leq n$, $\gcd(a, n) = 1$
- tali interi si dicono di Carmicheal
- il più piccolo di essi vale $561 = 3 \cdot 11 \cdot 17$
- esiste un criterio per descrivere tali numeri in generale (purtroppo è necessario conoscere la loro decomposizione in fattori primi per poterlo applicare)

Introduzione
Primi e Composti
Aritmetica

Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici

Cronologia
Fattorizzazione
Primalità

Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare

Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller

Crittografia

Numeri di Carmicheal

- Purtroppo esistono infiniti interi composti che si fingono primi rispetto al test di Fermat
- ossia sono a-pseudoprimi rispetto a tutti gli $1 \leq a \leq n$, $\gcd(a, n) = 1$
- tali interi si dicono di Carmicheal
- il più piccolo di essi vale $561 = 3 \cdot 11 \cdot 17$
- esiste un criterio per descrivere tali numeri in generale (purtroppo è necessario conoscere la loro decomposizione in fattori primi per poterlo applicare)

Numeri di Carmicheal

- Purtroppo esistono infiniti interi composti che si fingono primi rispetto al test di Fermat
- ossia sono a-pseudoprimi rispetto a tutti gli $1 \leq a \leq n$, $\gcd(a, n) = 1$
- tali interi si dicono di Carmicheal
- il più piccolo di essi vale $561 = 3 \cdot 11 \cdot 17$
- esiste un criterio per descrivere tali numeri in generale (purtroppo è necessario conoscere la loro decomposizione in fattori primi per poterlo applicare)

Test di Primalità

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

1 Introduzione
Primi e Composti
Aritmetica
2 Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
3 Cronologia
Fattorizzazione
Primalità
4 Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
5 Carmicheal
Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica

Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici

Cronologia
Fattorizzazione
Primalità

Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare

Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller

Crittografia

Criterio di Korselt

Teorema (Criterio di Korselt)

n è di Carmicheal sse $p - 1$ divide $n - 1$ per ogni fattore primo p di n e p^2 non divide n per ogni primo p.

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Criterio di Korselt

- Ad esempio $561 = 3 \cdot 11 \cdot 17$ e $560 = 2^4 \cdot 5 \cdot 7$
- solo 20 anni fa si è provato che esistono infiniti numeri di Carmicheal
- ricapitolando ogni numero di Carmicheal supera ogni test di Fermat, tranne quando $\gcd(a, n) \neq 1$
- sia $\varphi(n) = |\{a : 1 \leq a \leq n, \gcd(a, n) = 1\}|$ la funzione di Eulero
- allora φ è debolmente moltiplicativa, ossia $\varphi(ab) = \varphi(a)\varphi(b)$ se $\gcd(a, b) = 1$
- $\varphi(p^m) = p^{m-1}(p - 1)$ se p è primo
- allora $\varphi(561) = \varphi(3)\varphi(11)\varphi(17) = 2 \cdot 10 \cdot 16 = 320$
- la probabilità di scegliere a non coprimo con n vale $(561 - 320)/561 = 241/560 < 1/2$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Criterio di Korselt

- Ad esempio $561 = 3 \cdot 11 \cdot 17$ e $560 = 2^4 \cdot 5 \cdot 7$
- solo 20 anni fa si è provato che esistono infiniti numeri di Carmicheal
- ricapitolando ogni numero di Carmicheal supera ogni test di Fermat, tranne quando $\gcd(a, n) \neq 1$
- sia $\varphi(n) = |\{a : 1 \leq a \leq n, \gcd(a, n) = 1\}|$ la funzione di Eulero
- allora φ è debolmente moltiplicativa, ossia $\varphi(ab) = \varphi(a)\varphi(b)$ se $\gcd(a, b) = 1$
- $\varphi(p^m) = p^{m-1}(p - 1)$ se p è primo
- allora $\varphi(561) = \varphi(3)\varphi(11)\varphi(17) = 2 \cdot 10 \cdot 16 = 320$
- la probabilità di scegliere a non coprimo con n vale $(561 - 320)/561 = 241/560 < 1/2$

Criterio di Korselt

- Ad esempio $561 = 3 \cdot 11 \cdot 17$ e $560 = 2^4 \cdot 5 \cdot 7$
- solo 20 anni fa si è provato che esistono infiniti numeri di Carmicheal
- ricapitolando ogni numero di Carmicheal supera ogni test di Fermat, tranne quando $\gcd(a, n) \neq 1$
- sia $\varphi(n) = |\{a : 1 \leq a \leq n, \gcd(a, n) = 1\}|$ la funzione di Eulero
- allora φ è debolmente moltiplicativa, ossia $\varphi(ab) = \varphi(a)\varphi(b)$ se $\gcd(a, b) = 1$
- $\varphi(p^m) = p^{m-1}(p-1)$ se p è primo
- allora $\varphi(561) = \varphi(3)\varphi(11)\varphi(17) = 2 \cdot 10 \cdot 16 = 320$
- la probabilità di scegliere a non coprimo con n vale $(561 - 320)/561 = 241/560 < 1/2$

Criterio di Korselt

- Ad esempio $561 = 3 \cdot 11 \cdot 17$ e $560 = 2^4 \cdot 5 \cdot 7$
- solo 20 anni fa si è provato che esistono infiniti numeri di Carmicheal
- ricapitolando ogni numero di Carmicheal supera ogni test di Fermat, tranne quando $\gcd(a, n) \neq 1$
- sia $\varphi(n) = |\{a : 1 \leq a \leq n, \gcd(a, n) = 1\}|$ la funzione di Eulero
- allora φ è debolmente moltiplicativa, ossia $\varphi(ab) = \varphi(a)\varphi(b)$ se $\gcd(a, b) = 1$
- $\varphi(p^m) = p^{m-1}(p-1)$ se p è primo
- allora $\varphi(561) = \varphi(3)\varphi(11)\varphi(17) = 2 \cdot 10 \cdot 16 = 320$
- la probabilità di scegliere a non coprimo con n vale $(561 - 320)/561 = 241/560 < 1/2$

Criterio di Korselt

- Ad esempio $561 = 3 \cdot 11 \cdot 17$ e $560 = 2^4 \cdot 5 \cdot 7$
- solo 20 anni fa si è provato che esistono infiniti numeri di Carmicheal
- ricapitolando ogni numero di Carmicheal supera ogni test di Fermat, tranne quando $\gcd(a, n) \neq 1$
- sia $\varphi(n) = |\{a : 1 \leq a \leq n, \gcd(a, n) = 1\}|$ la funzione di Eulero
- allora φ è debolmente moltiplicativa, ossia $\varphi(ab) = \varphi(a)\varphi(b)$ se $\gcd(a, b) = 1$
- $\varphi(p^m) = p^{m-1}(p-1)$ se p è primo
- allora $\varphi(561) = \varphi(3)\varphi(11)\varphi(17) = 2 \cdot 10 \cdot 16 = 320$
- la probabilità di scegliere a non coprimo con n vale $(561 - 320)/561 = 241/560 < 1/2$

Criterio di Korselt

- Ad esempio $561 = 3 \cdot 11 \cdot 17$ e $560 = 2^4 \cdot 5 \cdot 7$
- solo 20 anni fa si è provato che esistono infiniti numeri di Carmicheal
- ricapitolando ogni numero di Carmicheal supera ogni test di Fermat, tranne quando $\gcd(a, n) \neq 1$
- sia $\varphi(n) = |\{a : 1 \leq a \leq n, \gcd(a, n) = 1\}|$ la funzione di Eulero
- allora φ è debolmente moltiplicativa, ossia $\varphi(ab) = \varphi(a)\varphi(b)$ se $\gcd(a, b) = 1$
- $\varphi(p^m) = p^{m-1}(p - 1)$ se p è primo
- allora $\varphi(561) = \varphi(3)\varphi(11)\varphi(17) = 2 \cdot 10 \cdot 16 = 320$
- la probabilità di scegliere a non coprimo con n vale $(561 - 320)/561 = 241/560 < 1/2$

Criterio di Korselt

- Ad esempio $561 = 3 \cdot 11 \cdot 17$ e $560 = 2^4 \cdot 5 \cdot 7$
- solo 20 anni fa si è provato che esistono infiniti numeri di Carmicheal
- ricapitolando ogni numero di Carmicheal supera ogni test di Fermat, tranne quando $\gcd(a, n) \neq 1$
- sia $\varphi(n) = |\{a : 1 \leq a \leq n, \gcd(a, n) = 1\}|$ la funzione di Eulero
- allora φ è debolmente moltiplicativa, ossia $\varphi(ab) = \varphi(a)\varphi(b)$ se $\gcd(a, b) = 1$
- $\varphi(p^m) = p^{m-1}(p - 1)$ se p è primo
- allora $\varphi(561) = \varphi(3)\varphi(11)\varphi(17) = 2 \cdot 10 \cdot 16 = 320$
- la probabilità di scegliere a non coprimo con n vale $(561 - 320)/561 = 241/560 < 1/2$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Criterio di Korselt

- Ad esempio $561 = 3 \cdot 11 \cdot 17$ e $560 = 2^4 \cdot 5 \cdot 7$
- solo 20 anni fa si è provato che esistono infiniti numeri di Carmicheal
- ricapitolando ogni numero di Carmicheal supera ogni test di Fermat, tranne quando $\gcd(a, n) \neq 1$
- sia $\varphi(n) = |\{a : 1 \leq a \leq n, \gcd(a, n) = 1\}|$ la funzione di Eulero
- allora φ è debolmente moltiplicativa, ossia $\varphi(ab) = \varphi(a)\varphi(b)$ se $\gcd(a, b) = 1$
- $\varphi(p^m) = p^{m-1}(p - 1)$ se p è primo
- allora $\varphi(561) = \varphi(3)\varphi(11)\varphi(17) = 2 \cdot 10 \cdot 16 = 320$
- la probabilità di scegliere a non coprimo con n vale $(561 - 320)/561 = 241/560 < 1/2$

Test di Primalità

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

1 Introduzione
Primi e Composti
Aritmetica
2 Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
3 Cronologia
Fattorizzazione
Primalità
4 Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
5 Carmicheal
Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- come è noto $x^2 = 1$ ammette solo due soluzioni $x = \pm 1$
- lo stesso vale in aritmetica modulare quando il modulo è primo
- infatti $x^2 \equiv_p = 1$ sse $x^2 - 1 \equiv_p 0$ sse $(x-1)(x+1) \equiv_p 0$
- siccome p è primo, p deve dividere uno dei due fattori, quindi $x = \pm 1$
- invece $x^2 \equiv_{12} 1$ ammette 4 soluzioni $1, 5, 7, 11$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- come è noto $x^2 = 1$ ammette solo due soluzioni $x = \pm 1$
- lo stesso vale in aritmetica modulare quando il modulo è primo
- infatti $x^2 \equiv_p 1$ sse $x^2 - 1 \equiv_p 0$ sse $(x-1)(x+1) \equiv_p 0$
- siccome p è primo, p deve dividere uno dei due fattori, quindi $x = \pm 1$
- invece $x^2 \equiv_{12} 1$ ammette 4 soluzioni $1, 5, 7, 11$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- come è noto $x^2 = 1$ ammette solo due soluzioni $x = \pm 1$
- lo stesso vale in aritmetica modulare quando il modulo è primo
- infatti $x^2 \equiv_p = 1$ sse $x^2 - 1 \equiv_p 0$ sse $(x-1)(x+1) \equiv_p 0$
- siccome p è primo, p deve dividere uno dei due fattori, quindi $x = \pm 1$
- invece $x^2 \equiv_{12} 1$ ammette 4 soluzioni $1, 5, 7, 11$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- come è noto $x^2 = 1$ ammette solo due soluzioni $x = \pm 1$
- lo stesso vale in aritmetica modulare quando il modulo è primo
- infatti $x^2 \equiv_p = 1$ sse $x^2 - 1 \equiv_p 0$ sse $(x-1)(x+1) \equiv_p 0$
- siccome p è primo, p deve dividere uno dei due fattori, quindi $x = \pm 1$
- invece $x^2 \equiv_{12} 1$ ammette 4 soluzioni $1, 5, 7, 11$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- come è noto $x^2 = 1$ ammette solo due soluzioni $x = \pm 1$
- lo stesso vale in aritmetica modulare quando il modulo è primo
- infatti $x^2 \equiv_p = 1$ sse $x^2 - 1 \equiv_p 0$ sse $(x-1)(x+1) \equiv_p 0$
- siccome p è primo, p deve dividere uno dei due fattori, quindi $x = \pm 1$
- invece $x^2 \equiv_{12} 1$ ammette 4 soluzioni $1, 5, 7, 11$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- come è noto $x^2 = 1$ ammette solo due soluzioni $x = \pm 1$
- lo stesso vale in aritmetica modulare quando il modulo è primo
- infatti $x^2 \equiv_p = 1$ sse $x^2 - 1 \equiv_p 0$ sse $(x-1)(x+1) \equiv_p 0$
- siccome p è primo, p deve dividere uno dei due fattori, quindi $x = \pm 1$
- invece $x^2 \equiv_{12} 1$ ammette 4 soluzioni $1, 5, 7, 11$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- come è noto $x^2 = 1$ ammette solo due soluzioni $x = \pm 1$
- lo stesso vale in aritmetica modulare quando il modulo è primo
- infatti $x^2 \equiv_p 1$ sse $x^2 - 1 \equiv_p 0$ sse $(x-1)(x+1) \equiv_p 0$
- siccome p è primo, p deve dividere uno dei due fattori, quindi $x = \pm 1$
- invece $x^2 \equiv_{12} 1$ ammette 4 soluzioni $1, 5, 7, 11$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- come è noto $x^2 = 1$ ammette solo due soluzioni $x = \pm 1$
- lo stesso vale in aritmetica modulare quando il modulo è primo
- infatti $x^2 \equiv_p = 1$ sse $x^2 - 1 \equiv_p 0$ sse $(x-1)(x+1) \equiv_p 0$
- siccome p è primo, p deve dividere uno dei due fattori, quindi $x = \pm 1$
- invece $x^2 \equiv_{12} 1$ ammette 4 soluzioni $1, 5, 7, 11$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- come è noto $x^2 = 1$ ammette solo due soluzioni $x = \pm 1$
- lo stesso vale in aritmetica modulare quando il modulo è primo
- infatti $x^2 \equiv_p = 1$ sse $x^2 - 1 \equiv_p 0$ sse $(x-1)(x+1) \equiv_p 0$
- siccome p è primo, p deve dividere uno dei due fattori, quindi $x = \pm 1$
- invece $x^2 \equiv_{12} 1$ ammette 4 soluzioni $1, 5, 7, 11$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- come è noto $x^2 = 1$ ammette solo due soluzioni $x = \pm 1$
- lo stesso vale in aritmetica modulare quando il modulo è primo
- infatti $x^2 \equiv_p = 1$ sse $x^2 - 1 \equiv_p 0$ sse $(x-1)(x+1) \equiv_p 0$
- siccome p è primo, p deve dividere uno dei due fattori, quindi $x = \pm 1$
- invece $x^2 \equiv_{12} 1$ ammette 4 soluzioni $1, 5, 7, 11$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- ad esempio sia $n = 13$ e $\gcd(a, n) = 1$, allora $a^{12} \equiv_{13} 1$
- quindi $b = a^6$ è soluzione di $x \overset{\equiv}{m} 1$, per cui $b \equiv_{13} \pm 1$
- se $b \equiv_{13} -1$ mi fermo
- altrimenti $c = b^3$ è soluzione di $x \overset{\equiv}{m} 1$
- in generale dico che un numero dispari composto n è uno pseudoprimo forte in base a se si comporta come un primo rispetto all'estrazioni di radici quadrate di 1

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- ad esempio sia $n = 13$ e $\gcd(a, n) = 1$, allora $a^{12} \equiv_{13} 1$
- quindi $b = a^6$ è soluzione di $x \overset{\equiv}{}_m 1$, per cui $b \equiv_{13} \pm 1$
- se $b \equiv_{13} -1$ mi fermo
- altrimenti $c = b^3$ è soluzione di $x \overset{\equiv}{}_m 1$
- in generale dico che un numero dispari composto n è uno pseudoprimo forte in base a se si comporta come un primo rispetto all'estrazioni di radici quadrate di 1

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- ad esempio sia $n = 13$ e $\gcd(a, n) = 1$, allora $a^{12} \equiv_{13} 1$
- quindi $b = a^6$ è soluzione di $x \overset{\equiv}{}_m 1$, per cui $b \equiv_{13} \pm 1$
- se $b \equiv_{13} -1$ mi fermo
- altrimenti $c = b^3$ è soluzione di $x \overset{\equiv}{}_m 1$
- in generale dico che un numero dispari composto n è uno pseudoprimo forte in base a se si comporta come un primo rispetto all'estrazioni di radici quadrate di 1

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- ad esempio sia $n = 13$ e $\gcd(a, n) = 1$, allora $a^{12} \equiv_{13} 1$
- quindi $b = a^6$ è soluzione di $x \overset{\equiv}{_m} 1$, per cui $b \equiv_{13} \pm 1$
- se $b \equiv_{13} -1$ mi fermo
- altrimenti $c = b^3$ è soluzione di $x \overset{\equiv}{_m} 1$
- in generale dico che un numero dispari composto n è uno pseudoprimo forte in base a se si comporta come un primo rispetto all'estrazioni di radici quadrate di 1

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- ad esempio sia $n = 13$ e $\gcd(a, n) = 1$, allora $a^{12} \equiv_{13} 1$
- quindi $b = a^6$ è soluzione di $x \overset{\equiv}{_m} 1$, per cui $b \equiv_{13} \pm 1$
- se $b \equiv_{13} -1$ mi fermo
- altrimenti $c = b^3$ è soluzione di $x \overset{\equiv}{_m} 1$
- in generale dico che un numero dispari composto n è uno pseudoprimo forte in base a se si comporta come un primo rispetto all'estrazioni di radici quadrate di 1

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- sia n un intero dispari composto, $n-1=2^s t$, t dispari
- n di dice un a-pseudoprimo forte se $a^t \equiv_n 1$, oppure $a^{2^i t} \equiv_n -1$ per qualche $1 \leq i \leq s-1$
- ad esempio 341 è 2-pseudoprimo ma non è 2-pseudoprimo forte
- infatti $340 = 2^2 \cdot 85$, $2^8 5 \equiv_{341} 32$ e $32^2 \equiv_{341} 1$
- ossia 32 è soluzione di $x^2 \equiv_{341} 1$, ma $32 \not\equiv_{341} \pm 1$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- sia n un intero dispari composto, $n-1 = 2^s t$, t dispari
- n di dice un a-pseudoprimo forte se $a^t \equiv_n 1$, oppure $a^{2^i t} \equiv_n -1$ per qualche $1 \leq i \leq s-1$
- ad esempio 341 è 2-pseudoprimo ma non è 2-pseudoprimo forte
- infatti $340 = 2^2 \cdot 85$, $2^8 5 \equiv_{341} 32$ e $32^2 \equiv_{341} 1$
- ossia 32 è soluzione di $x^2 \equiv_{341} 1$, ma $32 \not\equiv_{341} \pm 1$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- sia n un intero dispari composto, $n-1 = 2^s t$, t dispari
- n di dice un a-pseudoprimo forte se $a^t \equiv_n 1$, oppure $a^{2^i t} \equiv_n -1$ per qualche $1 \leq i \leq s-1$
- ad esempio 341 è 2-pseudoprimo ma non è 2-pseudoprimo forte
- infatti $340 = 2^2 \cdot 85$, $2^8 5 \equiv_{341} 32$ e $32^2 \equiv_{341} 1$
- ossia 32 è soluzione di $x^2 \equiv_{341} 1$, ma $32 \not\equiv_{341} \pm 1$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- sia n un intero dispari composto, $n-1 = 2^s t$, t dispari
- n di dice un a-pseudoprimo forte se $a^t \equiv_n 1$, oppure $a^{2^i t} \equiv_n -1$ per qualche $1 \leq i \leq s-1$
- ad esempio 341 è 2-pseudoprimo ma non è 2-pseudoprimo forte
- infatti $340 = 2^2 \cdot 85$, $2^85 \equiv_{341} 32$ e $32^2 \equiv_{341} 1$
- ossia 32 è soluzione di $x^2 \equiv_{341} 1$, ma $32 \not\equiv_{341} \pm 1$

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Pseudoprimi forti

- sia n un intero dispari composto, $n-1 = 2^s t$, t dispari
- n di dice un a-pseudoprimo forte se $a^t \equiv_n 1$, oppure $a^{2^i t} \equiv_n -1$ per qualche $1 \leq i \leq s-1$
- ad esempio 341 è 2-pseudoprimo ma non è 2-pseudoprimo forte
- infatti $340 = 2^2 \cdot 85$, $2^8 5 \equiv_{341} 32$ e $32^2 \equiv_{341} 1$
- ossia 32 è soluzione di $x^2 \equiv_{341} 1$, ma $32 \not\equiv_{341} \pm 1$

Test di Primalità

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

1 Introduzione
Primi e Composti
Aritmetica
2 Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
3 Cronologia
Fattorizzazione
Primalità
4 Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
5 Carmicheal
Criterio di Korselt

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Teorema di Rabin-Miller

Teorema (Teorema di Rabin-Miller)

Sia n un intero dispari e composto. Allora n è a-pseudoprimo forte al più per $\varphi(n)/4$ basi a

Carmicheal forti

- la prima conseguenza è che non esistono numeri di Carmicheal forti
- la seconda è il teorema si traduce in un algoritmo probabilistico tipo Monte Carlo
- scelgo $1 \leq a \leq n$, se $\gcd(a, n) \neq 1$ allora n è composto
- altrimenti controllo se n supera il test di a-pseudoprimalità forte
- No: allora n è composto
- Si: la probabilità che sia composto è $\leq 1/4$
- dopo s tentativi la probabilità che un numero composto finga di essere primo rispetto a questi test di pseudoprimalità forte è circa $1/4^s$, ossia molto probabilmente n è primo

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Carmicheal forti

- la prima conseguenza è che non esistono numeri di Carmicheal forti
- la seconda è il teorema si traduce in un algoritmo probabilistico tipo Monte Carlo
- scelgo $1 \leq a \leq n$, se $\gcd(a, n) \neq 1$ allora n è composto
- altrimenti controllo se n supera il test di a-pseudoprimalità forte
- No: allora n è composto
- Si: la probabilità che sia composto è $\leq 1/4$
- dopo s tentativi la probabilità che un numero composto finga di essere primo rispetto a questi test di pseudoprimalità forte è circa $1/4^s$, ossia molto probabilmente n è primo

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Carmicheal forti

- la prima conseguenza è che non esistono numeri di Carmicheal forti
- la seconda è il teorema si traduce in un algoritmo probabilistico tipo Monte Carlo
- scelgo $1 \leq a \leq n$, se $\gcd(a, n) \neq 1$ allora n è composto
- altrimenti controllo se n supera il test di a-pseudoprimalità forte
- No: allora n è composto
- Si: la probabilità che sia composto è $\leq 1/4$
- dopo s tentativi la probabilità che un numero composto finga di essere primo rispetto a questi test di pseudoprimalità forte è circa $1/4^s$, ossia molto probabilmente n è primo

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Carmicheal forti

- la prima conseguenza è che non esistono numeri di Carmicheal forti
- la seconda è il teorema si traduce in un algoritmo probabilistico tipo Monte Carlo
- scelgo $1 \leq a \leq n$, se $\gcd(a, n) \neq 1$ allora n è composto
- altrimenti controllo se n supera il test di a-pseudoprimalità forte
- No: allora n è composto
- Si: la probabilità che sia composto è $\leq 1/4$
- dopo s tentativi la probabilità che un numero composto finga di essere primo rispetto a questi test di pseudoprimalità forte è circa $1/4^s$, ossia molto probabilmente n è primo

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Carmicheal forti

- la prima conseguenza è che non esistono numeri di Carmicheal forti
- la seconda è il teorema si traduce in un algoritmo probabilistico tipo Monte Carlo
- scelgo $1 \leq a \leq n$, se $\gcd(a, n) \neq 1$ allora n è composto
- altrimenti controllo se n supera il test di a-pseudoprimalità forte
- No: allora n è composto
- Si: la probabilità che sia composto è $\leq 1/4$
- dopo s tentativi la probabilità che un numero composto finga di essere primo rispetto a questi test di pseudoprimalità forte è circa $1/4^s$, ossia molto probabilmente n è primo

Carmicheal forti

- la prima conseguenza è che non esistono numeri di Carmicheal forti
- la seconda è il teorema si traduce in un algoritmo probabilistico tipo Monte Carlo
- scelgo $1 \leq a \leq n$, se $\gcd(a, n) \neq 1$ allora n è composto
- altrimenti controllo se n supera il test di a-pseudoprimalità forte
- No: allora n è composto
- Si: la probabilità che sia composto è $\leq 1/4$
- dopo s tentativi la probabilità che un numero composto finga di essere primo rispetto a questi test di pseudoprimalità forte è circa $1/4^s$, ossia molto probabilmente n è primo

Carmicheal forti

- la prima conseguenza è che non esistono numeri di Carmicheal forti
- la seconda è il teorema si traduce in un algoritmo probabilistico tipo Monte Carlo
- scelgo $1 \leq a \leq n$, se $\gcd(a, n) \neq 1$ allora n è composto
- altrimenti controllo se n supera il test di a-pseudoprimalità forte
- No: allora n è composto
- Si: la probabilità che sia composto è $\leq 1/4$
- dopo s tentativi la probabilità che un numero composto finga di essere primo rispetto a questi test di pseudoprimalità forte è circa $1/4^s$, ossia molto probabilmente n è primo

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Testimoni e ipotesi di Riemann estesa

- il test di Rabin-Miller si trasforma in un algoritmo deterministico se controllo più di $\varphi(n)/4$ basi
- purtroppo tale algoritmo è esponenziale
- sia n dispari e composto, dico che a è un testimone per n se n non è a-pseudoprimo forte
- indico con $W(n)$ il minimo di questi testimoni (W sta per witness, testimone)
- Riemann ha ipotizzato che la funzione zeta definita come $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ ammette solo zeri della forma $s = 1/2 + it$, $i^2 = -1$
- se tale congettura (ERH=extended Riemann hypothesis) fosse vera allora $W(n) < 2 \ln n$
- quindi il test di Rabin-Miller diventa un algoritmo deterministico e polinomiale

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Testimoni e ipotesi di Riemann estesa

- il test di Rabin-Miller si trasforma in un algoritmo deterministico se controllo più di $\varphi(n)/4$ basi
- purtroppo tale algoritmo è esponenziale
- sia n dispari e composto, dico che a è un testimone per n se n non è a-pseudoprimo forte
- indico con $W(n)$ il minimo di questi testimoni (W sta per witness, testimone)
- Riemann ha ipotizzato che la funzione zeta definita come $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ ammette solo zeri della forma $s = 1/2 + it$, $i^2 = -1$
- se tale congettura (ERH=extended Riemann hypothesis) fosse vera allora $W(n) < 2 \ln n$
- quindi il test di Rabin-Miller diventa un algoritmo deterministico e polinomiale

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Testimoni e ipotesi di Riemann estesa

- il test di Rabin-Miller si trasforma in un algoritmo deterministico se controllo più di $\varphi(n)/4$ basi
- purtroppo tale algoritmo è esponenziale
- sia n dispari e composto, dico che a è un testimone per n se n non è a-pseudoprimo forte
- indico con $W(n)$ il minimo di questi testimoni (W sta per witness, testimone)
- Riemann ha ipotizzato che la funzione zeta definita come $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ ammette solo zeri della forma $s = 1/2 + it$, $i^2 = -1$
- se tale congettura (ERH=extended Riemann hypothesis) fosse vera allora $W(n) < 2 \ln n$
- quindi il test di Rabin-Miller diventa un algoritmo deterministico e polinomiale

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Testimoni e ipotesi di Riemann estesa

- il test di Rabin-Miller si trasforma in un algoritmo deterministico se controllo più di $\varphi(n)/4$ basi
- purtroppo tale algoritmo è esponenziale
- sia n dispari e composto, dico che a è un testimone per n se n non è a-pseudoprimo forte
- indico con $W(n)$ il minimo di questi testimoni (W sta per witness, testimone)
- Riemann ha ipotizzato che la funzione zeta definita come $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ ammette solo zeri della forma $s = 1/2 + it$, $i^2 = -1$
- se tale congettura (ERH=extended Riemann hypothesis) fosse vera allora $W(n) < 2 \ln n$
- quindi il test di Rabin-Miller diventa un algoritmo deterministico e polinomiale

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Testimoni e ipotesi di Riemann estesa

- il test di Rabin-Miller si trasforma in un algoritmo deterministico se controllo più di $\varphi(n)/4$ basi
- purtroppo tale algoritmo è esponenziale
- sia n dispari e composto, dico che a è un testimone per n se n non è a-pseudoprimo forte
- indico con $W(n)$ il minimo di questi testimoni (W sta per witness, testimone)
- Riemann ha ipotizzato che la funzione zeta definita come $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ ammette solo zeri della forma $s = 1/2 + it$, $i^2 = -1$
- se tale congettura (ERH=extended Riemann hypothesis) fosse vera allora $W(n) < 2 \ln n$
- quindi il test di Rabin-Miller diventa un algoritmo deterministico e polinomiale

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Testimoni e ipotesi di Riemann estesa

- il test di Rabin-Miller si trasforma in un algoritmo deterministico se controllo più di $\varphi(n)/4$ basi
- purtroppo tale algoritmo è esponenziale
- sia n dispari e composto, dico che a è un testimone per n se n non è a-pseudoprimo forte
- indico con $W(n)$ il minimo di questi testimoni (W sta per witness, testimone)
- Riemann ha ipotizzato che la funzione zeta definita come $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ ammette solo zeri della forma $s = 1/2 + it$, $i^2 = -1$
- se tale congettura (ERH=extended Riemann hypothesis) fosse vera allora $W(n) < 2 \ln n$
- quindi il test di Rabin-Miller diventa un algoritmo deterministico e polinomiale

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

Testimoni e ipotesi di Riemann estesa

- il test di Rabin-Miller si trasforma in un algoritmo deterministico se controllo più di $\varphi(n)/4$ basi
- purtroppo tale algoritmo è esponenziale
- sia n dispari e composto, dico che a è un testimone per n se n non è a-pseudoprimo forte
- indico con $W(n)$ il minimo di questi testimoni (W sta per witness, testimone)
- Riemann ha ipotizzato che la funzione zeta definita come $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ ammette solo zeri della forma $s = 1/2 + it$, $i^2 = -1$
- se tale congettura (ERH=extended Riemann hypothesis) fosse vera allora $W(n) < 2 \ln n$
- quindi il test di Rabin-Miller diventa un algoritmo deterministico e polinomiale

AKS

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

- nel 2004 Agrawal, Kayal e Saxena hanno trovato un algoritmo deterministico e polinomiale
- si tratta di una versione del teorema di Fermat applicata a polinomi i cui coefficienti sono interi sulla circonferenza
- non hanno più bisogno di appoggiarsi su ERH

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

AKS

- nel 2004 Agrawal, Kayal e Saxena hanno trovato un algoritmo deterministico e polinomiale
- si tratta di una versione del teorema di Fermat applicata a polinomi i cui coefficienti sono interi sulla circonferenza
- non hanno più bisogno di appoggiarsi su ERH

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

AKS

- nel 2004 Agrawal, Kayal e Saxena hanno trovato un algoritmo deterministico e polinomiale
- si tratta di una versione del teorema di Fermat applicata a polinomi i cui coefficienti sono interi sulla circonferenza
- non hanno più bisogno di appoggiarsi su ERH

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

RSA

- la determinazione di primi o primi di grandezza industriale (ossia composti che fingono molto bene di essere primi)
- ha applicazioni nello scambio di informazione sicura col protocollo a chiave pubblica
- ad esempio nelle transazioni commerciali tra interlocutori che non si sono mai incontrati fisicamente
- implementazione di firme elettroniche
- che non consentono di ripudiare una firma
- implementate dal 1976 da Rivest, Shamir e Adelman (RSA)

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

RSA

- la determinazione di primi o primi di grandezza industriale (ossia composti che fingono molto bene di essere primi)
- ha applicazioni nello scambio di informazione sicura col protocollo a chiave pubblica
- ad esempio nelle transazioni commerciali tra interlocutori che non si sono mai incontrati fisicamente
- implementazione di firme elettroniche
- che non consentono di ripudiare una firma
- implementate dal 1976 da Rivest, Shamir e Adelman (RSA)

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

RSA

- la determinazione di primi o primi di grandezza industriale (ossia composti che fingono molto bene di essere primi)
- ha applicazioni nello scambio di informazione sicura col protocollo a chiave pubblica
- ad esempio nelle transazioni commerciali tra interlocutori che non si sono mai incontrati fisicamente
- implementazione di firme elettroniche
- che non consentono di ripudiare una firma
- implementate dal 1976 da Rivest, Shamir e Adelman (RSA)

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

RSA

- la determinazione di primi o primi di grandezza industriale (ossia composti che fingono molto bene di essere primi)
- ha applicazioni nello scambio di informazione sicura col protocollo a chiave pubblica
- ad esempio nelle transazioni commerciali tra interlocutori che non si sono mai incontrati fisicamente
- implementazione di firme elettroniche
- che non consentono di ripudiare una firma
- implementate dal 1976 da Rivest, Shamir e Adelman (RSA)

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

RSA

- la determinazione di primi o primi di grandezza industriale (ossia composti che fingono molto bene di essere primi)
- ha applicazioni nello scambio di informazione sicura col protocollo a chiave pubblica
- ad esempio nelle transazioni commerciali tra interlocutori che non si sono mai incontrati fisicamente
- implementazione di firme elettroniche
- che non consentono di ripudiare una firma
- implementate dal 1976 da Rivest, Shamir e Adelman (RSA)

Introduzione
Primi e Composti
Aritmetica
Complessità
Algoritmi
Esponenziali
Polinomiali
Probabilistici
Cronologia
Fattorizzazione
Primalità
Fermat
Atomi e primi
Test di Fermat
Pseudoprimi
Aritmetica Modulare
Carmicheal
Criterio di Korselt
Pseudoprimi forti
Rabin-Miller
Crittografia

RSA

- la determinazione di primi o primi di grandezza industriale (ossia composti che fingono molto bene di essere primi)
- ha applicazioni nello scambio di informazione sicura col protocollo a chiave pubblica
- ad esempio nelle transazioni commerciali tra interlocutori che non si sono mai incontrati fisicamente
- implementazione di firme elettroniche
- che non consentono di ripudiare una firma
- implementate dal 1976 da Rivest, Shamir e Adelman (RSA)