Cryptography and Network Security

Introduction to Number Theory

Outline

- Numeri primi
- Piccolo teorema di Fermat
- Teorema di Eulero
- Test di primalità
- Teorema cinese del resto
- Logaritmi discreti

Numeri primi

Primo è un numero naturale > 1 avente come divisori $\in N^+$ soltanto 1 e se stesso

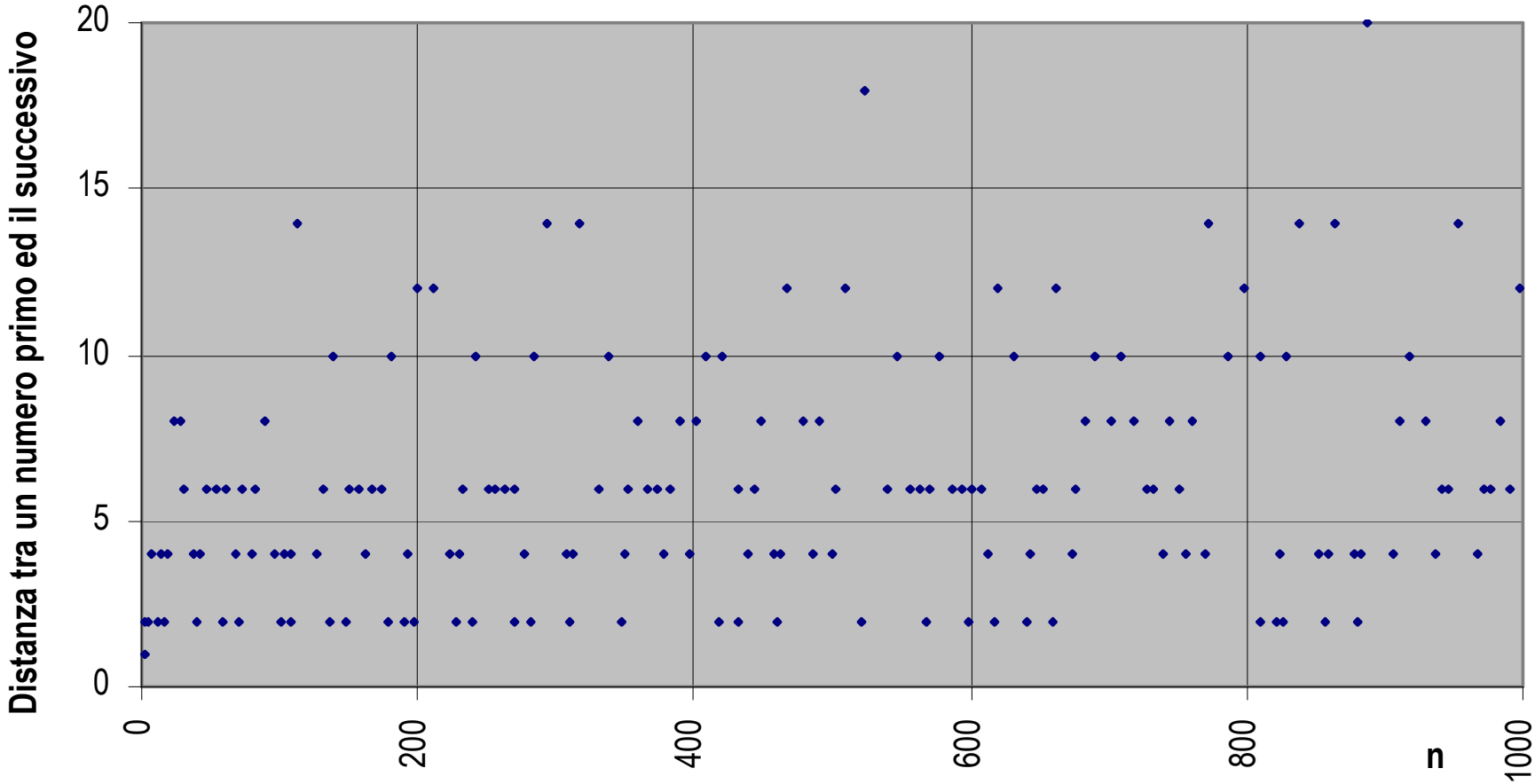
Numeri primi elemento centrale nella teoria dei numeri

Non possono essere espressi come prodotto di altri numeri

I primi 96 numeri primi sono:

2	3	5	7	11	13	17	19	23	31	37	41
43	47	53	59	61	67	71	73	79	83	89	97
101	103	107	109	113	127	131	137	139	149	151	157
163	167	173	179	181	191	193	197	199	211	223	227
229	233	239	241	251	257	263	269	271	277	281	283
293	307	311	313	317	331	337	347	349	353	359	367
373	379	383	389	397	401	409	419	421	431	433	439
443	449	457	461	463	467	479	487	491	499	503	509

Distanza tra numeri primi



Prime number properties

Il teorema dei numeri primi descrive la distribuzione asintotica dei primi

Esso dice che la probabilità che un qualsiasi numero naturale n sia primo è proporzionale a $\ln(n)$

La distanza tra un primo n e il successivo è $\approx \ln(n)$

Anche se molto studiati si ignorano molte cose

Congettura di Goldbach

Congettura dei primi gemelli

. . . . . .

Prime number properties (2)

Congettura di Goldback

Qualsiasi numero intero pari ≥ 4 può essere espresso come la somma di due primi e qualsiasi numero intero dispari > 7 può essere espresso come la somma di tre primi

```
4=2+2   6=3+3 8=3+5 ... 52=41+11 ...
11=5+3+3
```

Congettura dei primi gemelli

Esistono infiniti numeri primi p tali che $p + 2$ è primo

Due primi che soddisfano questa condizione sono chiamati gemelli

```
11+2=13   17+2=19 21+2=23 ...
```

Prime number properties (3)

Primi di Sophie Germain

Se entrambi p e $2p+1$ sono primi,
allora p è chiamato primo di Sophie Germain

I numeri di Sophie Germain a partire dai più piccoli sono
2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, . . .

Sophie Germain provò che l'ultimo teorema di Fermat (FLT)
è verificato per tutti questi numeri dispari

L'FLT stabilisce che non esistono tre interi > 0 a, b, e c tali che
$a^n + b^n = c^n$ per un qualsiasi intero $n > 2$

Non si sa se i primi di Sophie Germain siano in numero finito od infinito

Prime number properties (4)

Primi di Mersenne

Un primo tale $p = 2^n - 1$ è chiamato primo di Mersenne

I numeri di Mersenne a partire dai più piccoli sono
3, 7, 31, 127, 8191, 131071, 524287, 2147483647, . . .

Si può dimostrare facilmente che se p è primo anche n è primo

Pure di questi primi non si sa se siano in numero finito o infinito anche se la congettura di Lenstra-Pomerance-Wagstaff dice che sono infiniti

Utilizzati in diversi tipi di PRNG

Prime number properties (5)

Due numeri a, b sono **primi in modo relativo** (**relatively prime**) o **coprimi** se non hanno divisori comuni eccetto 1

p.e. 8 e 15 sono relatively prime perché i fattori di 8 sono 1,2 [3]
e quelli di 15 sono 1,3,5 così 1 è l'unico fattore comune

Tantissime altre proprietà dei numeri primi

Vedere → http://primes.utm.edu/

Strong primes

Numeri primi dotati di alcune proprietà particolari

Non esiste un accordo completo circa queste proprietà

Teoria dei numeri

Un numero primo è un numero primo forte se è maggiore della media aritmetica tra il più vicino numero primo più piccolo e il più vicino numero primo più grande

Se i primi p_i sono ordinati

$$p_i > \frac{p_{i-1} + p_{i+1}}{2}$$

Un numero primo strong è più vicino al successivo che non al precedente

Strong primes (2)

Criptografia

Un numero primo p è un numero primo forte se soddisfa 4 condizioni:

1. p è grande
2. p - 1 ha fattori primi grandi, cioè $p = a_1 q_1 + 1$ per qualche intero a_1 e un primo grande q_1
3. q_1 - 1 ha fattori primi grandi, cioè $q_1 = a_2 q_2 + 1$ per qualche intero a_2 e un primo grande q_2
4. $p + 1$ ha fattori primi grandi, cioè $p = a_3 q_3 - 1$ per qualche intero a_3 e un primo grande q_3

La strength di un numero primo influenza la velocità di ricerca dei suoi fattori primi (con ben precisi algoritmi)

Problemi computazionali

Prime factoring

Qualsiasi numero intero può essere fattorizzato in numeri primi in un unico modo

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

dove $p_1 < p_2 < \ldots < p_k$ e a_i denota un intero positivo

Questa proprietà può essere scritta: $a = \prod_{p \in P} p^{a_p}$

dove P denota l'insieme dei numeri primi

Prime factoring (2)

La moltiplicazione di due numeri interi è equivalente alla somma degli esponenti dei fattori corrispondenti

$$k = \prod_i p_i^{k_i} = m \cdot n \quad \Rightarrow \quad k_i = m_i + n_i \;\; \forall \;\; p \in P$$

Siccome un numero intero dalla forma p^k può essere diviso soltanto per un altro con lo stesso fattore primo e una potenza minore o uguale a quella del primo

$$a \mid b \Rightarrow a_p \leq b_p \;\; \forall \; p \in P$$

Prime factoring (3)

Fattorizzazione di numeri grandi è problema complesso rispetto a quello di moltiplicare i fattori per generarli

Determinazione della primalità o meno più semplice della fattorizzazione, quindi opportuno effettuare il test di primalità prima della scomposizione

Determinazione del *GCD*(a, b) facile se i due interi

a, b sono fattorizzati in primi

p.e. $300=2^2\times3^1\times5^2$ $18=2^1\times3^2$ quindi *GCD*(300,18)=$2^1\times3^1\times5^0$= 6

Fattorizzazione non triviale di un numero x

$x=y\cdot z$ con $1<y<x$ e $1<z<x$

y e z non hanno l'obbligo di primalità

Prime factoring (4)

Si può effettuare la fattorizzazione in primi effettuando prima una non trivial factorization, controllando quindi i fattori y e z per la primalità e, se compositi, effettuando la loro fattorizzazione

Dopo aver determinato che un numero x è composito si può tentare di dividerlo per tutti i fattori primi possibili ossia fino a $\sqrt{x}$

La procedura porta via nel caso peggiore $\sqrt{x}$ divisioni

Prime factoring (5)

Algoritmo ρ di Pollard

Input: Un intero composito x che non sia la potenza di un primo

Output: Un fattore non triviale d di x

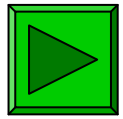
1. $a \leftarrow 2, \quad b \leftarrow 2$
2. For $i = 1, 2, \ldots$
   - 2.1 $a \leftarrow a^2 + 1 \bmod x, \quad b \leftarrow b^2 + 1 \bmod x, \quad b \leftarrow b^2 + 1 \bmod x$
   - 2.2 $d = \text{GCD}(a\text{-}b, x)$
   - 2.3 If $[1 < d < x]$ then return d e termina con successo
   - 2.4 If $[d = x]$ then terminare l'algoritmo con failure

Piccolo teorema di Fermat

$$\forall\left((a,p): p\in P, a\in N^{*}, p\nmid a\right)\ \ a^{p-1}\equiv 1\ (\mathrm{mod}\ p)$$

p.e. con a = 16 e p = 3; 16^3 (=4096) (mod 3) = 1

p.e. con a = 3 e p = 7; 3^6 (=729) (mod 7) = 1



Dimostrazione

Si considerino i p-1 numeri interi $a, 2a, 3a, \ldots, (p\text{-}1)a$

Nessuno di essi è divisibile per p

Se $p|ja$, siccome $p \nmid a$, dovrebbe essere $p|j$
cosa impossibile perché $1 \le j \le p\text{-}1$

Piccolo teorema di Fermat

Inoltre non esistono due tra i p-1 interi che siano congruenti modulo p

Infatti se si assumesse che $ja \equiv ka \pmod{p}$ con $1 \le j \le k \le p\text{-}1$

siccome se j, k, a e p sono interi tali che

$p > 0$, $GCD(a,p) = 1$ e $ja \equiv ka \pmod{p}$

dovrebbe essere $j \equiv k \pmod{p}$

Impossibile perché j e k interi > 0 e < p

Visto che i p-1 interi sono un insieme di numeri tutti non congruenti a 0 modulo p e siccome non ve ne sono due congruenti tra loro modulo p, allora i loro residui - presi in un qualche ordine - devono essere i primi p-1 interi

Piccolo teorema di Fermat

Quindi il prodotto dei p-1 interi $a, 2a, \ldots, (p\text{-}1)a$ è congruente modulo p al prodotto dei primi p-1 interi > 0

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

Quindi

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Siccome $GCD\big((p-1)!, p\big) = 1$

si può eliminare (p-1)! ottenendo

$$a^{p-1} \equiv 1 \pmod{p}$$

c.v.d.

Piccolo teorema di Fermat

Dal piccolo teorema di Fermat si ricava un altro teorema

Moltiplicando ambo i membri della relazione di F. per a si ha

$$a^p \equiv a \pmod{p}$$

D'altra parte, se $p|a$ allora $p|a^p$ quindi

$$a^p \equiv a \equiv 0 \pmod{p}$$

In conclusione

$$\forall\left((a,p): p \in P, a \in N^*\right) \quad a^p \equiv a \pmod{p}$$

Piccolo teorema di Fermat

Teorema utile nei sistemi a chiave pubblica e nei test di primalità

Il fatto che il teorema di Fermat valga sotto l'ipotesi di p primo non implica la non esistenza di numeri compositi per i quali valga la sua relazione

Un numero n non primo (ossia composito) che soddisfa la relazione

$$b^{n-1} \equiv 1 \pmod{n}$$

per tutti i $b \in N^*$ con $GCD(b,n) = 1$ è detto numero di Carmichael o anche pseudo primo assoluto

Funzione toziente di Eulero

Nota anche come funzione ϕ (phi-function) di Eulero

$\phi(n)$ (per n positivo) definito come il

numero di interi positivi minori di n e coprimi a n

Si vede subito che $\forall n \in P \quad \phi(n) = n-1$

Quindi per $n = 37 \quad \phi(n) = 36$

Vale anche l'opposto:

Se $n \in N^*$ e $\phi(n) = n\text{-}1$ allora n è primo

p.e. $n = 35$ Bisogna selezionare tra tutti gli interi positivi minori di 35 quelli che sono coprimi ad esso

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34

Questi interi sono 24, sicché $\phi(35) = 24$

Funzione toziente di Eulero (2)

Per convenzione $\phi(1) = 1$

Premesso che una funzione aritmetica è una funzione definita per tutti gli interi positivi

Una funzione aritmetica f è detta moltiplicativa se $f(mn) = f(m)f(n)$ ogniqualvolta m ed n sono interi positivi coprimi

Se $f(mn) = f(m)f(n)$ per tutti gli interi positivi allora f è detta completamente moltiplicativa

La funzione toziente è una funzione aritmetica moltiplicativa

Per p, q (p, q coprimi) $\phi(pq) = \phi(p)\phi(q)$

$\phi(p)$ è sempre pari per $n \geq 3$

Funzione toziente di Eulero (3)

La condizione di moltiplicatività facilità il calcolo del toziente

Ogni intero esprimibile come prodotto di potenze dei suoi fattori primi

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$$

$$\phi(n) = \phi(p_1^{a_1}) \cdot \phi(p_2^{a_2}) \cdot \ldots \cdot \phi(p_r^{a_r})$$

Il toziente di un numero $n \in N^*$ è esprimibile come la differenza tra n ed il numero degli interi positivi $\leq n$ che non sono coprimi ad n

Gli interi positivi $\leq p^a$ che non sono coprimi a p sono quegli interi $\leq p^a$ che sono divisibili per p ed essi sono p^{a-1}

Sicché $$\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i-1} = p_i^{a_i}\left(1-\frac{1}{p_i}\right)$$

Combinando i risultati si ottiene

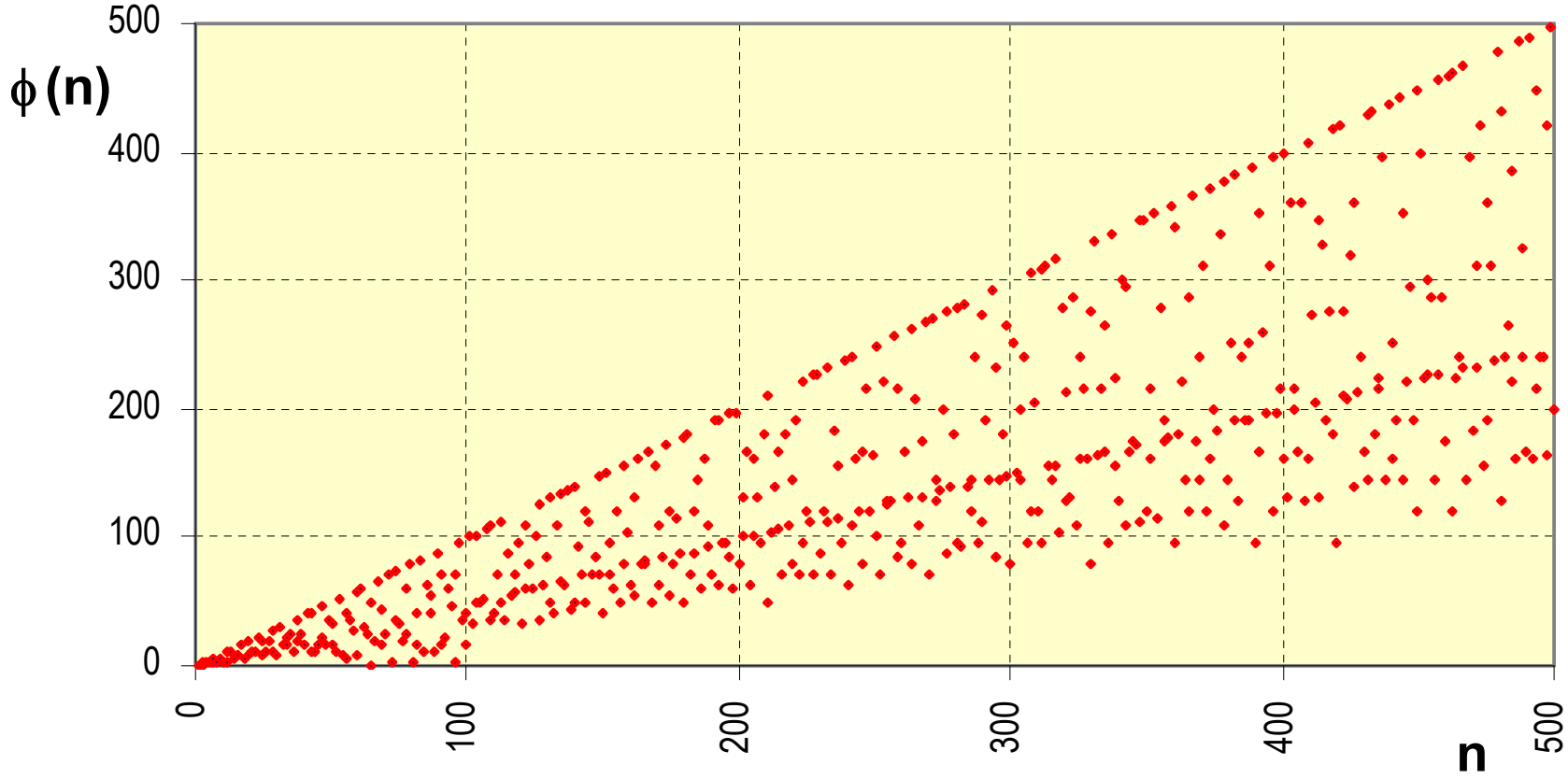
Funzione toziente di Eulero (4)

Relazione che permette di calcolare il toziente a partire

dalla decomposizione in fattori primi

È facile dimostrare che per $n > 2$ $\phi(n)$ è pari

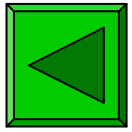
Funzione toziente di Eulero (5)



Teorema di Eulero

Una generalizzazione del (piccolo) teorema di Fermat

$$\forall\left[(a,n): a \in Z, n \in N^{*}, GCD(a,n)=1\right] \; a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$$



p.e.

a = 3; n = 10; $\phi(10) = 4$

$$3^4 = 81 \equiv 1 \ (\mathrm{mod}\ 10)$$

a = 10; n = 3; $\phi(3) = 2$

$$10^3 = 1000 \equiv 1 \ (\mathrm{mod}\ 3)$$

a = 2; n = 11; $\phi(11) = 10$

$$2^{10} = 1024 \equiv 1 \ (\mathrm{mod}\ 11)$$

Controllo di primalità

In criptografia si ha spesso bisogno di generare grandi (e random) numeri primi

Metodo più naturale è generare un numero random n di dimensione appropriata, e verificare se è primo

Serve quindi un test di primalità

Due tipi di test di primalità: deterministici e probabilistici

Un test deterministico determina con sicurezza la primalità

Diversi test deterministici: Crivello di Eratostene, test AKS, test di Lucas-Lehmer, test di curva ellittica, Pocklington, etc

Controllo di primalità (2)

Crivello basato sul tentativo esaustivo di divisione

Tenta di dividere il numero candidato (dispari) per tutti i numeri (primi) minori della sua radice quadrata

Molto lento $\rightarrow$ Possibile usarlo soltanto per numeri piccoli

Anche gli altri controlli deterministici sono molto lenti

Alternativa è l'uso dei test di primalità statistici

I test statistici solo raramente possono identificare un numero composito come primo (per quanto non viceversa)

Controllo di primalità (3)

Esistono diversi test statistici di primalità

- Fermat
- Solovay-Strassen
- Miller-Rabin
- Frobenius
- . . . . . .

Trattasi di metodi statistici che dicono che un numero è primo con una certa probabilità (p.e. 0,5 o 0,75), quindi per ottenere un dato livello di confidenza sulla primalità bisogna applicarli un numero elevato di volte

Per confrontare tra loro questi metodi bisogna valutare il prodotto del numero di applicazioni per il tempo impiegato per un'applicazione

Oggi il test più adoperato è quello di Miller-Rabin

Test di Fermat

Il piccolo teorema di Fermat stabilisce che

$$\forall\left((a,p): p\in P, a\in N^{*}, p\nmid a\right)\quad a^{p-1}\equiv 1\ (\mathrm{mod}\ p)$$

Volendo controllare se p è primo, si prende a caso un a

e si controlla se la congruenza è verificata

Se per un a non è verificata si sa che p è un composito

Se è verificata per molti valori di a si può dire che

p è probabilmente un primo

Esistono però dei numeri, (Carmichael) per i quali la relazione è verificata

per tutti i valori di a per i quali $GCD(a,p) = 1$

Il metodo è di uso non frequente

Algoritmo di Miller Rabin

Il test probabilistico più usato è il test di Miller-Rabin

Conosciuto pure come strong pseudoprime test

Sia n un candidato dispari ≥ 3

Consideriamo il numero pari n - 1

Può essere espresso come

$$n-1 = 2^k \cdot q \qquad \text{con } q \text{ dispari e } k>0$$

Scegliamo un intero a tale che $1 \leq a \leq n$-1

Algoritmo di Miller Rabin (cont)

Se $a^q \equiv 1 \pmod{n}$

o

$a^{2jq} \equiv -1 \pmod{n}$ per alcuni $0 \le j \le k-1$

allora n passa il test

Se n non passa il test con un valore di a

il numero è certamente un "composito"

Un numero primo passa il test con tutti i possibili a

Probabilità che il test riveli un pseudo-primo è < ¼

Considerazioni Probabilistiche

Statisticamente un numero composito passa
il test per al più 1/4 delle basi possibili

Se il test viene ripetuto t volte con numeri a casuali diversi
allora la probabilità che un numero composito passi tutti i test è

$$P[n \text{ composito dopo } t \text{ test}] \leq \frac{1}{4^t}$$

Distribuzione dei Primi

Quanti test si devono fare prima di trovare un primo ?

Un teorema dei numeri primi stabilisce che i primi

si presentano grossolanamente ogni $\ln(n)$ interi

Siccome si possono ignorare i pari e i multipli di 5,

in pratica servono solo 0.4 $\ln(n)$ test per i numeri

di grandezza n prima di trovare un primo

Notare che questo è un "valor medio", talvolta i primi

sono più vicini e altre volte sono più lontani

Un richiamo di algebra

Un algoritmo importante per gli interi è la divisione

Se a e b sono due interi $\neq 0$

esistono due e solo due interi q and r chiamati rispettivamente quoziente e resto, tali che:

$$a = bq + r, \qquad 0 \leq r < |b|$$

p.e.

$$826 = 25 \cdot 33 + 21$$

$$-3 = 7 \cdot (-1) + 4$$

Un richiamo di algebra (2)

Ricordiamo una definizione

$$Z_n = \{0,1,\ldots,(n-1)\}$$

è l'insieme dei residui modulo n

Realmente la relazione $\equiv \pmod{n}$ è una relazione di equivalenza perché divide gli interi in n classi di equivalenza, ciascuna classe con lo stesso residuo, che sono indicate come insieme Z_n

$$[0],[1],[2],\ldots,[n-1]$$

Ciascuna classe $[r]$ di residui modulo n è definita come

$$[r] = \{a : a \in Z, a \equiv r \pmod{n}\}$$

Un richiamo di algebra (3)

p.e. le classi di residui modulo 7 sono

$$[0][1][2][3][4][5][6]$$

Che possono essere sviluppate

$$[0] = \{\ldots -21, -14, -7, 0, 7, 14, 21, \ldots\}$$
$$[1] = \{\ldots -20, -13, -6, 1, 8, 15, 22, \ldots\}$$
$$[2] = \{\ldots -19, -12, -5, 2, 9, 16, 23, \ldots\}$$
$$[3] = \{\ldots -18, -11, -4, 3, 10, 17, 24, \ldots\}$$
$$[4] = \{\ldots -17, -10, -3, 4, 11, 18, 25, \ldots\}$$
$$[5] = \{\ldots -16, -9, -2, 5, 12, 19, 26, \ldots\}$$
$$[6] = \{\ldots -15, -8, -1, 6, 13, 20, 27, \ldots\}$$

Teorema cinese del resto

(Chinese remainder theorem)

Ch'in Chiu Shao (Trattato di matematica in nove capitoli) 1247 d.c.

Obiettivo è la soluzione del problema di trovare un intero n dati i resti della divisione per diversi numeri

p.e. trovare un numero che dà:

- Un resto di 1 quando diviso per 3 $\quad x \pmod 3 = 1$
- Un resto di 2 quando diviso per 5 $\quad x \pmod 5 = 2$
- Un resto di 3 quando diviso per 7 $\quad x \pmod 7 = 3$

Trattasi della risoluzione del sistema di congruenze

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$

Teorema cinese del resto (2)

Il teorema stabilisce che dato un sistema di congruenze del tipo:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x \equiv a_r \pmod{m_r}$$

per il quale i diversi moduli sono coprimi a coppie

$$\forall (i,j) | i \neq j : GCD(m_i, m_j) = 1$$

esiste una soluzione simultanea x a tutte le congruenze e che ogni due soluzioni sono congruenti ad 1 modulo M con

$$M = m_1 m_2 \ldots m_r$$

Teorema cinese del resto (3)

Il teorema CRT dice che una soluzione delle congruenze è:

$$x_0 = \sum_{i=1}^{r} a_i y_i \frac{M}{m_i}$$

dove y_i è un intero tale che

$$y_i \frac{M}{m_i} \equiv 1 \pmod{m_i}$$

Ogni altro x che sia $\equiv x_0 \pmod{M}$ è una soluzione

Teorema cinese del resto (4)

Esempio

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$

$$M = m_1 m_2 m_3 = 3 \cdot 5 \cdot 7 = 105$$

$$\frac{M}{m_1} y_1 \equiv 1 \pmod{m_1} \rightarrow \frac{105}{3} y_1 \equiv 1 \pmod 3 \rightarrow y_1 = 2$$
$$\frac{M}{m_2} y_2 \equiv 1 \pmod{m_2} \rightarrow \frac{105}{5} y_2 \equiv 1 \pmod 4 \rightarrow y_2 = 1$$
$$\frac{M}{m_3} y_3 \equiv 1 \pmod{m_3} \rightarrow \frac{105}{7} y_3 \equiv 1 \pmod 7 \rightarrow y_3 = 1$$

$$x_0 = 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 157$$

Soddisfa il sistema di congruenze

Teorema cinese del resto (5)

Usato per accelerare i calcoli modulari

Si lavora modulo un prodotto di numeri

p.e. mod $M = m_1 m_2 \ldots m_r$

Il teorema cinese del resto permette di lavorare

nei diversi moduli m_i separatamente

Siccome il costo computazionale è proporzionale alla dimensione,

ciò è più veloce di lavorare nel modulo M completo

Radici primitive

Il teorema di Eulero stabilisce che:

$$\forall\big((a,n) : GCD(a,n)=1\big)\ \ a^{\phi(n)} \equiv 1 \pmod{n}$$

Si consideri ora $a^m \equiv 1 \pmod{n}$ con $GCD(a,n) = 1$

Deve essere soddisfatta per $m = \phi(n)$ ma può esserlo anche per valori di m più piccoli

Il valore più piccolo è chiamato ordine di $a \pmod{n}$ o anche lunghezza del periodo generato da a

Si osservi un esempio

$a = 7,\ n = 19$

$\phi(19) = 18$

$7^1 = 7 \equiv 7 \pmod{19}$

$7^2 = 49 = 19\cdot 2 + 11 \equiv 11 \pmod{19}$

$7^3 = 343 = 19\cdot 18 + 1 \equiv 1 \pmod{19}$ 

$7^4 = 2401 = 19\cdot 126 + 7 \equiv 7 \pmod{19}$

.....

$7^{18} = 1628413597910449 = 19\cdot 85705978837392 + 1 \equiv 1 \pmod{19}$

Radici primitive (2)

In sostanza: per $a = 7,\ n = 19,\ m = 3$ $\qquad 7^3 \equiv 1 \pmod{19}$

Ora

$$7^{j+3} \pmod{19} = 7^j \cdot 7^3 \pmod{19} = \left[(7^j \bmod 19)(7^3 \bmod 19)\right] \bmod 19 =$$

$$= \left[(7^j \bmod 19) \cdot 1\right] \bmod 19 = 7^j \bmod 19$$

La sequenza delle potenze è periodica e la lunghezza del periodo è il più piccolo esponente positivo m, tale che $a^m \equiv 1 \pmod{n}$

Radici primitive (3)

Potenze degli interi (mod 19)

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^10	a^11	a^12	a^13	a^14	a^15	a^16	a^17	a^18
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Radici primitive (4)

Tutte le sequenze terminano in 1

La lunghezza delle sequenze è un divisore di $\phi(19) = 18$

Alcune sequenze hanno lunghezza 18

Se il più piccolo m è $= \phi(n)$ allora a
è detto una radice primitiva di n

Le potenze successive di una radice primitiva di n

$$a, a^2, \ldots, a^{\phi(n)}$$

sono distinte (mod n) e coprime ad n

Se n è primo, allora le potenze successive di a fino ad n-1 sono distinte

Non tutti gli interi posseggono radice primitiva

Sono utili, ma relativamente laboriose da trovarsi

Logaritmi Discreti o Indici

Il problema inverso alla esponenziazione è trovare

il **logaritmo discreto** di un numero modulo p

Cioè trovare x con $a^x = b \pmod{p}$

Scritto come $x = \log_a b \pmod{p}$ o $x = \mathrm{ind}_{o,p}(b)$

Se a è una radice primitiva il logaritmo discreto

esiste sempre, diversamente non è detto

$x = \log_3 4 \pmod{13}$ (x st $3x = 4 \bmod 13$) non ha risposta

$x = \log_2 3 \pmod{13} = 4$ provando le potenze successive

Mentre l'esponenziazione è relativamente facile, trovare un logaritmo discreto è generalmente un problema molto difficile