

Lezione del

4/10/2021

Test di Primarie -

OK 16:00



Primo (N)

fr (i=2; i < \sqrt{N} ; i++)

if ($N \% i = 0$) return FALSE;

$\hookrightarrow \Theta(\log^2 N)$

return TRUE

al più \sqrt{N} iterazioni, crescita di costo $\Theta(\log^2 N)$

I = insieme di input = $N \in \mathbb{N}, \mathbb{Z}$

$|I| = \text{dim. di } I = \Theta(\log_2 N)$

$$T(|I|) = \Theta(\underbrace{\sqrt{N} \cdot \log^2 N}_{|I|^2}) = \Theta(|I|^2 \cdot 2)$$

$|I|$

$$|I| = \Theta(\log n)$$

$$N = \Theta(2^{|I|})$$

$$\sqrt{N} = N^{1/2} = \Theta(2^{\frac{|I|}{2}})$$

Algoritmi Randomi

LAS VEGAS
(Quick Sort)

generano un risultato
SICURAMENTE CORRETTO
in un TEMPO
PROBABILMENTE BREVE

MONTE-CARLO
(test di primalità)

generano un risultato
PROBABILMENTE CORRETTO
in un tempo ~~scorso~~
SICURAMENTE BREVE

probabilmente erroneo
deve essere mettersi in
risultato e ottimamente
preciso

Test di primalità di MILLER - RABIN

N , ~~è~~ intero di n cifre, dispari

$$N-1 = 2^w \cdot z$$

z : dispari

$$N = 45 \quad N-1 = 44 = \underbrace{2^2 \cdot 11}$$

$w \in \mathbb{Z}$ si determina in $\mathcal{O}(\log N)$ passi

$$2 \leq y \leq N-1$$

intero arbitrario

N primo \Rightarrow

P1: $\text{MCD}(N, y) = 1$

(quindi pochi N è primo)

P2: $y^{\frac{2^w}{2}} \mod N = 1 \quad \text{OR}$

$\exists i, 0 \leq i \leq w-1$ t.c.

$$y^{2^i \cdot 2} \mod N = -1$$

$w \leq \log N$

Lemma (Miller, Robin)

Se N è un numero composto, il numero di infi (y) compresi tra 2 e $N-1$ che soddisfano entrambi i prediciuti P_1 e P_2 è minore di $N/4$

$$\#\{2 \leq y \leq N-1 \mid P_1(y) = \text{TRUE} \text{ AND } P_2(y) = \text{TRUE}\} < \frac{N}{4}$$

→

Probabilità di scegliere
un testimone y che
rende veri P_1 e P_2

$$< \frac{N/4}{N-2} < \frac{1}{4}$$

Idee

scelto a caso $y \in [2, N-1]$

\rightarrow se uno dei due predici è falso \Rightarrow N è sicuramente composto

\rightarrow se i predici sono entrambi veri

\Rightarrow N è composto con prob. $< \frac{1}{4}$

e dunque è primo con prob. $> 1 - \frac{1}{4} = \frac{3}{4}$

Iterando k volte con k scelte casuali e indipendenti
del testimone y :

\hookrightarrow prob. di errore \rightarrow a $(\frac{1}{4})^k$

VERIFICA (N, y) // controlla la validità del certificato y
 y è un certificato del fatto che N sia composto

```

if ( $P_1 == \text{false}$  OR  $P_2 == \text{false}$ ) return 1 //  $N$  è certamente
else return 0; //  $N$  è probabilmente primo
                (prob. errore  $\leq \frac{1}{4}$ )
    
```

TEST MR (N, k)

```

for ( $i=1$ ;  $i \leq k$ ;  $i++$ ) {
    - scopri a caso  $y \in [2, N-1]$  //  $N$  è certamente
    - if (VERIFICA ( $N, y$ ) == 1) return 0;
}
return 1; //  $N$  è primo con prob di errore  $\leq \left(\frac{1}{4}\right)^k$ 
    
```

$$N - 1 = 2^w \cdot z$$

$$w = 1$$

$$\Rightarrow z =$$

$$\frac{N-1}{z}$$

$$y^2 \bmod N$$

Algoritmo di ESPOENZIAZIONE VELoce

O della QUADRATURE SUCCESSIVE.

Dettivo \rightarrow # operazioni $O(\log z)$

$$x = 9^{65} \bmod 11 = 9^{32+8+4+1}$$

Calcoliamo le potenze

minore a 9^{32}

9^{2^i} , fermo ad.
 \downarrow
osservando come quadrato
dello precedente

$$9^{65} \bmod 11 = 9^{32+8+4+1}$$

$$9^2 \bmod 11 = 4$$

$$9^4 \bmod 11 = (4)^2 \bmod 11 = 5$$

$$9^8 \bmod 11 = 5^2 \bmod 11 = 3$$

$$9^{16} \bmod 11 = 3^2 \bmod 11 = 9$$

$$9^{32} \bmod 11 = 9^2 \bmod 11 = 4$$

5 multiplikation

in generale

~~def~~ t

multiplikation

$$t = \lceil \log_2 z \rceil$$

$$9^{65} = (9^{32} \bmod 11) * (9^8 \bmod 11) * (9^4 \bmod 11) * (9^2 \bmod 11)$$

$$4 * 3 * 5 * 9 \bmod 11: \quad (1)$$

$y^0(t)$
Multipl.

Algorithmus Quadrature Successive

- Si scomponе l'esponente z in una somma di potenze di 2

$$z = \sum_{i=0}^t k_i \cdot 2^i$$

- Si calcolano tutte le potenze

$$y^{2^i} \bmod s = (y^{2^{i-1}})^2 \bmod s$$

Come quadrato della potenza precedente

- Si calcola $x = y^z \bmod s$ come

$$x = \left(\prod_{i: k_i \neq 0} y^{2^i} \bmod s \right) \bmod s$$

$$\left\{ \begin{array}{l} x = y^z \bmod s \\ y, z, s \text{ sono} \\ \text{dello stesso ordine} \\ \text{di grandezza} \\ k_i \in \{0, 1\} \end{array} \right.$$

$$t = \lfloor \log_2 z \rfloor = \Theta(\log z)$$

$$\underbrace{\Theta(\log z)}_{1 \leq i \leq t} \text{ multipl.}$$

$$\underbrace{\Theta(\log z)}_{\text{Multiplic.}}$$

Valevazione di P2:

→ n' calcola (QS)

$$y^2 \bmod N$$

$$= 1$$

$$= -1$$

$$\neq \pm 1$$

ok

ok

else if 2

P2 = true

P2 = true

$$y^2 \bmod N$$



$$y^{2^2} \bmod N$$

else
2

$$y^{4^2} \bmod N$$

else
2

$$= -1$$



P2 vero

fi:

$$y^{2 \cdot 2^i} \bmod N = -1$$

$$0 \leq i \leq \omega - 1$$

$$\sum_{i=1}^{\omega} \Theta(\log N)$$

N

$$N-1 = 2^w z$$

$$z \leq \frac{N-1}{2}$$

es.

$$N-1 = 110 = 2 \cdot 55$$

$$w=1$$

$$z = \frac{N-1}{2}$$

$$N = 65$$

$$N-1 = 64 = 2^6 - 1$$

$$z=1$$

$$w = \log(N-1)$$

Generazione di numeri primi (quondam)

→ genera ziole di un numero casuale, seguite dal test di primalità.

↳ si ripete finché quando si ha un numero dichiarato primo (con prob. corretto $< \frac{1}{e^k}$)

Teorema

il numero di numeri interi primi è meno
di n tende a $\frac{N}{\log_e N}$ per $N \rightarrow +\infty$

↳ per N sufficcientemente grande, in un suo intorno
di ampiezza $\log_e N$ cade mediamente un numero primo

fatto su
polinomiale in $\log N$

↳ proporzionale allo stesso
dell' input (# cifre di N)

Primo(n) // n: #bit del numero primo da generare
(Significativa)

// genera un numero primo di almeno n bit (prob errore < $\frac{1}{e^k}$)

S = numero casuale di n-2 bit

N = 1 S 1

while (TestPR(N, k) == 0) N = N + 2

return N // N è un numero primo di n+1 bit

Costo

$\mathcal{O}(n^4)$

n = n° bit di N

$\hookrightarrow \mathcal{O}(n)$ volte il test PR
 $\hookrightarrow \mathcal{O}(n^3)$

CLASSE

RP

RANDOM POLYNOMIAL



→ dassi dei problemi decisionali VERIFICABILI
in tempo polinomiale randomico.

TI: problema decisionale

x : istanza di input di TI

y è un certificato probabilistico di x de

- y è di lunghezza al più polinomiale in $|x|$
- y è scritto perfettamente a caso da un insieme associato a x

dein. x
 \sim

A: Algoritmo di verifica polinomiale

$A(x, y)$

$A(x, y)$ è ottenuta in tempo polinomiale

da x NON possiede le proprietà $(\text{TI}(x) = 0)$

Con certezza

oppure

ottenuta da x possiede le proprietà $(\text{TI}(x) = 1)$

Con probabilità $> \frac{1}{2}$

$(\frac{3}{4} \text{ nel caso del test di primarietà})$

CONCLUSIONI

P $\not\subseteq$ RP $\not\subseteq$ NP