

CRITTOGRAFIA

lezione di
martedì 6 ottobre

ore 16:15



$$x = 9^{45} \bmod 11$$

$$45 = 2^5 + 2^3 + 2^2 + 2^0 = 32 + 8 + 4 + 1$$
$$32 + 8 + 4 + 1$$

$$x = 9 \bmod 11$$

$$= (9^{32} \bmod 11 \cdot 9^8 \bmod 11 \cdot 9^4 \bmod 11 \cdot 9^1 \bmod 11) \bmod 11$$

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

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

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

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

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

$$x = 4 * 3 * 5 * 9 \bmod 11$$

$$= 1$$

$$x = y^2 \bmod N$$

t quadrature

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

$O(t)$ multiplication

$$y \in [2, N-1]$$

N è primo \Rightarrow

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

P2

$$y^2 \bmod N = 1$$

OR

$$\exists i: i \in \{0, \omega-1\} \text{ t.c.}$$

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

$$\begin{cases} \omega = O(\log_2 N) \\ 2 = O(N) \end{cases}$$

$$y^2 \bmod N,$$

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

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

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

ω elezioni

al quadrato

$$\omega = O(\log N)$$

Generazione di numeri primi

→ generazione di un numero casuale,
seguito dal test di primalità

↳ si ripete fino a quando si ha un
numero dichiarato primo.

Densità dei numeri primi sull'asse degli interi

il numero di interi primi e minori di N

$$\rightarrow \frac{N}{\log_e N} \quad \text{per } N \rightarrow +\infty$$

↳ per N sufficientemente grande, in un buco intorno
di $\log_e N$ cade mediamente un numero primo
proportionalmente alla dimensione dell'intervallo

Primo $(n) \xrightarrow{k}$ // n: # di bit del numero primo generato

// genera un numero primo di

// almeno n bit (prob. di errore $< \left(\frac{1}{4}\right)^k$)

S = sequenza di n-2 bit prodotti da un generatore
binario pseudo-casuale

$N = \left(1 \ S^t \ 1\right)_2$ // N contiene n bit

while (TEST_MR(N, k) == 0) { } $\{ n = n + 2 \}$

return N;

costo
polinomiale
 $\tilde{O}(n = \log N)$

$\tilde{O}(n^3)$

Algoritmo polinomiale
 $\hookrightarrow \tilde{O}(n^4)$

$$n = \log N$$

n' pettati
 $O(n)$
volte

CLASSE

RP

random polynomial

↳ classe dei problemi decisionali verificabili in tempo
polinomiale randomizzato

Π

x : istanza di input

y : certificato probabilistico di x è

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

A : algoritmo di verifica polinomiale

$A(x, y)$

A(x, y)

in tempo polinomiale

Attesa con certezza che x NON possiede
le proprietà ($\pi(x) = 0$)

oppure attesa che x possiede le proprietà
esaminata dal problema con probabilità $> \frac{1}{2}$

~

3/4
per ogni
principio

P $\not\subseteq$ RP $\not\subseteq$ NP
CONG. CONG.

