

una possibile funzione unidirezionale

- moltiplicare due interi a n bit è **facile** (in $\mathcal{O}(n^2)$ con l'algoritmo usuale)
- trovare un primo a n bit, e verificare che è primo, è **facile** (vedremo poi)
- fattorizzare un numero a n bit è **difficile** ($2^{cn^{1/3}}$)
- si può costruire un crittosistema a chiave pubblica basato su questa osservazione?

crittosistema RSA

- Sia $N = pq$, p, q primi. Sia $\mathcal{P} = \mathcal{C} = \mathbb{Z}_N$.
- Lo spazio delle chiavi è

$$\mathcal{K} = \{(N, p, q, d, e) \mid de \equiv 1 \pmod{\phi(N)}\}.$$

- Se $k = (N, p, q, d, e)$ è una chiave, poniamo
- $e_k(x) = x^e \pmod{N}$
- N e e sono la **chiave pubblica**
- $d_k(y) = y^d \pmod{N}$
- p, q, d sono la **chiave privata**

Problemi facili

- ① dato un intero N , vedere se è primo
- ② dati a e N , trovare (a, N) ; se è 1, calcolare l'inverso di a modulo N (alg. di Euclide – polinomiale)
- ③ calcolare la f.ne $x \rightarrow x^e \pmod{N}$

Problemi difficili

- ④ dato un intero N , fattorizzarlo
- ⑤ dato un intero N , calcolare $\phi(N)$
- ⑥ dati N e e , trovare d tale che $(x^e)^d = x \pmod{N}$

problemi “facili” - primalità

- ci sono **infiniti numeri primi** (Euclide)
- la dimostrazione è per assurdo (è la più celebre dimostrazione per assurdo): supponiamo ci siano solo un numero finito di primi, e siano questi p_1, p_2, \dots, p_k
- consideriamo il numero $p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$
- questo numero non è divisibile per nessuno dei p_1, p_2, \dots, p_k – e allora quali sono i suoi fattori primi?
- ci sono infiniti primi – quanti sono i numeri primi che precedono un dato intero x ?

teorema dei numeri primi

- $\pi(x)$ = numero di primi p con $p \leq x$
- esempio: $\pi(30) = 4 + 4 + 2 = 10$
- **teorema dei numeri primi**: asintoticamente, $\pi(x) \approx \frac{x}{\log(x)}$
- congetturato da Legendre, Gauss fine 700 – dimostrato da Hadamard, de la Vallée Poussin fine 800
- dato un intero positivo N , la probabilità che un numero $< N$ scelto a caso sia primo è $\pi(N)/N$, per N molto grande $\approx 1/\log(N)$
- esempio: la probabilità che un numero casuale con al più 100 cifre decimali sia primo è $\approx 1/\log(10^{100}) \approx 1/230$
- se sappiamo controllare se un intero è primo, trovare primi grandi è facile

test di primalità

- dato un intero N a n bit, come scoprire se è un primo?
- posso provare a fattorizzarlo per **divisioni successive**: devo fare al più \sqrt{N} divisioni, quindi è in $\mathcal{O}(2^{n/2})$ – scopro se è primo, e trovo anche i fattori
- i test di primalità scoprono se N è primo **senza dire niente dei suoi fattori**
- un numero non primo si dice **composito**

test di primalità - AKS

- fino al 2002 si conoscevano solo test di primalità polinomiali **probabilistici**, non **deterministici**
- nel 2002, M. Agrawal insieme a due suoi dottorandi, Kayal e Saxena, hanno trovato un algoritmo **polinomiale** per determinare la primalità
- inizialmente, in $\mathcal{O}(n^{12})$ – nel 2005, Lenstra e Pomerance lo portano a $\mathcal{O}(n^6)$
- **primes** è in **P**

test deterministici e test probabilistici

- un test **deterministico** dà una risposta certa: N è primo o non lo è
- un test **probabilistico** \mathcal{T} consiste in una successione di test $\{\mathcal{T}_m\}_{m \in \mathbb{N}}$ e una successione che va a zero $\{\epsilon_m\}_{m \in \mathbb{N}}$ tale che,
 - se N **non** passa il test \mathcal{T}_m allora **non è primo**,
 - la probabilità che N superi i test $\mathcal{T}_1, \dots, \mathcal{T}_m$ e non sia primo è minore di ϵ_m
- i test di primalità probabilistici più usati sono quello di **Solovay-Strassen** (1977) e quello di **Miller-Rabin** (1980)
- il test di Miller-Rabin deriva da un test deterministico (dovuto a Miller) – che però assume l'ipotesi di Riemann generalizzata

- per mostrare che un numero N non è primo si mostra che non si comporta come un primo
- si “cercano prove” del fatto che N non si comporta come un primo
- senza cercare i suoi fattori

PT di Fermat e test di Fermat

- il PTdF dice che, se p è un primo e $1 \leq a \leq p - 1$, allora $a^{p-1} \equiv 1 \pmod{p}$
- vogliamo scoprire se N è primo – se trovo $a \leq N - 1$ e $a^{N-1} \not\equiv 1 \pmod{N}$ sappiamo per certo che N non è primo – senza sapere niente sui suoi fattori
- per esempio, $2^{322} \equiv 157 \pmod{323}$; quindi 323 non è primo ($323 = 17 \cdot 19$)
- si dice che 2 è un testimone di Fermat per 323
- questo è il **test di Fermat**
 - prendo $a < N$, calcolo (a, N) ; se $\neq 1$, N non è primo
 - se $(a, N) = 1$, calcolo $a^{N-1} \pmod{N}$ – se $\not\equiv 1 \pmod{N}$ allora N non è primo

pseudoprimi

- se però $a^{N-1} \equiv 1 \pmod{N}$ – non posso concludere che N è primo
- per esempio $2^{340} \equiv 1 \pmod{341}$, ma $341 = 11 \cdot 31$
- si dice che N è uno **pseudoprimo** in base a se N non è primo ma $a^N \equiv a \pmod{N}$. 341 è uno pseudoprimo in base 2.
- si dice anche in questo caso che 2 è un ‘bugiardo di Fermat’ per 341
- possiamo provare diversi valori per a : per esempio $3^{341} \not\equiv 3 \pmod{341}$ – quindi 341 non passa il test!

numeri di Carmichael

- non basta: esistono numeri N che sono **pseudoprimi** in base a **per ogni possibile base a** dove $1 < a < N$ e $(a, N) = 1$
- un tale N si dice **numero di Carmichael**
- per esempio, si può vedere che 561 è un ndC (è il più piccolo)
- il test di Fermat non va bene
- dà comunque un'idea di come può funzionare un test di primalità

critério di Eulero

- critério di Eulero: se p è primo, allora

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

- dato N , se esiste a tale che

$$\left(\frac{a}{N}\right) \not\equiv a^{\frac{N-1}{2}} \pmod{N}$$

allora N non è primo

- e a si dice testimone di Eulero per N
- per esempio, 15 non è primo (!) perchè $2^7 = 128 \equiv 8 \pmod{15}$ ma

$$\left(\frac{2}{15}\right) = 1$$

Test di Solovay-Strassen

- possiamo costruire un test del tutto analogo al test di Fermat usando il critério di Eulero
 - prendo $a < N$, calcolo (a, N) ; se $\neq 1$, N non è primo
 - se $(a, N) = 1$, calcolo $a^{\frac{N-1}{2}} - se \not\equiv \left(\frac{a}{N}\right) \pmod{N}$ allora N non è primo
- N si dice uno **pseudoprimo di Eulero** in base a se N non è primo ma passa il test:

$$\left(\frac{a}{N}\right) \equiv a^{\frac{N-1}{2}} \pmod{N}$$

- ma in questo caso le cose funzionano: ci sono “pochi” pseudoprimi di Eulero

Teorema

Sia N numero intero positivo dispari non primo. I numeri $a < N$ primi con N tali che N sia uno pseudoprimo di Eulero in base a , sono non più della metà di tutti i possibili a .