Fattorizzazione di interi e crittografia

Anna Barbieri

Università degli Studi di Udine

Corso di Laurea in Matematica

Il teorema fondamentale dell'aritmetica

Divisibilità in $\mathbb{N}$

Dati due numeri naturali a, $b \in \mathbb{N}$, diciamo che a divide b se esiste $n \in \mathbb{N}$ tale che $b = n \cdot a$.

Diciamo che a è un divisore di b e scriviamo $a|b$.

Numeri primi

Un numero naturale $a \in \mathbb{N}$ si dice primo se $a \neq 1$ e i suoi unici divisori sono 1 e a.

La primalità è un concetto che ha senso solo in $\mathbb{N}$?

Esempio

$$V = \{A, E, I, O, U\}$$

Moltiplicazione in V:

$A \cdot A = A$	$E \cdot A = A$	$I \cdot A = A$	$O \cdot A = A$	$U \cdot A = A$
$A \cdot E = A$	$E \cdot E = E$	$I \cdot E = I$	$O \cdot E = O$	$U \cdot E = U$
$A \cdot I = A$	$E \cdot I = I$	$I \cdot I = U$	$O \cdot I = A$	$U \cdot I = A$
$A \cdot O = A$	$E \cdot O = O$	$I \cdot O = A$	$O \cdot O = U$	$U \cdot O = A$
$A \cdot U = A$	$E \cdot U = U$	$I \cdot U = A$	$O \cdot U = A$	$U \cdot U = A$

I e O sono primi in V.

Il teorema fondamentale dell'aritmetica

Teorema fondamentale dell'aritmetica

Ogni intero maggiore di 1 si può scrivere, in modo unico a meno dell'ordine, come prodotto di numeri primi.

Esistono insiemi, anche numerici, in cui non vale l'unicità di fattorizzazione!

Esempio:

$$X := \{1, 5, 9, 13, 17, \dots\}$$

Il teorema fondamentale dell'aritmetica

$$X_4 := \{1, 5, 9, 13, 17, \dots\} = \{4k + 1,\ k = 0, 1, 2, \dots\}$$

$$\cdot : \text{quella definita in } \mathbb{N}$$

$$(4k + 1) \cdot (4h + 1) = 4\,(4kh + k + h) + 1 \in X$$

Vale

$$\left\{ \begin{array}{c} \text{elementi di } X_4 \\ \text{primi in } \mathbb{N} \end{array} \right\} \subset \left\{ \begin{array}{c} \text{elementi di } X_4 \\ \text{primi in } X_4 \end{array} \right\}$$

Infatti:

- Se $\alpha = 4k + 1$ è primo in $\mathbb{N}$ significa che è diviso solo da 1 e da sé stesso e quindi sarà primo anche in $X_4 \subset \mathbb{N}$.

MA

- esempio: $9 \in X_4$

  In $\mathbb{N}$ $\quad 9 = 3 \cdot 3$

  In X_4 esiste un divisore d di 9 con $1 < d < 9$??

  9 è primo in X_4!

Quindi esistono numeri che in $\mathbb{N}$ non sono primi, ma risultano primi in X_4.

$$9 \quad 21 \quad 49 \quad \in X_4, \quad \text{primi}$$

$$9 = 3 \cdot 3 \quad 21 = 3 \cdot 7 \quad 49 = 7 \cdot 7$$

eppure ...

$$9 \cdot 49 = 441 = (21)^2$$

Dunque in X_4 esistono dei numeri composti per i quali sono ammesse due distinte fattorizzazioni in prodotti di primi.

Il teorema fondamentale dell'aritmetica

$$X_5 = \{5k + 1 \mid k = 0, 1, 2, \dots\} = \{1, 6, 11, 16, \dots\}$$

$$21 \cdot 26 = 546 = 6 \cdot 91$$

X_4 e X_5 sono a fattorizzazione NON unica.

Scoperto il trucco!

Domanda: Quanto detto vale $\forall\ X_n,\ n \in \mathbb{N}_0$? $X_6,\ X_7,\ X_{11},\ \dots$

Il teorema fondamentale dell'aritmetica

Teorema fondamentale dell'aritmetica.

Ogni intero maggiore di 1 si può scrivere, in modo unico a meno dell'ordine, come prodotto di numeri primi.

Esistenza della fattorizzazione, ossia ogni numero naturale $n > 1$ è prodotto di primi.

Procediamo per induzione generalizzata:

- $n = 2$.
- Supponiamo che l'enunciato sia vero per ogni intero m con $1 < m < n$, vogliamo dimostrarlo per n.
  Caso 1) n è primo.
  Caso 2) n non è primo. $\exists a$ tale che $a \mid n$, $1 < a < n$.
  $n = a \cdot b$ e $1 < b < n$. Per ipotesi induttiva $a = a_1 \cdots a_r$, $b = b_1 \cdots b_t$, a_i, b_j primi. Pertanto $n = a_1 \cdots a_r b_1 \cdots b_t$.

Il teorema fondamentale dell'aritmetica

Unicità della fattorizzazione, a meno dell'ordine dei fattori.

$$n = p_1 \cdots p_h = q_1 \cdots q_k \textbf{, con } p_i, q_j \textbf{ primi}$$

$$\Downarrow$$

$$h = k \textbf{ e } \forall\ i = 1, \ldots, h\ \exists! j \in \{1, \ldots, k\} \textbf{ t. c. } p_i = q_j.$$

Sia per assurdo

$$N = p_1 \cdots p_h = q_1 \cdots q_k$$

minimo intero che si fattorizza in due modi diversi.

$\forall\ i \in \{1, \ldots, h\}$, $j \in \{1, \ldots, k\}$ vale $p_i \neq q_j$.

$$p_1 > q_1 \Rightarrow M = (p_1 - q_1)(p_2 \cdots p_h) = N - q_1 \cdot p_2 \cdots p_h < N.$$

Il teorema fondamentale dell'aritmetica

$$M = (p_1 - q_1)(p_2 \cdots p_h) = r_i \cdots r_t \cdot p_2 \cdots p_h =$$
$$= q_1 (q_2 \cdots q_k - p_2 \cdots p_h) = q_1 s_1 \cdots s_l,$$

r_i primi, s_j primi.

q_1 non compare nella prima fattorizzazione.

$M < N$ ammette due fattorizzazioni diverse, contro l'ipotesi che N fosse il minimo con questa proprietà.

Divisibilità in $\mathbb{N}$

I numeri naturali positivi $\mathbb{N}_0$

- l'unità 1
- i primi 2, 3, 5, 7, 11, 13, . . . , 2011, . . .
- i numeri composti 4, 6, 8, 9, . . . , 2013, . . .

Divisibilità in $\mathbb{N}$

Euclide, III sec. a. C.

Fermat, 1601-1665.

Gauss, 1777-1855.

Divisibilità in $\mathbb{N}$

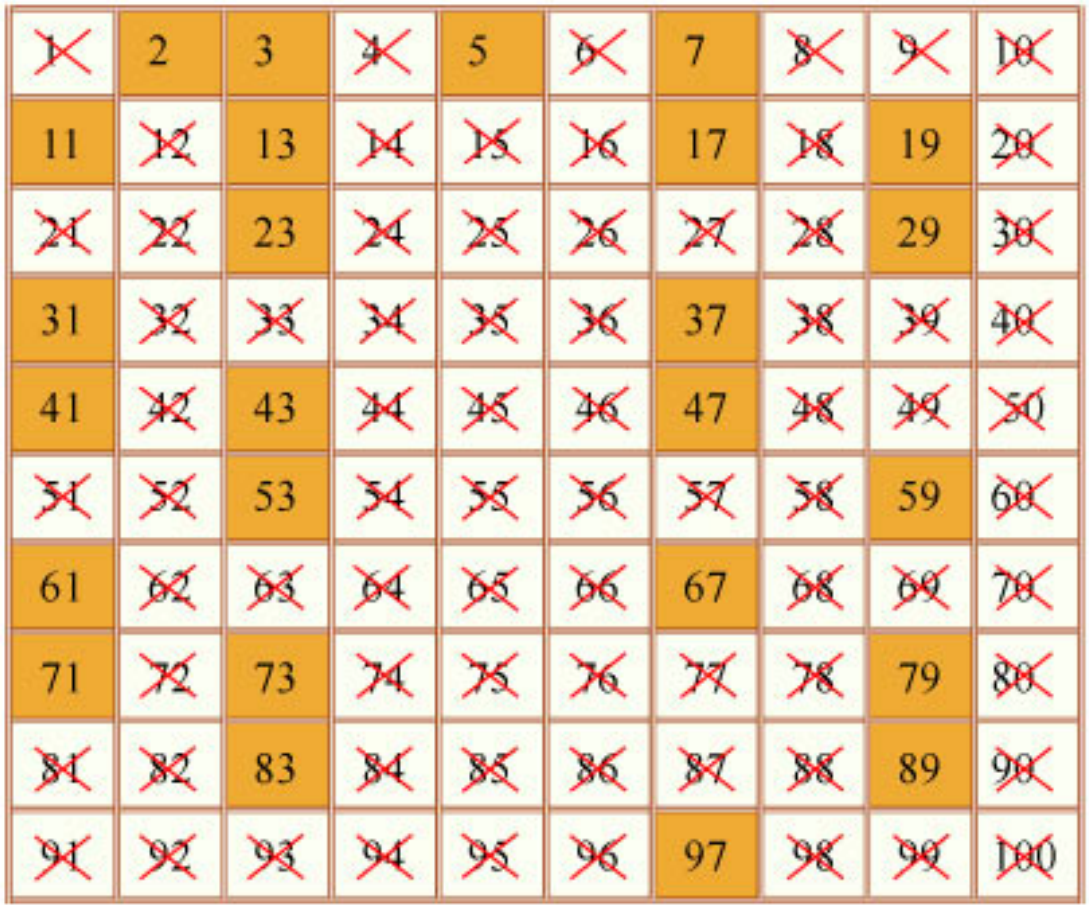
Quanto ancora ci resta da conoscere!

- la funzione di Riemann
- test di primalità
- algoritmi di fattorizzazione
- ...

Riemann, 1826-1866.

Il crivello di Eratostene

Algoritmo dovuto ad Eratostene di Cirene, che fornisce tutti i numeri primi in un intervallo fra 2 e un numero $N \in \mathbb{N}$.



In realtà ci accorgiamo subito che basta arrivare a $\frac{N}{2}$ nella cancellazione: i numeri fra $\frac{N}{2}$ ed N che non saranno già stati cancellati, potranno infatti cancellare solo interi maggiori di N.

Un'osservazione attenta della tabella generata mediante l'algoritmo di Eratostene ci suggerisce dunque che, da un certo punto in poi, tutti i numeri non precedentemente cancellati sono primi: nessuno di questi verrà cancellato nel corso di un'esecuzione ulteriore del procedimento.

Questo limite è $\sqrt{N}$

Divisibilità in $\mathbb{N}$

Dato un primo p e un intero $n \in \mathbb{N}$, stabilire se $p \mid n$.

- $p = 2$
- $p = 3$
- $p = 5$
- $p = 7$???

Divisibilità per 3

Criterio di divisibilità per 3.

$$10 = 3 \cdot 3 + 1;$$
$$100 = 99 + 1 = 3 \cdot 33 + 1$$
$$1000 = 999 + 1 = 3 \cdot 333 + 1$$
$$\dots$$

Dato $\mathbb{N} \ni n = n_m n_{m-1} \cdots n_0$, dove n_i siano le cifre che compongono il numero,

$$\begin{aligned} n &= n_m 10^m + n_{m-1} 10^{m-1} + \cdots + n_0 \\ &= n_m (3 \cdot k_m + 1) + n_{m-1} (3 \cdot k_{m-1} + 1) + \cdots + n_0 = \\ &= 3 \cdot (n_m \cdot k_m + \cdots + n_1 \cdot k_1) + \underbrace{n_m + n_{m-1} + \cdots + n_0}_{*} \end{aligned}$$

Divisibilità in $\mathbb{N}$

n è divisibile per 3 $\Leftrightarrow$ lo è la somma delle sue cifre.

$$2580471 \quad \rightarrow \quad 2+5+8+0+4+7+1=27 \quad \rightarrow \quad 2+7=9=3\cdot 3$$

Generalizzazione: $p \in \mathbb{N}$, $\mathrm{MCD}(p,10)=1$

$$\begin{aligned} n &= n_m 10^m + n_{m-1}10^{m-1} + \cdots + n_0 \\ &= n_m\left(p\cdot k_m + r_m\right) + n_{m-1}\left(p\cdot k_{m-1} + r_{m-1}\right) + \cdots + n_0 \\ &= p\cdot\left(n_m\cdot k_m + \cdots + n_1\cdot k_1\right) + \underbrace{n_m r_m + n_{m-1}r_{m-1} + \cdots + n_0}_{*} \end{aligned}$$

n è divisibile per p $\Leftrightarrow$ lo è $n_m r_m + n_{m-1}r_{m-1} + \cdots + n_0$.

Congruenza fra numeri interi

Dati n, $r \in \mathbb{Z}$ e $a \in \mathbb{Z}_0$, diciamo che $n \equiv r \pmod{a}$ se e solo se esiste un numero $q \in \mathbb{Z}$ tale che $n = q \cdot a + r$.

$$n = q \cdot a + r \qquad n \equiv r \pmod{a}$$

Scriviamo anche $n \equiv_a m$ per brevità. Si legga: n ed m sono congruenti *modulo* a.

Esempi

$$4 \equiv 1 \pmod{3} \qquad \text{perchè } 4 = 3 + 1$$
$$4 \equiv -2 \pmod{3} \qquad \text{perchè } 4 = 6 - 2 = 2 \cdot 3 - 2$$
$$27 \equiv 2 \pmod{5} \qquad \text{perchè } 27 = 25 + 2 = 5 \cdot 5 + 2$$

Divisibilità per 7

Criterio di divisibilità per 7.

$$
\begin{aligned}
1 &\equiv 1 \pmod 7 \\
10 &\equiv 3 \pmod 7 \\
100 &\equiv 2 \pmod 7 \\
1000 &\equiv 6 \equiv -1 \pmod 7 \\
10000 &\equiv 4 \pmod 7 \\
100000 &\equiv 5 \pmod 7 \\
1000000 &\equiv 1 \pmod 7 \\
10000000 &\equiv 3 \pmod 7 \\
&\dots
\end{aligned}
$$

Divisibilità per 7

Quindi basta moltiplicare ciascuna cifra del numero che stiamo studiando per un opportuno coefficiente e sommare.

1	10	100	1 000	10 000	100 000	
1	3	2	-1	4	5	

Uno schema ripetuto ogni 6 cifre.

Divisibilità per 7

Esempio: 852743

$$\underbrace{8}_{\cdot 5} \quad \underbrace{5}_{\cdot 4} \quad \underbrace{2}_{\cdot(-1)} \quad \underbrace{7}_{\cdot 2} \quad \underbrace{4}_{\cdot 3} \quad \underbrace{3}_{\cdot 1}$$

$$40 \quad 20 \quad -2 \quad 14 \quad 12 \quad 3 \quad = 87$$

$$8 \cdot 3 + 7 \equiv 8 \cdot 3 \not\equiv 0 \,(\text{mod } 7)$$

Esempio: 58961

$$\underbrace{5}_{\cdot 4} \quad \underbrace{8}_{\cdot(-1)} \quad \underbrace{9}_{\cdot 2} \quad \underbrace{6}_{\cdot 3} \quad \underbrace{1}_{\cdot 1}$$

$$\begin{array}{ccccccc} 20 & & -8 & & 18 & 18 & 1 \\ -1 & & -1 & & 4 & 4 & 1 \end{array} \quad = 7$$

Divisibilità in $\mathbb{N}$

Per i primi maggiori di 10 possiamo immaginare di scrivere i numeri in base 100 se p ha due cifre, 1000 se p ha tre cifre,...

Esempio: $p = 13$

$$
\begin{aligned}
1 &\equiv 1 \pmod{13} \\
100 &\equiv -4 \pmod{13} \\
10000 &\equiv 3 \pmod{13} \\
1000000 &\equiv 1 \pmod{13} \\
100000000 &\equiv -4 \pmod{13} \\
&\dots
\end{aligned}
$$

$$
\begin{array}{cccc}
\underbrace{1}_{\cdot 1} & \underbrace{23}_{\cdot 3} & \underbrace{83}_{\cdot -4} & \underbrace{93}_{\cdot 1} \\
1 & 69 & -332 & 93 \\
1 & 4 & 6 & 2
\end{array}
$$

$$\equiv 0 \pmod{13}$$

Divisibilità in $\mathbb{N}$

Sappiamo creare schemi che funzionano quando un numero N è scritto in base 10. Lo stesso ragionamento ci porta a determinare schemi per testare la divisibilità di un numero scritto in base 2 per un termini dispari.

Divisibilità per 3 e per 5 di un numero scritto in base 2.

	1	2	4	8	16	32	64	128	256
/3	1	2	1	2	1	2	1	2	1
/5	1	2	4	3	1	2	4	3	1

$$n = n_m n_{m-1} \dots n_2 n_1$$

$$n = n_m \cdot 2^{m-1} + n_{m-1} \cdot 2^{m-2} + \dots + n_3 \cdot 2^2 + n_2 \cdot 2 + n_1$$

Congruenza fra numeri interi

Dati n, $r \in \mathbb{Z}$ e $a \in \mathbb{Z}_0$, diciamo che $n \equiv r \pmod{a}$ se e solo se esiste un numero $q \in \mathbb{Z}$ tale che $n = q \cdot a + r$.

$$n = q \cdot a + r \qquad n \equiv r \pmod{a}$$

Scriviamo anche $n \equiv_a m$ per brevità. Si legga: n ed m sono congruenti *modulo* a.

Esempi

$$4 \equiv 1 \pmod{3} \qquad \text{perchè } 4 = 3 + 1$$
$$4 \equiv -2 \pmod{3} \qquad \text{perchè } 4 = 6 - 2 = 2 \cdot 3 - 2$$
$$27 \equiv 2 \pmod{5} \qquad \text{perchè } 27 = 25 + 2 = 5 \cdot 5 + 2$$

Altri esempi

$$10 \equiv 3 \pmod 7$$
$$13 \equiv 6 \equiv -1 \pmod 7$$
$$130 \equiv -3 \pmod 7$$
$$7 \equiv 14 \equiv \cdots \equiv 105 \equiv 0 \pmod 7$$

$$-1 \equiv 1 \pmod 2$$
$$-2 \equiv 4 \pmod 6$$
$$8 \equiv -3 \pmod{11}$$
$$126 \equiv 1 \pmod 5$$

Divisibilità

$$a \mid m \Leftrightarrow m = h \cdot a + 0 \Leftrightarrow m \equiv 0 \pmod{a}$$

Residui

I possibili resti non negativi della divisione euclidea di un intero per $a \in \mathbb{Z}_0$ sono detti *residui modulo a*

L'insieme dei residui è $\{0, \ldots, a-1\}$.

Modulo un intero a riconduciamo $\mathbb{Z}$ all'insieme finito dei residui.

$\mathbb{Z}$	0	1	2	3	4	5	6	7	8	9	10
	$\longrightarrow$										
$\mathbb{Z}$ mod 3	0	1	2	0	1	2	0	1	2	0	1

Proprietà: Se $m \equiv m' \pmod{a}$ e $s \equiv s' \pmod{a}$, allora anche

$$m + s \equiv m' + s' \pmod{a} \quad \text{e} \tag{1}$$
$$ms \equiv m's' \pmod{a}\,. \tag{2}$$

Ciclicità

Esempi

$$(1) \quad 4 \equiv 11 = 10 + 1 \equiv 3 + 1 \pmod{7}$$

$$(2) \quad 3 \cdot 2 \equiv 10 \cdot 100 = 1000 \equiv 6 = \pmod{7}$$

Applicazione

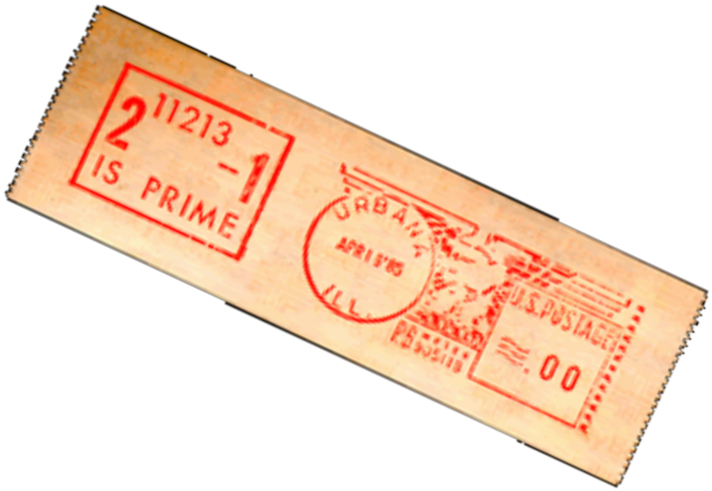
$$
\begin{aligned}
8^{720} &\equiv_3 2^{720} = 4^{360} \equiv_3 1^{360} = 1 \\
&\equiv_3 1 \pmod 3 \\
8^{720} &\equiv_5 3^{720} = \left(3^3\right)^{240} \equiv_5 2^{240} \equiv_5 2^{240} = \left(2^4\right)^{60} = 16^{60} \\
&\equiv_5 1^{60} \equiv_5 1 \pmod 5 \\
8^{720} &\equiv_{11} \left(8^2\right)^{360} \equiv_{11} -2^{360} = 2^{360} = \left(2^4\right) 60 \equiv_{11} 5^{60} \equiv_{11} \left(5^5\right)^{12} \\
&\equiv_{11} 3^{12} = \left(3^4\right)^3 \equiv_{11} 4^3 = 16 \cdot 4 \equiv_{11} 5 \cdot 4 = 20 \equiv_{11} 9 \pmod{11}
\end{aligned}
$$

$8^{720} - 1$?

Alcuni test di primalità

Algoritmi randomized per stabilire se un numero è

- primo
- composto



Distribuzione dei primi e probabilità.

Alcuni test di primalità

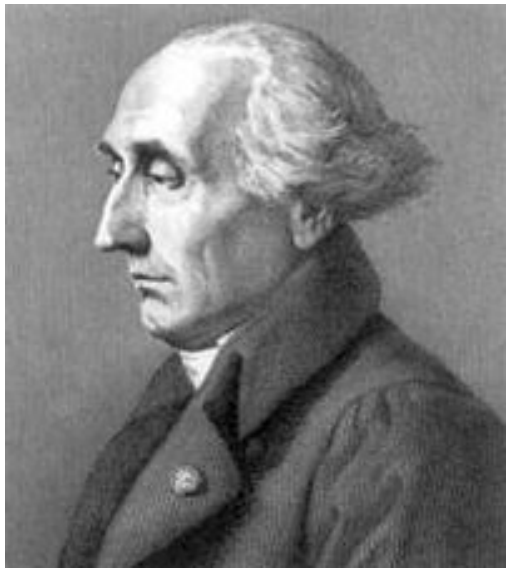
Teorema di Wilson

Un intero $n \geq 2$ è primo se e solo se $(n-1)! \equiv -1 \pmod{n}$.

(computazionalmente impegnativo se N è grande)

Ibn Al-Haytham.
Bassora, 965
Il Cairo, 1038.

Lagrange.
Torino, 1736
Parigi, 1813.



Alcuni test di primalità

Piccolo Teorema di Fermat

$$\mathbb{N} \ni p \text{ primo}$$
$$\Downarrow$$
$$a^p \equiv a \pmod{p} \ \forall\ a \in \mathbb{Z}.$$

Il Piccolo Teorema di Fermat può rivelarsi un metodo per escludere che un numero sia primo...

Alcuni test di primalità

. . . ma non è un buon test di primalità perchè

Esempi

- $2^{261} \equiv 2 \pmod{261}$, dove $261 = 3 \cdot 11 \cdot 17$;
- $3^{8911} \equiv 3 \pmod{9811}$, dove $8911 = 7 \cdot 19 \cdot 67$;
- . . .

Numeri pseudoprimi

Se n è un numero composto ed esiste $a \in \mathbb{N}$ tale che

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

allora n è chiamato poseudoprimo di base a.

Quindi se stiamo valutando n e troviamo $a \in \mathbb{N}$ tale che $a^n \not\equiv a \pmod{n}$ possiamo certamente escludere n primo ed affermare che n è composto, altrimenti possiamo affermare che n

FORSE è primo.

Alcuni test di primalità

Ipotesi: Se N NON è primo, almeno per metà dei suoi residui non nulli $a \in \mathbb{N}$ vale $a^N \not\equiv a \pmod{N}$.

Una ipotesi di tal genere suggerisce un algoritmo che sbaglia con probabilità non superiore ad $\frac{1}{2}$.

> `Prendi random un residuo` $a \pmod{N}$.
> `Se` $a^N \not\equiv a \pmod{N}$ `allora N è composto.`
> `Altrimenti N probabilmente è primo.`

Ripetendo il test la "probabilità d'errore" può essere abbassata.

MA

sfotunatamente l'ipotesi è falsa!

Numeri di Carmichael

Un numero composto $n \in \mathbb{N}$ tale che $a^n \equiv a \pmod{n}$ per ogni $a \in \mathbb{N}$ tale che $(a, n) = 1$ è detto un numero di Carmichael.

Alcuni test di primalità

Alcune osservazioni

- il test di Fermat nel caso di un numero di Carmichael fallisce decisamente!
- esistono infiniti numeri di Carmichael e il più piccolo è 561
- esistono infiniti numeri dispari pseudoprimi di base 2
- tutti i numeri di Carmichael sono dispari
- Rotkiewicz ha pubblicato un libro che contiene 58 problemi e 20 congetture sugli pseudoprimi

Alcuni test di primalità

$N, M \in \mathbb{N}$ simbolo di Legendre di N ed M $(M \mid N)$

Esiste un algoritmo che in tempo "buono" risponde alla questione se un numero sia primo sotto una certa soglia d'errore.

Prendi un intero random M fra 2 e $N-1$ e calcola (M, N).
Se $(M, N) > 1$ allora N è composto.
Altrimenti calcola $(M \mid N)$ e $M^{\frac{N-1}{2}} \pmod N$.
Se $(M \mid N) \not\equiv M^{\frac{N-1}{2}} \pmod N$. Allora N è composto.
Altrimenti N probabilmente è primo.

Alcuni test di primalità

Nel 2004 è stato pubblicato un algoritmo deterministico e di complessità polinomiale che determina se un numero è primo o composto.

Lemma

Sia $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$ e $(a, n) = 1$. Allora n è primo se e solo se

$$(x + a)^n \equiv x^n + a \pmod{n}.$$

Alcuni test di primalità

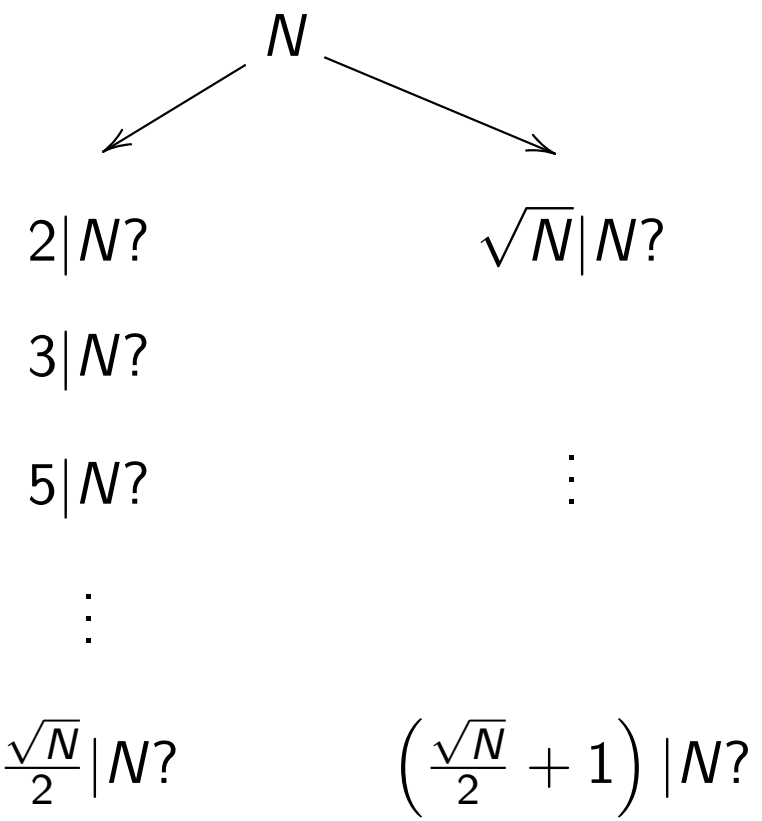
Test di primalità

$$\neq$$

fattorizzazione

Violare l'RSA

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~



Violare l'RSA

Fattorizzare un numero N di 100 cifre

$$\sqrt{N} \approx \sqrt{10^{100}} \approx 10^{50} \text{ divisioni}$$

Calcolatore potente $3 \cdot 10^9 \ \frac{\text{op}}{\text{s}}$

$$\text{tempo per 1 divisione } \frac{1}{3 \cdot 10^9} \approx 10^{-10} \text{ s}$$

10^9 processori a disposizione $\quad 10^9 \cdot 10^{10} = 10^{19} \ \frac{\text{div}}{\text{s}}$

$$\frac{10^{50}}{10^{19}} = 10^{31} \text{ s} \Rightarrow \frac{10^{31}}{3600} \text{ h} = \frac{\frac{10^{31}}{3600}}{24} \text{ gg} = \frac{\frac{\frac{10^{31}}{3600}}{24}}{365} \text{ aa}$$
$$\approx 3 \cdot 10^{23} \text{ anni!!!}$$

La *RSA Security Inc.* gestisce una sfida a livello mondiale, ove vengono premiati coloro che fattorizzano gli interi proposti da loro e pubblicati sul WEB in una particolare lista.

$$
\begin{aligned}
&7403756347956171282804679609742957314259318888923 1\\
&2890849362326389727650340282662768919964196251178 4\\
&3995894330502127585370118968098286733173273108930 9\\
&0055250511687706329907239638078671008609696253793 4\\
&650563796359
\end{aligned}
$$

Violare l'RSA

Fattorizzare $N = p_1 \cdot p_2$

- forza bruta
- sfruttare debolezze algoritmi che generano primi
- metodi più intelligenti??

Grazie!