NUMERI E CRITTOGRAFIA

Carlo Toffalori

I numeri naturali

La storia del linguaggio numerico

I numeri naturali $0,\ 1,\ 2,\ 3,\ 4,\ \ldots$ $\quad \mathbb{N}$

- apparentemente semplici e facili,
- nascondono i più grossi misteri della Matematica.

Due citazioni (libere)

L. Kronecker: *"sono i soli creati da Dio"*
A. Weil: *"dimostrano l'esistenza di Dio e del Diavolo".*

Ci sono problemi sui naturali che l'uomo non sa risolvere; in compenso sa dimostrare questa sua incapacità. Allora

* senso di qualcosa che ci trascende (Dio?)
* dispetto di provare solo la propria incapacità
  (un Diavolo si è messo di traverso?).

Neppure il modo con cui rappresentiamo normalmente i naturali, con l'uso delle cifre $0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9$ è conquista banale ma è la conclusione di un progresso durato millenni.

Ecco qualche cenno su come scrivevano i naturali alcuni nostri progenitori.

1) Egiziani:
   - scrittura geroglifica
   - scrittura ieratica
2) Babilonesi: scrittura cuneiforme
3) Greci:
   - attico
   - ionico (alfabetico): uso delle lettere per rappresentare i numeri
4) Romani: è il sistema che meglio conosciamo

   MCMLXXVIII significa 1978

5) Cinesi:
   - bastoncini

Invece le cifre cui siamo abituati

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9$$

ci giungono dagli Indiani attraverso gli Arabi.
La loro evoluzione è descritta in *"Storia della matematica"* di **C. Boyer**.

Da non sottovalutare: LA SCOPERTA E IL RUOLO DELLO ZERO come simbolo di posizione per distinguere, ad esempio,

$$12,\ 102,\ 100020 \quad \text{e via dicendo.}$$

Compare come $\cdot$ (come il moderno simbolo di prodotto), poi si allarga e diviene lo 0 che conosciamo(?).

Un professore di eccezione: **Nero Wolfe**, *"The zero clue"*
(letteralmente *"L'indizio zero"*, comparso in italiano col titolo *"Nero Wolfe fa* $2+2$*"*)

> *"L'uso del punto come simbolo di moltiplicazione è una trovata moderna. Ma gli antichi Indiani lo usavano in altro senso, per l'invenzione più geniale e fantastica dell'intera storia del linguaggio numerico. C'era infatti da trovare il modo di distinguere tra trentadue, trecentodue, tremiladue o trentamiladue. Questo è appunto il problema cruciale del linguaggio numerico, e i Greci e i Romani nonostante la loro abilità intellettiva non riuscirono a risolverlo. Ma gli Indiani ci arrivarono circa venti secoli fa. Capirono che il segreto era la posizione. Al giorno d'oggi usiamo lo zero esattamente come lo usavano loro, per mostrare una posizione: ma invece di 0, gli Indiani adoperavano un punto. Il punto nel primo linguaggio numerico indiano era uno zero."*

Un'altra conquista non banale: LA RAPPRESENTAZIONE IN BASE 10

$$1723 = 1 \cdot 10^3 + 7 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10$$

Fa ovvio riferimento al numero 10 delle dita delle mani (con cui si conta).

Si noti che 1723 - numero compreso fra $1000 = 10^3$ e $10000 = 10^4$ - si scrive con 4 cifre. Allo stesso modo

$$10^4 \leq 21456 < 10^5 \quad \text{richiede 5 cifre}$$

In genere la lunghezza della rappresentazione di un numero naturale N in base 10, ovvero il numero delle cifre di cui si compone, è approssimativamente il suo logaritmo in base 10, per la precisione

$$\lfloor \log_{10} N \rfloor + 1$$

dove $\lfloor\ \rfloor$ indica la parte intera.

La rappresentazione in base 10 non è comunque l'unica possibile.

RAPPRESENTAZIONE IN BASE 2: usa le sole cifre 0, 1 (come farebbero marziani con 1 dito per mano)
$\Rightarrow$ 0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, ...
(per 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 in base 10)

In generale

$$\begin{array}{lll} 11001 \quad \text{è} & 1\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 & \text{in base 2} \\ & = 16 + 8 + 1 = 25 & \text{in base 10} \end{array}$$

Si noti che

- 11001, cioè 25 in base 10, sta tra $2^4 = 16$ e $2^5 = 32$
- richiede 5 cifre per esser scritto in base 2.

Come per la base 10 si osserva che la lunghezza della scrittura di un naturale N in base 2 è approssimativamente $\log_2 N$, per la precisione

$$\lfloor \log_2 N \rfloor + 1$$

- maggiore che in base 10
- sostanzialmente proporzionale a quella in base 10, perché

$$\log_2 N = \log_{10} N \cdot \log_2 N$$

ESERCIZIO Al mondo ci sono 10 categorie di persone: quelli che capiscono la numerazione in base 2 e gli altri. Perché?

ESERCIZIO A che cosa corrisponde in base 10 il numero 1100100 in base 2?
(1100100 è $2^6 + 2^5 + 2^2$ cioè $64 + 32 + 4 = 100$ in base 10)

ESEMPIO Come si ottiene la rappresentazione in base 2 di un numero come 340 in base 10? Si divide 340 per 2, poi il quoziente ancora per 2, e così via

$$\begin{array}{rl} 340 = 2\cdot 170 & +\ 0 \\ 170 = 2\cdot 85 & +\ 0 \\ 85 = 2\cdot 42 & +\ 1 \\ 42 = 2\cdot 21 & +\ 0 \\ 21 = 2\cdot 10 & +\ 1 \\ 10 = 2\cdot 5 & +\ 0 \\ 5 = 2\cdot 2 & +\ 1 \\ 2 = 2\cdot 1 & +\ 0 \\ 1 = 0\cdot 1 & +\ 1 \end{array}$$

La sequenza dei resti dal basso 101010100 rappresenta 340 in base 2. Infatti

$$2^8 + 2^6 + 2^4 + 2^2 = 256 + 64 + 16 + 4 = 340.$$

ALTRE POSSIBILI RAPPRESENTAZIONI (in base 8):

cifre disponibili $0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,$ dunque

$$0, 1, 2, 3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 16, 17, 20, 21, 22, 23, 24, 25, 26, 27, 30$$

esprimono i numeri che in base 10 sono

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24$$

Ad esempio,

$$31 \quad \text{è} \quad 3 \cdot 8 + 1 = 24 + 1 = 25 \quad \text{in base 10}$$

Così Hallowen (31 ottobre) diventa Natale (25 dicembre), I. Asimov, "Il buon padre di famiglia", Il Taccuino dei Vedovi Neri.

UNA PROPRIETÀ FONDAMENTALE DEI NATURALI

Il Principio di induzione (Peano-Dedekind, fine Ottocento)
Se una proprietà è vera per 0 e si trasmette da ogni naturale n al successore $n+1$ (dunque da 0 a 1, da 1 a 2, e così via), allora la proprietà è vera per ogni naturale.

IN GENERALE
Se una proprietà è vera per un fissato naturale n_0 e si trasmette da ogni naturale n al successore $n+1$ (dunque da n_0 a n_0+1, da n_0+1 a n_0+2, e così via), allora la proprietà è vera per ogni naturale $n \geq n_0$.

ESEMPI

1. $1 + 2 + \ldots + n = \dfrac{n(n+1)}{2}$ per ogni $n \in \mathbb{N},\ n \geq 1$.

   Così

   $$\begin{array}{l} 1 \ + \ 2 \ + \ 3 \ + \ 4 \ + \ \ldots \ + \ 97 \ + \ 98 \ + \ 99 \ + \ 100 \quad = \\ (1+100) \ + \ (2+99) \ + \ \ldots \ + \ (49+52) \ + \ (50+51) \ = \ 50 \cdot 101 \end{array}$$

   (ci sono dunque 50 coppie con somma 101).

   Gauss ideò questo argomento da ragazzo durante un compito in classe: in generale, sono dati

   $$1, \quad 2, \quad 3, \quad 4, \quad \ldots, \quad n-3, \quad n-2, \quad n-1, \quad n.$$

La somma si scrive

$$(1+n) \ + \ (2+(n-1)) \ + \ (3+(n-2)) \ + \ \ldots$$

$$\Rightarrow \text{ coppie con somma } n+1.$$

Quante coppie?

* per n pari (come nel caso di 100)
  $\frac{n}{2} \ \Rightarrow$ la somma è $\frac{n}{2} \cdot (n+1) = \frac{n(n+1)}{2}$
* per n dispari (come nel caso di 9 qui sotto),
  $\frac{n-1}{2}$ coppie $+1$ elemento intermedio $\frac{n+1}{2} \ \Rightarrow$ la somma è
  $\frac{n-1}{2} \cdot (n-1) + \frac{n+1}{2} = \frac{n+1}{2}(n-1+1) = \frac{n+1}{2} \cdot n = \frac{n(n+1)}{2}$

Il caso $n = 9$

$$1 \ + \ 2 \ + \ 3 \ + \ 4 \ + \ 5 \ + \ 6 \ + \ 7 \ + \ 8 \ + \ 9 \ =$$
$$= \ (1+9) \ + \ (2+8) \ + \ (3+7) \ + \ (4+6) \ + \ 5 = \frac{9+1}{2}$$

Una dimostrazione alternativa col Principio di Induzione.

$n = 1: \ 1 = \frac{1 \cdot 2}{2} \quad \checkmark$

$n \Rightarrow n+1$: sappiamo $1+2+\ldots+n = \frac{n(n+1)}{2}$ e vogliamo provare $1+2+\ldots+n+n+1 = \frac{(n+1)\cdot(n+2)}{2}$. Infatti $1+2+\ldots+n+(n+1) = (1+2+\ldots+n)+n+1 = \frac{n(n+1)}{2}+n+1 = (n+1)(\frac{n}{2}+1) = \frac{(n+1)\cdot(n+2)}{2}$

2. Tutte le mele del mondo sono rosse

Dimostrazione: siccome c'è almeno una mela rossa, basta provare che tutte le mele del mondo hanno lo stesso colore, ovvero che, per ogni naturale $n \geq 1$, comunque si prenda un insieme di n mele, queste non hanno differenze di colore tra loro. Usiamo il principio di Induzione.

$n = 1$: chiaro

$n \Rightarrow n+1$: siano $M_1, \ M_2, \ \ldots, \ M_n, \ M_{n+1}$ $n+1$ mele. Se dimentichiamo M_{n+1}, abbiamo n mele $M_1, \ \ldots, \ M_n$, dunque nessuna differenza di colore tra $M_1, \ \ldots, \ M_n$. Allo stesso modo, dimenticando M_1, non abbiamo differenze di colore tra $M_2, \ \ldots, \ M_n, \ M_{n+1}$. Così anche M_1 e M_n hanno lo stesso colore di $M_2, \ \ldots, \ M_n$, e in totale $M_1, \ M_2, \ \ldots, \ M_n, \ M_{n+1}$ hanno tutte lo stesso colore.

Dov'è l'errore?

Le operazioni in $\mathbb{N}$

$+,\ \cdot$ sempre definite
$-,\ :$ talora impossibili

$*$ Per $a, b \in \mathbb{N}$, $a - b$ è l'elemento d tale che $b + d = a$ (se esiste)

$$3 - 2 = 1 \quad \text{perché } 1 + 2 = 3; \quad \text{ma } 2 - 3 = ?$$

La necessità di dare risultato numeri interi $0,\ \pm 1,\ \pm 2,\ \pm 3,\ \ldots$

$*$ Per $a, b \in \mathbb{N}$, $a : b$ è l'elemento q tale che $b \cdot q = a$ (se esiste)

- $4 : 2 = 2$
- $b = 1 \Rightarrow\ a = a \cdot 1$ per ogni a, così $a : 1 = a$ (e $a : a = 1$)
- $b = 0 \Rightarrow\ b \cdot q = 0$ per ogni q,

così la divisione è $\begin{cases} \text{impossibile} & \text{se} \quad a \neq 0 \\ \text{indeterminata} & \text{se} \quad a = 0 \end{cases}$

- $b \neq 0 \Rightarrow\ 2 : 3 = ?$

Teorema del quoziente e del resto
Se $a, b \in \mathbb{N}$ e $b \neq 0$, esistono sempre $q, r \in \mathbb{N}$ unici tali che $a = b \cdot q + r,\ r < b$.

$\left.\begin{array}{l} q = \text{quoziente} \\ r = \text{resto} \end{array}\right\}$ della divisione di a per b

La divisione è possibile in modo approssimato, con un errore r - il resto - che è racchiuso tra 0 e $b - 1$.

ESEMPIO $1723 = 15 \cdot 114 + 13$

$$\begin{array}{r|l} 1723 & 15 \\ \hline 22 & 114 \\ 73 & \\ 13 & \end{array}$$

Se $r = 0$, si dice che b è divisore di a (la divisione è precisa) o anche che a è multiplo di b.

Dimostrazione
ESISTENZA DI q, r Usiamo una variante sul tema dell'Induzione.

Principio di Induzione completa

Se una proprietà si trasmette, per ogni naturale a, dai naturali minori di a ad a, allora quella proprietà è vera per ogni naturale.

Procediamo per induzione completa su a: ammettiamo che quoziente e resto rispetto a b esistano per ogni naturale $< a$ e proviamo che altrettanto vale per a (ne segue che quoziente e resto per b esistono per ogni a).

$a < b$: $a = b \cdot 0 + a$, dunque $q = 0,\ r = a < b$
$a \geq b$: siccome $b > 0,\ a - b < a$, dunque ci sono q', r' tali che

$$a - b = bq' + r' \qquad r' < b$$

Sommando b

$$a = b + bq' + r' = b(1 + q') + r$$

dunque $1 + q' = q$ *e* $r' = r$.

UNICITÀ DI q, r Supponiamo $a = bq + r = bq' + r'$. Allora $bq - bq' = r' - r$, dunque $b(q - q') = r' - r$. Ma $0 \leq r' - r < b$, mentre $b(q - q')$ è multiplo di b. L'unica via di uscita è

$$r' - r = b(q - q') = 0$$

cioè $r = r'$ e $q = q'$.

Il costo delle operazioni

In genere si conviene che, nel calcolo di $+,\ \cdot,\ -,\ :$ (: semmai approssimata) per $a, b \in \mathbb{N}$ una singola operazione sulle cifre di a, b richiede 1 passo.

ESEMPI

1.

$$\begin{array}{r} 8723+ \\ 2734 = \\ \hline 11457 \end{array}$$

richiede 5 passi (in base 10)

2.

$$\begin{array}{r} 11011+ \\ 10110 = \\ \hline 110001 \end{array}$$

richiede 6 passi (in base 2)

Si verifica allora che il costo di un'operazione è al più quadratico rispetto alle lunghezze di a, b.

DA NOTARE:

- se b divide a, allora b divide ac per ogni c
  (si ha $a = bq$ per qualche q, dunque $ac = b(qc)$)

$*$ se b divide a, a', allora b divide anche $a + a'$ e $a - a'$ (se esiste)
(da $a = bq$ e $a' = bq'$ si deduce $a + a' = b(q + q')$)

Massimo comune divisore e minimo comune multiplo

Siano a, b due naturali, $a, b \neq 0$ (a evitare casi banali o privi di senso).

A) Si dice massimo comune divisore di a, b un naturale d tale che

$*$ d è divisore di a, b

$*$ ogni divisore comune di a, b è $\leq d$.

Notare:

- c'è al meno un divisore comune di a, b, cioè 1, e i divisori comuni di a, b sono $\leq a, b$, dunque sono un numero finito
  $\Rightarrow$ ce n'è uno massimo ...
- ... forzatamente unico.

$\Rightarrow$ simbolo specifico per denotare il massimo comune divisore di a, b

$$(a, b)$$

B) Si dice minimo comune multiplo di a, b un naturale $m \neq 0$ tale che

$*$ m è multiplo di a, b

$*$ ogni multiplo comune $\neq 0$ di a, b è $\geq m$.

Notare:

- c'è almeno un multiplo comune $\neq 0$ di a, b, ad esempio $a \cdot b$
  $\Rightarrow$ ce n'è uno minimo ...
- ... forzatamente unico.

$\Rightarrow$ simbolo specifico per denotare il minimo comune divisore di a, b

$$[a, b]$$

Come si calcolano (a, b) e $[a, b]$?

A) (a, b): si può usare l'algoritmo già noto a Euclide

Si divide a per b

$$a = bq_0 + r_0, \qquad r_0 < b$$

poi b per r_0

$$b = r_0 q_1 + r_1, \qquad r_1 < r_0$$

e così via, finché non si trova resto nullo (il resto diminuisce a ogni nuova divisione!). L'ultimo resto non nullo è (a, b).

OSSERVAZIONE $(a, b) = (b, r_0)$: infatti da $a = bq_0 + r_0$ e $r_0 = a - bq_0$ segue che a, b hanno gli stessi divisori di b, r_0.

ESEMPI

1. $(72, 22) = 2$

$$\left.\begin{array}{r} 72 = 22 \cdot 3 + 6 \\ 22 = 6 \cdot 3 + 4 \\ 6 = 4 \cdot 1 + 2 \\ 4 = 2 \cdot 2 \end{array}\right\} \; 22 > 6 > 4 > 2, \quad 2 \text{ è il massimo comune divisore}$$

2. $(1253, 27) = 1$

$$\left.\begin{array}{r} 1253 = 27 \cdot 46 + 11 \\ 27 = 11 \cdot 2 + 5 \\ 11 = 5 \cdot 2 + 1 \\ 5 = 1 \cdot 5 \end{array}\right\} \; 11 > 5 > 1, \quad 1 \text{ è il massimo comune divisore}$$

($\Rightarrow$ $1253, 27$ sono *primi tra loro*)

3. $(12, 4) = 4, \quad 12 = 4 \cdot 3$

Costo della ricerca di (a, b) con l'algoritmo di Euclide:

$$\left.\begin{array}{l} \text{- costo di ogni divisione: al più quadratico} \\ \text{- numero delle divisioni: al più lineare} \end{array}\right\} \text{ rispetto alla lunghezza di } a, b$$

Costo complessivo:
$\Rightarrow$ di grado al più 3 (in realtà al più 2) rispetto alle lunghezze di a, b.

B) $[a, b]$: vedremo $[a, b] = \frac{a \cdot b}{(a,b)}$

ESEMPI

1. $[72, 22] = \frac{72 \cdot 22}{2} = 72 \cdot 11$
2. $[1253, 27] = 1253 \cdot 27$
3. $[4, 12] = \frac{12 \cdot 4}{4} = 12$

Costo complessivo:
quello di trovare (a, b) $+1$ moltiplicazione $+1$ divisione (precisa)
$\Rightarrow$ ancora di grado al più 3 (in realtà al più 2) rispetto alle lunghezze di a, b.

I numeri primi

Un numero naturale N è

primo	se $N > 2$ e gli unici divisori di N sono 1, N;
composto	se $N \geq 2$ ma N non è primo (dunque N ha un divisore $a \neq 1, N$ e cioè $N = a \cdot b$ per $1 < a, b < N$)

Numeri composti: 4 (ha il divisore 2), 6 (ha i divisori 2, 3), ...
Numeri primi: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Si osserva che 2 è l'unico numero primo pari (un numero pari $\geqq 2$ ha divisore 2 e dunque non è primo).
Zassenhaus: *"2 is the oddest prime"* dove *oddest* può significare tanto "il più dispari", quanto "quello più fuori posto".

Ricordare $4 = 2^2,\ 6 = 2 \cdot 3,\ 8 = 2^3,\ 9 = 3^2,\ 10 = 2 \cdot 5,\ 12 = 2^2 \cdot 3,\ \ldots$

Teorema fondamentale dell'aritmetica
Ogni naturale $N \geq 2$ si decompone nel prodotto di fattori primi, e questa decomposizione è unica a meno dell'ordine dei fattori.
(Ad esempio $6 = 2 \cdot 3 = 3 \cdot 2$, ma questo è l'unico motivo di confusione.)

Dimostrazione
Esistenza Usiamo ancora il Principio di Induzione completa: facciamo vedere che l'esistenza di una decomposizione si trasferisce, per ogni $N \geq 2$, dai numeri minori di N (e ≥ 2) a N.

N primo:	$N = N$ è la decomposizione cercata nell'unico fattore N primo
N composto:	allora $N = a \cdot b$ per opportuni a, b con $2 \leq a, b < N$; ma a, b hanno la loro decomposizione in fattori primi; combinando queste decomposizioni, otteniamo quella di N.

Unicità È molto più complicata,

- usa ancora l'induzione completa
- sfrutta la seguente proprietà: se un primo p divide un prodotto $a \cdot b$, $\Rightarrow$ p divide almeno uno dei fattori a o b.

Falso in generale:

6 divide $12 = 4 \cdot 3$, ma 6 non divide né 4 né 3 (e 6 non è primo).

Due problemi

Determinare algoritmi effettivi che, per ogni naturale $N \geq 2$,

(PRIMI) stabiliscono se N è primo o composto

(FATTORIZZAZIONE) decompongono N nei suoi fattori primi

(come primo passo, trovano un divisore $d \neq 1, N$ di N).

UN ALGORITMO ELEMENTARE (già noto agli antichi Greci)
Consideriamo ogni possibile "candidato" d tra 2 e $N-1$, $2 \leq d < N-1$ e dividiamo N per d

- se la divisione è precisa per qualche d, N è composto

  (e abbiamo d come cercato);

- se la divisione non è esatta per nessun d, N è primo.

ESEMPIO

$N = 131$: si divide 131 per 2, 3, 4, 5, 6, ... , 130
$N = 31$: si divide 31 per 2, 3, 4, ... , 30

POSSIBILI SCORCIATOIE

- basta esplorare $1 < d \leq \sqrt{N}$

  (se $N = d \cdot d'$ con $1 < d, d'$, allora $d \leq \sqrt{N}$ o $d' \leq \sqrt{N}$, altrimenti per $d, d' > \sqrt{N}$, $d \cdot d' > \sqrt{N} \cdot \sqrt{N} = (\sqrt{N})^2 = N$)

- se d non funziona, inutile esplorare $2d$, $3d$, ...

Crivello di Eratostene ("moltiplicare è più facile che dividere")

- si scrivono i numeri da 2 a N disposti su righe, da 2 a 10, da 11 a 20, ...
- si segna 2 e si cancellano i suoi multipli > 2
- si segna il minimo sopravvissuto 3 e si cancellano i suoi multipli > 3
- si segna il minimo sopravvissuto 5 e si cancellano i suoi multipli > 5
- si prosegue fino a superare $\sqrt{N}$.

I numeri sopravvissuti sono i primi $\leq N$. N è primo se è uno di loro.

ESEMPIO $N = 31 \Rightarrow \sqrt{N} = 5, \ldots$ ($\Rightarrow$ l'analisi termina con 5)

	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									

I numeri sottolineati sono i primi rimasti.

Così l'argomento sembra chiuso. Ma ecco l'opinione che esprimeva al proposito 2 millenni dopo, nel 1801, **Gauss** nell'articolo 329 delle sue *"Disquisitiones Arithmeticae"*.

> *"Il problema di riconoscere i primi dai composti e di decomporre questi ultimi nei loro fattori primi è noto come uno dei più importanti e utili in Matematica. La dignità stessa della scienza sembra richiedere che ogni possibile mezzo sia esplorato per risolvere un problema così elegante e famoso."*

Perchè questa sollecitudine tanti secoli dopo i Greci?

> *"Le tecniche note in precedenza richiedono fatica intollerabile anche per il più instancabile calcolatore."*

L'ALGORITMO ELEMENTARE

- per controllare N può richiedere $N-2$ divisioni ($\sqrt{N}-1$ con la scorciatoia)
- ma la lunghezza $l(N)$ di N (ad esempio in base 2) è approssimativamente $\log_2 N$

$\Rightarrow$ il numero delle divisioni richieste è esponenziale rispetto a $l(N)$:

$$\text{circa } 2^{l(N)}-2, \text{ o } 2^{\frac{l(N)}{2}}-1 \text{ con la scorciatoia}$$

ESEMPIO Se N ha 128 cifre in base 2 (caso comune nelle applicazioni), la verifica può richiedere $\sim 2^{64}$ divisioni.

Ricordare l'aneddoto dell'inventore degli scacchi: come premio richiese

- 1 chicco di grano per il primo quadro della scacchiera
- poi, ad ogni nuovo quadro, il doppio della ricompensa del precedente.

Apparentemente, una domanda modesta. In realtà

$$1+2+2^2+2^3+\ \ldots\ +2^{63}=2^{64}-1 \quad \text{cioè una quantità inaccessibile!}$$

IL CRIVELLO DI ERATOSTENE

- pone gli stessi problemi
- in più richiede risorse inaccessibili anche di spazio (cioè di memoria per un calcolatore): per controllare N, si devono scrivere $N-1$ numeri!

$\Rightarrow$ ricerca di algoritmi più rapidi e accessibili,
che eventualmente scindano PRIMI da FATTORIZZAZIONE

(notare, che per N composto,

> a PRIMI è sufficiente sapere che N è, appunto, composto,
> FATTORIZZAZIONE vuole d divisore di N, $d \neq 1, N$).

Una parentesi: perché i numeri primi sono così misteriosi?

Invito alla lettura: **M. Du Sautoy**, *"L'enigma dei primi"* (*"The music of primes"*), Rizzoli.

Teorema. Esistono infiniti numeri primi.

Ci sono moltissime dimostrazioni di questo risultato. Presentiamo quella classicissima di Euclide.

Dimostrazione Mostriamo come sia possibile costruire da una qualche collezione finita di primi $p_0,\ p_1,\ p_2,\ \ldots,\ p_r$ un nuovo primo p diverso da $p_0,\ p_1,\ \ldots,\ p_r$. Basta formare

$$p_0 \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1$$

che è ovviamente ≥ 2 e dunque, per il Teorema fondamentale dell'Aritmetica, ha qualche fattore primo p. Ma $p \neq p_0,\ p_1,\ \ldots,\ p_r$, altrimenti

$$\left.\begin{array}{lll} p & \text{divide} & p_0 \cdot p_1 \cdot \ldots \cdot p_r \\ p & \text{divide} & p_0 \cdot p_1 \cdot \ldots \cdot p_r + 1 \end{array}\right\} \Rightarrow p \text{ divide } 1. -$$

D'altra parte la successione dei primi è irregolare e imprevedibile.

Esempi

1. Tra 11 e 20 ci sono 4 primi: 11, 13, 17, 19

   È il numero massimo possibile tra 10 numeri consecutivi ≥ 10, visto che dobbiamo certamente escludere i numeri pari (nel caso specifico 12, 14, 16, 18, 20) e i multipli di 5 (come 15).

   D'altra parte tra 10^7 e 10^7+100 (dunque su 101 numeri consecutivi) solo 2 risultano pari

   $$10^7 + 19, \quad 10^7 + 79$$

2. Due primi si chiamano gemelli se l'uno è p e l'altro è $p+2$ (dunque hanno differenza 2)

   Esempi

   $$3,5 \qquad 5,7 \qquad 11,13 \qquad 17,19 \qquad 29,31 \qquad \dots$$

   Controesempi

   $$7,11 \quad 13,17 \qquad 19,23 \qquad 23,29 \qquad \dots$$

   Non è chiaro quante siano le coppie di primi gemelli (infinite?).

Si noti che tre numeri come 24, 25, 26 (due pari, l'altro multiplo di 5 maggiore di 5) non possono essere primi $\Rightarrow$ 3 numeri consecutivi nessuno dei quali è primo. Più in generale

Teorema. Per ogni $M > 0$ si possono trovare M numeri consecutivi nessuno dei quali è primo.

Dimostrazione Basta considerare M numeri consecutivi

$$\begin{cases} (M+1)!+2 & > 2, & \text{divisibile per } 2 & \Rightarrow \text{ composto} \\ (M+1)!+3 & > 3, & \text{divisibile per } 3 & \Rightarrow \text{ composto} \\ \quad \dots & \dots & \dots & \dots \\ (M+1)!+M+1 & > M+1, & \text{divisibile per } M+1 & \Rightarrow \text{ composto} \end{cases}$$

Ricordare: $(M+1)!$ (che si legge $M+1$ fattoriale) è l'abbreviazione di $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (M-1) \cdot M \cdot (M+1)$. –

Alcune sequenze famose di numeri primi

1) I primi di Mersenne

Marin Mersenne fu religioso francese della fine del '500 e dell'inizio del '600. Con lui consideriamo le potenze di 2

$$2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16,\ 2^5 = 32,\ \dots,\ 2^m,\ \dots$$

e i loro predecessori

$$0,\ 1,\ 3,\ 7,\ 15,\ 31,\ \dots\ ,\ 2^m - 1,\ \dots$$

Trascuriamo pure 0, 1 e guardiamo gli altri

$$3,\ 7,\ 15,\ 31,\ \dots\ ,\ 2^m - 1,$$

alcuni primi

$$3,\ 7,\ 31,$$

altri composti, come 15.

Notare

$$\left.\begin{array}{r} 3 = 2^2 - 1 \\ 7 = 2^3 - 1 \\ 31 = 2^5 - 1 \end{array}\right\} \text{ l'esponente di 2 è primo}$$

mentre

$$15 = 2^4 - 1 \quad \text{(l'esponente di 2 è composto).}$$

Osservazione Se m è composto, $2^m - 1$ deve essere composto.
Infatti scriviamo $m = d \cdot q$ con $1 < d, q < m$, allora

$$2^m - 1 = 2^{d \cdot q} - 1 = (2^q)^d - 1^d \qquad \text{differenza di potenze } d\text{-me}$$
$$\Rightarrow \text{ si decompone } = (2^q - 1) \cdot (\dots).$$

Dubbio Se m è primo, $2^m - 1$ è primo?
Risposta: no, già $2^{11} - 1 = 2047 = 23 \cdot 89$.

Definiamo comunque, per ogni $m \geq 2$,

$$M(m) = 2^m - 1 \quad m\text{-mo numero di Mersenne}$$

La formula che caratterizza i numeri di Mersenne è assai semplice. È possibile usarla per costruire nuovi numeri e verificarne poi la primalità.
È questa la via più facile per costruire nuovi primi (ma attenzione: non è chiaro quanti siano in totale i primi di Mersenne - infiniti? -)

Esempi (uno per secolo)

$$\left.\begin{array}{l} \text{- } M(13) \quad \text{Eulero, 1722} \\ \text{- } M(22) \quad \text{Lucas, 1876} \end{array}\right\} \text{ senza calcolatori}$$
$$\text{- } M(216091) \quad \text{Slowinski, 1987} \quad \text{col calcolatore!}$$

Oggi c'è addirittura un software disponibile per chiunque vuole cercare numeri primi di Mersenne:

GIMPS Great Internet Mersenne Primes Search

$\Rightarrow$ nuovi esempi, uno per anno

- $M(20996011)$, Shafer, 2003
- $M(24036583)$, Findley, 2004
- $M(25964951)$, Nowack, 2005 (8 milioni di cifre in base 10)
- $M(30402457)$, Cooper-Boone, 2006 (9 milioni di cifre in base 10)

Definizione Un numero N è perfetto se è la somma dei suoi divisori $\neq N$.

ESEMPI

1. 6 è perfetto perché $6 = 1 + 2 + 3$

   (e 6 è il numero dei giorni della creazione secondo la Bibbia, come notato da S. Agostino nel De Civitate Dei; S. Agostino commenta che il numero perfetto 6 è la figura della Creazione perché nella Creazione il tutto si forma tramite le sue parti, come 6 tramite 1, 2, 3).

2. 28 è perfetto perché $28 = 1 + 2 + 4 + 7 + 14$.

UN COLLEGAMENTO TRA NUMERI PERFETTI E PRIMI DI MERSENNE

Per ogni $m \geq 2$,

$M(m) = 2^m - 1$ è primo se e solo se $(2^m - 1) \cdot M(m)$ è perfetto (pari)

ESEMPI

1. $m = 2 \Rightarrow M(m) = 3$ è primo e $2^1 \cdot 3 = 6$ è perfetto
2. $m = 3 \Rightarrow M(m) = 7$ è primo e $2^2 \cdot 7 = 28$ è perfetto
3. $m = 5$: sappiamo che $M(m) = 31$ è primo,
   otteniamo così il nuovo numero perfetto $2^4 \cdot 31 = 496$

PROBLEMI

* quanti sono i numeri perfetti?
  (in altre parole, quanti sono i primi di Mersenne?)
* esistono numeri perfetti dispari?

Ancora irrisolti!!!

2) I primi di Fermat

Pierre de Fermat fu giudice francese nella prima metà del Seicento.
Consideriamo con Fermat le potenze di 2

$$2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16,\ 2^5 = 32,\ \ldots\ ,\ 2^m,\ \ldots$$

e stavolta i loro successori

$$2,\ 3,\ 5,\ 9,\ 17,\ 33,\ \ldots\ ,\ 2^m + 1,\ \ldots$$

Trascuriamo 2; vediamo nei numeri che rimangono

- esempi di primi 3, 5, 17, poi 257, 65537, ...
- esempi di composti 9, 33, ...

Notiamo

$$\left.\begin{aligned} 3 &= 2^1+1 \\ 5 &= 2^2+1 \\ 17 &= 2^4+1 \\ 257 &= 2^8+1 \\ 65537 &= 2^{16}+1 \end{aligned}\right\} \quad \text{gli esponenti di 2 sono ancora potenze di 2}$$

Invece

$$\left.\begin{aligned} 9 &= 2^3+1 \\ 33 &= 2^5+1 \end{aligned}\right\} \quad \text{gli esponenti di 2 non sono potenze di 2}$$

OSSERVAZIONE Se m non è potenza di 2, allora 2^m+1 non può essere primo. Infatti sia $m = d \cdot q$ con $1 < d, q < m$, d dispari, allora

$$2^m + 1 = 2^{d\cdot q} + 1 = \underbrace{(2^q)^d + 1^d}$$

$\Rightarrow$ è somma di 2 potenze a esponente dispari: si decompone come $(2^q+1)\cdot(\dots)$

NOTAZIONE Per ogni $n \geq 0$,

$$F(n) = 2^{2^n} + 1 \quad n\text{-mo numero di Fermat.}$$

Congettura di Fermat Tutti i numeri $F(n)$ sono primi.

In effetti,

$$F(0) = 3,\ F(1) = 5,\ F(2) = 17,\ F(3) = 257,\ F(4) = 65537$$

depongono in questo senso, ma sono solo 5 esempi su infiniti possibili.
D'altra parte, è difficile calcolare

$$F(5) = 2^{2^5} + 1 = 2^{32} + 1,\ F(6) = 2^{2^6} + 1 = 2^{64} + 1,\ \dots$$

e lo era ancor di più ai tempi di Fermat, quando mancavano i computers.
Infatti solo un secolo dopo Fermat Eulero riuscì a contraddirlo e provò che

$$F(5) = 2^{2^5} + 1 = 641 \times 6700417 \quad \text{è composto}$$

La tecnica di Eulero

- classificare teoricamente tutti i possibili divisori primi di un numero di Fermat di $F(n)$

$$k \cdot 2^{n+1} + 1$$

- applicare questo criterio per la ricerca di possibili divisori primi di $F(5)$

$$641 = 10 \cdot 2^6 + 1$$

OGGI?

$*$ I primi di Fermat conosciuti sono gli stessi noti a Fermat

$$F(0),\ F(1),\ F(2),\ F(3),\ F(4)$$

(ma non è chiaro quanti possano essere in totale i primi di Fermat: infiniti?)

$*$ Per $5 \leq n \leq 30$, è noto che $F(n)$ è composto

- $5 \leq n \leq 11$: è conosciuta anche la decomposizione di $F(n)$ in fattori primi
- $n = 14,\ 20,\ 22,\ 24$: non è noto alcun fattore primo di $F(n)$
- per gli altri valori di $n \leq 30$, si sa qualche divisore primo ma non ancora l'intera decomposizione.

Del resto,

$$F(10) = 2^{2^{10}} + 1 \quad \text{si compone di oltre 100 cifre in base 10}$$

($\Rightarrow$ oltre 300 in base 2)

Si può provare $F(n) = F(0) \cdot F(1) \cdot \ldots \cdot F(n-1) + 2$

Un'applicazione:
costruzione di un poligono regolare di $n \geq 3$ lati con riga e compasso.

PROBLEMA STORICAMENTE FAMOSO:
dai Greci (che lo posero) a Gauss (che lo risolse) ... oggi forse superato:
riga e compasso sono strumenti antiquati nell'epoca dei computers.

ESEMPIO $n = 6$ (ci si basa sull'osservazione che il lato dell'esagono regolare uguaglia il raggio del cerchio circoscritto all'esagono)

Altri esempi famosi: $n = 3,\ 4,\ 5,\ 10,\ 12,\ \ldots$
Invece difficile trovare sui testi costruzioni per $n = 7,\ 9,\ 11,\ \ldots$

Notare: 3, 5 primi di Fermat

$$\left.\begin{array}{l} 6 = 2 \cdot 3 \\ 4 = 2^2 \\ 10 = 2 \cdot 5 \\ 12 = 2^2 \cdot 3 \end{array}\right\} \text{si decompongono con potenze di 2 e primi di Fermat distinti}$$

Invece, 7 e 11 non primi di Fermat e $9 = 3^2$ ha il primo di Fermat 3 che occorre 2 volte.

Il Teorema di Gauss Per $n \geq 3$, un poligono regolare di n lati si costruisce con riga e compasso se e solo se n si decompone in fattori primi come

$$2^h \cdot p_0 \cdot p_1 \cdot \ldots \cdot p_r$$

con 2^h potenza di 2 e $p_0,\ p_1,\ \ldots,\ p_r$ primi di Fermat 2 a 2 distinti (allo stato attuale delle conoscenze, tra 3, 5, 17, 257, 65537)

Così

- si conferma risposta positiva per

  3, 5, 17, 257, 65537, 6, 10, 34, ... , 4, 8, ... , 15, ...

- si dà risposta negativa per

  7, 9, 11, 13, 14, 18, ...

NOTA STORICA C'è chi ha costruito effettivamente un poligono regolare di 257 lati con riga e compasso. Non c'è nessuno che si è cimentato con 65537.

3) I primi di Germain

Sophie Germain, matematica francese di inizio Ottocento: per poter studiare e introdursi nel mondo accademico, si fece passare per uomo (si presentò per lettera a Gauss come Monsieur Leblanc; Gauss scoprì l'inganno, ne fu divertito, si adoperò per trovarle un posto alla sua Università di Gottingen; ma la Germain morì prima di poter approfittare dell'opportunità).

Un primo p è di Germain se anche $2p + 1$ è primo

ESEMPI: 3, 5, 11 (7, 11, 23 sono ancora primi)
CONTROESEMPI: 7, 13 (15 e 27 non sono primi)

Commento: usati da S. Germain per una soluzione parziale di un classico problema di Teoria dei Numeri, l'Ultimo Teorema di Fermat.

LA CONGETTURA DI GOLDBACH

Invito alla lettura: **A. Doxiadis**, *"Zio Petros e la Congettura di Goldbach"*, Bompiani.

C. Goldbach, 1742, lettera a Eulero: pone la domanda se

"ogni naturale $N \geq 6$ è la somma di al più 3 primi".

esempi: $6 = 2+2+2$, $7 = 7 = 2+2+3$, $8 = 3+5 = 2+3+3$, $9 = 3+3+3$, $10 = 3+7 = 2+3+5$, $11 = 11$, ...

La risposta di Eulero: non dimostra la proposizione, ma osserva che basta provare che

"ogni naturale pari ≥ 4 è la somma di 2 primi".

Infatti sia $N \geq 6$,

* se N è pari, allora $N-2$ è pari e $\geq 4 \Rightarrow N-2 = p_1 + p_2$ è la somma di 2 primi $\Rightarrow N = (N-2)+2 = p_1 + p_2 + 2$ è la somma di 3 primi;
* se N è dispari, allora $N \geq 7$ e $N-3$ è pari e $\geq 4 \Rightarrow N-3 = p_1 + p_2$ è la somma di 2 primi $\Rightarrow N = (N-3)+3 = p_1 + p_2 + 3$ è la somma di 3 primi.

Oggi si conviene di chiamare Congettura di Goldbach l'affermazione di Eulero.

CONGETTURA DI GOLDBACH Ogni naturale ≥ 4 è la somma di 2 primi

$4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 3+7 = 5+5$, $12 = 5+7$, $14 = 7+7 = 3+11$, ...

(Un problema ancora aperto nel 2006)

LA MATEMATICA DELL'OROLOGIO

Consideriamo $\mathbb{Z}$ insieme degli interi ... , -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, ...
I teoremi stabiliti per $\mathbb{N}$ si estendono a $\mathbb{Z}$ con le opportune modifiche.

Ad esempio si ha

* l'unico divisore di 1 in $\mathbb{N}$ è 1
* i divisori di 1 in $\mathbb{Z}$ diventano ± 1.

Un elemento a divisore di 1 si chiama in genere invertibile, e il quoziente q per cui $a \cdot q = 1$ si dice l'inverso di a e si indica a^{-1} (o anche $\frac{1}{a}$).
Dunque ± 1 sono gli unici elementi invertibili di $\mathbb{Z}$.

OSSERVAZIONE 1 Se alle 22 fissiamo un appuntamento tra 4 ore, intendiamo le 2 del mattino: $22+4$ fa 2 perché le 24 di oggi coincidono con le 0 di domani $\Rightarrow$ l'aritmetica dell'orologio modulo 24 (mod 24):

* 24 elementi 0, 1, 2, 3, ... , 22, 23, dopo di che

  $24 \equiv 0 (\text{mod } 24)$, $25 \equiv 1 (\text{mod } 24)$, $-1 \equiv 23 (\text{mod } 24)$

$*$ addizione e moltiplicazione

- si esegue l'operazione in $\mathbb{Z}$ $\quad 22+4=26,\ 22\cdot 4=88$
- si divide il risultato per 24 e si considera il resto
  $26=24\cdot 1+2,\ 88=24\cdot 3+16$

Dunque

$$22+4\equiv 2(\text{mod } 24),\quad 22\cdot 4\equiv 16(\text{mod } 24)$$

All'uguaglianza $=$ degli interi, si sostituisce cioè la congruenza modulo 24 $\equiv$ (mod 24)

OSSERVAZIONE 2 Nel corso delle sue numerose campagne militari, Giulio Cesare inviava ai suoi luogotenenti ordini criptati - in modo di renderli incomprensibili ai nemici che riuscissero ad intercettarli -.
Una maniera per criptare: spostare ogni lettera di 3 posti in avanti.

$$A\to D,\quad B\to E,\quad C\to F,\quad \dots$$

e le ultime 3 nelle prime 3

$$X\to A,\quad Y\to B,\quad Z\to C$$

La decodifica: riportare ogni lettera indietro di 3 posti.

Per semplicità riferiamoci alle lettere dell'alfabeto inglese e sostituiamo ogni lettera con un numero nel modo che segue.

$-$	A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Così $CIAO$ diventa 3 9 1 15

CODIFICA DI CESARE: si aggiunge 3 modulo 27

$$3+3\equiv 6(\text{mod } 27),\ 9+3\equiv 12(\text{mod } 27),\ 1+3\equiv 4(\text{mod } 27)$$
$$15+3\equiv 18(\text{mod } 27),\ 24+3\equiv 0(\text{mod } 27),\ \dots$$

Dunque

$*$ 27 elementi $0,\ 1,\ 2,\ 3,\ \dots\ ,\ 24,\ 25,\ 26 \quad (27\equiv 0(\text{mod } 27),\ \dots\ )$

∗ addizione e moltiplicazione come nel caso precedente,

ma in riferimento a 27

- si esegue l'operazione in $\mathbb{Z}$ $\quad 24+3=27, \quad 24\cdot 3=72$
- si divide il risultato per 27 e si considera il resto
  $27=27\cdot 1+0, \quad 72=27\cdot 2+18$
  così che
  $27+3\equiv 0(\text{mod } 27), \quad 27\cdot 3\equiv 18(\text{mod } 27).$

Le stesse nozioni si possono introdurre rispetto a qualunque intero $m\geq 2$, formando un insieme $\mathbb{Z}_m$ come descritto di seguito

∗ m elementi $\quad 0,\ 1,\ 2,\ \ldots\ ,\ m-1 \quad$ (i resti nella divisione per m)

∗ per $a,b\in\mathbb{Z}$

$a+b \pmod m$ si calcola sommando in $\mathbb{Z}$, dividendo per m e prendendo il resto

$a\cdot b \pmod m$ si calcola moltiplicando in $\mathbb{Z}$, dividendo per m e prendendo il resto

Le operazioni risultano ben definite.

ALTRI ESEMPI

∗ $m=2 \ \Rightarrow$ 2 elementi $0,\ 1$ (sarebbe più preciso scrivere $0_2,\ 1_2$ per sottolineare il riferimento a 2 ed evitare confusione), addizione e moltiplicazione sono descritte dalle tabelle.

$+$	0	1
0	0	1
1	1	0

$1+1\equiv 0(\text{mod } 2)$, dunque $1\equiv -1(\text{mod } 2)$

$\cdot$	0	1
0	0	0
1	0	1

∗ $m=3 \ \Rightarrow$ 3 elementi $0,\ 1,\ 2$ (per la precisione $0_3,\ 1_3,\ 2_3$)

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$*$ $m = 4 \Rightarrow$ 4 elementi $0,\ 1,\ 2,\ 3$ (o meglio $0_4,\ 1_4,\ 2_4,\ 3_4$)

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

La moltiplicazione presenta in particolare strane anomalie rispetto a $\mathbb{Z}$: ad esempio $2 \cdot 2$ fa 0.

Da ricordare In generale, per a, b interi,

$$a \equiv b (\mathrm{mod}\ m)$$

significa che $a = b + qm$ per qualche q intero, cioè che $a - b = qm$ per qualche q, cioè che m divide $a - b$ (ovvero ancora che a e b hanno lo stesso resto nella divisione per m).

Esempi

1) In $\mathbb{Z}$ non ci sono divisori dello zero: il prodotto di due fattori $\neq 0$ è ancora $\neq 0$. Ma

$$12 \not\equiv 0 (\mathrm{mod}\ 24),\ 2 \not\equiv 0 (\mathrm{mod}\ 24), \quad \text{eppure} \quad 12 \cdot 2 \equiv 24 \equiv 0 (\mathrm{mod}\ 24)$$
$$9 \not\equiv 0 (\mathrm{mod}\ 27),\ 3 \not\equiv 0 (\mathrm{mod}\ 27), \quad \text{eppure} \quad 9 \cdot 3 \equiv 27 \equiv 0 (\mathrm{mod}\ 27)$$

$$2 \not\equiv 0 (\mathrm{mod}\ 4), \ \text{eppure} \quad 2^2 = 2 \cdot 2 \equiv 4 \equiv 0 (\mathrm{mod}\ 4)$$

2) In $\mathbb{Z}$ i soli elementi invertibili sono ± 1. Ma modulo 8

$$1^2 \equiv 1 (\mathrm{mod}\ 8),\ 3^2 \equiv 1 (\mathrm{mod}\ 8),\ 5^2 \equiv 1 (\mathrm{mod}\ 8),\ 7^2 \equiv 1 (\mathrm{mod}\ 8)$$

$\Rightarrow$ 4 elementi su 8 sono invertibili

(ESERCIZIO Gli altri 3 diversi da 0, cioè 2, 4, 6, dividono lo zero).

ESEMPIO In $\mathbb{Z}_5$ i 4 elementi non nulli 1, 2, 3, 4 sono tutti invertibili

$$1^2 \equiv 1(\text{mod } 5),\ 2 \cdot 3 \equiv 1(\text{mod } 5),\ 4^2 \equiv (-1)^2 \equiv 1(\text{mod } 5)$$

ESERCIZI Che succede in $\mathbb{Z}_3$? $\mathbb{Z}_2$? $\mathbb{Z}_4$? Quali elementi sono invertibili? E quali sono divisori dello zero?

Da chiarire in generale: come riconoscere in $\mathbb{Z}_m$, per m arbitrario,

- gli elementi invertibili,
- i divisori dello zero.

OSSERVAZIONE Se a è invertibile in $\mathbb{Z}_m$, a non può dividere lo zero (e dunque, se a divide lo zero, allora a non può essere invertibile). Supponiamo infatti che ci siano a, c interi tali che

$$a \cdot b \equiv 1(\text{mod } m), \quad a \cdot c \equiv 0(\text{mod } m),$$

allora

$$c \equiv c \cdot 1 \equiv c \cdot (a \cdot b) \equiv (c \cdot a) \cdot b \equiv 0 \cdot b \equiv 0(\text{mod } m).$$

Ci serve qualche ulteriore risultato sul massimo comune divisore di due interi non nulli.

Identità di Bézout Siano a, b due naturali non nulli. Allora esistono due interi x, y (eventualmente negativi) per cui $(a, b) = ax + by$.

ESEMPI

1. Sappiamo $(72, 22) = 2$. Infatti si verifica $2 = 72 \cdot 4 + 22 \cdot (13)$
   (ma da dove si ottengono 4 e -13?)
2. $(3, 5) = 1$. Infatti $1 = 3 \cdot 2 + 5 \cdot (-1)$.

NOTA STORICA Étienne Bézout visse nella Francia del Settecento e scrisse manuali di matematica per artiglieri e guardie di marina.

COME TROVARE x, y?
Si fa riferimento all'algoritmo euclideo per la ricerca di (a, b).

Nel caso di 72, 22

$$\begin{aligned} 72 &= 22 \cdot 3 + 6 \\ 22 &= 6 \cdot 3 + 4 \\ 6 &= 4 \cdot 1 + 2 \end{aligned}$$

(da cui $2 = (72, 22)$ perché 2 è l'ultimo resto non nullo del procedimento, $4 = 2 \cdot 2$).

Idea: da ogni eguaglianza ricavare il resto

$$6 = 72 - 22 \cdot 3$$
$$4 = 22 - 6 \cdot 3$$
$$2 = 6 - 4 \cdot 1,$$

poi sostituire

$$4 = 22 - 6 \cdot 3 = 22 - (72 - 22 \cdot 3) = 22 - 72 \cdot 3 + 22 \cdot 9 = 22 \cdot 10 - 72 \cdot 3$$
$$2 = 6 - 4 \cdot 1 = 72 - 22 \cdot 3 - 22 \cdot 10 + 72 \cdot 3 = 72 \cdot 4 + 22 \cdot (-13)$$

$\Rightarrow \; x = 4, \; y = -13.$

ALTRO ESEMPIO: $1 = (3, 5)$. Dall'algoritmo di Euclide

$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$

($\Rightarrow$ 1 è $(3, 5)$ perché è l'ultimo resto non nullo, $2 = 2 \cdot 1$).
Si ricavano i resti

$$2 = 5 - 3 \cdot 1$$
$$1 = 3 - 2 \cdot 1$$

e si sostituisce

$$1 = 3 - (5 - 3 \cdot 1) \cdot 1 = 3 - 5 + 3 = 3 \cdot 2 + 5 \cdot (-1)$$

$\Rightarrow \; x = 2, \; y = -1.$

COSTO DI CALCOLARE x, y: è sostanzialmente lo stesso dell'algoritmo di Euclide, cioè quadratico rispetto alla massima lunghezza di a, b.

Teorema. a è invertibile modulo m se e solo se $(a, m) = 1$

Dimostrazione a è invertibile modulo $m \; \Leftrightarrow \; \exists \, x \in \mathbb{Z}$ tale che
$ax \equiv 1 (\text{mod } m) \; \Leftrightarrow \; \exists \, x, y \in \mathbb{Z}$ tali che $ax + my = 1 \; \Leftrightarrow \; (a, m) = 1$
dove l'ultimo passaggio si giustifica così:
($\Leftarrow$) è l'Identità di Bézout.
($\Rightarrow$) Sia $d = (a, m)$, allora d divide a e m, quindi anche $ax + my$, cioè 1.
Ma allora $d = 1$.

Notare L'inverso di a modulo m è l'intero x dell'Identità di Bézout: abbiamo visto come calcolarlo (con costo quadratico rispetto alla lunghezza di a e m).

Sia dunque $1 \leq a < m$,

* $(a, m) = 1 \Rightarrow$ a è invertibile modulo m
* $(a, m) = d \neq 1$: comunque $1 < d \leq a < m$, dunque d è divisore di m e $d \neq 1, m \Rightarrow \exists\, q$ tale che $d \cdot q = m$ e $1 < q < m$

  Quindi $q \not\equiv 0 (\text{mod } m)$, $dq \equiv 0 (\text{mod } m)$

  e di conseguenza $aq \equiv 0 (\text{mod } m)$.

  Dunque a è divisore dello zero modulo m.

ESEMPIO Modulo 4

* 1, 3 sono invertibili, e $(4, 1) = (4, 3) = 1$,
* 2 divide lo zero, e $(4, 2) = 2$.

OSSERVAZIONE Se m è primo, tutti gli elementi a tali che $1 \leq a < m$ sono primi con m, e quindi invertibili modulo m.
Ricordare: i casi $m = 3, 5$.

Un'altra conseguenza dell'Identità di Bézout

1) Se p divide $a \cdot b$ e $(p, a) = 1$, allora p divide b.

Attenzione: può essere che p divida $a \cdot b$ senza dividere né a né b.

Dimostrazione Siano $x, y \in \mathbb{Z}$ tali che $1 = px + ay$, allora

$$b = b \cdot 1 = b(px + ay) = pbx + aby$$

Ma p divide p, dunque pbx, e ab, dunque aby; così p divide anche $pbx + aby = b$.

2) Se p divide ab e p è primo, allora p divide a o p divide b.

Dimostrazione Se p non divide a, allora l'unico divisore di p che divide anche a è $1 \Rightarrow (p, a) = 1$: possiamo applicare il punto 1).

(Ne abbiamo accennato parlando del Teorema fondamentale dell'Aritmetica.)

A PROPOSITO DI MASSIMO COMUNE DIVISORE E MINIMO COMUNE MULTIPLO : ecco una via alternativa per calcolarli.

Siano a, b due naturali $\neq 0$.
Se $a = 1$, $(a, b) = 1$ e $[a, b] = b$. Analogamente se $b = 1$.
Così possiamo supporre $a, b > 1$ e decomporre a, b in fattori primi. Allora:

- (a, b) è il prodotto dei fattori primi comuni alle due decomposizioni con l'esponente minimo;

- $[a, b]$ è il prodotto dei fattori primi comuni e non comuni con l'esponente massimo.

ESEMPIO $72 = 2^3 \cdot 3^2,\ 22 = 2 \cdot 11 \ \Rightarrow\ (72, 22) = 2,\ [72, 22] = 2^3 \cdot 3^2 \cdot 11.$

Algoritmo preferibile a quello euclideo? Per a, b "grandi" certamente NO.

- L'algoritmo euclideo ha costo quadratico rispetto alle lunghezze di a, b
- Non è chiaro il costo di FATTORIZZAZIONE (cioè di decomporre a, b in fattori primi)

Comunque si deduce $(a, b) \cdot [a, b] = a \cdot b$ (e quindi $[a, b] = \frac{a \cdot b}{(a,b)}$)

ESEMPIO $72 \cdot 22 = 2^4 \cdot 3^2 \cdot 11 = (72, 22) \cdot [72, 22]$

CALCOLO DI POTENZE MODULO m

3^{100} è il prodotto di 100 fattori, tutti uguali a 3. Ma non c'è bisogno di operare 99 successive moltiplicazioni per ottenere questo risultato. Possiamo infatti osservare che $100 = 2 \cdot 50$ e dunque

$$3^{100} = (3^{50})^2$$

è il quadrato di 3^{50}. L'osservazione si può ripetere: $50 = 2 \cdot 25$, quindi

$$3^{50} = (3^{25})^2$$

e

$$3^{100} = ((3^{25})^2)^2$$

si ottiene da 3^{25} con due quadrature. Di nuovo $25 = 2 \cdot 12 + 1$, così

$$3^{25} = ((3^{12})^2) \cdot 3$$

Dalle successive divisioni per 2

* $12 = 2 \cdot 6$
* $6 = 2 \cdot 3$
* $3 = 2 \cdot 1 + 1$
* $1 = 2 \cdot 0 + 1$

si ottiene finalmente l'espressione

$$3^{100} = ((((((1 \cdot 3)^2 \cdot 3)^2)^2)^2 \cdot 3)^2)^2$$

che fornisce 3^{100} a partire da 1 con

- 3 moltiplicazioni per 3
- 6 elevamenti al quadrato

dunque con 9 moltiplicazioni, cioè con un numero di operazioni largamente inferiore alle 99 moltiplicazioni prospettate in partenza. Si noti che la sequenza dei resti delle divisioni che permettono questa semplificazione è da basso 1100100, che è l'espressione di 100 in base 2. Le cifre $0, 1$ che vi compaiono corrispondono per la precisione:

- 0 a quadrare
- 1 a quadrare e a moltiplicare per 3

Così se abbreviamo con

$*$ Q l'istruzione *"quadrare"*
$*$ X l'istruzione *"moltiplicare"* (in questo caso *per* 3)

il numero 1100100 determina la sequenza di istruzioni $QXQXQQQXQQ$ da applicare a 1 per ottenere 3^{100}. Naturalmente, quando si lavora modulo m, tutte queste istruzioni si svolgono modulo m, e i risultati possono essere ristretti tra $0,\ 1,\ \ldots,\ m-1$, al prezzo massimo di una divisione per ogni passaggio.

ESEMPIO Poniamo $m = 101$, e dunque calcoliamo 3^{100} modulo 101. Applicando le precedenti istruzioni $QXQXQQQXQQ$ a 1, otteniamo

$$\begin{aligned} 1 \ &\to_Q 1 \to_X 3 \to_Q 9 \to_X 27 \to_Q 729 \equiv 22 \to_Q 484 \equiv 80 \\ &\to_Q 6400 \equiv 37 \to_X 111 \equiv 10 \to_Q 100 \equiv -1 \to_Q 1 \,(\mathrm{mod}\ 101). \end{aligned}$$

Si deduce $3^{100} \equiv 1 (\mathrm{mod}\ 101)$.

L'algoritmo. In generale il procedimento da seguire per calcolare

$$a^k (\mathrm{mod}\ m)$$

per a, k, m interi, $k, m > 1$ è il seguente:

- rappresentare k in base 2;
- sostituire le cifre $0, 1$ della rappresentazione di k rispettivamente con le istruzioni
  - Q: quadrare
  - QX: quadrare e moltiplicare per a;
- applicare la sequenza di istruzioni così ottenuta a 1 modulo m.

ESEMPI

1. $2^{340} \equiv 1 (\text{mod } 341)$. Infatti già sappiamo che 340 in base 2 diviene 101010100. Si ha dunque la sequenza di istruzioni

$$QXQQXQQXQQXQQ,$$

che applicata ad $a = 2$ a partire da 1 produce

$$\begin{aligned} 1 \quad &\to_Q 1 \to_X 2 \to_Q 4 \to_Q 16 \to_X 32 \to_Q 1024 \equiv 1 \\ &\to_{QXQQXQ} 1 \to_Q 1 \, (mod\, 341) \end{aligned}$$

(si noti infatti che l'esecuzione delle prime 6 istruzioni conduce da 1 ancora a 1, e che le seconde 6 ripetono fedelmente le prime 6).

2. $5^7 \equiv 5 (\text{mod } 24)$. Infatti 7 in base 2 è 111, e genera la sequenza di istruzioni

$$QXQXQX$$

che, applicata a 1, produce

$$1 \to_Q 1 \to_X 5 \to_Q 25 \equiv 1 \to_X 5 \to_X 1 \to_X 5 \, (mod\, 24).$$

ESERCIZI

1. Si provi che $2^{560} \equiv 1 (\text{mod } 561)$.
2. Si determini 15^{15} modulo 15 (attenzione!).
3. Si determini 15^{15} modulo 17.

CRITERI DI DIVISIBILITÀ

Abbiamo già sottolineato come il problema di decomporre in fattori primi un naturale $a > 1$ non ha ancora trovato algoritmi capaci di soddisfarlo in modo rapido, almeno per grandi valori di a. A questo proposito può essere utile esplorare la seguente questione.

Problema. Siano $a \in \mathbb{Z}$, p primo: a è divisibile per p?

Ovviamente la domanda si può proporre per un p arbitrario, non necessariamente primo, e l'algoritmo più elementare che le risponde consiste nel dividere a per p, verificando che il resto è 0. Ma esistono talora metodi più rapidi che adesso discutiamo. Chiaramente possiamo assumere $a, p > 0$.

ESEMPIO Vogliamo controllare se 41257 è divisibile per 3. Ricordiamo che

$$41257 = 7 + 5 \cdot 10 + 2 \cdot 10^2 + 1 \cdot 10^3 + 4 \cdot 10^4.$$

Inoltre

$$10 \equiv 1 (\text{mod } 3)$$

dunque

$$10^k \equiv 1^k \equiv 1 (\text{mod } 3) \text{ per ogni } k \in \mathbb{N}$$

Allora

$$41257 \equiv 7 + 5 \cdot 1 + 2 \cdot 1 + 1 \cdot 1 + 4 \cdot 1 = 7 + 5 + 2 + 1 + 4 = 19 (\text{mod } 3)$$

Ma $3 \nmid 19$, così $3 \nmid 41257$.

Vediamo nei dettagli l'algoritmo usato nell'esempio precedente.

1. Calcolare le potenze di 10 modulo p.
2. Fissato a, scrivere a secondo la rappresentazione in base 10

   $$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_k \cdot 10^k + \ldots + a_n \cdot 10^n$$

   con $0 \leq a_0,\ a_1,\ \ldots,\ a_n \leq 9$.
3. Calcolare a modulo p usando questa rappresentazione e i risultati del punto 1.

In questo modo si spiegano i criteri di divisibilità forse già studiati alle scuole medie: ne ripresentiamo alcuni qui di seguito sotto questa nuova luce.

ESEMPI

1. $p = 2$. Allora $10 \equiv 0 (\text{mod } 2)$ e così $10^k \equiv 0 (\text{mod } 2)$ per ogni $k \in \mathbb{N}$, $k > 0$. Così, per ogni a, $a \equiv a_0 (\text{mod } 2)$ dove a_0 è la cifra delle unità di a, e

   $2|a$ se e solo se $2|a_0$, cioè se e solo se $a_0 = 0,\ 2,\ 4,\ 6,\ 8$.

2. $p = 5$. Come già per 2, $10 \equiv (\text{mod } 5)$ e così $10^k \equiv 0 (\text{mod } 5)$ per ogni $k \in \mathbb{N}$, $k > 0$. Di nuovo, per un dato a, $a \equiv a_0 (\text{mod } 5)$ e

   $5|a$ se e solo se $5|a_0$, cioè se e solo se $a_0 = 0$ o $a_0 = 5$.

3. $p = 3$. Come già osservato, $10^k \equiv 1 (\text{mod } 3)$ per ogni $k \in \mathbb{N}$. Così ogni a eguaglia $a_0 + \ldots + a_n (\text{mod } 3)$, e

   $3|a$ se e solo se $3|a_0 + a_1 + \ldots + a_n$;

   in altre parole a è divisibile per 3 se e solo se lo è la somma delle sue cifre.

4. $p = 11$. Stavolta $10 \equiv -1 (\text{mod } 11)$, così $10^k \equiv (-1)^k (mod 11)$ per ogni $k \in \mathbb{N}$. Allora $10^k \equiv 1 (\text{mod } 11)$ se k è pari e $10^k \equiv -1 (\text{mod } 11)$ se k è dispari. Segue che, per ogni a,

$$11|a \text{ se e solo se } 11|a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^n a_n$$

dunque a è divisibile per 11 se e solo se lo è la differenza tra la somma delle sue cifre di posto pari e quella delle sue cifre di posto dispari.

Ad esempio 4323 è multiplo di 11 perché tale è $(4 + 2) - (3 + 3) = 0$; 4257 invece no (perché?).

5. $p = 7$. In questo caso

$$10 \equiv 3 (\text{mod } 7)$$
$$10^2 \equiv 9 \equiv 2 (\text{mod } 7)$$

Moltiplicando membro a membro si ottiene

$$10^3 \equiv 2 \cdot 3 = 6 \equiv -1 (\text{mod } 7)$$
$$10^4 \equiv -3 (\text{mod } 7), \ \ldots$$

In particolare si ha che 7 divide un certo a se e solo se divide

$$a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 + \ \ldots$$

Ad esempio, $7|41257$ se e solo se $7|7 + 5 \cdot 3 + 2 \cdot 2 + 1 \cdot (-1) + 4 \cdot 4$.

Così il criterio per $p = 7$ non è affatto utile, e non fa risparmiare gran tempo rispetto alla divisione diretta di a per 7. Del resto, difficilmente alle scuole si impara e si insegna questo procedimento.

Esercizi

1. Si stabiliscano dei criteri di divisibilità per 4, 9 e per il primo $p = 101$ (si osservi in particolare che a è divisibile per 9 se e solo se lo è la somma delle sue cifre).

2. Si stabilisca un criterio di divisibilità generale per 2^n con n naturale positivo.

Un'altra applicazione: la prova del 9

Può essere che alle scuole elementari abbiamo imparato la prova del 9 adoperata per controllare la correttezza di varie operazioni tra interi, ad esempio della moltiplicazione. Oggi, con l'avvento dei calcolatori, l'uso di queste tecniche elementari sta scomparendo, perché si è sempre meno abituati a fare calcoli "a mano". Pur tuttavia vale la pena di cercare di capire il funzionamento di questa vecchia procedura. Ebbene, le proprietà delle congruenze ce

ne chiariscono il meccanismo. Ricordiamo dapprima che nel caso della moltiplicazione la prova del 9 consiste nel prendere ciascun fattore, sommarne le cifre, e poi eventualmente le cifre della somma risultante e così via fino ad ottenere un valore minore di 10; a questo punto si moltiplicano i numeri così ottenuti da ciascun fattore; la somma delle cifre di questo prodotto deve coincidere con la somma delle cifre del risultato da controllare (sempre assumendo di iterare le somme delle cifre fino a che non si ottengono valori inferiori a 10). Facciamo un esempio: consideriamo il prodotto $371 \cdot 4156$ il cui risultato presunto da controllare è 1541875. Procedendo come appena descritto

* da 371 si ottiene $3 + 7 + 1 = 11$ e poi $1 + 1 = 2$,
* da 4156 si ottiene $4 + 1 + 5 + 6 = 16$ e successivamente $1 + 6 = 7$,
* da 1541875 si ottiene $1 + 5 + 4 + 1 + 8 + 7 + 5 = 31$, da cui si ha poi $3 + 1 = 4$.

A questo punto si esegue il prodotto $2 \cdot 7 = 14$, che ha come somma delle cifre $1+4 = 5$, dunque un valore diverso della somma delle cifre del risultato presunto 1541875. Ne deduciamo che la moltiplicazione è sbagliata.
Cerchiamo adesso di capire in base a quale meccanismo possiamo acquisire questa certezza. Il prodotto $371 \cdot 4156 = 1541875$, se corretto, vale anche modulo 9

$$371 \cdot 4156 \equiv 1541875 (\text{mod } 9)$$

Ma modulo 9

$$371 \equiv 3 + 7 + 1 \equiv 11 \equiv 1 + 1 \equiv 2 (\text{mod } 9)$$

e, allo stesso modo,

$$4156 \equiv 7 (\text{mod } 9),$$
$$1541875 \equiv 4 (\text{mod } 9).$$

Così, invece di

$$371 \cdot 4156 \equiv 1541875 (\text{mod } 9)$$

possiamo controllare

$$2 \cdot 7 \equiv 4 (\text{mod } 9);$$

ma in realtà

$$2 \cdot 7 \equiv 14 \equiv 5 \not\equiv 4 (\text{mod } 9),$$

dunque il risultato 1541875 è sbagliato e va ricalcolato. In effetti si ha $371 \cdot 4156 = 1541876$, come anche la prova del 9 conferma, visto che

$$1541876 \equiv 5 (\text{mod } 9).$$

Si noti però che la prova non ha affidabilità assoluta e può talora essere ingannevole. Ad esempio, l'eventuale errore $371 \cdot 4156 = 1541885$ non viene segnalato perché 1541885 è congruo a 5 modulo 9 come il risultato esatto 1541876

$$1541885 \equiv 1 + 5 + 4 + 1 + 8 + 8 + 5 \equiv 32 \equiv 2 + 3 \equiv 5 (\text{mod } 9).$$

Finalmente è da osservare che una prova del 9 si potrebbe sostituire con una prova del 7, o del 13, o dell'11, o di qualunque altro numero ≥ 2. 9 si fa preferire perché è più facile calcolare la classe modulo 9 dei fattori e del risultato, tramite la somma delle loro cifre, mentre le basi differenti da 9 sono assai meno maneggevoli. In realtà, anche la base 3 andrebbe bene al posto di 9, ma i resti modulo 3 sono sono 0, 1, 2 e la possibilità che la prova modulo 3 non segnali errori effettivi aumenta sensibilmente rispetto al modulo 9.

Due proprietà dei primi:

1) Radici quadrate di 1 modulo N

Teorema. Se N è primo, allora le radici quadrate di 1 modulo N sono ± 1. In altre parole, per N primo, se $x^2 \equiv 1 (\text{mod } N)$, allora $x \equiv \pm 1 (\text{mod } N)$.

Dim. Sappiamo che N divide $x^2 - 1$. Ma $x^2 - 1 = (x-1)(x+1)$ ed N è primo, dunque N divide $x - 1$ o $x + 1$. Nel primo caso $x \equiv 1 (\text{mod } N)$, nel secondo $x \equiv -1 (\text{mod } N)$.

Esempi

1. $N = 2$: modulo 2 ci sono due valori distinti 0, 1 e solo 1 soddisfa $1^2 \equiv 1 (\text{mod } 2)$. Ma si ricordi $1 \equiv -1 (\text{mod } 2)$. Del resto, per ogni x intero,
$$x^2 - 1 \equiv x^2 - 2x + 1 \equiv (x-1)^2 (\text{mod } 2)$$
2. $N = 8$ (non primo!) $\Rightarrow$ le radici quadrate di 1 modulo 8 diventano 4
$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 (\text{mod } 8)$$
3. $N = 6$ (non primo) $\Rightarrow$ le radici quadrate di 1 modulo 6 sono ± 1
$$1^2 \equiv 5^2 \equiv 1 (\text{mod } 6) \quad (\text{mentre } 0^2,\ 2^2,\ 4^2 \not\equiv 1 (\text{mod } 6))$$

Dunque non è vero che, se le radici quadrate di 1 modulo N sono ± 1, allora N è primo.

2) Il Piccolo Teorema di Fermat

Abbiamo già incontrato Pierre de Fermat, giudice francese di inizio Seicento, matematico dilettante.

Teorema. Sia N primo. Allora, per ogni intero a,

$$a^N \equiv a(\text{mod } N)$$

Se poi a è primo con N, $a^{N-1} \equiv 1(\text{mod } N)$.

Cenni sulla dimostrazione
1^a parte. Si può assumere $a \geq 0$ e procedere per induzione su a

- $a = 0 \quad 0^N = 0 \equiv 0(\text{mod } N)$
- $a \Rightarrow a+1$: sappiamo che $a^N \equiv a(\text{mod } N)$ e dobbiamo provare che

$$(a+1)^N \equiv a+1(\text{mod } N)$$

In effetti si ha

$(a+1)^N \equiv a^N +$ termini divisibili per $N \; +1^N \equiv a^N + 1^N \equiv a+1(\text{mod } N)$

Ad esempio

$$(a+1)^2 \equiv a^2 + 2a + 1 \equiv a^2 + 1 \equiv a + 1(\text{mod } 2)$$
$$(a+1)^3 \equiv a^3 + 3a^2 + 3a + 1 \equiv a^3 + 1 \equiv a + 1(\text{mod } 3)$$

e così via.
Una prova rigorosa richiede calcolo combinatorio e ancora il Principio di Induzione.

2^a parte. N divide $a^N - a = a(a^{N-1} - 1)$. Se $(a, N) = 1$, N divide $a^{N-1} - 1$.

Esempi

1. 101 è primo, $(3, 101) = 1$. Abbiamo visto
$$3^{100} \equiv 1(\text{mod } 101)$$
2. 5 è primo, $(2, 5) = 1$, $2^4 = 16 \equiv 1(\text{mod } 5)$
3. 7 è primo, $(2, 7) = 1$, $2^6 = 64 \equiv 1(\text{mod } 7)$
4. 9 non è primo ma $(2, 9) = 1$. Si nota
$$2^8 = 256 \equiv 4 \not\equiv 1(\text{mod } 9)$$

Ricordiamo il nostro obiettivo in PRIMI
Per N intero ≥ 2, riconoscere se N è primo o composto.

Possibile assumere $N > 2$, N dispari

$$\begin{array}{lllll} (N \text{ pari:} & N = 2 & \Rightarrow & N & \text{primo} \\ & N > 2 & \Rightarrow & N & \text{composto}) \end{array}$$

Dubbio

1. Fissiamo $1 < a < N$, a primo con N, ad esempio $a = 2$ visto che si assume N dispari. Ci chiediamo:

   $$\text{Se vale} \quad a^{N-1} \equiv 1 (\text{mod } N), \quad N \text{ è primo?}$$

   (Si noti che $a^{N-1} \equiv 1 (\text{mod } N)$ verifica a basso costo: un elevamento a potenza e una divisione).
   Risposta: NO
   Esempio:
   341 non è primo, $341 = 11 \cdot 31$; $(2, 341) = 1$; $2^{340} \equiv 1 (\text{mod } 341)$

2. Più in generale ci chiediamo:

   $$\text{Se vale} \quad a^{N-1} \equiv 1 (\text{mod } N) \quad \text{per ogni } a \text{ primo con } N, \quad N \text{ è primo?}$$

   Attenzione: il costo di una singola verifica $a^{N-1} \equiv 1 (\text{mod } N)$ è basso, ma, per N primo, le congruenze da verificare sono $N - 2$, una per ogni $a = 2, 3, \ldots, N - 1$
   Di più, la risposta è NO
   Esempio:
   $561 = 3 \cdot 11 \cdot 17$ non è primo; ma si verifica $a^{560} \equiv 1 (\text{mod } 561)$ per ogni a con $1 < a < 561$, $(a, 561) = 1$.

Si chiama pseudoprimo di Carmichael un numero composto N tale che

$$a^{N-1} \equiv 1 (\text{mod } N) \quad \text{per ogni } a \text{ primo con } N$$

Minimo esempio: 561
Altri esempi: 1105, 1729
Alford-Grawille-Pomerance (1994): esistono infiniti pseudoprimi di Carmichael.

Notare Per N primo, tutti gli $N - 1$ naturali da 1 a $N - 1$ sono primi con N (se maggiori di 1 non possono dividere N e dunque l'unico divisore comune con N è 1).

Per ogni $N \geq 1$, poniamo

$$\varphi(N) = \text{numero dei naturali tra 1 e } N \text{ primi con } N$$

La funzione così definita si chiama la φ di Eulero.

Dunque: per N primo, $\varphi(N) = N - 1$
Ad esempio $\varphi(2) = 1,\ \varphi(3) = 2,\ \varphi(5) = 4,\ \ldots$

ALTRI ESEMPI

* $\varphi(1) = 1$
* $\varphi(4) = 2$ (i numeri tra 1 e 4 primi con 4 sono 1, 3)
* $\varphi(6) = 2$ (i numeri tra 1 e 6 primi con 6 sono 1, 5)
* $\varphi(8) = 4$ (i numeri tra 1 e 8 primi con 8 sono 1, 3, 5, 7)
* $\varphi(9) = 6$ (i numeri tra 1 e 9 primi con 9 sono 1, 2, 4, 5, 7, 8)
* $\varphi(10) = 4$ (i numeri tra 1 e 10 primi con 10 sono 1, 3, 7, 9)

Un algoritmo generale per il calcolo di φ?

1) Per p primo e $m \geq 1$, $\varphi(p^m) = p^{m-1} \cdot (p-1)$

   Infatti

   $$\varphi(4) = \varphi(2^2) = 2^1 \cdot (2-1) = 2$$
   $$\varphi(8) = \varphi(2^3) = 2^2 \cdot (2-1) = 4$$
   $$\varphi(9) = \varphi(3^2) = 3 \cdot (2-1) = 6.$$

   Del resto per $m = 1$ e p primo, $\varphi(p) = \varphi(p^1) = p^0 \cdot (p-1) = p - 1$.

   Altri esempi

   $$\varphi(25) = \varphi(5^2) = 5^1 \cdot (5-1) = 20$$
   $$\varphi(27) = \varphi(3^3) = 3^2 \cdot (3-1) = 18.$$

   In generale i p^m naturali tra 1 e p^m si suddividono tra

   * potenze di p $\quad 1 \cdot p, 2 \cdot p, 3 \cdot p, \ldots, p^m = p^{m-1} \cdot p \quad \Rightarrow p^{m-1}$
   * gli altri che interessano a noi $\quad \Rightarrow p^m - p^{m-1} = p^{m-1} \cdot (p-1)$.

2) Per a, b primi tra loro, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

   Infatti

   $$\varphi(6) = \varphi(2 \cdot 3) = \varphi(2) \cdot \varphi(3) = 1 \cdot 2 = 2$$
   $$\varphi(10) = \varphi(2 \cdot 5) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4.$$

   Ancora

   $$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8.$$

   Dimostrazione: non banalissima

ALGORITMO GENERALE È dato $N \geq 2$, ad esempio $N = 72$

- si decompone N in fattori primi $\quad 72 = 2^3 \cdot 3^2$
- si sfrutta 2) per avere $\varphi(N) = \varphi(72) = \varphi(2^3) \cdot \varphi(3^2)$
- si usa 1) per concludere

$$\varphi(72) = \varphi(2^3) \cdot \varphi(3^2) = 2^2 \cdot (2-1) \cdot 3 \cdot (3-1) = 24.$$

ESEMPI

$$\varphi(24) = \varphi(2^3 \cdot 3) = \varphi(2^3) \cdot \varphi(3) = 2^2 \cdot (2-1) \cdot (3-1) = 8$$
$$\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = 2 \cdot (2-1) \cdot 5 \cdot (5-1) = 40$$

Un caso che ci interesserà: per $N = p \cdot q$ con $p \neq q$ primi

$$\varphi(N) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$$

(infatti $\varphi(15) = \varphi(3 \cdot 5) = 2 \cdot 4 = 8$)

DIFETTO DELL'ALGORITMO: richiede la decomposizione in fattori primi di N (e non conosciamo algoritmi a basso costo per FATTORIZZAZIONE). Non si conoscono procedimenti più efficienti per il calcolo di φ.

Notare $\quad \varphi(N) = N - 1 \Longleftrightarrow N$ è primo

Generalizzazione di Eulero del Piccolo Teorema di Fermat

Sia N un intero ≥ 2 e sia $(a, N) = 1$. Allora

$$a^{\varphi(N)} \equiv 1 (\text{mod } N)$$

ESEMPI

1. Ricordare che, per N primo, $\varphi(N) = N - 1 \Rightarrow a^{N-1} \equiv 1 (\text{mod } N)$ è il piccolo Teorema di Fermat (quando a è primo con N).
2. Sia $N = 4$, così $\varphi(N) = 2$.
   Inoltre 3 è primo con 4 e $3^2 = 9 \equiv 1 (\text{mod } 4)$
3. Sia $N = 6$, così $\varphi(N) = 2$.
   Consideriamo $(5, 6) = 1 : \quad 5^2 = 25 \equiv 1 (\text{mod } 6)$.

Torniamo al problema PRIMI: cerchiamo algoritmi che distinguono

primi da composti

senza necessariamente decomporre in fattori primi.

Qualche esempio: si intende che N è un intero ≥ 2.

Teorema (Wilson) N è primo $\Longleftrightarrow (N-1)! \equiv N-1 (\text{mod } N)$

Ricordare $(N-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (N-2) \cdot (N-1)$.

Dimostrazione $N = 2$ è primo e $(2-1)! = 1! = 1 \equiv 2-1 (\text{mod } 2)$.
Assumiamo allora N primo, $N \neq 2 \Rightarrow N$ dispari.
Inoltre $1, 2, \ldots, N-1$ sono tutti invertibili modulo N

- inversi di se stessi, cioè radici di $x^2 \equiv 1 (\text{mod } N)$: solo 1 e -1, cioè $N-1$, modulo N; si noti $1 \not\equiv N-1 (\text{mod } N)$ per $N > 2$;
- gli altri: $N-3$ elementi, che si suddividono in coppie y, z tali che $yz \equiv 1 (\text{mod } N)$ (cioè l'uno inverso dell'altro modulo N); il loro prodotto complessivo è quindi 1 modulo N.

In conclusione

$$(N-1)! = 1 \cdot 2 \cdot \ldots \cdot (N-1) \equiv 1 \cdot (N-1) \equiv N-1 (\text{mod } N)$$

N composto $\Rightarrow$ esiste un divisore d di N tale che $1 < d < N \Rightarrow d$ divide $(N-1)!$ e, se vale $(N-1)! \equiv N-1 (\text{mod } N)$, d divide anche $N-1$, e quindi 1: assurdo. $-$

Esempio

$$\begin{array}{lll} N = 5 & \Rightarrow & (5-1)! = 4! = 24 \equiv 4 (\text{mod } N) \\ N = 6 & \Rightarrow & (6-1)! = 5! = 120 \equiv 0 \not\equiv 5 (\text{mod } 6) \end{array}$$

Difetto Il calcolo di $(N-1)!$ richiede $N-2$ moltiplicazioni e $N-2$ è esponenziale rispetto alla lunghezza di N.

Ritorniamo al Piccolo Teorema di Fermat.

Ci dice

N primo $\Rightarrow$ ogni intero a primo con N soddisfa $a^{N-1} \equiv 1 (\text{mod } N)$

Ma

$\Leftarrow$ è falso!

C. Pomerance: *"la congruenza di Fermat* $a^{N-1} \equiv 1 (mod\ N)$ *è così semplice che è un peccato doverci rinunciare"*

$\Rightarrow$ alcuni procedimenti basati sul Piccolo Teorema di Fermat.

Teorema (Lucas, 1876) Ammettiamo che esista a per cui

1. $a^{N-1} \equiv 1 (\text{mod } N)$
2. $a^m \not\equiv 1 (\text{mod } N)$ per ogni $m = 1, 2, \ldots, N-2$.

Allora N è primo.

Dimostrazione Da 1 segue che a è invertibile modulo N. Da 2 segue invece che gli $N-1$ elementi

$$1, a, a^2, \ldots, a^{N-2}$$

sono a 2 a 2 distinti modulo N.
Infatti, se vale $a^i \equiv a^j (\text{mod } N)$ per $N-1 > i > j \geq 1$, si divide per a^j (ricordando che a è invertibile modulo N) e si ricava

$$a^{i-j} \equiv 1 (\text{mod } N) \quad \text{con} \quad 1 \leq i-j < N-2$$

contraddicendo 2.
Segue che $\varphi(N) = N-1 \Rightarrow N$ è primo. $-$

DIFETTO 1 e 2 richiedono la verifica di $N-1$ congruenze, dunque $N-1$ divisioni, e $N-1$ è esponenziale rispetto alla lunghezza di N.

Teorema (Lucas, 1891) Ammettiamo che esista a per cui

1. $a^{N-1} \equiv 1 (\text{mod } N)$
2′. $a^m \not\equiv 1 (\text{mod } N)$ per ogni divisore m di $N-1$ diverso da $N-1$.

Allora N è primo.

VANTAGGIO Si fa riferimento solo ai divisori m di $N-1$.

DIFETTO È richiesta la fattorizzazione di $N-1$ (che è obiettivo non più facile della primalità di N)

Dim. Basta mostrare che $a^m \not\equiv 1 (\text{mod } N)$ per ogni $m = 1, \ldots, N-2$. Supponiamo invece che ci sia qualche $m = 1, \ldots, N-2$ per cui

$$a^m \equiv 1 (\text{mod } N).$$

Consideriamo $d = (m, N-1)$, allora

$$\begin{aligned} &* \quad 1 \leq d \leq m < N-1, \quad d \quad \text{è divisore di} \quad N-1 \\ &* \quad \text{ci sono} \quad x, \ y \quad \text{interi per cui} \quad d = mx + (N-1)y \end{aligned}$$

Allora vale

$$a^d = a^{mx+(N-1)y} = a^{mx} \cdot a^{(N-1)y} = (a^m)^x \cdot (a^{N-1})^y \equiv 1^x \cdot 1^y = 1(\text{mod } N)$$

e si contraddice $2'$. $-$

Un'altra elegante caratterizzazione dei primi che discende dal Piccolo Teorema di Fermat:
Teorema. Sia $(a, N) = 1$. Allora

$$N \text{ primo} \iff \begin{array}{l}\text{i polinomi } (x^N - a) \text{ e } (x-a)^N \text{ hanno i coefficienti} \\ \text{di ugual grado a 2 a 2 congrui modulo } N\end{array}$$

La dimostrazione: usa sostanzialmente gli stessi argomenti di quella del Piccolo Teorema di Fermat.

SVANTAGGIO: le coppie di coefficienti da confrontare sono $N + 1$.

ALGORITMI PROBABILISTICI

L'IDEA: sacrificare la precisione per aumentare la velocità.

Dunque si ammettono risposte sbagliate o incerte purché i tempi di lavoro siano accelerati e la probabilità di errore o di insicurezza sia bassa.

Émile Borel: *"Un evento che ha probabilità* $< 1/10^{50}$ *non accadrà mai, e se anche accade non sarà mai rilevato".*

Algoritmi

- tipo **Montecarlo**:
  risposte probabilmente vere in tempi certamente rapidi
- tipo **Las Vegas**:
  risposte certamente vere in tempi probabilmente rapidi

Nel 1^o caso è ammessa possibilità di errore
Nel 2^o caso è ammessa possibilità di tergiversare
} da rendere minime!

$\Rightarrow$ **Algoritmo Montecarlo di Miller-Rabin per PRIMI**

I prerequisiti

- se N è primo, le radici quadrate di 1 mod N sono ± 1
- il Piccolo Teorema di Fermat:
  per N primo, se $(a, N) = 1$, allora $a^{N-1} \equiv 1(\text{mod } N)$

Il procedimento di Miller-Rabin (MR per brevità) È dato l'input intero $N > 2$, N dispari. Dunque $N-1$ è pari (da tenere presente!).

Invochiamo un testimone a con $1 < a < N$

- $(a, N) \neq 1 \Rightarrow$ N COMPOSTO (si hanno addirittura informazioni sui divisori $\neq 1, N$ di N)
- $(a, N) = 1$: si calcola a^{N-1} modulo N
  - $a^{N-1} \not\equiv 1 (\text{mod } N) \Rightarrow$ N COMPOSTO
  - $a^{N-1} \equiv 1 (\text{mod } N)$: si ricorda che $N-1$ è pari e quindi $\frac{N-1}{2}$ è un intero ≥ 1; si calcola allora $a^{\frac{N-1}{2}}$ modulo N
    - $a^{\frac{N-1}{2}} \not\equiv \pm 1 (\text{mod } N) \Rightarrow$ N COMPOSTO
    - $a^{\frac{N-1}{2}} \equiv -1 (\text{mod } N) \Rightarrow$ N PROBABILMENTE PRIMO (?)
    - $a^{\frac{N-1}{2}} \equiv 1 (\text{mod } N)$, $\frac{N-1}{2}$ dispari $\Rightarrow$ N PROBABILMENTE PRIMO (?)
    - $a^{\frac{N-1}{2}} \equiv 1 (\text{mod } N)$, $\frac{N-1}{2}$ pari, cioè $\frac{N-1}{4}$ intero > 0: si calcola $a^{\frac{N-1}{4}}$ e si prosegue.

      ...

La risposta N COMPOSTO è sicura.
Quella N PROBABILMENTE PRIMO può essere sbagliata.

Ma la probabilità di errore dopo la consultazione di un testimone a è, al variare di a, al più $\frac{1}{4}$ (almeno 3 testimoni su 4 sono onesti).

Tempi di lavoro:

$$\begin{cases} \text{- ricerca di massimo comune divisore} \\ \text{- elevamenti a potenze} \\ \text{- congruenze } (\Rightarrow \text{ divisioni}) \end{cases}$$

di grado al più 5 rispetto alla lunghezza di N.

D'altra parte, dopo la consultazione di 100 testimoni a con esito concorde N PROBABILMENTE PRIMO

- probabilità di errore $\frac{1}{4^{100}} < \frac{1}{10^{50}}$ ("impossibile da rilevare")
- tempi di lavoro: ancora di grado al più 5 rispetto alla lunghezza di N.

ESEMPI

1. Supponiamo $N = 13$, dunque $N - 1 = 12 = 2^2 \cdot 3$. Affidiamoci ad $a = 2$, che è primo con 13. Notiamo

$$2^{12} \equiv 1 (\text{mod } 13)$$
$$2^6 = 64 \equiv 65 - 1 \equiv -1 (\text{mod } 13)$$

   Dichiariamo N PROBABILMENTE PRIMO (in effetti N è primo).

2. Prendiamo $N = 7$, così $N - 1 = 6 = 2 \cdot 3$. Facciamo ancora riferimento ad $a = 2$; $(2, 7) = 1$, e inoltre

$$2^6 \equiv 1 (\text{mod } 7)$$
$$2^3 \equiv 1 (\text{mod } 7)$$

   (dopo di che l'esponente 3 non è più divisibile per 2). Allora concludiamo N PROBABILMENTE PRIMO (e in effetti N è davvero primo).

3. Sia $N = 561 = 3 \cdot 11 \cdot 17$ composto, anzi pseudoprimo di Carmichael: per ogni b primo con N,

$$b^{560} \equiv 1 (\text{mod } 561)$$

   Osserviamo $N - 1 = 560 = 2^4 \cdot 35$.
   Scegliamo $a = 359 \equiv 2^{16} \equiv 2^{2^4} (\text{mod } 561)$. Allora $(359, 561)=1$ e

$$359^{560} \equiv (2^{560})^{2^4} \equiv 1^{2^4} \equiv 1 (\text{mod } 561)$$
$$359^{280} \equiv (2^{280})^{2^4} \equiv (2^{560})^{2^3} \equiv 1^{2^3} \equiv 1 (\text{mod } 561)$$
$$359^{140} \equiv (2^{140})^{2^4} \equiv (2^{560})^{2^2} \equiv 1^{2^2} \equiv 1 (\text{mod } 561)$$
$$359^{70} \equiv (2^{70})^{2^4} \equiv (2^{560})^2 \equiv 1^2 \equiv 1 (\text{mod } 561)$$
$$359^{35} \equiv (2^{35})^{2^4} \equiv 2^{560} \equiv 1 (\text{mod } 561)$$

   Siccome 35 è dispari, 359 dichiara 561 PROBABILMENTE PRIMO, mentre 561 è COMPOSTO. Ma se il testimone 359 non è attendibile, $a = 2$ lo è. Infatti $(2, 561) = 1$ e

$$2^{560} \equiv 1 (\text{mod } 561)$$
$$2^{280} \equiv 1 (\text{mod } 561)$$
$$2^{140} \not\equiv \pm 1 (\text{mod } 561)$$

   $\Rightarrow$ $N = 561$ è dichiarato COMPOSTO da $a = 2$.

L'algoritmo AKS

- Agrawal: informatico teorico, con interessi alla complessità computazionale (e dunque anche a PRIMI)

- Kayal, Saxena: matematici, dottorandi di Agrawal.

Agosto 2002: l'algoritmo AKS (Agrawal-Kayal-Saxena, appunto)

* distingue se un dato intero $N \geq 2$ è primo o composto

* lavora in tempo poco più che polinomiale di grado 8 rispetto alla lunghezza di N(corrispondente cioè a quel che la moderna Informatica Teorica e in particolare la Teoria della Complessità Computazionale ritengono un algoritmo dai costi ragionevoli)

$\Rightarrow$ soddisfa finalmente le richieste di Gauss (due secoli dopo la loro formulazione).

Ci si riferisce alla seguente caratterizzazione dei primi (già citata):

per N primo e $(a, N) = 1$,

N primo $\iff$ i polinomi $(x^N - a)$ e $(x - a)^N$ hanno i coefficienti di ugual grado a 2 a 2 congrui modulo N.

La difficoltà: $x^N - a$ e $(x - a)^N$ hanno grado $N \Rightarrow N + 1$ coppie da confrontare, dunque troppe rispetto ala lunghezza di N.

Idea: invece che $x^N - a$ e $(x - a)^N$, confrontare i loro resti nella comune divisione per un polinomio $x^r - 1$ con un r opportuno e "piccolo" rispetto alla lunghezza di N($\Rightarrow$ i resti hanno grado $< r$ o sono nulli).

Ultime notizie (conseguenze di AKS)

* 2004: algoritmo di Bernstein-Berrizbeitia (BB per semplicità)

  - probabilistico di tipo Montecarlo
  - lavora in tempo poco più che polinomiale di grado 4 rispetto alla lunghezza di N
  - assolutamente affidabile quando risponde N PRIMO
  - talora fallibile (ma con bassa probabilità di errore) quando dichiara N PROBABILMENTE COMPOSTO

  $\Rightarrow$ da usare in combinazione (e in parallelo) con l'algoritmo MR:

per ogni N

- se BB dichiara N PRIMO, si conclude N PRIMO
- se MR dichiara N COMPOSTO, si conclude N COMPOSTO
- se BB dice che N è PROBABILMENTE COMPOSTO e MR dice che N è PROBABILMENTE PRIMO, si ripete il procedimento con nuovi testimoni: il perdurare dell'incertezza è rarissimo.

∗ 2005: Lenstra-Pomerance propongono un ulteriore miglioramento di AKS che non è probabilistico e richiede tempo poco più che polinomiale di grado 6 rispetto alla lunghezza di N. È quanto di meglio si può attendere da AKS.

Il problema FATTORIZZAZIONE

∗ È dato un intero $N > 2$ dispari e composto.

∗ cerchiamo $1 < d < N$, d divisore di N

Commenti

1. Con le tecniche che conosciamo è rapido riconoscere i primi e i composti, e un numero primo N ha già la sua fattorizzazione N. Allora ci possiamo limitare alla fattorizzazione di numeri composti.

2. d si trova facilmente se N è pari: basta prendere $d = 2$. Così possiamo supporre N dispari e > 2.

3. Da d si ricava velocemente il quoziente q tale che $N = d \cdot q$

   - se d, q sono entrambi primi, $N = d \cdot q$ è la fattorizzazione cercata per N;
   - se d o q (o entrambi) sono composti, si applica di nuovo il procedimento a d, q; alla fine si raggiunge la fattorizzazione cercata.

4. L'eventuale appendice di lavoro per d, q e oltre non aggrava di per sé i tempi dell'eventuale procedimento.

Ma i tempi di lavoro degli algoritmi oggi conosciuti per FATTORIZZAZIONE sono esponenziali (o quasi) rispetto alla lunghezza dell'input N $l(N)$ nonostante l'impiego di strumenti e concetti avanzatissimi:

$e^{c \cdot \sqrt[3]{l(N) \cdot \log l(N)^2}}$ è il tempo di lavoro negli algoritmi più rapidi.

Lenstra: *"ammettiamo di avere un numero $N = dq$ con $d \neq q$ primi e di perdere d, q nella spazzatura; così ci resta solo N; deve essere avvertito come una sconfitta della scienza il prendere atto che il metodo migliore che oggi*

abbiamo per recuperare d, q è quello di cercare nella spazzatura".

UN ESEMPIO FAMOSO Nel 1903, ad un convegno dell'American Mathematical Society F. Cole comunicò di aver scoperto che $M(67)$ - il 67-mo numero di Mersenne $2^{67} - 1$ - è composto

$$2^{67} - 1 = 193707721 \times 761838257287$$

Ma Cole disse di aver speso "3 anni di domeniche" per trovare questa fattorizzazione (anche se oggi con GIMPS i tempi si accorcerebbero moltissimo).

QUALCHE TENTATIVO

1) La fattorizzazione alla Fermat

Un'osservazione già nota a Fermat. Per N composto dispari > 2,

$$\text{trovare} \quad d, q \quad \text{tali che} \quad 1 < d, q < N \quad \text{e} \quad N = d \cdot q$$

equivale a

$$\text{trovare} \quad t > s \quad \text{tali che} \quad N = t^2 - s^2 \quad \text{e} \quad t - s > 1$$

Invece che esprimere N come prodotto di due fattori > 1 possiamo cercare di rappresentarlo come differenza di quadrati.
Ecco perché: assumiamo $d \geq q$ per semplicità.
$(\Leftarrow)$ $N = t^2 - s^2 = (t + s) \cdot (t - s)$
$(\Rightarrow)$ Siccome N è dispari, anche d e q lo sono $\Rightarrow d \pm q$ sono pari, cioè $\frac{d \pm q}{2}$ sono naturali. Inoltre

$$\frac{d+q}{2} + \frac{d-q}{2} = \frac{d+d+q-q}{2} = d$$

$$\frac{d+q}{2} - \frac{d-q}{2} = \frac{d-d+q+q}{2} = q$$

dunque

$$N = d \cdot q = (\frac{d+q}{2} + \frac{d-q}{2})(\frac{d+q}{2} - \frac{d-q}{2}) = (\frac{d+q}{2})^2 - (\frac{d-q}{2})^2$$

dove $\frac{d+q}{2} = t$ e $\frac{d-q}{2} = s$.

ESEMPI

1. $N = 15 = 5 \cdot 3$ si scrive $N = 4^2 - 1^2 = 16 - 1$ per $4 = \frac{5+3}{2}$, $1 = \frac{5-3}{2}$
2. $N = 35 = 7 \cdot 5$ si scrive $N = 6^2 - 1^2 = 36 - 1$ per $6 = \frac{7+5}{2}$, $1 = \frac{7-5}{2}$

3. $N = 33 = 11 \cdot 3$ è anche $N = 7^2 - 4^2 = 49 - 16$ per $7 = \frac{11+3}{2}$, $4 = \frac{11-3}{2}$

IDEA: per N grande, cercare una decomposizione $N = t^2 - s^2$ invece che $N = dq$.

UN CASO FORTUNATO: d, q sono vicini tra loro, dunque a $\sqrt{N}$ (e d, q "grandi") $\Rightarrow$ anche $t = \frac{d+q}{2}$ è vicino a $\sqrt{N}$. Si noti che, per d piccolo o q piccolo, d e q sono più facili da scoprire.

TENTATIVO

1. Considerare $t = \lfloor\sqrt{N}\rfloor + 1, \lfloor\sqrt{N}\rfloor + 2, \ldots$ dove $\lfloor\sqrt{N}\rfloor$ è la parte intera di $\sqrt{N}$ (che in genere non è un intero!)
2. calcolare $t^2 - N$ e verificare che è un quadrato perfetto s^2
3. se sì $t^2 - N = s^2$ implica $N = t^2 - s^2 = (t+s)(t-s)$.

Per d, q non "vicini", possiamo seguire una procedura più complicata, ma simile:

1) per k intero positivo > 1, esplorare $t = \lfloor\sqrt{kN}\rfloor + 1, \lfloor\sqrt{kN}\rfloor + 2, \ldots$
2) calcolare $t^2 - kN$ e controllare se è un quadrato perfetto s^2
3) se sì, cioè $t^2 - kN = s^2$, si ha $kN = t^2 - s^2 = (t+s)(t-s)$; si considera $(N, t+s)$ o $(N, t-s)$ confidando che uno dei due si riveli un divisore $\neq 1, N$ di N.

ESEMPI

1. Sia $N = 200819$. Allora $\lfloor\sqrt{N}\rfloor = 448 \Rightarrow$ si esplorano 449, 450, $\ldots$

$$449^2 - 200819 = 782 \quad \text{non è un quadrato perfetto}$$
$$450^2 - 200819 = 1681 = 41^2 \quad \text{è un quadrato perfetto}$$

Così

$$200819 = 450^2 - 41^2 = (450 - 41) \cdot (450 + 41) = 409 \cdot 491.$$

ESERCIZIO: si controlli se 409, 491 sono primi o composti. Nel secondo caso si prosegua la decomposizione per 409 e/o per 491.

2. Sia $N = 141467$. Anzitutto $\lfloor\sqrt{N}\rfloor = 376 \Rightarrow$ da esplorare 377, 378, $\ldots$ D'altra parte i controlli se

$$\left.\begin{array}{l} 377^2 - 141467 \\ 378^2 - 141467 \\ 379^2 - 141467 \\ \ldots \end{array}\right\} \text{ sono quadrati perfetti}$$

proseguono senza successo fino al 38^o tentativo. Invece, per $k = 3$, si ha $\lfloor\sqrt{3N}\rfloor = 651$, e dunque sono da considerare 352, 353, ... Al quarto tentativo, si vede che

$$655^2 - 3 \cdot 141467 = 68^2 \quad \text{è un quadrato perfetto}$$

Così

$$3 \cdot 141467 = 655^2 - 68^2 = (655 + 68) \cdot (655 - 68)$$

e in effetti

$$(141467, 655 + 68) = 241$$

svela un divisore 241 di 141467: anzi si ha $141467 = 241 \times 587$.

CONCLUSIONE: procedimento macchinoso, basato sulla buona sorte (a priori non conosciamo d, q e possiamo solo sperare che si trovino in posizione a noi favorevole); esistono implementazioni che lo migliorano ma non in modo decisivo.

2) Il metodo ρ di Pollard

ρ è la lettera rho dell'alfabeto greco, quella che corrisponde alla nostra "r"; qui indica un ciclo o preceduto da una premessa $\Rightarrow \rho$. Le motivazioni di questo simbolo sono spiegate dal procedimento.

Ricordare:

- è dato $N > 2$ composto dispari
- cerchiamo $1 < d < N$, d divisore di N.

Per trovare d, fissiamo

- un intero arbitrario x_0 (ad esempio 1)
- un polinomio $f(x)$ a coefficienti interi nella variabile x (ad esempio $x^2 + 1$)

Costruiamo

$$x_1 = f(x_0), \quad x_2 = f(x_1), \quad x_3 = f(x_2), \ \ldots$$

$$\Rightarrow \ x_0, \ x_1, \ x_2, \ x_3, \ \ldots$$

Prima o poi ci sarà nella sequenza una ripetizione modulo il misterioso divisore d: infatti ci sono solo d elementi distinti modulo d $\Rightarrow$ per $j < k$ si ha

$$x_k \equiv x_j (\text{mod } d),$$

cioè d divide $x_k - x_j$. Ma d divide anche N, così possiamo sperare di ottenere d come $(N, x_k - x_j)$.

ESEMPIO $N = 91$ (composto).
Come detto, scegliamo

$$x_0 = 1, \quad f(x) = x^2 + 1,$$

allora

$$\begin{aligned} x_1 &= 2, \\ x_2 &= 2^2 + 1 = 5, \\ x_3 &= 5^2 + 1 = 26, \ \ldots \end{aligned}$$

Notiamo $(x_3 - x_2, N) = (26 - 5, 91) = (21, 91) = 7$.
Si deduce che 7 divide 91, e si calcola facilmente $91 = 7 \cdot 13$.

OSSERVAZIONE Fissato $k \in \mathbb{N},\ k > 0$, dobbiamo calcolare $(x_k - x_j, N)$ per ogni naturale $j < k$, dunque per $k - 1$ valori di j: per k grande, sono prevedibili tempi lunghi. Tuttavia, se $j < k$ rivelano

$$d = (x_k - x_j, N) \neq 1, N,$$

e se $j_1 < k_1$ soddisfano $k_1 - j_1 = k - j$ (cioè $k_1 - k = j_1 - j$), allora si ha che d divide $(x_{k_1} - x_{j_1}, N)$
Infatti

$$x_{j_1} = f^{j_1 - j}(x_j) \equiv f^{k_1 - k}(x_k) = x_{k_1} (\text{mod } d)$$

Naturalmente può capitare che $(x_{k_1} - x_{j_1}, N)$ sia $> d$: ma la probabilità è piccola.

ALGORITMO ρ DI POLLARD (1975) Sia $k \in \mathbb{N},\ k > 0$ e sia h tale che

$$2^h \leq k < 2^{h+1}$$

Consideriamo $j = 2^h - 1$, e calcoliamo per questo unico $j \quad d = (x_k - x_j, N)$.
Se $d \neq 1, N$, siamo a posto. Altrimenti si passa a $k + 1$.

Da ricordare

$$\begin{array}{rlll} k = 1, & \text{cioè} \quad k = 2^0 & \Rightarrow & h = 0 \\ 2 \leq k < 4, & \text{cioè} \quad 2^1 \leq k < 2^2 & \Rightarrow & h = 1 \\ 4 \leq k < 8, & \text{cioè} \quad 2^2 \leq k < 2^3 & \Rightarrow & h = 2 \\ 8 \leq k < 16, & \text{cioè} \quad 2^3 \leq k < 2^4 & \Rightarrow & h = 3 \\ 18 \leq k < 32, & \text{cioè} \quad 2^4 \leq k < 2^5 & \Rightarrow & h = 4 \end{array}$$

e via dicendo.
Così

$$\begin{array}{lcl} x_1 & \text{fa riferimento} & \text{a} \quad x_0 \\ x_2,\ x_3 & & \text{a} \quad x_1 \\ x_4,\ x_5,\ x_6,\ x_7 & & \text{a} \quad x_3 \\ x_8,\ x_9,\ \ldots,\ x_{15} & & \text{a} \quad x_7 \end{array}$$

e via dicendo.

ESEMPIO Ritorniamo a $N = 91$. Facciamo ancora riferimento a

$$x_0 = 1, \quad f(x) = x^2 + 1, \qquad \forall x \in \mathbb{N}$$

$$\Rightarrow \quad x_1 = 2,\ x_2 = 5,\ x_3 = 26,\ x_4 = 677 \equiv 40 (\text{mod } 91),\ \ldots$$

Col metodo ρ si considerano

$$\begin{aligned}(x_1 - x_0, N) &= (2-1, 91) = (1, 91) = 1\\ (x_2 - x_1, N) &= (5-2, 91) = (3, 91) = 1\\ (x_3 - x_1, N) &= (26-2, 91) = (24, 91) = 1\end{aligned}$$

si salta poi $(x_3 - x_2, N)$, che era stata la scelta fortunata in precedenza, si passa invece a

$$(x_4 - x_3) = (40 - 26, 91) = (14, 91) = 7$$

che rivela comunque il divisore 7.

VANTAGGIO DEL METODO
Per ogni $k > 0$, c'è un unico j per cui calcolare $(x_k - x_j, N)$.

SVANTAGGIO
Può capitare di saltare in questo modo qualche coppia "vincente" $j < k$.

Supponiamo comunque che $j < k$ siano tali che

$$(x_k - x_j, N) = d \neq 1, N$$

ma che il metodo ρ trascuri la coppia $j < k$.
Sia poi

$$2^h \leq k < 2^{h+1}$$

Consideriamo

$$\begin{aligned}j_1 &= 2^{h+1} - 1\\ k_1 &= j_1 + (k - j)\end{aligned}$$

Allora

$$2^{h+1} \leq k_1 < 2^{h+2}, \quad j_1 = 2^{h+1} - 1$$

dunque la coppia $j_1 < k_1$ è presa in esame dal metodo ρ e, come osservato in precedenza, c'è alta possibilità che

$$(x_{k_1} - x_{j_1}, N) \quad \text{riveli un divisore} \neq 1, N \ \text{ di } N$$

Inoltre

$$k_1 < 2^{h+2} = 4 \cdot 2^h \leq 4k$$

dunque k_1 è considerato entro il 4-uplo dei passi di k.

ESEMPIO Sia $N = 4087$. Stavolta facciamo riferimento a

$$x_0 = 2, \quad f(x) = x^2 + x + 1 \qquad \forall x \in \mathbb{N}$$

Allora

$$\begin{aligned}
&x_1 = 4 + 2 + 1 = 7,\\
&x_2 = 7^2 + 7 + 1 = 57,\\
&x_3 = 3307,\\
&x_4 \equiv 2745 \pmod{4087},\\
&x_5 \equiv 1343 \pmod{4087},\\
&x_6 \equiv 2626 \pmod{4087},\\
&x_7 \equiv 3734 \pmod{4087},\\
&\quad \ldots
\end{aligned}$$

Col metodo ρ si ha

$$\begin{aligned}
&(x_1 - x_0, N) = (7 - 2, 4087) = (5, 4087) = 1\\
&(x_2 - x_1, N) = (57 \cdot 7, 4087) = (50, 4087) = 1\\
&(x_3 - x_1, N) = (3300, 4087) = 1\\
&(x_4 - x_3, N) = (2745 - 3307) = 1\\
&(x_5 - x_3, N) = (1343 - 3307) = 1\\
&(x_6 - x_3, N) = (2626 - 3307) = 1\\
&(x_7 - x_3, N) = (3734 - 3307, 4087) = 61
\end{aligned}$$

Così $61|4087$, anzi $4087 = 61 \cdot 67$.

QUALCHE CONSIGLIO SULLA SCELTA DI $x_0,\ f$

* x_0 arbitrario
* $f(x)$ polinomio di grado 2 (evitare $f(x)$ di grado 1!)

Argomenti di probabilità mostrano che, salvo queste minime precauzioni, la scelta di $x_0,\ f$ è del tutto ininfluente sul buon esito della ricerca di d.