Questo fascicolo contiene la lezione di venerdì 27 maggio 2019

Gli argomenti trattati sono:

- test di primalità
- pseudo primi di Fermat e pseudo primi forti
- teorema e test di Miller-Rabin

Inoltre vedremo l'applicazione di questi risultati al <u>computer</u>

Lezione di mercoledì 26 aprile (1)

Un problema fondamentale: distinguere i numeri primi dai numeri composti.

C'è una frase di Gauss del 1801 (Disquisitiones arithmeticae), nella quale si dice che ci si deve adoperare con ogni sforzo per risolvere due pb. fondamentali
- distinguere i (numeri) primi dai (numeri) composti
- fattorizzare i numeri composti.
(Eventualmente riportare la frase originale in latino).

Il primo dei due problemi può essere considerato sostanzialmente risolto.

La situazione attuale è la seguente: esistono tre importanti test di primalità. Due di questi test sono "probabilistici" (Solovay-Strassen e Miller-Rabin (1976-77) e "polynomial-time". Probabilistici significa questo:
- se il numero dispari n è sottoposto al test e la risposta è "n è composto", la risposta è certa (cioè il numero è composto e non c'è altro da dire)
- se la risposta è "il numero dispari n è probabilmente primo", significa che non si è certi di questo fatto, ma, con alta probabilità, il numero è primo.

Tra l'altro questa probabilità può essere resa arbitrariamente alta (a prezzo di sforzi sempre maggiori)!

- Esiste un test, detto A.R.S. (2004), dal nome degli scopritori, i tre matematici indiani Agrawal, Kayal e Saxena, che è deterministico e "polynomial-time".

L'aggettivo deterministico significa che se il numero n è sottoposto al test e la risposta è "n è composto", la risposta è certa. Altrettanto se la risposta è "n è primo", ancora la risposta è certa.

C'è però un problema: l'implementazione di questo test non è del tutto soddisfacente: è infatti piuttosto lunga e laboriosa. Nella pratica si tratta del test meno usato, pur essendo deterministico.

Osserviamo anche che i due test precedenti, cioè Solovay-Strassen e Miller-Rabin, da "probabilistici" diventano deterministici (cioè con risposta certa nei due casi), sotto condizione.

Precisamente, se si ammette vera una fondamentale congettura di teoria dei numeri, detta congettura di Riemann generalizzata, i due test precedenti sono deterministici e "polyno-

mial-time", oltre che di facile imple-
mentazione (in particolare il test di Miller-
Rabin, che è il più usato nella pratica)
Il test di Solovay-Strassen è un test di proba-
bilità euleriana ed è basato sulla possibilità
di valutare, in tempo polinomiale, il simbolo
di Jacobi. Alla base di questo test c'è un
importante risultato teorico di teoria dei nu-
meri, precisamente la "legge di reciprocità
quadratica".

- Il test di Miller-Rabin (quello più
usato in pratica) è basato, sostanzialmente, su
un perfezionamento del teorema di Fermat, teo-
rema che dice che se n è un primo dispari
allora $b^{n-1} \equiv 1 \pmod{n}$, per ogni base b
con $1 \leq b \leq n-1$.
Vediamo ora come questo teorema può essere uti-
lizzato.

Per motivare le definizioni che daremo di numero
"pseudo primo di Fermat per la base b" e di numero
"fortemente pseudo primo per la base b", facciamo qual-
che considerazione.
Se vogliamo sapere se il numero dispari n è
primo o no, possiamo scegliere una base b (a
caso) con $1 < b < n$, e procedere come segue:

- si calcola $(b,n)=d$. Se $d>1$ si risponde "n è composto", e la risposta è certa.
- se viceversa $(b,n)=1$ si calcola anche b^{n-1} (mod n)
se $b^{n-1} \not\equiv 1 \pmod n$ si risponde
"n è composto", e la risposta è certa.
- Se $b^{n-1} \equiv 1 \pmod n$
non si può rispondere con certezza, perché come è noto, ci sono numeri che, pur essendo composti si comportano come se fossero numeri primi, per una certa base b.
Vediamo un esempio
(dare un esempio) (Far vedere che $n=91$ è pseudo primo di Fermat per la base $b=3$)
Questo fatto motiva la definizione seguente:
Definizione di pseudo-primo di Fermat per una base b.
Un numero naturale n dispari si dice pseudo primo di Fermat per la base b, se n è composto e verifica la congruenza

$$(*) \quad b^{n-1} \equiv 1 \pmod n.$$

Se n fosse pseudo-primo per "poche" basi b si potrebbe pensare di cambiare base e scoprire così la vera natura di n. Purtroppo le cose non stanno così, infatti esistono numeri dispari e composti n tali che sono pseudo-primi per tutte le possibili basi b con $(b,n)=1$, cioè la congruenza di Fermat

$$x^{n-1}\equiv 1 \pmod n$$

ha $\varphi(n)$ soluzioni.

Questi numeri eccezionali sono detti numeri di Carmichael. È stato per parecchio tempo in discussione se fossero infiniti o no, finchè nel 1994 (Pomerance ed altri) hanno dimostrato che sono effettivamente infiniti.

È chiaro che l'esistenza di infiniti numeri di Carmichael è un ostacolo che pone un limite molto severo all'utilizzazione della sola congruenza di Fermat come base per un test di primalità veramente attendibile. Fortunatamente si può superare questa difficoltà cercando di utilizzare al meglio tutta l'informazione contenuta nella congruenza di Fermat, nel modo seguente.

Supponiamo che n sia il numero dispari da testare. Quindi $n-1$ è pari e possiamo scrivere

$$n-1=2^s t \quad \text{con } t \text{ dispari}$$

raccogliendo la massima potenza di 2 che divide $n-1$. La congruenza di Fermat, cioè $x^{n-1}\equiv 1 \pmod n$, può essere riscritta nel modo seguente

$$x^{n-1}-1 = x^{2^s t}-1 = \left(x^{2^{s-1}t}-1\right)\left(x^{2^{s-1}t}+1\right)=\left(x^{2^{s-2}t}-1\right)\left(x^{2^{s-2}t}+1\right)\left(x^{2^{s-1}t}+1\right)=$$

$$\otimes \quad = \cdots\cdots = \left(x^{t}-1\right)\left(x^{t}+1\right)\left(x^{2t}+1\right)\left(x^{2^2t}+1\right)\cdots\cdots\left(x^{2^{s-1}t}+1\right)\equiv$$

$$\equiv 0 \pmod n$$

A questo punto osserviamo che se n fosse primo dovrebbe dividere uno almeno dei fattori a sinistra di ⊠, cioè dovrebbe essere verificata una almeno delle congruenze

$$\left\{\begin{array}{l} x^{t} \equiv 1\ (n) \\ x^{t} \equiv -1\ (n) \\ x^{2t} \equiv -1\ (n) \\ \vdots \\ x^{2^{s-1}t} \equiv -1\ (n) \end{array}\right. \quad (**)$$

(Osserviamo che solamente una delle congruenze qui a fianco può essere verificata (perché?)).

Questo motiva la definizione seguente:

Def. di numero fortemente pseudo primo per la base b.

Un numero dispari e composto n si dice fortemente pseudo primo per la base b (con $1 \leq b < n$) se una delle congruenze seguenti è verificata

$$\left\{\begin{array}{l} b^{t} \equiv 1\ (n) \\ b^{t} \equiv -1\ (n) \\ b^{2t} \equiv -1\ (n) \\ \vdots \\ b^{2^{s-1}t} \equiv -1\ (n) \end{array}\right. \quad (***)$$

Osservazione

È evidente che se un numero dispari n è fortemente pseudo primo per la base b è anche pseudo primo (di Fermat) per la base b, mentre il viceversa non è, in generale vero, come è facile capire (perché?) ed illustrare con esempi.

Quindi (far vedere che $n = 91$ è pseudo primo, ma non fortemente pseudo primo per $b = 3$)

$$\left\{\begin{array}{l} n \text{ fortemente pseudo primo} \\ \text{per la base } b \end{array}\right. \Rightarrow n \text{ pseudo primo per la base } b$$

$\not\Leftarrow$ (no)

- La definizione di fortemente pseudo primo primo per la base b è molto più restrittiva della definizione di pseudo primo per la base b, e su di essa si può basare un efficientissimo test probabilistico di primalità. Si può infatti dimostrare il seguente

Teorema (Miller_Rabin)

Sia n un intero dispari e composto.
Indicando con N il numero della basi b per le quali n è fortemente pseudo primo si ha

$$N \leq \frac{n}{4}$$

È chiaro che sul teorema di Miller-Rabin si può basare un efficientissimo test probabilistico di primalità procedendo nel modo seguente.
Si deve testare il numero dispari n.

Passo 1

— Si scelgono k basi casualmente, diciamo $b_1, b_2, \ldots, b_k$ e si calcola (b_i, n) per ogni $i = 1, \ldots, k$. Se esiste j tale che $(b_j, n) = d_2$ si risponde "n è composto" (risposta certa); se viceversa si ha $(b_i, n) = 1$ per ogni $i = 1, 2, \ldots, k$ si procede.

Passo 2

Si valuta la forte pseudo primalità di n rispetto alle basi scelte. Se per almeno una base b_j (con $1 \leq j \leq k$) nessuna delle congruenze (***) è soddisfatta si risponde "n è composto" (risposta certa).

Se, viceversa, n risulta essere fortemente pseudo primo per tutte le basi scelte $b_1, b_2 \ldots, b_k$, lo si dichiara "probabilmente primo" (con probabilità $P < \frac{1}{4^k}$)
In quest'ultimo caso la risposta non è certa.

— Se si ammette la congettura di Riemann generalizzata si può dimostrare che:
Se n è dispari e composto, esiste una base b, con $1 \leq b \leq 2 \lg^2 n$ per la quale n non è fortemente "pseudo-primo". (Cioè esiste un "testimone" molto piccolo (rispetto ad n) del fatto che n è composto).
Quindi, sotto condizione, il test di Miller-Rabin diviene "polynomial-time" e deterministico (risposta sempre certa)

— Si tratta di una specie di gratta e vinci: se testando n con tutte le basi b con $1 \leq b \leq 2 \lg^2 n$ si dà una risposta errata si vince qualche milione di dollari. Infatti si dimostrerebbe che la congettura di Riemann generalizzata è falsa, e per questo parecchie università americane offrono premi in denaro.
C'è anche un'altra scuola di pensiero che dice che non è credibile che testando, ad esempio, 500 basi $b_1, \ldots, b_{500}$ casuali, si dia una risposta errata. Questo perché un evento che ha una probabilità P di verificarsi, con $P \leq \frac{1}{4^{500}}$ non verrà mai osservato