ALGEBRA COMPUTAZIONALE

Programma del corso

(i) impossibilità, incompatibilità, indecidibilità, complessità (P v NP) con riferimento particolare alla speciale posizione che ha avuto il problema PRIME.

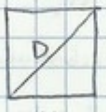
(ii) dimostrazione dell'infinità dei numeri primi; criteri di primalità, primo per n particolari (Mersenne, Fermat), poi per n generali. In particolare, il metodo Aks, che nel 2004 è stato il primo ad essere deterministico, incondizionato, polinomiale.

(iii) Distribuzione dei numeri primi: risultati di Bertrand ($\exists\, p \;/\; n < p < 2n$), Chebyshev ($\exists\, A, B$ esplicitamente calcolabili tali per cui $A \cdot \frac{n}{\log n} \leq \pi(n) < B \cdot \frac{n}{\log n}$, Nair.

(iv) Fattorizzazione: primalità, sequenze ricorrenti, gruppo delle ellittiche e delle coniche.

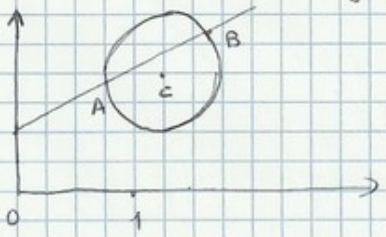
(v) Frazioni continue e applicazioni (equazione di Pell)

(i)



$D = \frac{m}{n} \cdot U \longrightarrow 2 = \frac{m^2}{n^2} \longrightarrow 2n^2 = m^2$ ⁂

Altri problemi classici sono la duplicazione del cubo, la trisezione di 60°, la quadratura del cerchio, da ottenere con riga e compasso.



- siano i coefficienti delle equazioni di retta e circonferenza $\in \mathbb{Q}$

coord(A), coord(B) $\in K_1$, con $[K_1 : \mathbb{Q}] = 2$

Reiterando, sostituendo l'$\in \mathbb{Q}$ con un'$\in K_1$, si ottiene $[K_2 : K_1] = 2$, ovvero $[K_2 : \mathbb{Q}] = 4$

In generale $[K_n : \mathbb{Q}] = 2^n$

Ora, sia $F = \mathbb{Q}[\sqrt[3]{2}]$; $[F : \mathbb{Q}] = 3$. Supponendo che per un dato n sia $\mathbb{Q} \subseteq F \subseteq K_n$, sarà $[K_n : \mathbb{Q}] = [K_n : F] \cdot [F : \mathbb{Q}]$, cioè $2^n = [K_n : F] \cdot 3$, assurdo poiché banalmente $3 \nmid 2^n$.

- In maniera analoga, consideriamo la costruzione di poligoni con p^t lati, dove p è un primo diverso da 2.
Allora, $[\mathbb{Q}(\alpha_{p^t}) : \mathbb{Q}] = \varphi(p^t) = p^{t-1}(p-1)$, con come polinomio minimo di α_n, Φ_n, di grado $\varphi(n)$.
$\mathbb{Q}(\alpha_{p^t}) \subseteq \mathbb{K} \Rightarrow \varphi(p^t) \mid 2^n \Rightarrow p^{t-1}(p-1) \mid 2^n \Rightarrow t = 1$
$\Rightarrow p-1 \mid 2^n \Rightarrow p-1 = 2^k \Rightarrow p = 2^k + 1$
$\Rightarrow p = 2^{2^s}+1 = F_s$ (Fermat)
$n = 2^k \cdot p_1 \cdot \dots \cdot p_m$ p_i sono primi di Fermat distinti

- Altro problema è l'impossibilità di risolvere la quintica, in generale, con radicali.
  - Nicola Tartaglia 1500 - 1557
  - Scipione del Ferro 1465 - 1526 | cubica
  - Girolamo Cardano 1501 - 1576
  - Ludovico Ferrari 1522 - 1565 quartica
  - Ruffini 1765 - 1822
  - Abel 1802 - 1829 | quintica

$f(x)$ è risolubile per radicali $\Leftrightarrow G(f(x), \mathbb{Q}) = G$
ovvero se $\exists H_i \mid H_n = \{1_G\}$, $H_1 = G$, $H_{i+1} \trianglelefteq H_i$
campo di spezzamento di $f(x)$, e H_i/H_{i+1} è abeliano.
Se $f(x)$ ha grado $p \geq 5$ primo e ha esattamente 2 radici non reali allora $G(f(x), \mathbb{Q}) = S_p$
Es: $f(x) = x^5 - 6x + 3$
$G(f(x), \mathbb{Q}) = S_5$
$S_5 \trianglerighteq A_5 \trianglerighteq \{1\}$

- (Cantor) I reali non sono numerabili
3. $\forall \alpha$ $\alpha < 2^\alpha$
$\overline{\overline{X}} < \overline{\overline{\mathcal{P}(X)}}$
$\overline{\overline{\mathbb{R}}} = \overline{\overline{\mathcal{P}(\mathbb{N})}}$
$c > \omega$

2. (diagonalizzazione)
1) $0, a_{11} a_{12} a_{13}$
2) $0, a_{21} a_{22} a_{23}$
⋮
n) $0, a_{n1} a_{n2} a_{n3}$
$\alpha = 0, b_1 b_2 \dots b_n \dots$ scelgo $b_n \neq a_{nn}$

1. Sia L una lista numerabile di reali $L = \{b_1, b_2, \dots, b_n, \dots\}$
$\exists$ allora almeno un reale che $\notin L$.

Dim. Se $\forall\, b_i, b_j$, $\exists\, b_k$, tale che b_k è compreso tra b_i e b_j, allora si dice che L ha la proprietà dell'elemento intermedio.

Se L non ha questa proprietà è dimostrato.

Supponiamo ora che ce l'abbia.

Realizziamo una sequenza in questo modo:

- $a_1 = b_1$
- $a_2 = b_2$
- a_n : primo elemento della lista compreso tra a_{n-1} e a_{n-2}.

Gli a_{2k+1} crescono e si mantengono minori di tutti gli a_{2k+2}, che decrescono. Siano:

- $\lim a_{2k+1} = \alpha$
- $\lim a_{2k+2} = \beta$

Allora $[\alpha, \beta] \not\subseteq L$, ed eventualmente $\alpha \notin L$ se $\alpha = \beta$.

Applicazioni:

$I =]0,1[$, si consideri $I \cap \mathbb{Q}$

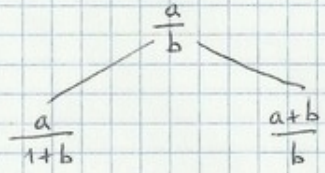
$$L = \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}\right\}$$

$$\text{Cantor}(L) = \left\{\frac{F_n}{F_{n+1}} : n \geq 1\right\}$$ F_n n-esimo numero di Fibonacci.

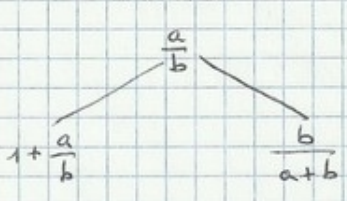
$\lim \frac{F_n}{F_{n+1}} = \frac{1}{\phi}$, il che prova la sua irrazionalità

Alberi:

CALKIN - WILF



KEPLERO



- dato un alfabeto finito Σ, $\Sigma^* = \{\text{stringhe finite su } \Sigma\}$
  $|\Sigma^*| = \omega$
- l'insieme delle stringhe finite di interi è numerabile
- i numeri algebrici sono numerabili
- fissato un linguaggio di programmazione, l'insieme di tutti i programmi in $\mathcal{L}$ è numerabile.

- Un numero α si dice computabile se esiste un programma che calcola la sequenza delle cifre di α.
  L'insieme dei numeri reali computabili è numerabile.

  Un insieme numerabile si dice listabile se esiste un programma che scrive in tempo finito ogni suo elemento.
  L'insieme dei programmi che computano i numeri reali non è listabile.
  Supponiamo infatti per assurdo che lo sia. Allora esiste P che in un tempo finito scrive i listati dei programmi che calcolano i numeri reali.
  Facciamo girare P_1 per un passo: otteniamo a_{11}
  " P_2 " 2 passi: " a_{21}, a_{22}
  " P_n " n passi: " $a_{n1}, a_{n2}, \dots, a_{nn}$
  Scriviamo un programma che computi $\beta = 0, b_1 b_2 \dots b_n \dots$, con $b_n \neq a_{nn}$; questo non appartiene ad alcuno dei precedenti.

19.10.2010

- $A \subseteq \mathbb{Z}$, A si dice listabile se esiste un programma che scrive in tempo finito ogni suo elemento.
- Supponiamo A numerabile. Allora esiste g tale per cui $g: \mathbb{N} \to A$
  $A = \{a_1, a_2, \dots, a_n, \dots\}$ $\quad a_n = g(n)$
- Il programma P esegue computazioni C_1, C_2. Quando C_i termina, si può produrre un elemento di A, oppure nessun risultato.
  In un determinato tempo, produce $\{a_{i_1}, a_{i_2}, \dots\}$
- Abbiamo già visto che esistono insiemi numerabili non listabili
  $\mathbb{Z}$ è listabile, $\mathbb{N}$ è listabile.
  Prendiamo per esempio $A_3 = \{a \in \mathbb{Z} : \exists x_1, x_2, x_3 \in \mathbb{Z} \quad a = x_1^3 + x_2^3 + x_3^3\}$
  Sia C_1 la lista dei risultati ottenuti prendendo $|x_i| \le 10$;
  C_2 " $|x_i| \le 10^2$;
  in generale, C_n " $|x_i| \le 10^n$
  Mettendo di seguito i risultati, si prova che A_3 è listabile.
- Definiamo un insieme $A \subseteq \mathbb{Z}$ <u>diofantino</u> se esiste un polinomio $f \in \mathbb{Z}[t, x_1, \dots, x_n]$ $(f \in \mathbb{Z}[t, \vec{x}])$ tale per cui
  $A = \{t \in \mathbb{Z} : \exists \vec{x} \in \mathbb{Z}^n \ / \ f(t, x_1, \dots, x_n) = f(t, \vec{x}) = 0\}$
- Esempi: A_3 è diofantino ponendo $f(t, x_1, x_2, x_3) = t - x_1^3 - x_2^3 - x_3^3$
  $\mathbb{N}$ è diofantino ponendo $f(t, x_1, x_2, x_3, x_4) = t - \sum_{i=1}^{4} x_i^2$,
  per il noto teorema di Lagrange sulla somma dei quattro quadrati.
- Definiamo un insieme $A \subseteq \mathbb{Z}$ <u>computabile</u> se esiste un programma che calcola la sua funzione caratteristica.

$$\forall x \in \mathbb{Z} \qquad \varphi_A(x) \begin{cases} 0 & x \notin A \\ 1 & x \in A \end{cases}$$

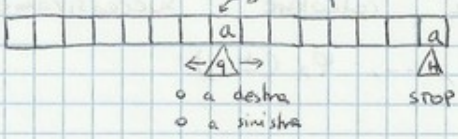
- <u>Computabilità $\Rightarrow$ listabilità</u>
  infatti dato P che calcola φ_A si fabbrica P' che lista A.
  P' chiama P e gli fa calcolare successivamente.
  $\varphi_A(0)$, $\varphi_A(\pm 1)$, $\varphi_A(\pm 2)$, ..., $\varphi_A(\pm n)$
- <u>Diofantinità $\Rightarrow$ listabilità</u>
  facile

- Teorema DPRM (Davies, Putnam, Robinson, Matijasievich)
  Afferma che vale anche listabilità $\Rightarrow$ diofantinità,
  e che dunque diofantinità $\Leftrightarrow$ listabilità.
  Il risultato colpì in particolare per quanto riguarda
  l'insieme dei numeri primi: esso è ovviamente listabile
  (basta il crivello di Eratostene), ma allora è anche
  diofantino, e dunque esiste un polinomio che lo genera.
  Esso è stato determinato esplicitamente, ed è di grado 25.
  $P = \{t \in \mathbb{N} : \exists\, x_1, \dots, x_{26} \quad f(t, \vec{x}) = 0\}$
  $F(t, \vec{x}) = t(1 - f(t, \vec{x})^2)$
  $P = \{t \in \mathbb{N} : \exists\, \vec{x} \quad F(t, \vec{x}) > 0\}$
  Il problema della sua utilizzo per ~~g~~ trovare nuovi
  numeri primi è però ostacolato dal fatto che
  molto spesso il risultato esce negativo.

- Uno dei problemi proposti da Hilbert nel 1900 (il decimo)
  può essere proposto in forma moderna nel modo seguente:
  ci si chiede se esiste un programma tale che, data
  un'equazione diofantina $f(\vec{x}) \in \mathbb{Z}[x]$, $f(\vec{x}) = 0$, ci dica
  se essa possiede soluzioni oppure meno.
  Sia $\mathcal{Q}$ la proposizione "esistono insiemi che sono listabili
  ma non computabili". Allora $\mathcal{Q}$ + DPRM $\Rightarrow \neg$ 10° H.
  Sia A listabile ma non computabile. Allora A per
  DPRM è diofantino e $\exists f \; A = \{a \in \mathbb{Z} : \exists\, \vec{x} \quad f(a, \vec{x}) = 0\}$
  Per l'ipotesi $\mathcal{Q}$, A non è computabile. Allora non c'è
  alcun programma. ☠

MACCHINE DI TURING

- Modello di computazione:



- insieme $\mathcal{Q}$ di stati $\quad H \in \mathcal{Q} \quad |\mathcal{Q}| = n$
  H = halt $\quad n$ stati $\neq H$
  $F \subseteq \mathcal{Q}$
  $F = \{\text{stati finali}\} \quad H \in F$

- $|\Sigma| = s$ s simboli

  alfabeto: sono le lettere che legge e scrive

  $\exists \lambda \in \Sigma$ blank

  $\sum_{0=\lambda} = \{0,1\}$ nastro vuoto

- Una macchina di Turing M è una funzione parziale, ovvero non necessariamente ovunque definita, tale per cui:

  $M: Q \times \Sigma \to Q \times \Sigma \times MOV$

  con $MOV = \{R, L\}$ insieme di cardinalità 2 delle possibili mosse: o un passo a sinistra, o uno a destra.

- Consideriamo un indice temporale discreto $t = 0, 1, 2, \ldots$

  Per $t = 0$, la testina si trova in un punto del nastro fissato nello stato iniziale $q_0 \in Q$

  Per un t generico, la macchina si trova in uno stato $q_t \in Q$; se $q_t = H$, allora la macchina si ferma con successo.

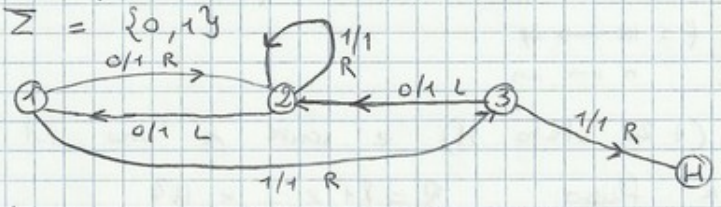
  Per $q_t \neq H$ invece, la macchina legge il simbolo $a \in \Sigma$ che si trova nella cella sotto di lei, e calcola:

  $M(q_t, a)$ — se non è def. su (q_t, a) → si ferma in stato $\neq H$, stop con insuccesso

  se è def. su (q_t, a) → al tempo $t+1$ passa nello stato q_{t+1}, scrive b e si sposta di mov

  La macchina si ferma con insuccesso anche se esce dal nastro.

- Una possibile rappresentazione si può ottenere tramite diagramma di flusso:



  dove la prima cifra prima della barra indica ciò che viene letto e la seconda ciò che viene scritto.

- Un' altra rappresentazione si può avere con delle cartelline:

	①
0	0R4
1	0L2

	②
0	1R3
1	1L2

	③
0	1R1
1	1R3

	④
0	0L4
1	0L5

	⑤
0	0R4
1	1L5

Tematica interessante da sviluppare è quella della computabilità e della decidibilità di una macchina di Turing.

La tesi di Church afferma che ogni algoritmo è equivalente alla macchina di Turing.

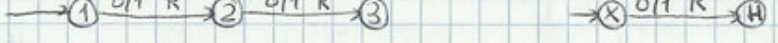
- Ogni linguaggio di programmazione noto è equivalente alla macchina di Turing, nell'ipotesi di non avere limitazioni di macchina come la finitezza della memoria
- Definiamo anche la funzione Σ di Rado come la funzione che conta gli "uno".
  Sia $B(n)$ l'insieme delle macchine di Turing con esattamente n stati; $B(n)$ è finito.
  Sia $Ferm(n) \subseteq B(n)$ l'insieme delle macchine di $B(n)$ che si fermano con successo sul nastro vuoto.
  Sia $\Sigma(n)$ il massimo numero di 1 lasciati sul nastro da una M e $Ferm(n)$. Si sa che:
  - $\Sigma(1) = 1$
  - $\Sigma(2) = 4$ (Rado, 1962)
  - $\Sigma(3) = 6$ (Rado, Lin, 1965)
  - $\Sigma(4) = 13$ (Brady, 1983)
  - $\Sigma(5) \geq 4098$ (Herxen)
  - $\Sigma(6) > 1,29 \cdot 10^{865}$ (Herxen, Bentrock)

22.10.2010

① $\exists T$: se parte dal nastro vuoto con x "uno", si ferma lasciando $2x$ "uno" sul nastro.

Consideriamo macchine che calcolano funzioni $f: \mathbb{N} \to \mathbb{N}$, dove $n \in \mathbb{N}$ è rappresentato in forma unaria.
Si dice che M_f calcola f se per ogni input $= n$ la M_f si ferma e lascia nel nastro $f(n)$ "uno".
T calcola le $\begin{cases} f: \mathbb{N} \to \mathbb{N} \\ n \mapsto 2n \end{cases}$

② $I^{(x)}$ ha x stati (+ lo stato H) e scrive x "uno" sul nastro vuoto
codice diagramma a flusso $Q = \{1, 2, \dots, x, H\}$



③ Se M_f calcola f e M_g calcola g, $\exists M_{g \circ f}$ che calcola $g \circ f$, che ha $n_1 + n_2$ stati se M_f ha n_1 stati e M_g ha n_2 stati.

Def. • $B(n)$ = insieme delle macchine con n stati; $B(n)$ è finito

• $Ferm(n) = \{M \in B(n)$ che si fermano con successo partendo dal nastro vuoto$\}$

• Funzione di rado $G : \mathbb{N} \to \mathbb{N}$

• $G(n)$ = max numero di "uno" scritto da una macchina $M \in Ferm(n)$

Teor. Se $f : \mathbb{N} \to \mathbb{N}$ è computabile allora per ogni n sufficientemente grande si ha $G(n) \geq f(n)$.

Dim. Definiamo $F(n) = \sum_{k=1}^{n} f(k)$. Allora:

$\forall n \quad F(n) \geq f(n) \qquad (I)$

$m \geq n \Rightarrow F(m) \geq F(n) \qquad (II)$

F è computabile

$\exists M_F$ che calcola F

M_F ha c stati

Definiamo anche $U^{(x)} = M_F \circ T \circ I^{(x)}$

$\forall x \quad U^{(x)}(x) = F(2x)$

$U^{(x)}$ computa $F(2x)$

$U^{(x)}$ ha $c+5+x$

$U^{(x)} \in Ferm(c+5+x)$

$n = c+5+x \qquad U^{(x)} \in Ferm(n)$

$G(n) \geq F(2x)$

Se $n \geq 2c+10 \iff x \geq c+5$

Se $x \geq c+5$, allora $2x \geq x+c+5 = n$

Se $x \geq c+5 \Rightarrow 2x \geq n \Rightarrow F(2x) \geq F(n) \geq f(n)$

allora $G(n) \geq f(n)$

Cor. G non è computabile

Dim. Se G fosse computabile, lo sarebbe anche $G+1$, ovvero $G(n)+1$, per n grande a sufficienza.

$G(n) \geq G(n) + 1$, assurdo.

Es. $G(5) \stackrel{?}{=} 4098$

$Q = \{A, B, C, D, E, H\}$

$Mov = \{R, L\}$

$\Sigma = \{0, 1\}$

stato	lett.	scrit.	mov.	nuovo
A	0	1	R	B
A	1	1	L	C
B	0	1	R	C
B	1	1	R	B
C	0	1	R	D
C	1	0	L	E
D	0	1	L	A
D	1	1	L	D
E	0	1	R	H
E	1	0	L	A

n. passi	5000	10 000	20 000	100 000	⋮	47.176.870
n. "uno"	87	175	223	394 (tra le posizioni 49.461 e 50.028)	⋮	4.098

Consideriamo una biezione $G : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, in questo modo:

$G(m,n) = 2^{m-1}(2n-1)$

$n \in \mathbb{N}$, $n = G(a,s)$, $n = 2^{a-1}(2s-1)$ (per il TFA)

Macchina di Turing:

$M : Q \times \Sigma \to Q \times \Sigma \times MOV$

$|Q| = n$, $|\Sigma| = q$

$Q = \{1,2,\dots,n\}$, $\Sigma = \{1,2,\dots,q\}$

$MOV = \{1,2\}$

Consideriamo la sequenza dei primi:

$p_1, p_2, \dots, p_n = \text{prime}(n)$

$s \in Q$, $a \in \Sigma$

$M(s,a) = (t,b,m)$

Si calcola $G(s,a)$ e si considera: $e(s,a) = 2^t \cdot 3^b \cdot 5^m$

Consideriamo anche $\text{NUMAC}(M) \triangleq \prod_{s=1}^{n} \prod_{a=1}^{q} p_{G(s,a)}^{e(s,a)}$

macchine Turing $\leftrightarrow \mathbb{N}$

$\text{numac}(\text{Ferm}) \subseteq \mathbb{N}$ $\quad \text{Ferm} = \{\text{macchine Turing che si fermano partendo dal nastro vuoto}\}$

$\text{Ferm} = \bigcup_{n \geq 1} \text{Ferm}(n)$

$\mathcal{F} = \text{numac}(\text{Ferm}) \subseteq \mathbb{N}$

(1) $\mathcal{F}$ è listabile

Prendiamo infatti tutte le macchine in $\mathcal{F}$ che sono $\leq 2^k$, e le facciamo girare per 2^k passi. Facciamo variare $k = 1,2,3,\dots$ e scriviamo le macchine che si fermano.

(2) $\mathcal{F}$ non è computabile

Se ci fosse W che calcola $\mathcal{F}$, si potrebbe agire così: preso $B(n)$, che è finito, si chiede a W se $M_{n,i} \in \mathcal{F}$ per ogni i. Allora sarebbe possibile trovare $\text{Ferm}(n)$ e in un tempo finito calcolare $G(n)$, assurdo.

Ciò dà l'effettiva risposta negativa al decimo problema di Hilbert.

DECIDIBILITÀ

Un problema si dice decidibile se ogni sua istanza è decidibile in tempo finito da un algoritmo.

È indecidibile per esempio il problema dell'arresto.

- Realizziamo un programma in questo modo:
  - si produce la sequenza dei primi
  - ci si ferma se si trova p per cui $\begin{cases} p \equiv 3 & (8) \\ 2^{\frac{p-1}{2}} \equiv 1 & (p) \end{cases}$

Il sistema non è verificato per alcun primo, poiché

$p \equiv 3 \ (8) \implies 2^{\frac{p-1}{2}} \equiv -1 \ (p)$

- Alternativamente, prendiamo in input $\varepsilon > 0$, e calcoliamo $p_1, \dots, p_n$. Ci si ferma se ad un certo punto si ha $\frac{p_{n+1} - p_n}{\log p_n} < \varepsilon$.

  Nel 2005 Goldston, Yıldırım, Pintz hanno dimostrato che:

  $$\liminf_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n} = 0$$

- O ancora, si calcolano $p_i, p_{i+1}, \dots$, $p_i > M$ e ci si ferma se $p_{i+1} - p_i = 2$ (congettura dei primi gemelli)
- O infine, partendo da n, si considera la successione di Collatz. $T(n) = \begin{cases} n/2 & \text{se } n \text{ è pari} \\ 3n+1 & \text{se } n \text{ dispari} \end{cases}$, e ci si ferma se $\exists s \ / \ T^{(s)}(n) = 1$

Se l'arresto fosse decidibile, si potrebbe individuare $\text{Ferm}(n)$ e calcolare $G(n)$, il che ci fa ancora pervenire ad un assurdo.

Turing ha dimostrato l'esistenza di una macchina universale. Essa prende il codice di una T qualsiasi, e un input, ed esegue la computazione di T su quell'input.

Sono universali:

TM (stati 2, simboli 18)	Rogozhin	1996
TM (3, 9)		
TM (4, 6)		
TM (5, 5)		
TM (7, 4)	Minsky	1962
TM (10, 3)		
TM (19, 2)	Baiocchi	2001

universale $\implies$ indecidibilità

COMPLESSITÀ

classe P: polinomiale; un problema ha una soluzione in tempo polinomiale se, data una qualsiasi istanza x del problema, si arriva ad una soluzione in un numero (finito) di passi che è $O(|x|^k)$ con k fissato (non dipende da x)

Un esempio è dato dal calcolo dell'$MCD(a,b)$, con $b < a$; si arriva infatti in un numero di passi che è $O(\log(b))$, che ha crescita sottolineare.

Altri esempi analoghi sono dati da:

- calcolo di $a^n \bmod m$ $\quad O(\log(n))$

n è una potenza perfetta?

$\exists\, a, b > 1 \quad n = a^b$ è polinomiale

$\log n = b \cdot \log a$

$1 < b \leq \log n$

si sceglie una base $b = 2, \ldots, [\log n]$ e vedo se n è potenza b-esima.

(26.10.2010)

Problemi:

1) n è una potenza perfetta?
2) n è primo?
3) Il grafo G è hamiltoniano?
4) Il grafo G è euleriano?
5) Knapsack (zaino): dato $A = \{a_1, \ldots, a_n\}$, $a_i > 0$, e dato S, $\exists\, B \subseteq A : \sum B = S$?
6) commesso viaggiatore: dato un grafo G pesato e $k > 0$, $\exists$ un percorso hamiltoniano di peso $\leq k$?
7) fattorizzare n
8) Dato G e dati $g, x \in G$ (logaritmo discreto)
   trovare se esiste $y : g^y = x$
9) Dato G e dati $x \in G$, $e > 0$
   trovare $y : y^e = x$ (radice)

Note:

- Un percorso hamiltoniano in G è un percorso sui lati di G che passa una volta per ogni vertice.
- Un percorso euleriano in G è un percorso sui vertici di G che passa una volta per ogni lato.

- Un grafo è tale (ham/eul) se ammette almeno un percorso [ham/eul]
- Diciamo che $\mathcal{P} \in P$ se $\exists$ un alg., $k \geq 0$, $\forall I \in \mathcal{P}$, l'algoritmo risponde sì o no in un tempo $T(I) \in O(|I|^k)$

  Es. I = grafo G, $|I|$ = peso delle istanze I

  $|G|$ = numero vertici

  $|I| = |n| = \log n$ $\qquad I = n \in \mathbb{N}$

- Con riferimento ai problemi precedenti, sappiamo che 1), 2), 4) $\in P$, mentre non sappiamo degli altri.
- Introduciamo ora la

  classe NP: non deterministicamente polinomiale; esiste una macchina non deterministica che risponde in tempo polinomiale.

- T.M. $M : Q \times \Sigma \to Q \times \Sigma \times MOV$

  M è una funzione parziale

  non è necessariamente ovunque definita

- T.M. non def. $M \subseteq (Q \times \Sigma) \times (Q \times \Sigma \times MOV)$

  $M : Q \times \Sigma \to Q \times \Sigma \times MOV$

  può essere anche non funzionale

  $M(s,a) \subseteq Q \times \Sigma \times MOV$

- $\mathcal{P} \in NP$ se $\forall I \in \mathcal{P}$ $\exists$ certificato, verificabile in tempo polinomiale, che ci dice se la risposta è sì.
- Ancora con riferimento ai problemi precedenti, tutti i problemi $\in NP$. Si noti che $P \subseteq NP$



Problemi irrisolti sono:

- $P = NP$?
- $P = NP \cap co\text{-}NP$
- $co\text{-}NP \neq NP$?

RIDUZIONE

- $\mathcal{P} \leq \mathcal{Q}$ significa che esiste una funzione f computabile in tempo polinomiale, $\forall I \in \mathcal{P} \Rightarrow f(I) \in \mathcal{Q}$

  e I ha risp. sì $\iff$ $f(I)$ ha risp. sì

  In questo caso, se si sa risolvere $\mathcal{Q}$ in tempo polinomiale, allora si sa risolvere anche $\mathcal{P}$ in tempo polinomiale.
- Un problema $\mathcal{P}$ si dice NP-completo se $\mathcal{P} \in NP$ e $\forall \mathcal{S} \in NP$ si ha $\mathcal{S} \leq \mathcal{P}$

- Problema SAT

  Sono date n variabili proposizionali $x_1, \dots, x_n$, ovvero variabili per le quali siano ammissibili soltanto i valori 0 e 1.

  $E = (a_1 \vee a_2 \vee \dots \vee a_s) \wedge (b_1 \vee \dots \vee b_u) \wedge \dots \wedge (z_1 \vee \dots \vee z_k)$

  dove $a_i, b_j, z_v \longrightarrow x_t$ oppure $\neg x_t$

  $\exists$ una distribuzione di valori di verità a $x_1, x_2, \dots, x_n$ tale che E è vero?

  La soluzione, data da Levin - Cook, permette di affermare che SAT è NP - completo.

  Un' estensione può essere data dal problema 3-SAT.

- Un problema simile può essere dato dal completamento di un sudoku: data una griglia con alcuni numeri, è possibile determinare in tempo polinomiale se è completabile?

  Non è stato dimostrato, ma ragionevolmente sembrerebbe di no.

- Campo minato: è completabile?

  Anche questo è NP - completo, quindi, come il caso precedente, a meno che le classi collassino l'una sull'altra, non è risolvibile in tempo polinomiale. Se infatti si sapesse risolvere uno di questi problemi in tempo polinomiale, allora li sarebbero risolvibili tutti, e dunque dovrebbe essere P = NP.

- Consideriamo uno schema crittografico realizzato nel seguente modo:

  $A = \{a_1, a_2, \dots, a_n\}$ pubblico

  $M = \{b_1, b_2, \dots, b_n\}$ bit

  $\sum_{i=1}^{n} a_i b_i = A \cdot M = S$

  $S \longrightarrow B$

  B lo deve ricevere? ☺

  L'idea è quella di:

  1) usare una successione speciale per la quale sia risolubile il problema
  2) nascondere la successione, trasformandola in modo segreto e pubblicandola

- Per ovviare al primo problema, utilizziamo una successione supercrescente : $\forall i \quad a_i > \sum_{k=1}^{i-1} a_k$

Supponiamo ora A supercrescente : $A = \{a_i\}_{i=1}^{n}$

Ricevo $M \cdot A = \sum_{i=1}^{n} b_i a_i = S \quad b_i \in \{0,1\}$

Ora, si controlla la condizione $S > a_n$.

- Se è verificata, $b_n = 1$, e $S' = S - a_n$
- Se non è verificata, $b_n = 0$, e $S' = S$

Si ripete poi con S' e $(a_1, \dots, a_{n-1})$, e così via.

- Vediamo ora cosa succede ragionando modulo $m > 2 \cdot a_n$.

Sia $w \in \mathbb{Z}_n^*$. Calcoliamo w^{-1} segreto, e la sequenza

$c_i = w \cdot a_i \mod m$.

Si pubblicano $c_1, c_2, \dots, c_n = C$;

poi $M = \{b_i\}$ e $M \cdot C = S$

Si calcola poi $Sw^{-1} \bmod m = \sum b_i c_i w^{-1} \bmod m$

$= \sum b_i a_i \bmod m = T$

(29.10.2010)

Algoritmo crittografico (chor rivest ; Merckle Hellman Knapsack)

$\mathbb{K} = GF(p^h) = \mathbb{Z}_p[x]/(f(x)) = \mathbb{F}(t)$ $f(x)$ irriducibile in $\mathbb{Z}_p(x)$ di grado h

$f(x)$ irriducibile in $\mathbb{Z}_p[x]$ di grado h

$t : f(t) = 0 \qquad t \in \mathbb{K}$

$[k : \mathbb{Z}_p] = h$

$k^* = \langle g \rangle \qquad \log_g v = e$, per $v \in k^*$, se $g^v = e$

π permutazione di $0, 1, \dots, p-1$

$d \in \mathbb{Z}_{(p^h-1)} \qquad p^h - 1 = |\mathbb{K}^*|$ $\qquad p \sim 200, \ h \sim 25$

segreti g, π, d

Consideriamo ora la quantità $d + \log_g(t + \pi(i)) := c_i$, modulo $p^h - 1$.

Ne segue che $0 \le c_i \le p^h - 2$.

Abbiamo dunque : chiave pubblica $c_0, c_1, \dots, c_{p-1}$ p, h

Sia ora un messaggio $M = (m_0, m_1, \dots, m_{p-1})$ m_i bit $0, 1$

Con $\sum_{i=0}^{p-1} m_i = h$. La codifica sia :

$C = E(M) \triangleq M \cdot c = \sum v_i c_i \mod p^h - 1$

A riceve C, e calcola $g^{C - hd}$.

Calcolando sempre in modulo $p^h - 1$, abbiamo che :

$$C - hd = \sum_{i=0}^{p-1} m_i c_i - hd = \sum_{i=0}^{p-1} m_i (d + \log(t + \pi(i))) - hd$$

$$= d \cdot \sum_i m_i + \sum_i m_i \log_g (t + \pi(i)) - hd$$

$$= \sum_i m_i \log_g (t + \pi(i))$$

$g^{c-hd} = \prod_i g^{m_i \cdot \log_g(t+\pi(i))} = \prod_i (t+\pi(i))^{m_i}$ è un polinomio di grado h in t in $\mathbb{Z}_p[x]$.

fattorizzo e trovo i $\pi(i)$ e quindi gli indici tali per cui $m_i = 1$, da cui si può poi trovare M. $\sum v_i = h$

Se $\prod_i (t+\pi(i))^{n_i} = \prod_i (t+\pi(i))^{m_i} \in K$, allora:

$t^h + a_1 \cdot t^{h-1} + \dots = t^h + b_1 \cdot t^{h-1} + \dots$

$a_i = b_i \quad \forall i$

Lemma $c \in G$, n intero, $n = \prod_{i=1}^{k} p_i^{e_i}$ (per G finito)

n è il periodo di $c \iff \begin{cases} c^n = 1 = 1_G & (1) \\ c^{n/p_i} \neq 1 \quad \forall i \quad 1 \le i \le k & (2) \end{cases}$

Dim. $\Rightarrow$ banale

$\Leftarrow$ $\text{per}_G(c) = v$

la (1) $v \mid n$

$\Rightarrow v = p_1^{v_1} \cdot \dots \cdot p_i^{v_i} \cdot \dots \cdot p_k^{v_k} \quad \forall i \; v_i \le e_i$

Per la (2), dato $1 \le i \le k$, $c^{n/p_i} \neq 1$, e quindi $v \nmid \frac{n}{p_i}$

$\frac{n}{p_i} = p_1^{e_1} \cdot \dots \cdot p_i^{e_i - 1} \cdot \dots \cdot p_n^{e_n}$

Lucas

n è primo $\iff \exists a \begin{cases} a^{n-1} \equiv 1 \mod n \\ a^{\frac{n-1}{q_i}} \neq 1 \mod n \quad \forall i \quad 1 \le i \le s \end{cases}$

Infatti: $n-1 = \prod_{i=1}^{s} q_i^{v_i} = \text{per}_{(\mathbb{Z}_n^*)}(a)$

$\Rightarrow n-1 \mid \varphi(n) \Rightarrow \varphi(n) = n-1 \Rightarrow n$ è primo

(L1) PNT $\pi(n) \sim \frac{n}{\log n}$

(L2) n con 200 cifre in base 10

primi di n sono circa: $\sim \frac{10^{200}}{200 \cdot 2,3}$

certificato di Pratt

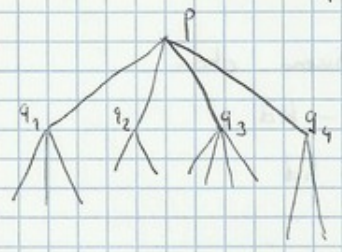
l'ente calcola i fattori di $p-1$

$p-1 = \prod_{i=1}^{k} q_i^{v_i}$

Calcoliamo a in modo che valgano (L1), (L2)

La procedura darà: $(q_1, q_2, \dots, q_n, a)$

Possiamo realizzare un albero, detto albero di Pratt, in cui q sta sotto al primo p se $q \mid p-1$;



$|A(p)| = 1 \iff p = 2$

p

$q = 2$

$p - 1 = 2^k$

$p = 2^k + 1 = 2^{2^n} + 1$

$|A(p)| = 2$

Teorema di Pratt $|A(p)| \leq 4 \cdot \log p - 4 = 4(\log p - 1)$

Dim. Detto n il numero di primi sotto p, se $k = 1$:

$|A(p)| = 2 \Rightarrow p = 2^k + 1$, $p \geq 3$

$4 \cdot \log 3 - 4 \cong 2.3 > 2 = |A(p)|$

Supponiamolo ora vero per ogni primo $< p$ e proviamolo per p. Si ha infatti:

$$|A(p)| = 1 + \sum_{i=1}^{k} |A(q_i)| \leq 1 + \sum_{i=1}^{k} (4 \cdot \log q_i - 4)$$
$$= 1 - 4k + 4 \cdot \sum_{i=1}^{k} \log q_i$$
$$= 1 - 4k + 4 \cdot \log \prod_{i=1}^{k} q_i$$
$$< 1 - 4k + 4 \cdot \log p < 4 \cdot \log p - 4$$

per ogni $k \geq 2$.

Questo ha permesso di affermare che il problema Prime fosse un problema NP, fatto che non era precedentemente noto.

Risultati sui primi

- Esistono infiniti primi (Euclide)

  Dato infatti un elenco finito $L = \{p_1, p_2, \dots, p_r\}$, allora esiste un primo q che non appartiene a L.

  Infatti, la quantità $s = p_1 \cdot \dots \cdot p_r + 1$ è divisa da un primo q, eventualmente sè stesso, che non può essere uno tra i p_i, in quanto $s \equiv 1 \ (p_i)$ per ogni i.

- Esistono infiniti primi congrui a 3 modulo 4.

  Sia ancora un elenco finito di siffatti primi:

  $L = \{p_1, p_2, \dots, p_r\}$, con appunto $p_i \equiv 3 \ (4)$.

  Sia $n = 4 \cdot p_1 p_2 \cdot \dots \cdot p_s - 1$. Naturalmente $n \equiv 3 \ (4)$, e deve esistere q primo $/ \ q \mid n$, $q \equiv 3 \ (4)$, $q \neq p_i \ \forall i$.

  Infatti, ~~se~~ appunto che $p_i \nmid n \ \forall i$, tutti i (nuovi) fattori non possono essere $\equiv 1 \ (4)$, altrimenti lo sarebbe il loro prodotto (si noti che 2 non può starci in quanto è dispari). Dunque c'è almeno un nuovo primo $\equiv 3 \ (4)$

- Esistono infiniti primi congrui a 1 modulo 4

  Ancora $L = \{p_1, p_2, \dots, p_r\}$, $p_i \equiv 1 \ (4)$

  Sia $n = 4 \cdot p_1^2 \cdot \dots \cdot p_r^2 + 1$

  $\exists \ q \mid n \ / \ n \equiv 0 \ (q) \iff p \equiv 1 \ (4)$

  $4 \cdot p_1^2 \cdot \dots \cdot p_s^2 \equiv -1 \ (q)$ $\quad a^2 \equiv -1 \ (q)$

  $q \equiv 1 \ (4)$

- Generalizzazione di Dirichlet: dati a, n coprimi, esistono infiniti numeri primi tali per cui $p \equiv a \ (n)$.
  In precedenza noi abbiamo visto i casi $(a,n) = (1,4)$ e $(3,4)$.
- Esiste una versione più semplice anche se meno potente, dovuta a Bertuccioni e detto Dirichletino. Esso tratta unicamente il caso $a = 1$.
- Rivediamo intanto un attimo i polinomi ciclotomici:

$$x^n - 1 = \prod_{d|n} \phi_d(x)$$

$$\phi_n(x) = \prod_{(i,n)=1} (x - \alpha_n^i)$$

$$\alpha_n = e^{\frac{2\pi i}{n}}$$

$$\alpha_n^k = e^{\frac{2\pi k i}{n}} = \cos\left(2\pi \cdot \frac{k}{n}\right) + i \cdot \sin\left(2\pi \cdot \frac{k}{n}\right)$$

Esempi:

$\phi_1(x) = x - 1$ (rad. primitiva 1)

$\phi_2(x) = x + 1$ (rad. primitiva -1, così come $[1]$ genera $(\mathbb{Z}_2, +)$)

$\phi_3(x) = 1 + x + x^2$ (rad. primitive $-\frac{1}{2} \pm \frac{\sqrt{3}}{2} i$, così come $[1], [2]$ generano $(\mathbb{Z}_3, +)$)

$\phi_4(x) = x^2 + 1$ (rad. primitive $\pm i$, così come $[1], [3]$ generano $(\mathbb{Z}_4, +)$)

...

$\phi_p(x) = 1 + x + \dots + x^{p-1}$ per ogni p (in quanto ogni $[1], [2], \dots, [p-1]$ genera $(\mathbb{Z}_p, +)$)

- **Lemma**

$$\left.\begin{array}{l} e \mid n \\ e < n \end{array}\right\} \Rightarrow \phi_n(x) \Big| \frac{x^n - 1}{x^e - 1} \qquad (1)$$

Infatti

$$x^n - 1 = \prod_{d|n} \phi_d(x) = \phi_n(x) \cdot R_n(x) \quad \text{dove} \quad R_n(x) = \prod_{\substack{d|n \\ d<n}} \phi_d(x)$$

dall'ipotesi $x^e - 1 \mid R_n(x) \Rightarrow R_n(x) = g(x)(x^e - 1)$

$$x^n - 1 = \phi_n(x) \cdot g(x) \cdot (x^e - 1)$$

$$\frac{x^n - 1}{x^e - 1} = \phi_n(x) \cdot g(x)$$

$q \neq p_k$, c intero, $q \mid f_k(c) \Rightarrow q \nmid c^{n/p_k} - 1 \qquad (2)$

Dim.

Per semplicità di notazione, poniamo innanzitutto $p = p_k$

Sia $f_k(c) = \dfrac{c^n - 1}{c^{\frac{n}{p}} - 1}$. Si definisce $b = c^{\frac{n}{p}} - 1$. Allora:

$$f_k(c) = \frac{(b+1)^p - 1}{b} = \frac{\sum_{h=0}^{p} \binom{p}{h} b^h - 1}{b}$$

$$= \frac{1 + pb + \binom{p}{2} b^2 + \dots + b^p - 1}{b}$$

$$= p + \binom{p}{2} b + \dots + b^{p-1} = p + mb$$

Per ipotesi $q \mid p + mb$. Se $q \mid c^{n/p} - 1$ allora $q \mid b \Rightarrow q \mid p$ ovvero $q = p$, assurdo

- Passiamo ora al teorema: per ogni n, esistono infiniti primi tali per cui $p \equiv 1 \ (n)$.

  Dimostrazione:

  Sia $Q = \{q_1, \dots, q_t\}$, con $q_i \equiv 1 \pmod n$, eventualmente anche vuoto.

  Poniamo $n = \prod_{i=1}^{s} p_i^{e_i}$, $c = u q_1 \cdot \dots \cdot q_t \cdot p_1 \cdot \dots \cdot p_s$,

  u tale che $|\phi_n(c)| \geq 2$.

  La tesi diventa che ogni $q | \phi_n(c)$ è $q \equiv 1 \ (n)$

  Abbiamo che:

  $$q | \phi_n(c) \mid c^n - 1 \Rightarrow q | c^n - 1 \Rightarrow c^n \equiv 1 \pmod q \Rightarrow \begin{matrix} q \neq q_i \\ q \neq p_j \end{matrix}$$

  Per ①:

  $$q | \phi_n(c) \left| \frac{c^n - 1}{c^{n/p_n} - 1} \right. = f_k(c) \Rightarrow q | f_k(c) \overset{\text{per } ②}{\Rightarrow} q \nmid c^{n/p_k} - 1$$

  Per il risultato sul periodo:

  $$\Rightarrow n = \text{per}_{2_q^*} c \Rightarrow n | q - 1 \Rightarrow q \equiv 1 \ (n)$$

(02.11.2010)

- Dimostrazione di Eulero dell'esistenza di infiniti numeri primi

  Sia $0 < \alpha < 1$. Sappiamo che $\frac{1}{1-\alpha} = \sum_{k=0}^{\infty} \alpha^k$. Se $\alpha = \frac{1}{p}$, possiamo scrivere $\frac{1}{1 - \frac{1}{p}} = (1 - p^{-1})^{-1} = \sum_{k=0}^{\infty} \frac{1}{p^k}$.

  Sia P un insieme finito di numeri primi, $\{p_1, \dots, p_s\}$.

  Definiamo $\langle P \rangle \triangleq \{n \in \mathbb{N} : n = p_1^{e_1} p_2^{e_2} \cdot \dots \cdot p_s^{e_s}\}$.

  Sia: $\prod_{p_i \in P} (1 - p_i^{-1})^{-1} = \prod_{p_i \in P} \sum_{k_i=0}^{\infty} \frac{1}{p_i^{k_i}} = \sum_{k_i=0}^{\infty} \frac{1}{p_1^{k_1} p_2^{k_2} \cdot p_s^{k_s}} = \sum_{n \in \langle P \rangle} \frac{1}{n}$

  La serie converge ad un razionale qualsiasi sia $P \subseteq \mathbb{P}$.

  Supponiamo ora che esistano solamente s numeri primi, ovvero quelli di P. Allora in questo caso $P = \mathbb{P}$, e $\langle P \rangle = \mathbb{N}$.

  Ne consegue che $\prod_{p_i \in P} (1 - p_i^{-1})^{-1} = \sum_{n \in \mathbb{N}} \frac{1}{n}$, assurdo poichè il termine di destra diverge.

- Dimostrazione di Polya

  L'idea è quella di produrre una successione di interi a due a due coprimi, utilizzando gli interi di Fermat, ovvero quelli della forma $F_n = 2^{2^n} + 1$. Il fatto che gli F_n siano coprimi deriva dalla formula ricorsiva $F_n = F_0 \cdot F_1 \cdot \dots \cdot F_{n-1} + 2$, che si può provare per induzione: banalmente si verifica che $F_1 = F_0 + 2$ e che $F_2 = F_0 \cdot F_1 + 2$, e supposto vero fino ad n, la prova per $n+1$ discende dal fatto che

  $$F_{n+1} = (F_n - 1)^2 + 1 = F_n^2 - 2 \cdot F_n + 1 + 1 = F_n (F_n - 2) + 2$$
  $$= F_n (F_0 \cdot F_1 \cdot \dots \cdot F_{n-1}) + 2$$

Prendiamo F_m e F_n, supponendo, senza perdita di generalità, che $m < n$. Allora, se $MCD(F_m, F_n) = d$, poiché $F_n = F_{n-1} \cdot \ldots \cdot F_m \cdot \ldots \cdot F_0 + 2$, dovrà essere $d \mid 2$, da cui $d = 1$ oppure $d = 2$. Il secondo caso tuttavia si esclude immediatamente osservando che gli F_i sono dispari.

- Dimostrazione di Furstenberg

Definiamo una topologia (generale) su $\mathbb{Z}$: come sottobase di aperti di $\mathbb{R}$ prendiamo $\mathcal{R} \triangleq \{[a]_n, a \in \mathbb{Z}, n \geq 1\}$, e sia $\mathcal{B} = \{\text{intersezioni finite degli elementi di } \mathcal{R}\}$

Dimostriamo che, se $A \in \mathcal{B}$ e $A = \emptyset$, allora A è infinito.

Consideriamo $[a]_n$ e $[b]_m \in \mathcal{R}$, e sia $[a]_n \cap [b]_m \neq \emptyset$.

Allora se esiste c tale per cui $\begin{cases} c \equiv a \pmod n \\ c = b \pmod m \end{cases}$, allora ne esistono infiniti; c può non esistere, nel caso in cui le due congruenze si contraddicano, ma dalla teoria dei sistemi di congruenze, se ce n'è uno ce ne sono infiniti.

Questo dimostra la cosa per due; l'estensione ad un numero finito qualsiesi è immediata.

Sia ora $\mathcal{J}$ la famiglia degli aperti.

Se $A \in \mathcal{J}$, $A \neq \emptyset$, allora A è infinito.

Posto $\mathcal{A} = \{[0]_p : p \in \mathbb{P}\}$, vale $\bigcup_P \mathcal{A} = \mathbb{Z} - \{\pm 1\}$

Osseviamo che gli aperti $[a]_n \in \mathcal{R}$ sono anche chiusi, poiché $= \mathbb{Z} - \bigcup_{b \neq 0} [b]_n$ per un opportuno b.

Supponiamo ora che $\mathbb{P}$ sia finito.

Allora $\bigcup \mathcal{A}$ è unione finita di chiusi, dunque chiuso.

Il complementare $\{\pm 1\}$ è pertanto aperto, ma ciò è assurdo, in quanto abbiamo dimostrato che gli aperti non vuoti sono infiniti.

- Dimostrazione di Erdos

Sia $P = \{p_1, p_2, \ldots, p_s\}$, con $P \subseteq \mathbb{P}$.

Definiamo $g_P(x) = |\{y \in \langle P \rangle : y \leq x\}|$. Prendiamo un y qualunque scrivendolo nella forma $y = a^2 \cdot p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_s^{b_s}$, con i b_i uguali a 0 oppure a 1.

Se $y \leq x$, allora $a^2 \leq x$, ergo $a \leq \sqrt{x}$. Possiamo produrre così $[\sqrt{x}] \cdot 2^s$ numeri, e dunque:

$$g_P(x) \leq [\sqrt{x}] \cdot 2^s \leq \sqrt{x} \cdot 2^s$$

Supponiamo ora $\mathbb{P}$ finito, facendo coincidere $\mathbb{P}$ con P.
Allora, $g_P(x) = x$, in quanto tutti gli y da 1 a x sarebbero generati da elementi di P.
Ne seguirebbe che $x \leq \sqrt{x} \cdot 2^s$, da cui $x^2 \leq x \cdot 2^{2s} \Rightarrow x \leq 2^{2s}$, e dunque sarebbe possibile generare solo un numero finito di interi.

- Risultato di Erdos

Teor. $\sum_{p \in \mathbb{P}} \frac{1}{p}$ diverge

Dim. Supponiamo che $\sum_{p \in \mathbb{P}} \frac{1}{p}$ converga. Allora $\forall \varepsilon > 0 \ \exists j / \sum_{i>j} \frac{1}{p_i} < \varepsilon$.
Sia per esempio $\varepsilon = \frac{1}{2}$. Ne seguirebbe naturalmente che:
$\exists j / \sum_{i>j} \frac{1}{p_i} < \frac{1}{2}$
Sia $P = \{p_1, p_2, \dots, p_j\}$. Si avrebbe la seguente conseguenza:
$x - g_P(x) \leq \left[\frac{x}{p_{j+1}}\right] + \left[\frac{x}{p_{j+2}}\right] + \dots \leq \frac{x}{2}$
$\sqrt{x} \cdot 2^s \geq g_P(x) \geq \frac{x}{2}$
$x \leq \sqrt{x} \cdot 2^{s+1} \Rightarrow \sqrt{x} \leq 2^{s+1} \Rightarrow x \leq 2^{2s+2}$, assurdo poiché x qualsiasi.
Si veda, in generale, Crandall - Pomerance "Prime Numbers"

- Cenni sulla distribuzione dei primi

Sia $y \leq x$, $y = \prod_{i=1}^{s} p_i^{e_i} = \prod_{i=1}^{\pi(x)} p_i^{e_i}$; naturalmente $p_i^{e_i} \leq x$.
Possiamo stabilire una biezione tra $\{y \leq x\}$ e $E \subseteq \{(e_1, \dots, e_n) : 0 \leq e_i \leq \log x\}$.
Per ogni $0 \leq e_i \leq [\log x]$ ci sono $1 + [\log x]$ scelte; ci sono pertanto in tutto $(1 + [\log x])^{\pi(x)}$ scelte, da cui $x \leq (1 + \log x)^{\pi(x)}$.
Prendendo i logaritmi da entrambi i membri, abbiamo:
$\log x \leq \pi(x) \cdot \log(1 + \log x)$. Algebricamente e analiticamente:
$\pi(x) \geq \frac{\log x}{\log(1 + \log x)} = L(x)$
$\lim_{x \to \infty} L(x) = \infty$
Dunque $\pi(x)$ non è limitata, ed esistono infiniti primi.

- Con argomenti di Lagrange

Sia $A(x, y) = |\{\text{interi } a : a \leq x, a \text{ non è divisibile per alcun primo} \leq y\}|$
Per il principio di inclusione - esclusione, vale:
$A(x, y) = x - \sum_{i=1}^{s} \left[\frac{x}{p_i}\right] + \sum_{1 \leq i < j \leq s} \left[\frac{x}{p_i p_j}\right] + \dots + (-1)^s \cdot \left[\frac{x}{p_1 p_2 \cdots p_s}\right]$
dove $p_1, p_2, \dots, p_s$ sono i primi $\leq y$
Abbiamo inoltre che $A(x, \sqrt{x}) = \pi(x) - \pi(\sqrt{x}) + 1$, da cui
$\pi(x) = A(x, \sqrt{x}) + \pi(\sqrt{x}) - 1$.
Al solito, supponiamo che esistano solo s primi.
Sia $n = p_1 \cdot p_2 \cdot \dots \cdot p_s$, pertanto $\pi(n) = \pi(n^2) = s$.

Dalla formula precedente:

$\pi(n^2) = A(n^2, n) + \pi(n) - 1$

il che implica $A(n^2, n) = 1$.

Tuttavia, avevamo una formula esplicita:

$$A(n^2, n) = n^2 - \sum_{i=1}^{s} \left[\frac{n^2}{p_i}\right] + \sum_{1 \le i < j \le s} \left[\frac{n^2}{p_i p_j}\right] + \dots + (-1)^s \cdot \frac{n^2}{p_1 \cdots p_s}$$

che chiaramente può valere 1 solo se $n = 1$.

(e allora l'insieme dei primi è vuoto e l'unico intero positivo è il numero 1!)

- Dimostrazione di Chaitin.

Si basa sull'assertione che l'informazione non sia comprimibile

Consideriamo un array di n bit, composto da 2^n elementi.

Ci si chiede quanti di questi siano compribili di k bit.

Possiamo dire che sono al più 2^{n-k}, in quanto la funzione di compressione deve chiaramente essere iniettiva.

In proporzione ce n'è $\frac{2^{n-k}}{2^n} = \frac{1}{2^k}$.

Come mai allora utilizzando un qualsiasi software di zip la dimensione dei file viene spesso ridotta notevolmente?

Il motivo è che le strutture dati dei nostri computer sono tutt'altro che casuali.

Utilizziamo argomenti analoghi per dimostrare l'infinità dei primi.

Supponiamo $\{p_1, p_2, \dots, p_s\} = P$; ogni n si scrive come $p_1^{e_1} \cdot \dots \cdot p_s^{e_s}$.

Possiamo associare a n il vettore $(e_1, e_2, \dots, e_s)$, con $e_i \le \log n$;

n può essere pertanto codificato come un array di s esponenti dell'ordine di $\log n$, ovvero s array di $\log(\log n)$ bit. Ne seguirebbe che:

$\log n$ bit $\rightarrow$ $s \log\log n$ bit

n bit $\rightarrow$ $s \log n$ bit

e dunque troppa informazione sarebbe comprimibile.

05. 11. 2010

CRITERI DI PRIMALITÀ

- Wilson: n è primo $\iff (n-1)! \equiv -1 \pmod n$

  Dim. $\Leftarrow$ Hp. $2, 3, \dots, n-1 = -1 + kn$
  $\Downarrow$
  $2, 3, \dots, n-1$ non dividono n
  $\Downarrow$
  n è primo

  $\Rightarrow$ Hp: n è primo.
  Allora $\mathbb{Z}_n$ è un campo, e $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$
  Si ha che $(n-1)! = 1 \cdot 2 \cdot \dots \cdot (n-1)$
  Poiché ogni elemento ha inverso, possiamo scrivere:
  $(n-1)! = 1 \cdot (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) \cdot (c \cdot c^{-1}) \cdot (-1) = -1$ in $\mathbb{Z}_n$
  poiché $a = a^{-1}$ soltanto se $a = \pm 1$ (essendo in un dominio)

- Solobsy - Strassen: n è primo $\iff \forall a \in \mathbb{Z}_n^* \ \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod n$
  - Un intero composto si dice pseudoprimo sulla base $a \in \mathbb{Z}_n^*$ se $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod n$. Il risultato ci dice che non ci sono numeri compositi su tutte le basi.

- Criterio AKS (Agrawal, Kajal, Saxena):
  ① Se n è primo allora $\forall a \in \mathbb{Z}_n$ si ha $(x+a)^n = x^n + a$ in $\mathbb{Z}_n[x]$
  Spiegazione: $(x+a)^n = \sum_{h=0}^{n} \binom{n}{h} x^{n-h} a^h = x^n + a^n$
  Se n è primo $n \mid \binom{n}{h}$ $\forall h$ $1 \le h \le n-1$
  infine per il piccolo teorema di Fermat $a^n = a \mod n$
  ② Se n è composto allora $\forall a \in \mathbb{Z}_n^*$ si ha
  $(x+a)^n \neq x^n + a^n$ in $\mathbb{Z}_n[x]$
  Dim Per ipotesi, $\exists\, p \mid n$, $p \neq n$, $p^e \| n$ (ovvero $p^e \mid n$ e $p^{e+1} \nmid n$)
  $\binom{n}{p} = \frac{n(n-1) \cdot \dots \cdot (n-(p-1))}{p!}$.
  Poiché $p \mid n$, se $p \mid n-k$ allora $p \mid k$, ma
  $p \nmid 1, 2, \dots, p-1$, per cui $p \nmid (n-i)$ $\quad 1 \le i \le p-1$
  $p^e \|$ numeratore $\qquad p \|$ denominatore $= p!$.
  $p^{e-1} \| \binom{n}{p} \Rightarrow p^e \nmid \binom{n}{p} \Rightarrow n \nmid \binom{n}{p}$
  $(x+a)^n = \sum_{h=0}^{n} \binom{n}{h} x^{n-h} a^h = x^n + \dots + \binom{n}{p} x^{n-p} a^p + \dots + a^n$
  e $\binom{n}{p} x^{n-p} a^p \neq 0$

  Dunque n è primo $\iff \exists\, a \in \mathbb{Z}_n^* \ (x+a)^n = x^n + a^n$ in $\mathbb{Z}_n[x]$

- **AKS** Cambiamo l'ambiente, consideriamo $\frac{\mathbb{Z}_n[X]}{(X^r-1)}$.

Prendiamo $n, r, a \in \mathbb{Z}_n^*$, e calcoliamo $(x+a)^n$ in $A_{n,r}$.

Se viene $x^n + a^n$, diciamo che n è pp Aks sulla base (a,r)

Qualche appunto di notazione:

$\left(\frac{a}{p}\right)$ simbolo di Legendre

vale 1 se $a \in Q_p = \{b^2 : b \in \mathbb{Z}_p^*\}$

" 0 se $p \mid a$

" -1 se $a \notin Q_p$

$\left(\frac{a}{n}\right)$ simbolo di Jacobi

vale $\left(\frac{a}{n}\right) \triangleq \prod_{i=1}^{s} \left(\frac{a}{p_i}\right)^{e_i}$, dove $n = p_1^{e_1} \cdot \ldots \cdot p_s^{e_s}$

legge di reciprocità quadratica:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \qquad p \neq q$$

leggi simili:

$\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \mod 8$

$= -1 \iff p \equiv \pm 3 \mod 8$

$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \mod 4$

$\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \mod 12$

$= -1 \iff p \equiv \pm 5 \mod 12$

- **Lucas** n è primo $\iff$ posto $n-1 = \prod_{i=1}^{t} q_i^{\mu_i} \implies \exists a \,/\, \begin{cases} a^{n-1} \equiv 1 & \mod n \\ a^{\frac{n-1}{q}} \not\equiv 1 & \mod n \end{cases}$

Sia $n = 2^k + 1$. Allora n è primo $\iff \exists a \in \mathbb{Z}_n^* \,/\, a^{\frac{n-1}{2}} \equiv -1 \ (n)$

$\Rightarrow$ Hp: n primo $\quad \mathbb{Z}_n^* = \langle a \rangle$

$$(a^{\frac{n-1}{2}})^2 = a^{n-1} = 1 \mod n$$

$$y = a^{\frac{n-1}{2}} \qquad y^2 = 1 \mod n \implies y = \pm 1 \implies y = 1$$

$\Leftarrow$ Si basa sul teorema di Lucas.

$\exists$ nel nostro caso un solo $q = 2$.

n è primo se $\exists a$ $\begin{cases} a^{n-1} \equiv 1 \pmod n \\ a^{\frac{n-1}{2}} \not\equiv 1 \pmod n \end{cases}$

$$a^{\frac{n-1}{2}} = -1 \implies a^{n-1} = 1 \pmod n$$

- **Pepin** F_n è primo $\iff \exists a \quad a^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$

$$\iff \quad 3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

con $F_n = 2^{2^n}+1$ numeri di Fermat

$\left(\frac{3}{F_n}\right) = -1 \qquad F_n \equiv 5 \ (12) \qquad n \geq 1$

$F_i \equiv 5 \ (12) \implies F_{i+1} \equiv 5 \ (12)$

(si prova dalla formula ricorsiva)

- Mersenne $M_n = 2^n - 1$

  Innanzitutto abbiamo una condizione necessaria: n deve essere primo, altrimenti si fattorizza elementarmente (se $n = km$, allora $2^k - 1 \mid 2^n - 1$).

  Proviamo i primi numeri di Mersenne.

  $M_2 = 3$ $\quad M_3 = 7$ $\quad M_5 = 31$ $\quad M_7 = 127$ $\quad M_{11} = 2047$

  I primi quattro sono numeri primi, il quinto è composto.

  Si trova un'analogia tra i numeri di Mersenne e i numeri perfetti pari:

  $2M_2 = 6$ $\quad 2^2 M_3 = 28$ $\quad 2^4 M_5 = 496$ $\quad 2^6 M_7 = 8128$

  Definita $\sigma(n) = \sum_{d \mid n} d$, n si dice perfetto se $\sigma(n) = 2n$, ovvero se il numero è pari alla somma di tutti i suoi divisori, tranne il numero stesso.

- Euclide: se $2^p - 1$ è primo (ovvero M_p è primo) allora $2^{p-1}(2^p - 1)$ è perfetto.

  Dim. Constatato che σ è moltiplicativa (ma non completamente), è sufficiente conoscerla sulle potenze dei primi. Vale:

  $$\sigma(p^e) = 1 + p + p^2 + \dots + p^e = \frac{p^{e+1} - 1}{p - 1}$$

  e, in particolare:

  $$\sigma(2^s) = 2^{s+1} - 1$$

  $$\sigma\left(2^{p-1}(2^p - 1)\right) = \sigma(2^{p-1})\,\sigma(2^p - 1) = (2^p - 1) \cdot 2^p$$
  $$= 2\left(2^{p-1}(2^p - 1)\right)$$

- Eulero: se P è un numero perfetto pari allora $P = 2^{p-1}(2^p - 1)$ con $2^p - 1$ primo:

  Dim. L'ipotesi è che $\sigma[P] = 2P$ e P pari.

  Quindi $P = 2^s t$, t dispari, $s \geq 1$, $(2^s, t) = 1$. Dunque:

  $$\sigma(P) = 2P$$

  $$\sigma(P) = \sigma(2^s t) = \sigma(2^s)\,\sigma(t) = (2^{s+1} - 1) \cdot \sigma(t)$$

  $$2P = 2^{s+1} t$$

  $$\Rightarrow (2^{s+1} - 1)\,\sigma(t) = 2^{s+1} t$$

  $$\frac{t}{\sigma(t)} = \frac{2^{s+1} - 1}{2^{s+1}}$$

  $$2^{s+1} - 1 \mid 2^{s+1} \cdot t \quad \Rightarrow \quad 2^{s+1} - 1 \mid t \quad \Rightarrow \quad \frac{t}{2^{s+1} - 1} = q \text{ intero}$$

  $$\sigma(t) = \frac{2^{s+1} t}{2^{s+1} - 1} \qquad \sigma(t) = t + q$$

  $$= t + \frac{t}{2^{s+1} - 1}$$

  Supponiamo ora che $q > 1$.

  Allora $\frac{t}{2^{s+1} - 1} = q \neq 1$; in particolare $t \neq 2^{s+1} - 1$

- Assumiamo che $q = 2^{s+1} - 1$. Allora $t = q^2$, e $G(t) \geq 1 + q + q^2$, dove $q \neq 1$ altrimenti s non sarebbe positivo. Vale la catena:

  $G(t) \geq 1 + q + q^2 > q + q^2 = q(q+1)$

  $\frac{t}{G(t)} < \frac{t}{q(q+1)}$ che può essere ricondotto ad un assurdo,

  ma più semplicemente avevamo detto $G(t) = t + q$, e qui $G(t) > t + q$, assurdo.

- Se invece $q \neq 2^{s+1} - 1$, vale:

  $G(t) \geq 1 + (2^{s+1} - 1) + q + t$

  $= 1 + (2^{s+1} - 1)$

  ...

  $G(t) \geq 2^{s+1}(q+1)$

  Allora:

  $\frac{t}{G(t)} \leq \frac{t}{2^{s+1}(q+1)} = \frac{q(2^{s+1}-1)}{2^{s+1}(q+1)} = \left(\frac{q}{q+1}\right)\left(\frac{2^{s+1}-1}{2^{s+1}}\right) < \frac{2^{s+1}-1}{2^{s+1}}$, assurdo.

  Quindi $q = 1$ necessariamente, e $G(t) = t + 1$.

  Perciò t è primo, e $t = 2^{s+1} - 1 = 2^{p-1}$ $\quad s+1 = p \Rightarrow s = p-1$

  $P = 2^s t = 2^{p-1}(2^p - 1)$

(09.11.2010)

Ci si pone ora il problema di come provare la primalità di M_p.

Lemmi: (1) $M_n \equiv 7 \mod 12$ $\forall n$ dispari, $n \geq 3$

(2) M_p primo $\Rightarrow \left(\frac{3}{M_p}\right) = -1$

(3) M_p primo $\Rightarrow \left(\frac{2}{M_p}\right) = 1$

Dim. (1) Base: $M_3 = 2^3 - 1 = 7$ ok

Passo: $M_{n+2} = 2^{n+2} - 1 = 4 \cdot 2^n - 1 \equiv_{12} 4 \cdot 8 - 1 \equiv_{12} 31 \equiv_{12} 7$

(2) Segue da (1) e da che $\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \mod 12$

(3) Poiché $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \mod 8$

è sufficiente provare che $M_p \equiv \pm 1 \mod 8$.

Ciò è verificato poiché, per $p \geq 3$, $2^p - 1 \equiv -1 \mod 8$

Lemma: (4) $L_{n+1} = L_n^2 - 2$ dove $L_1 = 4$

Dim. $L_2 = 16 - 2 = 14$

Consideriamo $x^2 - 4x + 1$ e le sue radici

$\alpha = 2 + \sqrt{3}$, $\beta = 2 - \sqrt{3}$.

Allora $L_n = \alpha^{2^{n-1}} + \beta^{2^{n-1}}$

Dim. (4) $n = 1 \Rightarrow \alpha + \beta = 4$

Passo induttivo:

$$L_{n+1} = L_n^2 - 2 = (\alpha^{2^{n-1}} + \beta^{2^{n-1}})^2 - 2 = \alpha^{2^n} + \beta^{2^n} + 2(\alpha\beta)^{2^{n-1}} - 2$$
$$= \alpha^{2^n} + \beta^{2^n} + 2 \cdot (1)^{2^{n-1}} - 2 = \alpha^{2^n} + \beta^{2^n}$$

Il che prova la nostra tesi.

Consideriamo ora $x^2 - \sqrt{2}\,x - 1$. Le sue radici sono

$$\gamma, \delta = \frac{\sqrt{2} \pm \sqrt{2+4}}{2} = \frac{\sqrt{2} \pm \sqrt{2}\cdot\sqrt{3}}{2} = \frac{1 \pm \sqrt{3}}{\sqrt{2}}$$

$$\gamma^2 = \frac{1+3+2\sqrt{3}}{2} = 2+\sqrt{3} = \alpha$$

Per il lemma (3), $\sqrt{2} \in \mathbb{Z}_{M_p} \Rightarrow \sqrt{2}^{-1} \in \mathbb{Z}_{M_p} \Rightarrow \gamma \in \mathbb{Z}_{M_p}(\sqrt{3})$.

Inoltre $\gamma^{M_p - 1} = 1$.

Abbiamo che $\gamma \in \mathbb{Z}_{M_p}(\sqrt{3})$ è una estensione propria di $\mathbb{Z}_{M_p}$, di grado 2 per il lemma 2.

Consideriamo ora l'automorfismo di Frobenius:

$$\begin{cases} \phi : K \to K & \text{char}(K) = p \\ \phi : a \mapsto a^p & f(x) \in \mathbb{Z}_p[x] \end{cases}$$

Se $f(\alpha) = 0$, e $\beta = \phi(\alpha)$, allora $f(\beta) = 0$.

ϕ permuta le radici di un polinomio $f(x)$ con coefficienti in $\mathbb{Z}_p$.

Nel nostro caso $f(x) = x^2 - \sqrt{2}\,x - 1 \in \mathbb{Z}_{M_p}[x]$; γ, δ zeri di $f(x)$

$\phi(\gamma) = \gamma^{M_p}$ $\begin{cases} \gamma \text{ no perché } \gamma \notin \mathbb{Z}_{M_p} \\ \delta \text{ ok} \end{cases}$

Dunque $\gamma^{M_p} = \delta$.

La tesi cui giungeremo ora è che M_p è primo $\iff M_p \mid L_{p-1}$.

Dim. I Supponiamo M_p primo. Siano in $K = \mathbb{Z}_{M_p}(\sqrt{3})$ α, β, γ.

Allora $L_{p-1} \cdot \alpha^{2^{p-2}} = (\alpha^{2^{p-2}} + \beta^{2^{p-2}}) \cdot \alpha^{2^{p-2}} = \alpha^{2^{p-1}} + (\alpha\beta)^{2^{p-2}}$

$= \alpha^{2^{p-1}} + 1 = (\gamma^2)^2 + 1 = \gamma^2 + 1 = -1 + 1 = 0$, che è possibile solo se la caratteristica del campo divide L_{p-1}. Dunque $M_p \mid L_{p-1}$

II Supponiamo ora $M_p \mid L_{p-1}$, e sia per assurdo M_p composto.

Allora $\exists\, q$ primo $/\ q \le \sqrt{M_p}$, $q \mid M_p$.

Consideriamo il campo $F = \mathbb{Z}_q(\sqrt{3})$. Per ipotesi $q \mid M_p \mid L_{p-1}$ e dunque $q \mid L_{p-1}$. Ne consegue che $L_{p-1}\,\alpha^{2^{p-2}} = \alpha^{2^{p-1}} + 1 = 0$ in $\mathbb{F} \Rightarrow \alpha^{2^{p-1}} = -1$ in F^*, e $\alpha^{2^p} = 1$ in F^*.

Pertanto il periodo in F^* di α divide 2^p, ed è della forma 2^k. Ma per il risultato su 2^{p-1}, necessariamente $k = p$. Segue che $2^p \mid |F^*|$, che porta a due casi:

(i) $|F^*| = q - 1$ $\quad (\mathbb{F} = \mathbb{Z}_q,\ (\frac{3}{q}) = 1)$

(ii) $|F^*| = q^2 - 1$ $\quad (\mathbb{F} = GF(q^2),\ (\frac{3}{q}) = -1)$

Si avrebbe $2^p \le q^2 - 1 < q^2 \le M_p = 2^p - 1$, assurdo.

- Supponiamo ora di conoscere una fattorizzazione parziale di $n-1 = RF$, con $F = \prod_{i=1}^{s} q_i^{v_i}$ parte fattorizzata.

  Assumiamo anche che $\forall i$, $1 \le i \le s$, $\exists\, a_i$ tale per cui:

  $$\begin{cases} a_i^{n-1} \equiv 1 \pmod n & \text{(i)} \\ (a_i^{\frac{n-1}{q_i}} - 1, n) = 1 & \text{(ii)} \end{cases}$$

  Allora per ogni primo p che divide n si ha:

  $p \equiv 1 \mod F$ ovvero $F \mid p-1$

  Per dimostrarlo, si prenda un primo $p \mid n$, e si consideri un $1 \le i \le s$

  Per (i), $a_i^{n-1} \equiv 1 \pmod p$; si pone $e_i = \text{per}_{\mathbb{Z}_p^*} a_i$, da cui ne segue che $e_i \mid n-1$.

  Se $e_i \mid \frac{n-1}{q_i}$ allora avremmo $a_i^{\frac{n-1}{q_i}} \equiv 1 \pmod p$ e quindi avremmo $p \mid a_i^{\frac{n-1}{q_i}} - 1$, ma allora $p \mid (a_i^{\frac{n-1}{q_i}} - 1, n)$, falso per (ii).

  Da questo segue che:

  $$e_i \mid n-1 \;;\; e_i \mid \frac{n-1}{q_i} \Rightarrow q_i^{v_i} \mid e_i \mid p-1 \Rightarrow q_i^{v_i} \mid p-1 \Rightarrow \prod q_i^{v_i} \mid p-1 \Rightarrow F \mid p-1.$$

- Nelle ipotesi precedenti se $F \ge \sqrt{n}$ allora n è primo

  Dim. Nelle ipotesi se $p \mid n$, $F \mid p-1$, allora $F < p \Rightarrow \sqrt{n} \le F < p$ $\Rightarrow p > \sqrt{n}$, dunque non ci sono primi minori della sua radice che lo dividano, e pertanto n è primo.

- Proth Sia $n = m \cdot 2^k + 1$ e $2^k > m$

  n è primo $\Leftrightarrow \exists\, a \;/\; a^{\frac{n-1}{2}} \equiv -1 \mod n$

  Dim. $\Rightarrow$ si può dare per assunto sulla base di alcuni risultati precedenti

  $\Leftarrow$ Scrivendo $n-1 = m \cdot 2^k$, possiamo considerare la fattorizzazione parziale RF con $F = 2^k$. Ora, $\exists!\, q$ $(q=2)$. Valgono le ipotesi del sistema precedente (di Pocklington), inoltre $F^2 > 2^k 2^k > m 2^k + 1$ da cui $F \ge \sqrt{n}$, per cui è valevole pure il secondo teorema di Pocklington

SUCCESSIONI RICORRENTI LINEARI

Definiamo il polinomio caratteristico di una successione $(a_n)_{n=0}^{\infty}$ come:

$$f(x) = x^m - \sum_{i=1}^{m} h_i x^{m-i}$$
$$= x^m - h_1 x^{m-1} - h_2 x^{m-2} - \dots - h_m$$

se, $\forall n \geq m$: $a_n = h_1 a_{n-1} + h_2 a_{n-2} + \dots + h_m a_{n-m}$

Supponiamo che gli zeri di $\alpha_1, \dots, \alpha_m$ di $f(x)$ siano distinti e non nulli, e sia $\mathbb{F}$ il campo di spezzamento di $f(x)$.

Una successione lineare ricorrente di grado m è determinata dal polinomio caratteristico e dagli m valori iniziali $a_0, \dots, a_{m-1}$.

Se si fissa $f(x)$ si ha un insieme $R_{\mathbb{F},f(x)} = \{(a_n) : (a_n) \text{ ricorre con } f(x)\}$.

- $(a_n) + (b_n) \in R_{\mathbb{F},f(x)}$
- $\lambda (a_n) = (\lambda a_n) \in R_{\mathbb{F},f(x)}$

$R_{\mathbb{F},f(x)}$ è uno spazio vettoriale su $\mathbb{F}$ di dimensione m.

Una base è formata dalla sequenza che hanno come condizioni iniziali $(1,0,\dots,0), (0,1,\dots,0), \dots, (0,0,\dots,1) = (v_1, v_2, \dots, v_m)$

$$(a_n) = \sum_{i=0}^{m-1} a_i v_{i+1}$$

Consideriamo α_i zeri di $f(x)$, $f(\alpha_i) = 0$.

Allora $\alpha_i^m = \sum_{j=1}^{m} h_j \alpha_i^{m-j}$, e $\alpha_i^n = \sum_{j=1}^{m} h_j \alpha_i^{n-j}$ se $n \geq m$.

Risultato cruciale è che $(\alpha_i^n)_{n=0}^{\infty} \in R_{\mathbb{F},f(x)}$, $\forall \alpha_i$ zero di $f(x)$

$1, \alpha, \alpha^2, \dots, \alpha^n$ ricorre con $f(x)$, $f(\alpha) = 0$.

(12.11.2010)

Teorema di Binet: siano $S_i = (\alpha_i^n)_{n=0}^{\infty}$. Allora $S_1, \dots, S_m$ formano una base di $R_{\mathbb{F},f(x)}$

Dim. Prendiamo $A = (a_n) \in R_{\mathbb{F},f(x)}$, e lo vogliamo scrivere in modo unico come $A = \sum_{i=1}^{m} \lambda_i S_i$. Questo significa che $\forall n$ $a_n = \sum_{i=1}^{m} \lambda_i \alpha_i^n$. Le equazioni sono pertanto:

$$a_0 = \lambda_1 \alpha_1^0 + \lambda_2 \alpha_2^0 + \dots + \lambda_m \alpha_m^0$$
$$a_1 = \lambda_1 \alpha_1^1 + \lambda_2 \alpha_2^1 + \dots + \lambda_m \alpha_m^1$$
$$a_j = \lambda_1 \alpha_1^j + \lambda_2 \alpha_2^j + \dots + \lambda_m \alpha_m^j$$

Il determinante dei coefficienti è:

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_m^2 \\ \dots & \dots & \dots & \dots \\ \alpha_1^{m-1} & \alpha_2^{m-1} & \dots & \alpha_m^{m-1} \end{vmatrix} = \prod_{i<j} (\alpha_i - \alpha_j) \neq 0$$

poiché $\alpha_i \neq \alpha_j$ per ipotesi.

Si ha pertanto un'unica soluzione

Definiamo ora la matrice compagna di $f(x)$ nel seguente modo:

$$\text{comp}(f(x)) = \begin{bmatrix} 0 & \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \\ h_m & h_{m-1} \dots h_1 \end{bmatrix} = M$$

Indicato con $\text{polchar}(M)$ il suo polinomio caratteristico, vale:

$\text{polchar}(\text{comp}(f(x))) = f(x)$

Un risultato di Cayley afferma inoltre che $f(\text{comp}(f(x))) = 0$, ovvero che $M^m - \sum_{i=1}^{m} h_i M^{m-i} = 0$. Ne segue che

$M^m = \sum_{i=1}^{m} h_i M^{m-i}$

e, $\forall n \geq m$, $M^n = \sum_{i=1}^{m} h_i M^{n-i} = h_1 M^{n-1} + h_2 M^{n-2} + \dots + h_m M^{n-m}$

Abbiamo pertanto una successione ricorrente di matrici:

$\mathcal{M} = (M^n)_{n=0}^{\infty} \in \mathcal{R}_{\text{Mat}(n,\mathbb{F}),f(x)}$

Se $M = (M_{s,t})$, $1 \leq s,t \leq m$, denotato con $M^n_{s,t} \overset{\text{def.}}{=} (M^n)_{s,t}$, varrà $M^n_{s,t} = \sum h_i M^{n-i}_{s,t}$

Poniamo ora $\mathcal{R}_R = \bigcup \mathcal{R}_{R,f(x)}$, con $f(x)$ monico, $f(x) \in R[x]$

Siano $A, B \in \mathcal{R}_R$, e nello specifico $A \in \mathcal{R}_{R,f(x)}$, $B \in \mathcal{R}_{R,g(x)}$.

Allora $A+B \in \mathcal{R}_{R,f(x)g(x)}$, e pertanto $\mathcal{R}_R$ è un R-modulo, o un R-spazio vettoriale se R è un campo. $\mathcal{R}_R$ è anche un'algebra, in quanto chiusa rispetto al prodotto.

Sia $C = AB$ prodotto di Hadamard, ovvero $(c_n) = (a_n)(b_n)$.

Il polinomio di ricorrenza di C è $\text{polchar}(\text{comp}(A) \otimes \text{comp}(B))$

I calcoli possono essere effettuati per blocchi.

Affrontiamo ora il caso particolare in cui il grado sia 2.

Allora lavoriamo con $W_n(a,b,h,k)$, a,b condizioni iniziali, ricorrenza con $f(x) = x^2 - hx + k$, in modo tale che $h = \alpha+\beta$, $k = \alpha\beta$.

Vediamo che $\mathcal{R}_{R,f(x)} = \{(W_n(a,b,h,k) : a,b \in \mathbb{R})$. Inoltre definiamo:

$W_n(0,1,h,k) = U_n(h,k)$ serie di Fibonacci generalizzata

$W_n(1,0,h,k) = T_n(h,k)$

in modo tale da poter scrivere, per linearità:

$W_n(a,b,h,k) = a \cdot T_n(h,k) + b \cdot U_n(h,k)$

Definiamo anche:

$W_n(2,h,h,k) = V_n(h,k)$

Studiamo gli andamenti di U e T. Osserviamo che:

$(U_n(h,k)) = 0, 1, h, h^2-k, \dots$

$(T_n(h,k)) = 1, 0, -k, -hk, \dots$

Si può notare che $T_n(h,k) = -k \cdot U_{n-1}(h,k)$

Esistono delle formule di Binet che permettono di esprimere in maniera chiusa il termine generico di una successione.

Siano α, β gli zeri di $f(x) = x^2 - hx + k$. Allora:

$U_n(h,k) = \lambda_1 \alpha^n + \lambda_2 \beta^n$.

Dalle condizioni richieste: $\begin{cases} 0 = \lambda_1 + \lambda_2 \\ 1 = \lambda_1 \alpha + \lambda_2 \beta \end{cases}$ che implica

$\lambda_1 = \frac{1}{\alpha-\beta}$, $\lambda_2 = \frac{-1}{\alpha-\beta}$. Si arriva pertanto alla semplice formula:

$U_n(h,k) = \lambda_1 \alpha^n + \lambda_2 \beta^n = \frac{\alpha^n - \beta^n}{\alpha-\beta}$

Un esempio è dato dalla serie di Fibonacci $U_n(1,-1)$, il cui polinomio caratteristico è $x^2 - x - 1$. In questo caso $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$, e $F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right]$

Dalla formula di prima si ricava che $T_n(h,k) = -k \cdot \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha-\beta}$.

Inoltre, per $V_n(h,k)$, si ha: $\begin{cases} V_0 = 2 = \lambda_1 + \lambda_2 \\ V_1 = h = \lambda_1 \alpha + \lambda_2 \beta \end{cases}$

Poiché $\alpha + \beta = h$, segue che

$\lambda_1 = \lambda_2 = 1$ e $V_n = \alpha^n + \beta^n$. Questo spiega l'importanza della successione V_n: il generico termine è semplicemente la somma delle potenze n-esime delle radici.

In termini computazionali, vediamo diversi metodi. Il primo è naturale:

$\text{comp}(x^2 - hx + k) = \begin{pmatrix} 0 & 1 \\ -k & h \end{pmatrix} = M(h,k)$

$\text{Tr}(M) = h$; $\text{Det}(M) = k$; $\text{polchar}(M) = x^2 - hx + k$

$M^2 - hM + kI = 0$

Abbiamo che $M^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $M^1 = \begin{bmatrix} 0 & 1 \\ -k & h \end{bmatrix}$.

Si nota che: $M^n_{1,1} = W_n(1,0,h,k) = T_n = -k \cdot U_{n-1}$

$M^n_{1,2} = W_n(0,1,h,k) = U_n$

$M^n_{2,1} = W_n(0,-k,h,k) = -k \cdot U_n = T_{n+1}$

$M^n_{2,2} = W_n(1,h,h,k) = U_{n+1}$

Possiamo quindi scrivere $M^n = \begin{bmatrix} -k \cdot U_{n-1} & U_n \\ -k \cdot U_n & U_{n+1} \end{bmatrix}$

Si ha $\det(M) = k \Rightarrow \det(M^n) = k^n = -k \cdot U_{n-1} \cdot U_{n+1} + k \cdot U_n^2$

$\Rightarrow U_n^2 - U_{n-1} \cdot U_{n+1} = k^{n-1}$ (regola di Cassini)

Si calcola velocemente $W_n(a,b,h,k)$ mod b per n grande.

Considerando inoltre che $M^m \cdot M^n = M^{m+n}$:

$$\begin{bmatrix} -k\cdot U_{m+n-1} & U_{m+n} \\ -k\cdot U_{m+n} & U_{m+n+1} \end{bmatrix} = \begin{bmatrix} -k\cdot U_{m-1} & U_m \\ \dots & \dots \end{bmatrix} \cdot \begin{bmatrix} \cdot & U_n \\ \cdot & U_{n+1} \end{bmatrix}$$

possiamo ricavare che:

- $U_{m+n} = -k\cdot U_{m-1}\cdot U_n + U_m \cdot U_{n+1}$
- $U_{2n} = -k\cdot U_{n-1}\cdot U_n + U_n \cdot U_{n+1}$ (ponendo $m=n$)

Si noti che, in generale, ponendo $m=(t-1)n$:

- $U_{tn} = -k\cdot U_{(t-1)n-1}\cdot U_n + U_{(t-1)n}\cdot U_{n+1}$
  $= U_n\cdot(-k)\cdot U_{(t-1)n-1} + U_{n+1}\cdot U_{(t-1)n}$
  $= \quad " \quad + U_{n+1}\cdot\left[-k\cdot U_{(t-2)n-1}\cdot U_n + U_{(t-2)n}\cdot U_{n+1}\right]$
  $= \dots$

Reiterando sufficientemente si può raccogliere U_n e perciò $U_n \mid U_{tn}$. Dunque $m \mid n \Rightarrow U_m \mid U_n$.

Vediamo ora il caso del prodotto: $(M^m)^n = M^{mn}$. Sia $n = km$:

$$(M^m)^k = M^n = \begin{bmatrix} \cdot & U_n \\ \cdot & \cdot \end{bmatrix}$$

$$\begin{bmatrix} T_n & U_m \\ T_{n+1} & U_{m+1} \end{bmatrix} = \begin{bmatrix} \cdot & U_n \\ \cdot & \cdot \end{bmatrix}$$

Sia $M^m = B$ e calcoliamo le sue potenze.

Risulta che $\text{polchar}(B) = x^2 - (T_m + U_{n+1})x + k^m$;

$\det(B) = \det(M^m) = k^n$

Inoltre $W_n(0, U_m, T_m + U_{n+1}, k^n) = U_n$

$U_m(h,k)\cdot U_n(T_m + U_{m+1}, k^m) = U_m(h,k)$

Il caso di V_n invece è più immediato, in quanto $V_n = \text{Tr}(M^n)$ $[V_n = W_n(2, h, h, k)]$.

Il secondo metodo computazionale si basa invece sui polinomi.

Consideriamo $\frac{R[x]}{(x^2-hx+k)}$, e sia $x^2 = hx - k$ una relazione fondamentale.

Prendiamo $\{a+bx : a, b \in R\}$ e calcoliamo:

$(a+bx)(c+dx) = ac + adx + bcx + bdx^2 = ac + adx + bcx + bd(hx-k)$

$= (ac - bdk) + (ad + bc + bdh)x$

$(a,b)\cdot(c,d)$

$(0,1)^{\circ n}$

$x^0 = 1 + 0x$

$x^1 = 0 + 1x$

$x^2 = -k + hx$

$x^n = T_n + U_n x$

AC

16-11-10

Vista che $m \mid n \Rightarrow U_m(h,k) \mid U_n(h,k)$, $\forall h,k \in R_{R,\S(x)}$

Successi di qto genere si chiamano succ di divisibilità

è $R[x]/(x^2-hx+k) = R_{R,\S(x)}$.

x è zero di x^2-hx+k e quindi la sua radice coniugata è $h-x$

$(x+(h-x)=h$ ✓ , e inoltre $x(h-x)=hx-x^2=k)$
(il prodotto da k)

Formule di Binet, ci dicono che,

$$U_n(h,k) = \frac{x^n-(h-x)^n}{x-(h-x)} \quad , \quad V_n(h,k) = x^n+(h-x)^n .$$

E noi vogliamo vedere che prendendo num interi , p primo:

(1) $U_p - \left(\frac{\Delta}{p}\right) \equiv 0 \pmod p$

(2) $U_{p-\left(\frac{\Delta}{p}\right)} \equiv 0 \pmod p$

(3) $V_p - h \equiv 0 \pmod p$

Allora $\Delta = h^2-4k$ e ho sempre 2 casi

(I) $\left(\frac{\Delta}{p}\right) = 1$

(II) $\left(\frac{\Delta}{p}\right) = -1$

Noi prendiamo $R = \mathbb{Z}_p$ e quindi il nostro ideale è $\mathbb{Z}_p[x]/(x^2 - hx + k)$ che

nel caso I) $\cong$ (isomorfo) $\mathbb{Z}_p \times \mathbb{Z}_p$

nel caso II) $\cong GF(p^2)$

① I) caso

$$U_p = \frac{x^p - (h-x)^p}{x-(h-x)} \overset{\text{per } \cong \mathbb{Z}_p \times \mathbb{Z}_p \text{ il piccolo Th Fermat}}{=} \frac{x-(h-x)}{x-(h-x)} \overset{\text{sempre mod } p.}{=} 1 = \left(\frac{\Delta}{p}\right)$$

$U_p \equiv \left(\frac{\Delta}{p}\right) \pmod p$ ✓

II) caso | in qte caso si scambiano le radici. Omomorf di Frobenius

$$U_p = \frac{x^p - (h-x)^p}{x-(h-x)} = \frac{(h-x)-x}{x-(h-x)} = -1 = \left(\frac{\Delta}{p}\right) \checkmark$$

② I) caso |

$\left(\frac{\Delta}{p}\right) = 1$ e calcolo $U_{p-1} = \frac{x^{p-1} - (h-x)^{p-1}}{x-(h-x)} \overset{\text{uguale a ① caso I}}{=} \frac{1-1}{x-(h-x)} = 0$ ✓.

II) caso |

$$U_{p+1} = \frac{x^{p+1} - (h-x)^{p+1}}{x-(h-x)} \overset{\text{anche una vg}}{=} \frac{(h-x)x - x(h-x)}{x-(h-x)} = 0 \checkmark.$$

③ $V_p = x^p + (h-x)^p$ che nun un caso e nell'altro rimane sempre

$= x + (h-x) = h \pmod p$ ✓

AC

16-11-10

Prima di utilizzare gte, vediamo una cosa generale:

Abbiamo visto che le pot di una matrice si creano delle cose ricorrenti

...

Prendiamo $\alpha \in \mathbb{C}$ $\alpha = a+bi$ e $\bar{\alpha} = a-bi$

e così α è zero del suo pol minimo che è $x^2 - 2ax + (a^2+b^2)$

e se continui a fare le potenze di α:

$\alpha^n = 2a\alpha^{n-1} - (a^2+b^2)\alpha^{n-2}$ che spezzandolo in parte reale e im

sarà $\alpha^n = a_n + b_n i$ dove

$a_n = 2a a_{n-1} - (a^2+b^2) a_{n-2}$

$b_n =$ IDEM

Quindi si possono calcolare ricorsivamente:

Esempio:

$\alpha = 2+i$. α^n ricorre con $x^2 - 4x + 5$ e quindi

$a_n = 4a_{n-1} - 5a_{n-2}$

$Re(\alpha^0) = 1$, $Re(\alpha^1) = 2$, 3, ...

Che con la nostra notazione $a_n = W_n(1,2,4,5)$

Se prendiamo

$\alpha = \cos\theta + i\,\mathrm{sen}\theta$, il pol caratt che c'è il pol minimo è $x^2 - 2\cos\theta x + 1$

Se ora $\alpha^n = a^n + b^n i$ allora

	Re	Im
α^0	1	0
α^1	$\cos\theta$	$\mathrm{sen}\theta$
α^2	$2\cos^2\theta - 1$	$2\,\mathrm{sen}\theta\cos\theta$

→ Mah adesso, cosa sono gli a_n? So che $\alpha^n = \cos n\theta + i\,\mathrm{sen}\,n\theta$

e quindi $\cos n\theta = 2\cos\theta\cos(n-1)\theta - \cos(n-2)\theta$

Se poniamo $y=\cos\theta$, la colonna infinita delle parti reali diventano polinomi in y

$$T_n(2\cos\theta,1) = T_n(2y,1) = \underbrace{C_n(y)}_{\text{pol in } y}$$

$$\boxed{C_n(y) = 2yC_{n-1}(y) - C_{n-2}(y)} \quad \text{con } C_0(y)=1 \text{ e } C_1(y)=y$$

sono i famosissimi pol di Chebycher di prima specie.

Altra cosa:

Voglio risolvere $x^2 \equiv a \pmod p$ (p primo). Fino a 1904 nessuno ce l'aveva. Data da Cipolla. Noi diamo una versione successiva da Lucas

Si basa sulle seq ricorrenti.

Per risolvere qta è necessario che $\left(\frac{a}{p}\right)=1$. Quindi sarà ipotesi.

Ora cerco un h tc ~~$h^2-4a=\Delta$~~ se $h^2-4a=\Delta$ valga che $\left(\frac{\Delta}{p}\right)=-1$

(si vede che si trova in fretta).

Considereremo x^2-hx+a che ha come $\Delta = h^2-4k$ ($k=a$)

TEOREMA $\pm\frac{1}{2}V_{\frac{p+1}{2}}(h,a)$ sono le soluzioni di $x^2 \equiv a \pmod p$

D// $$\left(\pm\frac{1}{2}V_{\frac{p+1}{2}}(h,a)\right)^2 = \left(\pm\frac{1}{2}\left(x^{\frac{p+1}{2}}+(h-x)^{\frac{p+1}{2}}\right)\right)^2 = \frac{1}{4}\left(x^{p+1}+(h-x)^{p+1}+2(x(h-x))^{\frac{p+1}{2}}\right)$$

$$= \frac{1}{4}\left(x(h-x)+(h-x)x+\left(x(h-x)\right)^{\frac{p-1}{2}}(x(h-x))\right) = \frac{1}{4}\left(a+a+2a^{\frac{p-1}{2}}\cdot a\right) = (*)$$

$x(h-x)$ è il prod delle radici $=a$

$(*)$ = calcolata all'inizio, caso $\left(\frac{\Delta}{p}\right)=-1$

AC

16-11-10

$\left(\frac{q}{p}\right) = 1 \to 1$

- come (crit di Eulero) $a^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \bmod p$

$\Rightarrow (\#) = \frac{1}{4}(4q) = q$ ✓

- Una roba sulle matrici (pedir)

Altra cosa

Rango di apparizione, $p_g(n)$ → il solito polinomio $f(x) = x^2 - hx + k$

di n nella sequenza $U_m(h,k)$ è per definizione il minimo m tale che $n \mid U_m(h,k)$,

nelle ipotesi $(n, 2k\Delta) = 1$

Quindi per definizione $n \mid U_{p_g(n)}(h,k)$.

- Se n è primo $\overset{n=p}{\Rightarrow} p \mid U_{p-\left(\frac{\Delta}{p}\right)}$ (visto prima) e allora dalla definizione $p_g(p) \leq p - \left(\frac{\Delta}{p}\right)$ e quindi $p_g(p)$ esiste.

Allora se ho che $p \mid U_{p_g(p) - \left(\frac{\Delta}{p}\right)}$

$q \mid U_{p_g(q) - \left(\frac{\Delta}{q}\right)}$

AC

12-11-10

CAA!! è l'ultimo foglio di 12-11-10!!

$\text{polchar}(B) = x^2 - (T_m + U_{m+1})x + k^{m+n}$

$\det(B) = \det(M^m) = k^n$

$W_n(0, U_m, T_m + U_{m+1}, k^n) = U_n$

pero'

$W_n(0, U_m, T_m + U_{n+1}, k^n) = U_m(h,k)\, U_n(T_m + U_{m+1}, k^m)$

$\Rightarrow U_n(h,k) = U_m(h,k)\, U_n(T_m + U_{m+1}, k^m)$

③ Per concludere qlc cosa delle matrici:

$$\boxed{V_n = Tr(M^n)}$$, perché $V_n = W_n(2, h, h, k)$

$M^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $M = \begin{pmatrix} 0 & 1 \\ -k & h \end{pmatrix}$ —

METODO 2 (polinomi)

Consideriamo $\mathbb{R}[x]/(x^2 - hx + k) = \{ a + bx : a, b \in \mathbb{R} \}$

Possiamo implementare un prodotto, $(a+bx)(c+dx) = ac + adx + bcx + bdx^2 \underset{\uparrow}{=} ac + adx + bcx + bd(hx - k) = (ac - bdk) + (ad + bc + bdh)x$.

$x^2 = hx + k$

Quindi posso scrivere $(a,b) \cdot (c,d) = (\quad, \quad)$

Guarda che (scrivo come $a + bx$):

$x^0 = 1 + 0x$

$x^1 = 0 + 1x$

$x^2 = -k + hx$ ... $x^n = T_n + U_n x$ $\quad x^2 = hx + k \Rightarrow x^n = hx^{n-1} - kx^{n-1}$

AC

16-11-10

$\grave{e}$ $m = mcm\left(p-\left(\frac{\Delta}{p}\right), 7-\left(\frac{\Delta}{7}\right)\right)$

e $V_{p-\frac{\Delta}{p}} \mid V_m \Rightarrow p,7 \mid V_m$

Per riuscire a dim per tutti gli n devo fare un lavoro precedente

$\mathcal{O}_{n,g} = \mathbb{Z}_n[x]/(x^2-hx+k)$

$=$

$R_{\mathbb{Z}_n,g}$ anellissimo

ordine $\downarrow$

$\mathcal{O}_{n,g} = \{a+bx : a,b \in \mathbb{Z}_n\}$, per ciò, $|\mathcal{O}_{n,g}| = n^2$

invece $|\mathcal{O}_{n,g}^*| = ??$

Prima $\forall$ n = p primo:

$\mathcal{O}_{p,g}$ caso I) $\forall \left(\frac{\Delta}{p}\right) = 1 \simeq \mathbb{Z}_p \times \mathbb{Z}_p$

caso II) $\forall \left(\frac{\Delta}{p}\right) = -1 \simeq GF(p^2)$

$\mathcal{O}_{p,g}^*$ $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$ $GF(p^2)^*$ e quindi $|\mathcal{O}_{p,g}^*| < (p-1)^2$ (p^2-1) NA

per mettere tutti e due casi insieme: $|\mathcal{O}_{p,g}^*| = (p-1)\left(p-\left(\frac{\Delta}{p}\right)\right)$

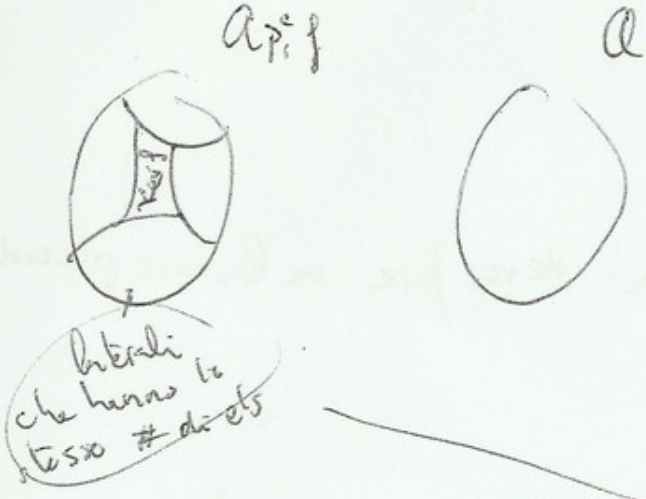
Ora se $n = p^e$:

sia l'anello $\mathcal{O}_{p^e,g}$ e sia $\pi : \mathcal{O}_{p^e,g} \twoheadrightarrow \mathcal{O}_{p,g}$

$a+bx \longmapsto a+bx$ con a,b resti modulo p

con $a,b \in \mathbb{Z}_{p^e}$

quindi π è un epimorfismo



$\ker\pi = \{a+bx \text{ t.c. } \pi(a+bx)=0\} = \{a+bx \in \mathbb{Q}_{p^e,\beta} \text{ t.c. } p \mid a \wedge p \mid b\}$

ci sono p^{e-1} a possibili e p^{e-1} b possibili, perciò

$|\ker\pi| = p^{2(e-1)}$ e quindi anche di tutte le altre classi

A me, però, interessa il gruppo molt $\mathbb{Q}_{p,\beta}^*$

$\pi/\mathbb{Q}_{p^e,\beta}^* : \mathbb{Q}_{p^e,\beta}^* \xrightarrow{\text{epi??}} \mathbb{Q}_{p,\beta}^*$. Sr, è epimorfismo xché:

devo vedere che se uno è invertibile in $\mathbb{Q}_{p,\beta}^*$ allora è

è in $\mathbb{Q}_{p^e,\beta}^*$. Quindi mi chiedo: Quando $a+bx$ è invertibile

in $\mathbb{Q}_{p,\beta}$?

con $(x) = h-x$
2 coniugati

$\Rightarrow \text{con}(a+bx) = a+b\,\text{con}(x) = a+b(h-x)$

norma $\rightarrow N(a+bx) = (a+bx)(a+bh-bx) = a^2 - abh - \cancel{abx} + \cancel{abx} + b^2hx - b^2x^2 =$

$$a^2 + hab + b^2\underbrace{(hx-x^2)}_{=k} = \boxed{a^2+hab+b^2k}$$

Rispetto al prodotto $(a,b)\cdot(c,d) = (ac-bdk, ad+bc+hbd)$ la norma è

8 moltiplicativa - (prod di norme è norma del prod)

AC

16-11-10

$$(a+bx)^{-1} = \frac{\text{con}(a+bx)}{N(a+bx)} = \frac{a+bh-bx}{a^2+hab+kb^2}$$

norma

e $(a+bx)^{-1}$ esiste in $\mathbb{Q}_{p,\beta}$ se $\Leftrightarrow p \nmid a^2+hab+kb^2$

Il bello è che in $\mathbb{Q}_{p^e,\beta}$ si fa uguale, cioè

$(a+bx)^{-1}$ è ~~esiste~~ in $\mathbb{Q}_{p^e,\beta} \Leftrightarrow N(a+bx)$ è invertibile in $\mathbb{Z}_{p^e}$

Allora,

$$N(a+bx) \in \mathbb{Z}_p^* \Leftrightarrow (p^e, N(a+bx)) \Leftrightarrow p \nmid N(a+bx) \Leftrightarrow$$

$$a+bx \in \mathbb{Q}_p^*$$

Perciò, sì, $\Pi/\mathbb{Q}^*_{p^e,\beta}$ è epimorfismo che lo chiamo solo Π e ci permette di dire quante gente ce in $\mathbb{Q}^*_{p^e,\beta}$:

$$|\mathbb{Q}^*_{p^e,\beta}| = |\mathbb{Q}^*_{p,\beta}|\,|\ker\Pi| = (p-1)\left(p-\left(\tfrac{\Delta}{p}\right)\right) p^{2(e-1)}$$

E allora siamo in grado di dire quell'è l'ordine per un n qualsiasi (uso teor cin dei resti)

Se $n = \prod_i p_i^{e_i}$, $|\mathbb{Q}^*_{n,\beta}| \overset{\uparrow}{=} \prod |\mathbb{Q}^*_{p_i^{e_i},\beta}| = \prod p_i^{2(e_i-1)}(p_i-1)\left(p_i-\left(\tfrac{\Delta}{p_i}\right)\right)$

TCin Resti

(Qui si evidenzia la funzione ~~fi~~ $\varphi(n)$) $\varphi(n) \prod p_i^{e_i-1}\left(p_i-\left(\tfrac{\Delta}{p_i}\right)\right)$

$\varphi_n(n)$ $(\varphi_\Delta(n))$ def

Esempio: $f(x) = x^2 - x + 2$, $h=1$, $k=2$

$\Delta = -7$

$n = 45$

$P_1 = 3$, $P_2 = 5$, $n = P_1^2 \cdot P_2$, $\left(\frac{-7}{3}\right) = -1$, $\left(\frac{-7}{5}\right) = -1$

$\varphi_\Delta(n) = \varphi_\Delta(45) = \varphi(45) = \varphi(9)\,\varphi(5) = 4 \cdot 6 = 24$

$\Psi_\Delta(45) = 3(3+1) \cdot 5^0 (5+1) = 12 \cdot 6 = 72$

e quindi $|\mathcal{Q}^*_{45,f}| = 72 \cdot 24 = 1728$

Esercizio: Calcoliamo un inverso

Prendo $38+39x$ e $\mathcal{Q}_{45,f}$ dove $f = x^2 - x + 2$. Voglio vedere se è invertibile: $N(38+39x) = 5968 \mod 45 = 28$

la norma è invert? sì, $28^{-1} \mod 45 = 37$

e quindi chi è l'inverso? $\text{con}(38+39x) = 77 - 39x \mod 45 =$

$= 32 + 6x$

Guarda:

$37(32+6x) = 1184 + 222x \mod 45 = 14 + 42x$:

$$(38+39x)(14+42x) = 1 \mod 45$$

$\mathcal{Q}^*_{n,f} / \mathbb{Z}_n^* = G_{n,f}$. $|G_{n,f}| = |\mathcal{Q}^*_{n,f}| / |\mathbb{Z}_n^*| = \dfrac{\varphi(n)\,\Psi_\Delta(n)}{\varphi(n)}$

$\Rightarrow |G_{n,f}| = \Psi_\Delta(n)$.

cosa centra ste con il rango di apparizione

AC

16-11-10

gli elem di $G_{n,f}$ si indicano con $[a+bx]$ dove $a+bx \in \mathbb{Q}_{n,f}^*$

$$[a+bx] = \{ \lambda(a+bx) \text{ tc } \lambda \in \mathbb{Z}_n^* \}$$

$$[x]^m = [T_m(h,k) + U_m(h,k)x]$$

(già dimostrato)

Ma qual è il 1 dentro qto gruppo? È la classe di tutti gli scalari

Quindi, quando $[x]^m = 1$? $[x]^m = 1 \iff U_m(h,k) \equiv 0 \bmod n$

$\iff n \mid U_m(h,k)$

Quindi sappiamo dire che il rango di app esiste e ohi è:

in base a quello visto il minimo m per cui $[x]^m = [1]$ è

il minimo m per cui $n \mid U_m(h,k)$ che è il rango di apparizione

~~$\rho_f(n)$~~ $\rho_f(n)$. Ma il minimo m per cui $[x]^m = [1]$ è

il periodo di $[x]$ in $G_{n,f}$.

Quindi il rango di apparizione esiste sempre e

$$\rho_f(n) = \text{per}_{G_{n,f}}[x]$$

$\Downarrow$

$\rho_f(n) \mid \varphi_\Delta(n)$ (quindi $\rho_f(n)$ al massimo è $\varphi_\Delta(n)$)

(23.11.2010)

- $G_{n,f} = \left(\frac{\mathbb{Z}_n[x]}{(f(x))} \right)^* \Big/ \mathbb{Z}_n^*$ $\qquad f(x) = x^2 - hx + k$ $\qquad (n, \Delta k) = 1$

$|G_{n,f}| = \psi_\Delta(n)$

$= \prod_{i=1}^{s} p_i^{e_i - 1} \left(p_i - \left(\frac{\Delta}{p_i}\right) \right)$ $\qquad n = \prod_{i=1}^{s} p_i^{e_i}$

- $[x] \in G_{n,f}$ $\qquad [x]^n = [T_n + U_n x]$

per $G_{n,f}[x] = \rho_f(n) =$ rango di apparizione, ovvero:

$\rho_f(n) = \min \{ m : n \mid U_m \}$

$\rho_f(n) \mid \psi_\Delta(n)$

- $n \mid U_n \iff \rho_f(n) \mid m$

se n è primo, $\psi_\Delta(p) = p - \left(\frac{\Delta}{p}\right)$

$\Rightarrow \rho_f(p) \mid p - \left(\frac{\Delta}{p}\right)$

$\Rightarrow p \mid U_m \iff \rho_f(p) \mid m$

Esempio:

$|G_{15,f}| = \psi_\Delta(15) = \left(3 - \frac{\Delta}{3}\right)\left(5 - \frac{\Delta}{5}\right)$

$|\mathbb{Z}_{15}^*| = \varphi(15) = 2 \cdot 4 = 8$

$2 \cdot 4 = 8$
$4 \cdot 6 = 24$
$4 \cdot 4 = 16$
$2 \cdot 6 = 12$

In generale abbiamo 2^s ordini possibili se s sono i fattori primi di n.

- Teorema di Morrison

Consideriamo n dispari, $\left(\frac{n}{\Delta}\right) = -1$, $F \mid n+1$, p primo per cui $p \mid n$.

Allora se:

① $U_{n+1} \equiv 0 \pmod n$

② $\forall q \mid F \quad \left(U_{\frac{n+1}{q}}, n\right) = 1$

ne consegue $p \equiv \left(\frac{\Delta}{p}\right) \bmod F$ con $F \mid p - \left(\frac{\Delta}{p}\right)$

Dimostrazione

Prendiamo $p \mid n$. Dalla ① segue che $U_{n+1} \equiv 0 \bmod p$

$\Rightarrow \rho_f(p) \mid n+1$. La ② implica che $\rho_f(p) \nmid \frac{n+1}{q}$ perché se $\rho_f(p) \mid \frac{n+1}{q}$ avremmo $\begin{cases} p \mid U_{\frac{n+1}{q}} \\ p \mid n \end{cases} \Rightarrow p \mid \left(U_{\frac{n+1}{q}}, n\right) \Rightarrow p \mid 1$, assurdo.

Pertanto scrivo $F = \prod_q q^{a_q}$, da ① e ② $q^{a_q} \mid \rho_f(p)$

$\forall q \mid F \Rightarrow q^{a_q} \mid \rho_f(p) \Rightarrow F \mid \rho_f(p)$.

Per un risultato precedente $\rho_f(p) \mid p - \left(\frac{\Delta}{p}\right)$ e perciò $F \mid p - \left(\frac{\Delta}{p}\right)$, come volevasi dimostrare.

Corollario 1

Nelle ipotesi precedenti, se $F > \sqrt{n} + 1$, allora n è primo

Dim Per ipotesi $F \mid p - \left(\frac{\Delta}{p}\right) \Rightarrow \sqrt{n}+1 < F \leq p - \left(\frac{\Delta}{p}\right) \leq p+1$,

dunque $p > \sqrt{n}$, ovvero ogni primo che divide n è maggiore di $\sqrt{n}$, e perciò $p = n$ (n è primo)

Corollario 2

$n = m \cdot 2^k - 1$

$2^k > \sqrt{n} + 1 \qquad 2^k = F$

Se $\left(\frac{\Delta}{n}\right) = -1 \qquad (n, 2k\Delta)$

$$\begin{cases} U_{n+1} \equiv 0 \pmod n \\ \left(U_{\frac{n+1}{2}}, n\right) = 1 \end{cases}$$

Per n generale si usano, per essere veloci, criteri probabilistici.

- Es: Fermat: consideriamo una base $a \in \mathbb{Z}_n^*$, ed effettuiamo un test del tipo $a^{n-1} \equiv 1 \mod n$.

  Ci chiediamo se esistono n che passano il test per ogni base.

  La risposta è sì, e sono i numeri di Connaliael, caratterizzati da:

  $$\begin{cases} n = \prod p_i \\ \forall i \;\; p_i - 1 \mid n-1 \end{cases}$$

  Tali numeri sono detti anche pseudoprimi di Fermat.

- Eulero: sia ancora una base $a \in \mathbb{Z}_n^*$, facciamo un test:

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

  Se la risposta è sì ed n è composto, n è pseudoprimo di Eulero

  $\forall a \in \mathbb{Z}_n^* \qquad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n \iff n$ è primo

Teorema Se n è composto e $a \in \mathbb{Z}_n^*$ casuale, allora le probabilità che n passi il test di Eulero è $\leq \frac{1}{2}$.

Dim. Prendiamo $f, g : G \to G \qquad \{x \in G : f(x) = g(x)\} \leq G$ (sottogruppo)

$G = \mathbb{Z}_n^* \qquad f(x) = \left(\frac{x}{n}\right) \qquad g(x) = x^{\frac{n-1}{2}} \qquad \left(\frac{xy}{n}\right) = \left(\frac{x}{n}\right)\left(\frac{y}{n}\right)$

$x^{\frac{n-1}{2}} y^{\frac{n-1}{2}} = (xy)^{\frac{n-1}{2}}$ f, g morfismi

$H \leq \{a \in \mathbb{Z}_n^* : f(a) = g(a)\} \leq \mathbb{Z}_n^*$

$H \leq \{a \in \mathbb{Z}_n^* : \left(\frac{a}{n}\right) = a^{\frac{n-1}{2}}\} \leq \mathbb{Z}_n^*$

$H \leq \{$testimoni a favore di $n\}$

La probabilità che n passi è $\frac{|H|}{\varphi(n)}$

Sappiamo che $|H| \mid |\mathbb{Z}_n^*|$, per il teorema sugli ordini dei sottogruppi; dunque $|H| \mid \varphi(n)$.

In particolare $|H| \leq \frac{\varphi(n)}{2}$, e la probabilità si può scrivere come:

$\frac{|H|}{\varphi(n)} \leq \frac{\varphi(n)/2}{\varphi(n)} = \frac{1}{2}$, come volevasi dimostrare.

Segue che, prese k basi, la probabilità che passi il test di Eulero per tutte è $\leq \frac{1}{2^k}$ (i risultati sono indipendenti).

Vediamo ora il criterio di Miller.

Per Fermat, se n è primo e dispari, allora $a \in \mathbb{Z}_n^* \Rightarrow a^{n-1} \equiv 1 \mod n$, e $n \mid a^{n-1} - 1$. Inoltre $n-1 = 2^k m$, con m dispari, $k \geq 1$.

Si ha che:

$a^{n-1} - 1 = a^{2^k m} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \cdot \ldots \cdot (a^{2^{k-1} m} + 1)$

Se n è primo:

$n \mid a^{n-1} - 1 \Rightarrow n$ divide il prodotto $\Rightarrow n$ divide almeno un fattore.

Inoltre $a^m \equiv 1 \pmod n$, pertanto dovrà essere $a^{2^i m} \equiv -1 \pmod n$, per un $0 \leq i < k$.

Teorema La probabilità che n composto passi Miller su $a \in \mathbb{Z}_n^*$ è $\leq \frac{1}{4}$, a meno che $n = 9$.

Lemma G ciclico, $|G| = n$. Allora il numero di soluzioni di $x^m = 1$ in G è (m, n).

Dim. $G = \langle g \rangle$ $\log_g x^m = \log_g 1 = 0$

$x^m = 1$ in $G \iff \log_g x^m \equiv 0 \mod n$

$m \cdot \log_g x \equiv 0 \pmod n$

$m \cdot y \equiv 0 \pmod n$

che ha (m, n) soluzioni. □

L'insieme delle basi favorevoli $B = \{x \in \mathbb{Z}_n^* : x^m = 1 \vee \exists i \ 0 \leq i \leq k-1, x^{2^i m} = -1\}$ abbia cardinalità $|B|$.

La probabilità che n composto ($n - 1 = 2^k m$) passi Miller su di una base casuale è $\frac{|B|}{\varphi(n)}$.

Def. Sia ℓ tale per cui 2^ℓ è la massima potenza di 2 tale che $\forall p \mid n$, $2^\ell \mid p - 1$.

Def. $B' := \{x \in \mathbb{Z}_n^* : x^{2^{\ell-1} m} = \pm 1\}$

Lemma $B \subseteq B'$

Dim. $x \in B$. Se $x^m = 1$, allora $x^{2^{\ell-1} m} = 1$, dunque $x \in B'$.

Se invece $x^{2^i m} = -1$ per un dato $0 \leq i \leq k-1$, allora $x^{2^{i+1} m} = 1$, per cui $\begin{cases} (x^m)^{2^i} = -1 \\ (x^m)^{2^{i+1}} = 1 \end{cases}$. Segue che per $\mathbb{Z}_p^*$ $x^m = 2^{i+1}$

$\Rightarrow \forall p \mid n$, $2^{i+1} \mid p - 1 \Rightarrow i + 1 \leq \ell$

$i \leq \ell - 1$

$\Rightarrow x^{2^{\ell-1}m} = (x^{2^i m})^{\ell-1-i} = (-1)^{\ell-1-i} = \pm 1$

Ragionando analogamente a quanto visto prima, possiamo già asserire che la probabilità che il test sia passato è $\leq \frac{1}{2}$; cosa che può essere dimostrata anche osservando che uno pseudoprimo di Miller è anche uno pseudoprimo di Eulero.

Noi però chiediamo un risultato più fine: $\frac{|B'|}{\varphi(n)} \leq \frac{1}{4}$.

Naturalmente è sufficiente provare che $\frac{|B'|}{\varphi(n)} \leq \frac{1}{4}$

Sia $n = \prod_p p^{a_p}$, i $\mathbb{Z}_{p^{a_p}}^*$ sono gruppi ciclici.

$|\{x \in \mathbb{Z}_{p^{a_p}}^* : x^{2^{\ell-1}m} = 1\}| = (2^{\ell-1}m, p^{a_p-1}(p-1))$.

Poiché $2^{\ell-1} \mid p-1$, $(p^{a_p-1}, m) = 1$, abbiamo anche che:

$(2^{\ell-1}m, p^{a_p-1}(p-1)) = 2^{\ell-1}(m, p-1)$

$\{x \in \mathbb{Z}_n^* : x^{2^{\ell-1}m} = 1\} = \prod_p 2^{\ell-1}(m, p-1)$

$|\{x \in \mathbb{Z}_{p^{a_p}}^* : x^{2^{\ell-1}m} = -1\}| = 2^{\ell-1}(m, p-1)$

$|\{x \in \mathbb{Z}_{p^{a_p}}^* : x^{2^\ell} = 1\}| = (2^\ell m, p^{a_p-1}(p-1)) = 2^\ell (m, p-1)$

Dunque:

$|B'| = 2 \cdot \prod_p 2^{\ell-1}(m, p-1)$

$\frac{|B'|}{\varphi(n)} = \frac{2 \cdot \prod_p 2^{\ell-1}(m, p-1)}{\prod_p p^{a_p-1}(p-1)}$

e la nostra tesi diventa:

$2 \cdot \prod_p \frac{2^{\ell-1}(m, p-1)}{p^{a_p-1}(p-1)} \leq \frac{1}{4}$.

Supponiamo ora per assurdo che:

$\frac{1}{4} < 2 \cdot \prod \frac{2^{\ell-1}(m, p-1)}{p^{a_p-1}(p-1)}$

Allora:

$2^\ell \mid p-1 \Rightarrow 2^{\ell-1} \mid \frac{p-1}{2} \Rightarrow 2^{\ell-1}(m, p-1) \mid \frac{p-1}{2} \Rightarrow 2^{\ell-1}(m, p-1) \leq \frac{p-1}{2}$

$\frac{1}{4} < 2 \cdot \prod \frac{\frac{p-1}{2}}{p^{a_p-1}(p-1)} = 2 \cdot \prod \frac{1}{2 \cdot p^{a_p-1}} \leq 2 \cdot \prod_p \frac{1}{2} = 2 \cdot \frac{1}{2^t} = \frac{1}{2^{t-1}}$

dove t è il numero dei primi che dividono n.

Per la disuguaglianza stretta, $t = 1$ oppure $t = 2$.

Se $t = 1$, allora $n = p^{a_p}$, con $a_p > 1$ poiché n è composto.

Si ha $\frac{1}{4} < 2 \cdot \frac{1}{2p^{a_p-1}} = \frac{1}{p^{a_p-1}}$, vera solo se $p = 3$, $a_p = 2$,

e si riscontra il caso $n = 9$ escluso in precedenza.

Se $t=2$, $n = p^{a_p} q^{a_q}$, ma:

$$\frac{1}{4} < 2 \cdot \prod \frac{\frac{p-1}{2}}{p^{a_p-1}(p-1)} = 2 \cdot \prod \frac{1}{2 \cdot p^{a_p-1}}$$

$$\frac{1}{4} < 2 \cdot \frac{1}{2 \cdot p^{a_p-1}} \cdot \frac{1}{2 \cdot q^{a_q-1}}$$

e dunque necessariamente $a_p = a_q = 1$.

Dovrà pertanto essere $n = pq$, e:

$$\frac{1}{4} < \frac{2^\ell (p-1, m)}{p-1} \cdot \frac{2^{\ell-1}(q-1, m)}{q-1}$$

$$\frac{1}{2} < \frac{2^\ell (p-1, m)}{p-1} \cdot \frac{2^\ell (q-1, m)}{q-1}$$

$$2 > \frac{p-1}{2^\ell (p-1, m)} \cdot \frac{q-1}{2^\ell (q-1, m)}$$

e i fattori a secondo membro sono entrambi uguali a 1 poichè interi positivi il cui prodotto è strettamente minore di 2.

$2^\ell (p-1, m) = p-1$ $\qquad$ $2^\ell (q-1, m) = q-1$

Sarà:

$n = pq \Rightarrow n-1 = pq-1 = 2^k m$

$m \mid pq-1 \Rightarrow (p-1, m) \mid pq-1$

$pq \equiv 1 \mod (p-1, m)$

$(p-1)q + q \equiv 1 \mod (p-1, m)$

$q \equiv 1 \mod (p-1, m)$

$(p-1, m) \mid q-1$

$(p-1, m) \mid 2^\ell (q-1, m)$

$(p-1, m) \mid (q-1, m)$

Per simmetria anche $(q-1, m) \mid (p-1, m)$, ma allora $(p-1, m) = (q-1, m)$, da cui $p = q$, assurdo.

(26.11.2010)

BAILLIE TEST (WASTGAFF)

Consideriamo:

1) n non divisibile per $p < L$
2) test di Miller sulla base 2

Se passa:

3) Lucas con $h = 1$, e si cerca $D = h^2 - 4k$ nella sequenza $5, -7, 9, -11, 13, \ldots$ tale che $\left(\frac{D}{n}\right) = -1$. In questo caso $D = h^2 - 4k = 1 - 4k \Rightarrow k = \frac{D-1}{4}$.
Si vede se $n \mid U_{n+1}(1,k)$.

Nessun numero composto passa entrambi i test, nella pratica.
Una dimostrazione dell'effettiva primalità ~~no~~ di tutti i numeri che passano entrambi i test non esiste, e anzi alcuni come Pomerance ritengono che ne esistano di composti e pure in numero tale per cui la densità del rispettivo insieme sia > 0, ma per l'uso pratico (isprime(n), Prime?(n)), si può ritenere primo un numero che passa.

Abbiamo visto (Morrison, Pocklington) che metodi deterministici e non polinomiali diventano polinomiali per numeri di forma particolare; inoltre ci siamo imbattuti in metodi probabilistici polinomiali.
Vedremo ora metodi deterministici e polinomiali ma condizionati, ovvero basati su ipotesi e congetture non dimostrate.
Essi dipendono in generale dalle cosiddette ERH.

- Iniziamo ricordando, in generale, la definizione di carattere di G: si tratta di un morfismo $\delta : G \to \mathbb{C}^*$. Ci interesseranno in particolare i caratteri dei gruppi abeliani finiti.
- $|G| = n$ è riducibile se $G = H \times K$, $H, K \neq G$, $H, K = \{1_G\}$
- $\mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3$
- $\mathbb{Z}_9$ non è riducibile. Infatti, sia $C_n = \langle x \rangle$. $C_{pq} = H \times K$, $H, K \leq G$ $G = H \times K$ equivale a dire che $\exists\, \bar{H}, \bar{K} \trianglelefteq G$, $\bar{H} \cap \bar{K} = \{1_G\}$, $G = \bar{H}\bar{K}$.
Ma ~~A~~ $A \times B$ è ciclico se e solo se A e B sono ciclici e $(|A|, |B|) = 1$. Pertanto $\mathbb{Z}_9 = \mathbb{Z}_m \times \mathbb{Z}_n$ si può solo scrivere con $(m, n) = (1, 9)$ o viceversa, e dunque non si ha riducibilità.

- Ricordiamo la definizione di p-Sylow di G: in generale, è
  $H \leq G : |H| = p^e$ con $p^e \,||\, |G|$

  Se G è abeliano:
  $n = \prod p_i^{e_i}$ $\qquad G = \prod H_i$
  $\exists!\ H_i \trianglelefteq G \qquad |H_i| = p_i^{e_i}$
  $i \neq j : \quad H_i \cap H_j = \{1_G\}$

- Per esempio, se $|G| = 45$, $G = H_1 \times H_2$, $|H_1| = 5$, $|H_2| = 9$.
  $|G| = p^e$, se non è ciclico, si decompone nel prodotto $G = G_1 \times \dots \times G_t$ ciclici, dove $|G_i| = p^{v_i}$, $\sum v_i = p$
  Se $|G| = 9$, $G = C_9\ (\mathbb{Z}_9)$, oppure $G = \mathbb{Z}_3 \times \mathbb{Z}_3$
  Se $|G| = 32$, considerando le sette partizioni di 5, si ottengono altrettanti gruppi di tale ordine:
  $5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$
  $\mathbb{Z}_{32}$; $\mathbb{Z}_{16} \times \mathbb{Z}_2$; $\mathbb{Z}_8 \times \mathbb{Z}_4$; $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2$; $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$; $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
  I gruppi abeliani finiti di ordine n, a meno di isomorfismi, sono: $\prod_{i=1}^{t} \text{part}(e_i)$, se $n = \prod_{i=1}^{t} p_i^{e_i}$, dove $\text{part}(n)$ è il numero di partizioni di n (e.g., come visto sopra, $\text{part}(5) = 7$)
  Per esempio, se $|G| = 288 = 32 \cdot 9 = 2^5 \cdot 3^2$, ci sono $\text{part}(5) \cdot \text{part}(2) = 7 \cdot 2 = 14$ gruppi abeliani finiti di ordine n.

- $\hat{G} = \{\text{caratteri di } G\} = \{\chi : G \to \mathbb{C}^*, \chi \text{ morfismi}\}$
  $\chi, \eta \in \hat{G}$
  $$\begin{cases} \chi\eta : G \to \mathbb{C}^* \\ \chi\eta : x \mapsto \chi(x) \cdot \eta(x) \end{cases}$$
  è un morfismo, infatti:
  $\cdot\ \chi\eta(xy) = \chi(xy)\,\eta(xy) = \chi(x)\chi(y)\eta(x)\eta(y) = \chi(x)\eta(x)\chi(y)\eta(y) = \chi\eta(x)\chi\eta(y)$
  Esiste l'elemento neutro, dato da:
  $\cdot\ \tilde{1} : G \to \mathbb{C}^* \qquad \tilde{1} : x \longmapsto 1 \qquad \tilde{1}\eta = \eta$
  ed esiste anche l'inverso:
  $\cdot\ \chi^{-1} : G \to \mathbb{C}^* \qquad \chi^{-1} : x \longmapsto (\chi(x))^{-1} = \overline{\chi(x)}$
  poichè sul cerchio unitario del piano di Gauss gli inversi corrispondono ai coniugati. Infatti, se $|G| = n$, $\forall\, g \in G$, $g^n = 1_G$, e dunque $\chi(g^n) = [\chi(g)]^n = 1$

Vogliamo arrivare all'obiettivo $G \cong \hat{G}$

Sia $G = C_n = \langle x \rangle$.

Un elemento generico di C_n è x^h.

$\theta \in \hat{G}$, $\theta(x^h) = \theta(x)^h$

$\theta(x) \in U_n = \langle \alpha_n \rangle$

$\theta(x^h) = [\theta(x)]^h = (\alpha_n^k)^h$ dove $\alpha_n^k = \theta(x)$

Scriviamo $\theta = \theta_k^{(n)}$, $0 \le k \le n-1$

$\theta_0^{(n)}(x) = \alpha_n^0 = 1$

$\theta_1^{(n)}(x) = \alpha_n^1 = \alpha_n$

$\theta_k^{(n)}(x) = (\theta_1^{(n)}(x))^k = \alpha_n^k$

Se $|G| = n$, $n = \prod p_i^{e_i}$, allora $G = \prod_{j=1}^{s} C_j$, con $C_j = \langle x_j \rangle$

$\theta : G \to \mathbb{C}^*$, $\theta / C_j : C_j \to \mathbb{C}^*$

$|C_j| = n_j$ $\prod_{j=1}^{s} n_j = n$

$\hat{C_j} = \{\theta_h^{(n_j)} \quad 0 \le h \le n_j - 1\}$

$\theta(x) = \prod_{j=1}^{s} \theta_{h_j}^{(n_j)}(x_j) = \prod \alpha_{n_j}^{h_j}$

$= \prod_{j=1}^{s} \theta_{h_j}^{(n_j)}(g_j^{k_j}) = \prod (\alpha_{n_j}^{h_j})^{k_j} = \prod_{j=1}^{s} \alpha_{n_j}^{h_j k_j}$

Poiché $\alpha_{n_j} = \alpha_n^{\frac{n}{n_j}} = \left(e^{\frac{2\pi i}{n}}\right)^{\frac{n}{n_j}} = e^{2\pi i n_j}$:

$\prod_{j=1}^{s} \alpha_{n_j}^{h_j k_j} = \prod_{j=1}^{s} e^{\frac{2\pi i h_j k_j}{n_j}}$

$\theta \longleftrightarrow (\theta^{(n_1)}, \dots, \theta^{(n_s)})$

$\hat{G} \cong G$, come volevasi dimostrare.

Esempi:

- $G = \{1_G\}$ $\hat{G} = \{\tilde{1}\}$, il solo carattere principale
- $G = \mathbb{Z}_2$

Possiamo costruire la cosiddetta tavola dei caratteri:

	θ_0	θ_1
1	1	1
x	1	-1

$\theta_1^{(2)}(x) = \alpha_2 = -1$

- $G = C_3$

	$\theta_0^{(3)}$	$\theta_1^{(3)}$	$\theta_2^{(3)}$
1	1	1	1
x	1	α_3	α_3^2
x^2	1	α_3^2	α_3

$\theta_1^{(3)}(x) = \alpha_3$

$x^3 - 1 = (x-1)(x^2+x+1)$

$\alpha_3^4 = \alpha_3$

- $G = C_4$

	$\theta_0^{(4)}$	$\theta_1^{(4)}$	$\theta_2^{(4)}$	$\theta_3^{(4)}$
1	1	1	1	1
x	1	i	-1	-i
x^2	1	-1	1	-1
x^3	1	-i	-1	i

- $G = C_2 \times C_2$

	$\theta_0^{(2)}\theta_0^{(2)}$	$\theta_0^{(2)}\theta_1^{(2)}$	$\theta_1^{(2)}\theta_0^{(2)}$	$\theta_1^{(2)}\theta_1^{(2)}$
(1,1)	1	1	1	1
(1,x)	1	-1	1	-1
(x,1)	1	1	-1	-1
(x,x)	1	-1	-1	1

Si noti che la somma degli elementi della prima riga è n, così come quella degli elementi della ~~seconda riga~~ prima colonna. Le somme di altre righe e di altre colonne sono invece nulle. Questa viene detta legge di ortogonalità dei caratteri, e può essere meglio formalizzata nel seguente modo:

Legge Sia θ un carattere di G, allora $\frac{1}{n} \cdot \sum_{g \in G} \theta(g) \begin{cases} 1 & \text{se } \theta = \hat{1} \\ 0 & \text{altrimenti} \end{cases}$

Dim. Il caso $\theta = \hat{1}$ è banale.

Sia pertanto $\theta \neq \hat{1}$: proviamo che $\sum_{g \in G} \theta(g) = 0$

$S = \sum_{g \in G} \theta(g)$

Per ipotesi $\exists\, h \in G \quad \theta(h) \neq 1$

$\theta(h)\, S = \theta(h) \cdot \sum_{g \in G} \theta(g) \Rightarrow (\theta(h) - 1)\, S = 0$

da cui $\theta(h) \neq 1$ e quindi $S = 0$

(infatti $\sum_{g \in G} \theta(h)\theta(g) = \sum_{g \in G} \theta(hg)) = S$

Analogamente:

Legge Sia g un elemento di G, allora $\frac{1}{n} \cdot \sum_{\theta \in \hat{G}} \theta(g) \begin{cases} 1 & \text{se } g = 1_G \\ 0 & \text{altrimenti} \end{cases}$

Dim. $S = \sum_{\theta \in \hat{G}} \theta(g)$ Se $g \neq 1_G$:

$\exists\, \eta \in \hat{G} : \eta(g) \neq 1$

$\eta(g)\, S = \eta(g) \sum_{\theta \in \hat{G}} \theta(g) = \sum_{\theta \in \hat{G}} \eta(g)\theta(g) =$

$= \sum_{\theta \in \hat{G}} \eta\theta(g) = S \quad \Rightarrow \quad S = 0$

Corollario

Dato α_n, $\frac{1}{n} \sum_{r=0}^{n-1} \alpha_n^{r(i-j)} \begin{cases} 1 & \text{se } i = j \pmod n \\ 0 & \text{se } i \neq j \pmod n \end{cases}$

Dim. Se $i = j$ è banale.

Se $i \neq j$, $\alpha_n^{r(i-j)} = \theta_{i-j}^{(n)}(x^r)$, dove $C_n = \langle x \rangle$

$\frac{1}{n} \cdot \sum_{r=0}^{n-1} \alpha_n^{r(i-j)} = \frac{1}{n} \cdot \sum_{r=0}^{n-1} \theta_{i-j}^{(n)}(x^r)$

$\theta_{i-j}^{(n)} \in \hat{C_n} \qquad \frac{1}{n} \cdot \sum_{g \in C_n} \theta_{i-j}^{(n)}(g)$

vale 1 su $\theta_{i-j}^{(n)} = \hat{1} \Leftrightarrow i = j \pmod n$

0 altrimenti

(30.11.2010)

Data α_n, definiamo $F_{ij} = \frac{1}{\sqrt{n}} \alpha_n^{ij}$.

Poiché, se $x^j \in C_n = \langle x \rangle$, $\hat{C}_n = \{\delta_i^{(n)} : 0 \le i \le n-1\}$,

$\delta_i^{(n)}(x^j) = \alpha_n^{ij}$, F_{ij} è la matrice dei caratteri, a meno del fattore moltiplicativo $\frac{1}{\sqrt{n}}$.

Consideriamo ora la matrice coniugata $\overline{F}_{ij} = \frac{1}{\sqrt{n}} \overline{\alpha_n^{ij}}$, dove vengono coniugati (nel senso di complessi coniugati) gli elementi.

Valgono: (i) $\overline{F}_{ij} = \frac{1}{\sqrt{n}} \alpha_n^{-ij}$ e (ii) $F\overline{F} = I_n$.

Dimostriamo il secondo risultato.

Si ha:

$M = F\overline{F}$

$M_{ij} = \sum_{k=0}^{n-1} F_{ik} \overline{F_{kj}}$

$= \frac{1}{n} \cdot \sum_{k=0}^{n-1} \alpha_n^{ik} \alpha_n^{-kj} = \frac{1}{n} \cdot \sum_{k=0}^{n-1} \alpha_n^{k(i-j)} = \delta(i,j)$ (poiché siamo modulo n)

Ricordando che $\sum_{k=0}^{n-1} \alpha^{k(i-j)} \begin{cases} n & \text{se } i \equiv j \ (n) \\ 0 & \text{se } i \not\equiv j \ (n) \end{cases}$, si ottiene la tesi.

Dunque la coniugata è l'inversa.

Questa operazione viene definita trasformazione di Fourier discreta (DFT)

(Crandall - Pomerance) Sia un anello commutativo R, e siano:

$n^{-1} \in R$ $\quad \alpha_n \in R^*$ $\quad$ cioè $C_n \le R^*$

$\mathcal{R}_{n,R} \triangleq (R^n, *)$ $\quad \mathcal{H}_{n,R}(R^n, \odot)$

$\mathcal{R}_{n,R} \cong \frac{R[x]}{(x^n-1)} \cong RC_n$

$(x * y)_i = \sum_{h+k \equiv i \ (n)} x_h y_k$ $\quad (x \odot y)_i = x_i y_i$

Teor. $\quad DFT : \mathcal{R}_{n,R} \xrightarrow{\sim} \mathcal{H}_{n,R}$

$x \longmapsto X$

dove $X_i = \sum_{k=0}^{n-1} \alpha^{ik} x_k$ è la trasformata mediante F (senza $\frac{1}{\sqrt{n}}$)

Ha inversa: $\quad DFT^{-1}(X) = x$

$x_i = \frac{1}{n} \cdot \sum_{k=0}^{n-1} \alpha^{-ik} X_k$

Teor. $\quad DFT(x * y) = DFT(x) \odot DFT(y)$

$x * y = DFT^{-1}(DFT(x) \odot DFT(y))$

Dim. $\quad [DFT^{-1}(DFT(x) \odot DFT(y))]_i = [DFT^{-1}(z)]_i$

$= \frac{1}{n} \cdot \sum_{k=0}^{n-1} \alpha^{-ik} z_k$, dove:

$z = DFT(x) \odot DFT(y)$

$z_k = [DFT(x) \odot DFT(y)]_k = [DFT(x)]_k \cdot [DFT(y)]_k$

$= \left(\sum_{j=0}^{n-1} \alpha^{kj} x_j \right) \left(\sum_{h=0}^{n-1} \alpha^{kh} x_h \right)$

Dunque $\frac{1}{n} \cdot \sum_{k=0}^{n-1} \alpha^{-ik} z_k = \frac{1}{n} \cdot \sum_{k,j,h} \alpha^{-ik} \alpha^{kj} \alpha^{kh} x_j y_h$

$= \frac{1}{n} \cdot \sum_{k,j,h} \alpha^{k(j+h-i)} x_j y_h$

Sommando rispetto a k nella sommatoria si ottiene:

n se $j+h-i \equiv 0$, 0 se $j+h-i \not\equiv 0 \pmod n$

Questo permette di giungere alla tesi:

$$\frac{1}{n} \cdot \sum_{k,j,h} \alpha^{k(j+h-i)} x_j y_h = \sum_{\substack{j+h=i \\ (\mathrm{mod}\ n)}} x_j y_h$$

Esiste un algoritmo, detto FFT (fast fourier transform) che permette di calcolare velocemente le DFT.

(Danilson - Lanczos) Sia n pari. Allora:

$$[DFT(x)]_k = \frac{1}{n} \cdot \sum_{k=0}^{n-1} \alpha^{ki} x_i$$

$$= \frac{1}{n} \cdot \sum_{k=0}^{n/2-1} x_{2i} (\alpha^2)^{ik} + \frac{1}{n} \cdot \alpha^k \cdot \sum_{i=0}^{n/2-1} x_{2i+1} (\alpha^2)^{ik}$$

Si può usare poi ricorsivamente su $n = 2^d$.

Questo permette di avere un costo computazionale di $O(n \cdot \log n)$ piuttosto che di $O(n^2)$ (pagina 439, capitolo 9)

Definiamo ora il prodotto aciclico come:

$$v = (x \times y)_m = \sum_{i+j=m} x_i y_j = v_m \qquad m = 0, 1, \dots, 2n-2 \text{ e si pone } v_{2n-1} = 0$$

Tale prodotto può essere utilizzato per calcolare prodotti di numeri interi. Consideriamo infatti $23 \cdot 47$, nella base consueta $B = 10$ possiamo scrivere:

$3 + 2 \cdot 10 \longrightarrow \overset{x_0\ x_1\ x_2\ x_3}{(3, 2, 0, 0)} = x$

$7 + 4 \cdot 10 \longrightarrow \overset{y_0\ y_1\ y_2\ y_3}{(7, 4, 0, 0)} = y$

e calcolare:

$$(x \times y)_0 = \sum_{i+j=0} x_i y_j = x_0 y_0 = 21$$

$$(x \times y)_1 = \sum_{i+j=1} x_i y_j = x_0 y_1 + x_1 y_0 = 12 + 14 = 26$$

$$(x \times y)_2 = \sum_{i+j=2} x_i y_j = x_1 y_1 = 8$$

$$x \times y = (21, 26, 8, 0)$$

Si ha $21 + 26 \cdot 10 + 8 \cdot 100 = (3 + 2 \cdot 10)(7 + 4 \cdot 10)$, come verificabile.

Sfruttando il fatto che $DFT^{-1}(DFT(x) \odot DFT(y)) = x * y$, possiamo generare un algoritmo per il prodotto veloce:

1) riempire di zeri x, y fino a lunghezza $2n$
2) $X = DFT(x)$, $Y = DFT(y)$ con FFT
3) $Z = X \odot Y$
4) $z = DFT^{-1}(Z)$
5) round(z) (che ci rende già il prodotto)
6) riporti

```
carry = 0;
for (0 ≤ m ≤ 2n) {v = z_m + carry;
    z_m = v mod B;
    carry = ⌊v/B⌋ }
```

7) si eliminano gli eventuali zeri inutili

Vediamo un'applicazione; con $n=2$, $x=57$, $y=68$:

$x = (7,5,0,0)$ $\qquad$ $y = (8,6,0,0)$

La DFT usa α_{2n}, nel nostro caso $\alpha_4 = i$

$$(DFT(x))_k = \sum_{j=0}^{3} i^{jk} x_j$$

$DFT(8,6,0,0) = (14, 8+6i, 2, 8-6i) = Y$

$DFT(7,5,0,0) = (12, 7+5i, 2, 7-5i) = X$

$Z = X \odot Y = (168, 26+82i, 4, 26-82i)$

$DFT^{-1}(Z) = (\underset{z_0}{56}, \underset{z_1}{82}, \underset{z_2}{30}, \underset{z_3}{0})$

Vale $57 \cdot 68 = 3876 = 56 \cdot 1 + 82 \cdot 10 + 30 \cdot 100$

Utilizziamo ora il metodo del carry per aggiustare i riporti.

carry = c

$c = 0$ $\qquad$ $v = z_0 + 0 = 56$

$z_0 = 56 \bmod 10 = 6$ $\qquad$ $z_0 = 6$

$c = \lfloor 56/10 \rfloor = 5$

$c = 5$ $\qquad$ $v = z_1 + 5 = 87$

$z_1 = 87 \bmod 10 = 7$ $\qquad$ $z_1 = 7$

$c = \lfloor 87/10 \rfloor = 8$

$c = 8$ $\qquad$ $v = z_2 + 8 = 38$

$z_2 = 38 \bmod 10 = 8$ $\qquad$ $z_2 = 8$

$c = \lfloor 38/10 \rfloor = 3$

$c = 3$ $\qquad$ $v = z_3 + 3 = 3$

$z_3 = 3 \bmod 10 = 3$ $\qquad$ $z_3 = 3$

$q = \lfloor 3/10 \rfloor = 0$

Torniamo ora ai caratteri. Definiamo un carattere modulare, modulo n, un $\vartheta \in \hat{\mathbb{Z}}_n^*$ esteso a tutto $\mathbb{Z}$. Esso vale 0 su m se $(m,n) \neq 1$, mentre vale $\Theta(m)$ se $(m,n) = 1$, e quindi $m \in \mathbb{Z}_n^*$.

Per esempio, se $n=2$, $\mathbb{Z}_2^* = \{1\}$, $\hat{\mathbb{Z}}_2^* = \{\chi_0\}$

χ_0 è il carattere principale e vale sempre 1 o 0.

	1	2	3	4	5	6
χ_0	1	0	1	0	1	0

$n=3$, $\mathbb{Z}_3^* = \{1,2\} = \langle 2 \rangle$ $\qquad$ $\vartheta_1^{(2)} = \chi_1$

	1	2	3	4	5	6
χ_0	1	1	0	1	1	0
χ_1	1	-1	0	1	-1	0

$n = 4$, $\mathbb{Z}_4^* = \{1,3\} = \langle 3 \rangle$

	1	2	3	4	5	6	7	8
χ_0	1	0	1	0	1	0	1	0
χ_1	1	0	-1	0	1	0	-1	0

In generale, per calcolare l'analogo di $\mathbb{Z}_n^*$ con n composto e non necessariamente potenza di primo, si procede per scomposizione.

Vediamo per esempio cosa accade nel caso di $\mathbb{Z}_{15}^* = \mathbb{Z}_3^* \times \mathbb{Z}_5^*$.

Abbiamo innanzitutto che $\mathbb{Z}_3^* = \{1,2\} = \langle 2 \rangle$, $\mathbb{Z}_5^* = \{1,2,3,4\} = \langle 2 \rangle$

Associamo ad $a \in \mathbb{Z}_{15}^*$ la coppia (a mod 3, a mod 5). Nel caso:

$1 \to (1,1)$ $\quad 2 \to (2,2)$ $\quad 4 \to (1,4)$ $\quad 7 \to (1,2)$

$8 \to (1,3)$ $\quad 11 \to (2,1)$ $\quad 13 \to (1,3)$ $\quad 14 \to (2,4)$

$g \in \mathbb{Z}_p^*$ $\quad g = g_1^{v_1} g_2^{v_2}$ $\quad g \to (2^{v_1}, 2^{v_2})$

	$g_0^{(2)} g_0^{(2)}$	$g_0^{(2)} g_1^{(2)}$
(0,0)	1	
(0,1)	7	
(0,2)	4	
(0,3)	13	
(1,0)	11	
(1,1)	2	
(1,2)	14	
(1,3)	8	

$\chi_i^{(2)} \chi_j^{(2)} (u,v)$

$\alpha_2^{iu} \alpha_4^{jv} = (-1)^{iu+jv}$ $\quad \left(\frac{a}{15}\right)$

(03.12.2010)

$$\prod_{p\in\mathbb{P}} (1-p^{-s})^{-1} = \sum_{n\in\langle\mathbb{P}\rangle} \frac{1}{n^s} \qquad \mathbb{P}=\{p_1,\dots,p_t\} \qquad \langle\mathbb{P}\rangle = \{p_1^{k_1}\cdot\dots\cdot p_t^{k_t}\}$$

$$\prod_{p\in\mathbb{P}} (1-p^{-s})^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad \text{passando al limite } (\mathbb{P} \text{ insieme di tutti i primi})$$

Dunque $\zeta(s)$, funzione zeta di Riemann, convergente in ambito reale per $s>1$, può essere definita equivalentemente dalle due diciture precedenti.

Passando ai caratteri:

χ_6 con modulo m $\qquad \chi : \mathbb{Z}_m^* \to \mathbb{C}^*$

$$\prod_{p\in\mathbb{P}} (1-\chi(p)\cdot p^{-s})^{-1} = \prod_{p\in\mathbb{P}} \frac{1}{1-\frac{\chi(p)}{p^s}} \qquad |\chi(p)|<1, \quad \left|\frac{\chi(p)}{p^s}\right|<1$$

$$= \prod_{p\in\mathbb{P}} \sum_{k=0}^{\infty} \left(\frac{\chi(p)}{p^s}\right)^k = \prod_{p\in\mathbb{P}} \sum_{k=0}^{\infty} \frac{\chi(p^k)}{p^{ks}} = \sum_{p_i\in\mathbb{P}} \frac{\chi(p_1^{k_1})\cdot\chi(p_2^{k_2})\cdot\dots\cdot\chi(p_t^{k_t})}{(p_1^{k_1}p_2^{k_2}\cdot\dots\cdot p_t^{k_t})^s}$$

$$= \sum_{p_i\in\mathbb{P}} \frac{\chi(p_1^{k_1}\cdot\dots\cdot p_t^{k_t})}{(p_1^{k_1}\cdot\dots\cdot p_t^{k_t})^s} = \sum_{n\in\langle\mathbb{P}\rangle} \frac{\chi(n)}{n^s}$$

Dunque:

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p\in\mathbb{P}} (1-\chi(p)\,p^{-s})^{-1}$$

Definiamo:

$$L(s,\chi) = \prod_{p\in\mathbb{P}} (1-\chi(p)\,p^{-s})^{-1} = \sum_{n\in\langle\mathbb{P}\rangle} \frac{\chi(n)}{n^s} \quad \text{funzione di Dirichlet}$$

Se poniamo χ_0 il carattere che vale 1 se $(m,n)=1$ e 0 altrimenti, vale:

$$\zeta(s) = L(s,\chi_0)\cdot \prod_{p\mid m} (1-p^{-s})^{-1}$$

Tutto questo permette di arrivare al risultato di Dirichlet:

$\exists\ \infty$ primi $/\ p\equiv a\ (n) \qquad \forall n,\ \forall a\in\mathbb{Z}_n^*$

Abbiamo già visto il caso $a=1$.

Vediamo ora un esempio dell'applicazione che porta alla formulazione generale, nel caso $(a,n)=(1,4)$.

Sia χ_1 il carattere non principale modulo 4.

$$\zeta(s)\cdot L(s,\chi_1) = \prod_{p\in\mathbb{P}} (1-p^{-s})^{-1}\cdot \prod_{p\in\mathbb{P}} (1-\chi_1(p)\,p^{-s})$$

$$= (1-2^{-s})^{-1}\cdot \prod_{q\equiv 1} (1-q^{-s})^{-1}\cdot \prod_{r\equiv 3} (1-r^{-s})^{-1}\cdot \prod_{q\equiv 1} (1-q^{-s})^{-1}\cdot \prod_{r\equiv 3} (1+r^{-s})^{-1}$$

$$= (1-2^{-s})^{-1}\cdot \prod_{q\equiv 1} (1-q^{-s})^{-2}\cdot \prod_{r\equiv 3} (1-r^{-2s})^{-1}$$

$$\lim_{s\to 1^+} \zeta(s) = \lim_{s\to 1^+} \sum_{n=1}^{\infty} \frac{1}{n^s} = +\infty$$

$$L(s,\chi_1) = \sum_{n=1}^{\infty} \frac{\chi_1(n)}{n^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s}$$

$$\lim_{s\to 1^+} L(s,\chi_1) = \operatorname{atan}(1) = \frac{\pi}{4}$$

Ne consegue che $\lim_{s\to 1^+} [\zeta(s)\cdot L(s,\chi_1)] = +\infty$

Abbiamo che $\lim_{s\to 1^+} \prod_{q\equiv 1} (1-q^{-s})^{-2} = +\infty$, dunque $\exists$ ∞ primi $q \equiv 1 \pmod 4$.

Infatti, proviamo ora che $\lim_{s\to 1^+} \prod_{r\equiv 3} (1-r^{-2s})^{-1}$ è finito, il che implica che debba essere il fattore sopra infinito ($(1-2^{-s})^{-1}$ è ovviamente finito):

$$\prod_{r\equiv 3} (1-r^{-2s})^{-1} \leq \prod_{r\equiv 3} (1-r^{-2})^{-1} \leq \prod_{p\in P} (1-p^{-2})^{-1} = \zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

L'IPOTESI DI RIEMANN

$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, s complesso, converge se $\mathrm{Re}(s) > 1$.

L'idea è quella di estendere tramite prolungamento analitico $\zeta(s)$ su tutto $\mathbb{C}$, e poi di ricercarne gli zeri.

Non ci sono zeri per $\mathrm{Re}(s) \geq 1$; per $\mathrm{Re}(s) < 0$ si trovano tutti sull'asse x e sono detti zeri banali.

Vengono detti zeri non banali quelli per cui $0 \leq \mathrm{Re}(s) < 1$.

L'ipotesi di Riemann afferma che tutti gli zeri non banali sono tali per cui $\mathrm{Re}(s) = \frac{1}{2}$.

Fino ad ora non sono stati trovati controesempi, mentre sono state riscontrate un numero notevole di occorrenze che annullano non banalmente la funzione zeta di Riemann.

CONSEGUENZE

Consideriamo la funzione di Möbius:

$$M(x) = \sum_{n\leq x} \mu(n)$$

con μ definita nel seguente modo:

- $\mu(1) = 1$
- $\mu(n) = 0$ se, scomposto $n = \prod_i p_i^{e_i}$, $\exists j \mid e_j > 1$
- $\mu(n) = (-1)^k$ se $n = p_1 \cdot \ldots \cdot p_k$, tutti distinti.

L'ipotesi di Riemann può essere scritta equivalentemente come:

$|M(n)| \in O(n^{1/2+\varepsilon})$ $\forall \varepsilon > 0$, ovvero:

(RH1) $\forall \varepsilon > 0$ $\exists c > 0$ $\exists N$ $\forall n > N$ $|M(n)| < c\cdot n^{1/2+\varepsilon}$

Nel 1897 Mertens congetturò che $|M(n)| \leq n^{1/2}$. Von Steinck si spinse oltre pochi anni dopo, congetturando $|M(x)| < \frac{1}{2} x^{1/2}$, ma questo si provò falso nel 1960 (Durkat, senza controesempio), e poi si trovò che 7.725.030.629 era effettivamente un controesempio.

Anche l'ipotesi di Mertens fu disprovata nel 1985, quando si provò che $\limsup_{x\to\infty} M(x)\, x^{-1/2} > 1.06$ e $\liminf_{x\to\infty} M(x)\, x^{-1/2} < -1.009$. Tuttavia non sono ancora stati trovati controesempi a tutt'oggi.

Un'altra formulazione equivalente è la seguente:

(RH2) $\left|\pi(x) - \frac{x}{\log x}\right| \in O(x^{1/2+\varepsilon})$

e anche la formulazione di Lagarias:

$\forall n \geq 1, \quad G(n) \leq H(n) + e^{H(n)} \cdot \log(H(n))$

$G(n) = \sum_{d|n} d \qquad H(n) = \sum_{s=1}^{n} \frac{1}{s}$

Esiste anche una versione estesa dell'ipotesi di Riemann:

$\pi(x, a, n) = |\{p \text{ primo}, p \equiv a \pmod n, p \leq x\}|$.

Ci si aspetta che $\pi(x, a, n) = \frac{\pi(x)}{\varphi(n)}$ se $(a, n) = 1$

Due formulazioni equivalenti della ERH sono:

- gli zeri nella fascia critica di $L(s, \chi)$, $\chi \neq \chi_0$, hanno $\mathrm{Re}(z) = \frac{1}{2}$
- $\left|\pi(x, a, n) - \frac{\pi(x)}{\varphi(n)}\right| \in O(x^{1/2+\varepsilon})$

Un risultato collegato è quello di Ankeny - Bach:

ERH implica che, se χ è un carattere non principale mod n, allora $\exists a < 2 \cdot \log^2 n \ / \ \chi(a) \neq 1$

Cor. Se $H \subsetneq \mathbb{Z}_n^*$ allora $\exists a \in \mathbb{Z}_n^* \ / \ a < 2 \cdot \log^2 n, \ a \notin H$

Dim. Sia $H \subsetneq \mathbb{Z}_n^*$, allora esiste $G = \mathbb{Z}_n^* / H$, $G \neq \{1_G\}$.

Si avrà $\mathbb{Z}_n^* \xrightarrow{\pi} G \xrightarrow{\theta} \mathbb{C}^*$ $\qquad \theta \neq \tilde{1}$

Esiste $v \in G \ / \ \theta(v) \neq 1$; esiste $a \in \mathbb{Z}_n^* \ / \ \pi(a) = v$, $\theta(\pi(a)) = \theta(v) \neq 1$;

in parti $v \neq 1_G$, $v = \pi(a) = aH$, $aH \neq H$, $a \notin H$.

Dunque $\chi(a) \neq 1 \Rightarrow a \notin H$, donde la tesi.

Ne segue:

Teor. n è primo $\iff \forall a \in \mathbb{Z}_n^*, \left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod n$

$H = \{a \in \mathbb{Z}_n^* : \left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod n\}$

$H \leq \mathbb{Z}_n^* \Rightarrow \exists a < 2 \cdot \log^2 n \quad (a \notin H)$

$\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \pmod n$

Se è vera la ERH, si avrebbe dunque un algoritmo (Miller) deterministico e polinomiale condizionato.

Possono contribuire i seguenti risultati:

- Nair se $n \geq 9$, $d_n^* \geq 2^n$, dove $d_n = \mathrm{mcm}\{1, 2, \ldots, n\}$
- Chebyshev $\exists A, B \ / \ A \cdot \log x \leq \pi(x) \leq B \cdot \log x$

$\pi(n) \geq \log 2 \cdot \frac{n}{\log n}$

(07.12.2010)

Dimostreremo i seguenti tre risultati:

- Nair: $d_n \geq 2^n$ per $n \geq 9$, dove $d_n = \operatorname{mcm}\{1,2,\dots,n\}$
- Chebyshev: $\exists\ A, B$ computabili tali per cui $A \cdot \frac{n}{\log n} \leq \pi(n) \leq B \cdot \frac{n}{\log n}$
- Bertrand: $\forall\ n \geq 1 \quad \exists\ p$ primo $/\ n < p < 2n$

- Iniziamo con il definire:

$$I(m,n) = \int_0^1 x^{m-1}(1-x)^{n-m}\,dx \qquad 1 \leq m \leq n \in \mathbb{N}$$

① Abbiamo che $d_n \cdot I(m,n)$ è intero. Infatti:

$$I(m,n) = \int_0^1 x^{m-1} \cdot \sum_{h=0}^{n-m}\left[\binom{n-m}{h} \cdot (-1)^h \cdot x^h\right]dx$$

$$= \sum_{h=0}^{n-m}\left[\binom{n-m}{h} \cdot (-1)^h \cdot \int_0^1 x^{m+h-1}\,dx\right]$$

$$= \sum_{h=0}^{n-m}\left[\binom{n-m}{h} \cdot (-1)^h \cdot \frac{1}{m+h}\right] \qquad \text{svolgendo l'integrale}$$

$$d_n \cdot I(m,n) = \sum_{h=0}^{n-m}\binom{n-m}{h} \cdot (-1)^h \cdot \frac{d_n}{m+h}$$

la quantità $m+h$, per h che va da 0 a $n-m$, vale $m, m+1, \dots, n$, assumendo comunque valori $\leq n$. Poiché $m+h \mid d_n$ per ogni h, qualunque $\frac{d_n}{m+h}$ è intero.

② Più precisamente, vale:

$$I(m,n) = \frac{1}{m \cdot \binom{n}{m}}$$

Infatti, integrando per parti:

$$I(m,n) = \int_0^1 x^{m-1} \cdot (1-x)^{n-m}\,dx = \left[\frac{x^m}{m}(1-x)^{n-m}\right]_0^1 + \int_0^1 \frac{x^m}{m}(n-m)(1-x)^{n-m-1}\,dx$$

$$= \frac{n-m}{m} \cdot \int_0^1 x^m (1-x)^{n-(m+1)}\,dx = \frac{n-m}{m} \cdot I(m+1,n)$$

Applicando ricorsivamente:

$$I(m,n) = \frac{n-m}{m} I(m+1,n) = \frac{n-m}{m} \cdot \frac{n-(m+1)}{m+1} \cdot I(m+2,n) = \dots$$

$$= \frac{(n-m)(n-m-1)\cdot\ldots\cdot 1}{m(m+1)\cdot\ldots\cdot(n-1)} I(n,n) = \dots \cdot \frac{1}{n}$$

$$= \frac{1}{m} \cdot \frac{(n-m)!}{(m+1)\cdot\ldots\cdot(n-1)\cdot n} = \frac{1}{m} \cdot \frac{1}{\binom{n}{n-m}} = \frac{1}{m} \cdot \frac{1}{\binom{n}{m}}$$

③ Notare che ne segue, $\forall\ m, n$, $1 \leq m \leq n$, $m \cdot \binom{n}{m} \mid d_n$, poiché dai risultati precedenti si ha che $\frac{d_n}{m\binom{n}{m}}$ è intero.

In particolare, si ha che:

$$n \cdot \binom{2n}{n} \mid d_{2n} \mid d_{2n+1} \qquad (n+1)\binom{2n+1}{n+1} \mid d_{2n+1}$$

e inoltre:

$$(n+1)\binom{2n+1}{n+1} = (2n+1) \cdot \binom{2n}{n}$$

riarrangiando opportunamente i fattoriali.

Si ha pertanto che:

$n\binom{2n}{n} \mid d_{2n+1}$ $\qquad$ $(2n+1)\cdot\binom{2n}{n} \mid d_{2n+1}$

Poiché però $(n, 2n+1) = 1$, sarà:

$n(2n+1)\binom{2n}{n} \mid d_{2n+1}$

$d_{2n+1} \geq n(2n+1)\binom{2n}{n}$

Ora:

$(2n+1)\cdot\binom{2n}{n} \geq (1+1)^{2n}$

perché:

$2^{2n} = (1+1)^{2n} = \sum_{h=0}^{2n}\binom{2n}{h} \leq (2n+1)\cdot\binom{2n}{n}$

dal momento che ognuno degli $(2n+1)$ addendi è al più $\binom{2n}{n}$.

Ne consegue che:

- se $n \geq 2$, $d_{2n+1} \geq n\cdot 4^n \geq 2\cdot 4^n = 2^{2n+1}$
- se $n \geq 4$, $d_{2n+2} \geq d_{2n+1} \geq n\cdot 4^n \geq 4^{n+1} = 2^{2n+2}$

Si ha dunque $d_N \geq 2^N$ per ogni N dispari ≥ 5 e per ogni N pari ≥ 10 e ciò prova il teorema di Nair.

- Come noto, possiamo scrivere $d_n = \prod p^{\alpha_p}$, dove $p^{\alpha_p} \leq n \leq p^{\alpha_p+1}$

Vale dunque $2^n \leq d_n \leq \underbrace{\prod n}_{\substack{\text{tante volte}\\ \text{quanti sono i}\\ \text{primi} \leq n}} = n^{\pi(n)}$

Passando ai logaritmi:

$\pi(n)\cdot\log n \geq n\cdot\log 2$

$\pi(n) \geq \log 2\cdot\dfrac{n}{\log n}$

Abbiamo dunque trovato un valore di A per il teorema di Chebyshev:

$A = \log 2$.

- Definiamo ora $P_n = \prod_{n<p<2n} p$. Subito $P_n \mid \binom{2n}{n}$ perché $\binom{2n}{n} = \dfrac{(2n)!}{n!\cdot n!}$ e se $n < p < 2n$ allora $p \mid (2n)!$, $p \nmid n!$, pertanto $p \mid$ numeratore e $p \nmid$ denominatore e dunque $p \mid \frac{\text{num}}{\text{den}}$ ovvero $p \mid \binom{2n}{n}$

Similmente a prima:

$2^{2n} = (1+1)^{2n} = \sum_{h=0}^{2n}\binom{2n}{h} \geq \binom{2n}{n}$

dunque $P_n \leq 2^{2n}$

Pertanto $P_n = \prod_{n\leq p\leq 2n} p > \prod n = n^{\pi(2n)-\pi(n)}$

e allora $n^{\pi(2n)-\pi(n)} \leq 2^{2n}$

Ponendo $n = 2^t$:

$2^{t(\pi(2^{t+1})-\pi(2^t))} \leq 2^{2^{t+1}}$

$t\cdot\pi(2^{t+1}) - t\cdot\pi(2^t) \leq 2^{t+1}$

$(t+1)\cdot\pi(2^{t+1}) - t\cdot\pi(2^t) \leq 2^{t+1} + \pi(2^{t+1}) \leq 2^{t+1} + 2^t \leq 2^t(2+1) = 3\cdot 2^t$

Sommiamo ora quanto ottenuto per $0 \le t \le k$:

$t = 0$ $\quad \pi(2) - 0$

$t = 1$ $\quad 2 \cdot \pi(2^2) - \pi(2)$

$t = 2$ $\quad 3 \cdot \pi(2^3) - 2 \cdot \pi(2^2)$

...

La somma a sinistra è telescopica e vale $(k+1) \cdot \pi(2^{k+1})$, mentre quella a destra vale $3 \cdot \sum_{t=0}^{k} 2^t = 3(2^{k+1} - 1) \le 3 \cdot 2^{k+1}$

Otteniamo pertanto $(k+1) \cdot \pi(2^{k+1}) \le 3 \cdot 2^{k+1}$.

Dato n, esiste k tale per cui $2^k \le n < 2^{k+1}$, e passando ai logaritmi: $\log n < (k+1) \cdot \log 2 \Rightarrow k+1 > \frac{\log n}{\log 2}$

Si ha anche:

$\pi(n) \le \pi(2^{k+1})$

$$\pi(n) \le \frac{3 \cdot 2^{k+1}}{k+1} \le \frac{6 \cdot 2^k}{k+1} \le \frac{6 \cdot 2^k \cdot \log 2}{\log n} \le 6 \cdot \log 2 \cdot \frac{n}{\log n}$$

Abbiamo trovato anche la nostra $B = 6 \cdot \log 2$

- Verifichiamo ora la seguente proprietà:

$$\binom{2n}{n} > \frac{4^n}{2\sqrt{n}} \qquad \forall n \ge 2$$

che si dimostra per induzione:

- per $n = 2$, $\binom{4}{2} = 6 > 8/\sqrt{2}$
- supposta vera per n, è anche vera per $n+1$:

$$\binom{2(n+1)}{n+1} = \frac{(2n+2)!}{(n+1)!\,(n+1)!} = \frac{(2n+2)(2n+1)(2n)!}{(n+1)(n+1)\,n!\,n!}$$

$$> 2 \cdot \frac{2n+1}{n+1} \cdot \frac{4^n}{2\sqrt{n}} = 2 \cdot \frac{2n+1}{\sqrt{n(n+1)}} \cdot \frac{4^n}{2\sqrt{n+1}}$$

$$(2n+1)^2 = 4n^2 + 4n + 1 > 4n^2 + 4n = 4n(n+1)$$

$$2n+1 > 2\sqrt{n(n+1)}$$

dunque:

$$2 \cdot \frac{2n+1}{\sqrt{n(n+1)}} \cdot \frac{4^n}{2\sqrt{n+1}} > 2 \cdot 2 \cdot \frac{4^n}{2\sqrt{n+1}} = \frac{4^{n+1}}{2\sqrt{n+1}}$$

- Scriviamo un fattoriale in una forma:

$$n! = \prod_p p^{e(p,n)}$$

dove $e(p,n)$ è il numero di volte che appare il fattore p nella fattorizzazione di $n!$, ed è dato da $e(p,n) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$

- Scriviamo anche:

$\binom{2n}{n} = \prod p^{e_p}$, al solito $p^{e_p} \| \binom{2n}{n}$

Vale $e_p = e(p,2n) - 2e(p,n) = \sum_{k=1}^{\infty} \left(\left[\frac{2n}{p^k}\right] - 2 \cdot \left[\frac{n}{p^k}\right] \right)$

che è pari a 0 se $\left[\frac{n}{p^k}\right]$ è pari, a 1 se $\left[\frac{n}{p^k}\right]$ è dispari.

Vale la seguente proprietà:

$p^{e_p} \le 2n$

Infatti, consideriamo p^t massima potenza di $p \le 2n$.

Si ha $p^t \le 2n < p^{t+1}$; $\left[\frac{2n}{p^{t+1}}\right] = 0 \Rightarrow \left[\frac{n}{p^{t+1}}\right] = 0$

Per $k \ge t+1$ gli addendi in Θ sono 0.

Ci sono al più t addendi non ~~molti~~ nulli $\Rightarrow e_p \le t$

Segue $p^{e_p} \le p^t \le 2n$ da cui la tesi.

(10.12.2010)

- Provato che $\left[\frac{2n}{a}\right] - 2\cdot\left[\frac{n}{a}\right] \begin{cases} 0 \text{ se } \left[\frac{2n}{a}\right] \text{ è pari} \\ 1 \text{ se } \left[\frac{2n}{a}\right] \text{ è dispari} \end{cases}$,

e dimostrati gli altri risultati:

$\binom{2n}{n} = \prod_{p \le 2n} p^{e_p}$ $\qquad e_p = \sum_{k=1}^{\infty} \left(\left[\frac{2n}{p^k}\right] - 2\cdot\left[\frac{n}{p^k}\right]\right)$ (*)

$p^{e_p} \le 2n$ (iv) $\qquad \binom{2n}{n} > \frac{4^n}{2\sqrt{n}}$ (v)

possiamo provare altre tre affermazioni: $(p \ge 3)$

(i) $p \ge \sqrt{2n} \Rightarrow e_p \le 1$

(ii) $\frac{2}{3}n < p \le n \Rightarrow e_p = 0$

(iii) $n < p < 2n \Rightarrow e_p = 1$

Dim.

(i) $p \ge \sqrt{2n} \Rightarrow p^2 \ge 2n \Rightarrow p^2 > 2n \Rightarrow \left[\frac{2n}{p^2}\right] = 0$

$\Rightarrow$ nella sommatoria (*) c'è al più un addendo $\neq 0$

$\Rightarrow e_p \le 1$

(ii) $\frac{2}{3}n < p \le n \Rightarrow \frac{2n}{p} < 3$, $\left[\frac{2n}{p}\right] \le 2$, $\left[\frac{2n}{p}\right] \ge 2 \Rightarrow \left[\frac{2n}{p}\right] = 2$

$\Rightarrow \left[\frac{2n}{p}\right] - 2\cdot\left[\frac{n}{p}\right] = 0$

$\Rightarrow p^2 = p\cdot p > p\cdot\frac{2n}{3} \ge 2n \Rightarrow p^2 > 2n$

$\Rightarrow$ quindi tutti gli addendi sono $0 \Rightarrow e_p = 0$

(iii) $n < p < 2n \Rightarrow \left[\frac{2n}{p}\right] = 1$, $\left[\frac{2n}{p^2}\right] = 0 \Rightarrow e_p = 1$

- Varrà anche:

$2^n = \sum_{h=0}^{n} \binom{n}{h}$

se n è dispari, $\binom{n}{k}$ appare due volte nella sommatoria, per $h=k$ e $h=n-k$

dunque $2^n = \dots + 2\cdot\binom{n}{k} + \dots \Rightarrow 2\cdot\binom{n}{k} \le 2^n \Rightarrow \binom{n}{k} \le 2^{n-1}$

- Verifichiamo anche che:

$\prod_{p \le x} p < 4^x$ (1)

Dim. È vero per $1 \le x \le 3$

Oss. Se si prova la (1) per ogni n dispari, $n \ge 3$, allora la (1) vale $\forall x \in \mathbb{R}$, $x \ge 3$. Infatti, $\forall x$, $\exists n$ dispari $/ n \le x < n+2$, e $\prod_{p \le x} p = \prod_{p \le n} p < 4^n \le 4^x$.

Proviamolo dunque per n dispari.

Come base dell'induzione poniamo il già verificato caso $n = 3$; supponiamo ora vera la (1) per qualunque dispari minore di n e verifichiamone la veridicità anche per n.

Sia $n = 2k \pm 1$, dove il segno viene scelto in maniera tale che k sia dispari.

Sia $k < p \leq n$; seguiranno $p \leq n \Rightarrow p \mid n!$, $p > k \Rightarrow p \nmid k!$.

Da $n = 2k \pm 1$ segue anche $n - k = k \pm 1 \leq k + 1$; sappiamo pure che $p > k$ e che sono entrambi dispari, dunque:

$p > k+1 \geq n-k \Rightarrow p > n-k \Rightarrow p \nmid (n-k)!$.

Allora $p \mid n!$, $p \nmid k!$, $p \nmid (n-k)!$, pertanto $p \mid \binom{n}{k}$, e generalizzando su tutti i primi di nostro interesse, $\prod_{k<p\leq n} p \mid \binom{n}{k} \leq 2^{n-1}$

Ne consegue che $\prod_{p\leq n} p = \prod_{k<p\leq n} p \cdot \prod_{p\leq k} p < 2^{n-1} \cdot 4^k = 2^{2k+n-1} \leq 2^{2n} = 4^n$ poiché $2k - 1 \leq n$. Questo prova la tesi.

- Raccogliendo ora un po' di risultati:

$$\binom{2n}{n} = \prod_{p\leq 2n} p^{e_p} = \prod_{p\leq n} p^{e_p} \cdot \prod_{n<p<2n} p^{e_p} \overset{(iii)}{\leq} \prod_{p\leq n} p^{e_p} \cdot \prod_{n<p<2n} p = \prod_{p\leq n} p^{e_p} \cdot P_n$$

$$\overset{(ii)}{\leq} \prod_{p\leq \frac{2}{3}n} p^{e_p} \cdot P_n = Q_n \cdot P_n$$

Per provare il teorema di Bertrand, sarebbe dunque sufficiente verificare che $P_n > 1$, ovvero che contenga almeno un fattore.

Utilizzando ancora i risultati precedenti:

$$Q_n = \prod_{p\leq \frac{2n}{3}} p^{e_p} \overset{(i)}{\leq} \prod_{p\leq \frac{2n}{3}} p \cdot \prod_{p<\sqrt{2n}} p^{e_p} \overset{(iv)}{<} 4^{\frac{2n}{3}} \cdot (2n)^{\sqrt{\frac{2n}{2}}} = 4^{\frac{2n}{3}} \cdot (2n)^{\sqrt{n}} \quad (vi)$$

$$\binom{2n}{n} = Q_n P_n \Rightarrow P_n = \binom{2n}{n} \cdot Q_n^{-1}$$

$$P_n > 4^n \cdot (2\sqrt{n})^{-1} \cdot 4^{-\frac{2n}{3}} \cdot (2n)^{-\sqrt{n}} = 4^{\frac{n}{3}} \cdot (2\sqrt{n})^{-1} \cdot (2n)^{-\sqrt{n}} = (2n)^x$$

$P_n = \prod_{n<p<2n} p < (2n)^{\pi(2n)-\pi(n)}$; ciò ci permette di dare una prima valutazione di x, come $x < \pi(2n) - \pi(n)$. Più precisamente, però:

$$x \cdot \log(2n) = \frac{n}{3} \cdot \log 4 - \log(2\sqrt{n}) - \sqrt{\frac{n}{2}} \cdot \log(2n)$$

$$= \frac{n}{3}\left[\log 4 - \frac{3}{n}\log(2\sqrt{n}) - \frac{3}{n}\cdot\sqrt{\frac{n}{2}} \cdot \log(2n)\right]$$

Tale quantità è maggiore di 1 per $n > 2500$. Segue che:

$$\pi(2n) - \pi(n) > x > \frac{n}{3 \cdot \log 2n} \quad \text{per } n > 2500$$

$$\pi(2n) - \pi(n) > \frac{n}{3 \cdot \log 2n} \quad \text{sempre (si può verificare per i casi } n \leq 2500)$$

il che prova il teorema di Bertrand.

Esiste anche una limitazione superiore:

$$4^n \geq \binom{2n}{n} \geq P_n = \prod_{n<p<2n} > n^{\pi(2n)-\pi(n)} \longrightarrow \pi(2n) - \pi(n) \log n \leq n \cdot \log 4$$

$$\pi(2n) - \pi(n) \leq \log 4 \cdot \frac{n}{\log n}$$

Torniamo ora al nostro problema di determinazione della primalità.
Nel 2002 è uscito un articolo di Agrawal, Kajal, Saxena, rilasciato anche nei Math Annals, denominato "Prime is in P", in cui viene proposto un algoritmo che determina la primalità di n che è deterministico, polinomiale, incondizionato. Questo algoritmo è divenuto noto come algoritmo AKS, e si svolge così:

input n

① se n è una potenza perfetta, $n = a^b$ con $a, b > 1$
return (FALSE)

② $r = 2$;
while $(r < n)$
{
if $((r,n) > 1)$ return (FALSE);
if $(\forall i,\ 1 \le i \le 4 \cdot [\log^2 n],\ n^i \neq 1 \pmod r)$ break;
$r = r + 1$
}

③ if $(r == n)$ return (TRUE)

④ for $(1 \le j \le 2 \cdot [\sqrt{r}]\,([\log n] + 1))$
{
if $(x+j)^n \neq x^n + j$ in $\frac{\mathbb{Z}_n[x]}{(x^r - 1)}$ return (FALSE)
}

⑤ return (TRUE)

Vediamo alcuni particolari:
Supponiamo n composto, $\exists p$, $p < n$, $p \mid n$.
Quando si arriva a ④, abbiamo un r, $r < n$, / $(r,n) = 1$
$n \in \mathbb{Z}_r^*$ e per $\mathbb{Z}_r^*$ $n > 4 \cdot [\log^2 n]$ $n > p > r$. Definiamo ora:

$$R_{\mathbb{Z}_n,r} = \frac{\mathbb{Z}_n[x]}{(x^r-1)} = a_{n,r}$$

$$R_{\mathbb{Z}_p,r} = \frac{\mathbb{Z}_p(x)}{(x^r-1)} = a_{p,r}$$

$\pi : a_{n,r} \longrightarrow a_{p,r}$

Dato $a(x) \in a_{p,r}$, definiamo:

$$C(a) = \{k \in \mathbb{Z} : a(x^k) = a(x)^k\}$$

$$D(k) = \{a(x) \in a_{p,r} : a(x^k) = a(x)^k\}$$

Si ha $1 \in C(a)$, $1 \in D(k)$, $\forall a, k$ perché la $a_{p,r}$ ha elementi
$C(a)$ e $D(k)$ sono anche chiusi rispetto al prodotto, infatti:

$k, k' \in C(a) \Rightarrow a(x^k) = a(x)^k$, $a(x^{k'}) = a(x)^{k'}$

$(a(x))^{kk'} = (a(x)^k)^{k'} = a(x^k))^{k'} = a(x^{kk'})$

$a, b \in D(k) \Rightarrow ab(x) = a(x)\, b(x)$

per ipotesi $a(x^k) = a(x)^k$, $b(x^k) = b(x)^k$

$(ab(x))^k = (a(x)\, b(x))^k = a(x)^k\, b(x)^k = a(x^k)\, b(x^k) = ab(x^k)$

Si ottiene il morfismo di Frobenius, infatti:

- poiché $a_{p,r}$ ha char p, $a(x)^p = a(x^p)$
- $(a(x)^p) = (a_0 + a_1 x + \dots + a_{r-1} x^{r-1})^p$

$= \sum (a_i x^i)^p = \sum a_i^p (x^p)^i = \sum a_i (x^p)^i = a(x^p)$

(14.12.2010)

Abbiamo definito:

$C(a) = \{k \in \mathbb{Z} : a(x^k) = a(x)^k\}$ dove $a(x) \in a_{p,r} = \frac{\mathbb{Z}_p[x]}{(x^r-1)}$

$D(k) = \{a \in a_{p,r} : a(x^k) = a(x)^k\}$

Si ha che:

- $C(a)$, $D(k)$ sono sempre chiusi rispetto al prodotto
- $1, p \in C(a)$; $1 \in D(k)$

- Definiamo ora un morfismo:

$\tau : a_{p,r} \longrightarrow \mathbb{F}$

$a(x) \mapsto a(\alpha)$

dove $\mathbb{F}$ è il campo di spezzamento di $x^r - 1$ su $\mathbb{Z}_p$, $\alpha \in \mathbb{F}$ è radice primitiva r-esima di 1, $U_r \leq \mathbb{F}^*$, $U_r = \langle \alpha \rangle$

Si verifica agevolmente che τ è ben definito: infatti se $b(x) = a(x) + \eta(x)(x^r - 1)$, allora $\tau(b) = b(\alpha) = a(\alpha) + \eta(\alpha)(\alpha^r - 1) = a(\alpha)$.

- Definiamo anche l'insieme $S(n) = \tau(D(n))$.

Supponiamo che n sia composto, n non potenza perfetta, quindi $\exists\, p, q \;/\; p, q \mid n$

Poniamo $t = |\langle p, n \rangle_r|$ dove $\langle p, n \rangle_r \leq \mathbb{Z}_r^*$ è il sottogruppo di $\mathbb{Z}_r^*$ generato da p ed n.

Allora otteniamo un primo risultato di rilievo: $|S(n)| < n^{2\lfloor \sqrt{t} \rfloor}$

Dim. Sia $I = \{n^u p^v : 0 \leq u, v \leq \lfloor \sqrt{t} \rfloor\}$

Se $(u, v) \neq (u', v')$, i numeri $n^u p^v$ e $n^{u'} p^{v'}$ sono diversi, poiché q vi appare con potenza diversa.

Dunque $|I| = (\lfloor \sqrt{t} \rfloor + 1)^2 > t$.

Ora, $\langle p, n \rangle_r = \{n^u p^v \bmod r : u, v \in \mathbb{Z}\}$, e $|\langle p, n \rangle_r| = t$.

Poiché $|I| > t$, devono esistere $k, k' \in I$, $k \neq k'$ e $k \equiv k' \pmod r$

Prendiamo $\beta \in S(n)$. Per definizione $\beta = \tau(a)$, con $a \in D(n)$.

Se $a \in D(n)$, allora $n \in C(a)$; ma del resto $p \in C(a)$, e $C(a)$ è ~~chiusa~~ chiusa rispetto al prodotto, dunque:

$$\Rightarrow I \subseteq C(a) \Rightarrow k, k' \in C(a)$$

$$\Rightarrow a(x^k) = [a(x)]^k \quad \text{e} \quad a(x^{k'}) = [a(x)]^{k'} \quad (*)$$

Sappiamo che $\beta = \tau(a) = a(\alpha)$, da cui:

$$\Rightarrow \odot \begin{cases} \beta^k = [a(\alpha)]^k = a(\alpha^k) \\ \beta^{k'} = [a(\alpha)]^{k'} = a(\alpha^{k'}) \end{cases} \text{per } (*)$$

Abbiamo che $\alpha^k = \alpha^{k'}$ perché $k \equiv k' \bmod r$ e α è radice r-esimo di 1

$$\Rightarrow a(\alpha^k) = a(\alpha^{k'}) \overset{\odot}{\Rightarrow} \beta^k = \beta^{k'}$$

$$\Rightarrow \beta \text{ è zero di } x^k - x^{k'} \in \mathbb{Z}_p[x]$$

Ogni β in $S(n)$ è zero di $x^k - x^{k'}$.

Poiché però siamo in $\mathbb{Z}_p$, che è un campo:

$$\Rightarrow \text{il numero di zeri di } x^k - x^{k'} \text{ è} \leq \deg(x^k - x^{k'}) \leq \max(k, k')$$

$$\Rightarrow |S(n)| \leq \max(k, k') < n^{2[\sqrt{t}]}$$

dal momento che:

$$k, k' \in I = \{n^u p^v : 0 \leq u,\ v \leq [\sqrt{t}]\}$$

$$k, k' = n^u p^v < n^{u+v} \leq n^{2[\sqrt{t}]}$$

$$\max(k, k') < n^{2[\sqrt{t}]}$$

- Nelle stesse ipotesi di prima, supponiamo che si abbia $(x+j)^n = x^n + j$ in $\mathcal{A}_{p,r}$ per tutti i j tali che $1 \leq j \leq \ell$.

Allora $|S(n)| \geq 2^{\min(\ell, t)} - 1$.

Dim. Poniamo per comodità $m = \min(\ell, t)$, e definiamo l'insieme:

$$V = \left\{ \prod_{j=1}^{m} (x+j)^{e_j} : e_j = 0, 1 \ ; \ \sum e_j < m \right\}$$

Abbiamo che:

- $D(n) = \{a(x) : a(x)^n = a(x^n)\}$
- $a(x) = x + j \qquad 1 \leq j \leq \ell$
- $a(x)^n = (x+j)^n$
- $a(x^n) = x^n + j$

] uguali per ipotesi

Poiché $m \leq \ell$, sono uguali $(x+j)^n$ e $x^n + j$, il che implica:

$$\Rightarrow (x+j)^{e_j} \in D(n)$$

$$\Rightarrow \prod_{j=1}^{m} (x+j)^{e_j} \in D(n) \quad \forall (e_1, e_2, \dots, e_m) \quad e_i = 0, 1$$

e:

$$\deg\left(\prod_{j=1}^{m} (x+j)^{e_j}\right) \leq \sum e_j < m \leq t = |\langle p, n \rangle_r| < r$$

Ne segue che $|V| = 2^m - 1$.

Poiché $\tau(D(n)) = S(n)$, $|V| = 2^m - 1$, $V \subseteq D(n)$, è sufficiente provare che $\tau|_V$ è iniettiva.

Prendiamo dunque $g, h \in V \subseteq D(n)$: la cosa implica $\begin{cases} n \in C(g) \cap C(h) \\ p \in C(g) \cap C(h) \end{cases}$

Sappiamo che tutti gli interi $n^n p^r \in C(g) \cap C(h)$.

Supponiamo che $\tau(g) = \tau(h)$, allora $g(\alpha) = h(\alpha)$.

Tutti i $k \in \langle n, p \rangle_r$ sono in $C(g) \cap C(h)$;

$\forall k \in \langle n, p \rangle_r$, $g(x^k) = g(x)^k$, $h(x^k) = h(x)^k$

$\Rightarrow g(\alpha)^k = h(\alpha^k) \Rightarrow g(\alpha^k) = h(\alpha^k)$

Segue che tutti gli α^k con $k \in \langle p, n \rangle_r$ sono zeri di $g-h$, dove $g, h \in V$, quindi $g-h$ ha t zeri distinti, perchè $\alpha^k \neq \alpha^{k'}$ se $k, k' \in \langle p, n \rangle_r$ perchè $k \not\equiv k' \pmod r$ e α è radice primitiva r-esima di 1.

Sia g che h hanno grado $< m \leq t$, dunque $\deg(g-h) < t$, ma $g-h$ ha t zeri distinti, pertanto non potrà che essere $g-h \equiv 0$.

- Arriviamo dunque alla limitazione $2^{\min(\ell,t)} - 1 \leq |S(n)| < n^{2\lfloor\sqrt{t}\rfloor}$

Supponiamo ora che ci sia un n composto, non potenza perfetta, che arriva al passo 4 dell'algoritmo, e supera lo sbarramento per ℓ / $1 \leq j \leq \ell$ ("le ipotesi")

Ora, nelle ipotesi, se $\ell = 2 \cdot \lfloor\sqrt{r}\rfloor \cdot (\lfloor \log n \rfloor + 1)$, segue che $2^{\min(\ell,t)} - 1 > n^{2\lfloor\sqrt{t}\rfloor}$, il che contraddice la nostra limitazione precedente

Dim. Riscriviamo la disuguaglianza come:

$$2^{\min(\ell,t)} - 1 > 2^{2\lfloor\sqrt{t}\rfloor \cdot \log n}$$

A questo punto, è sufficiente provare che $\min(\ell, t) > 2\lfloor\sqrt{t}\rfloor \cdot \log n$, ovvero che: $\begin{cases} \ell > 2\lfloor\sqrt{t}\rfloor \cdot \log n & (i) \\ t > 2\lfloor\sqrt{t}\rfloor \cdot \log n & (ii) \end{cases}$

(i) è vera poichè $\ell = 2\lfloor\sqrt{r}\rfloor \cdot (\lfloor \log n \rfloor + 1) > 2\lfloor\sqrt{t}\rfloor \cdot \log n$ e $r \geq t$;

quanto a (ii), sappiamo che $\text{per}_{2,r}^* n > 4 \cdot \log^2 n$, e poichè $t = |\langle n, p \rangle_r|$, si ha $t \geq \text{per}_{2,r}^* n > 4 \cdot \log^2 n$, e infine:

$t > 4 \cdot \log^2 n \Rightarrow \sqrt{t} > 2 \cdot \log n \Rightarrow t \geq 2 \cdot \sqrt{t} \cdot \log n \geq 2 \cdot \lfloor\sqrt{t}\rfloor \cdot \log n$.

- AKS $\in$ P

Iniziamo osservando che la difficoltà sta tutta nella grandezza di r. Dobbiamo trovare r, $(r, n) = 1$, $\text{per}_{2,r}^* n > 4 \cdot \log^2 n$.

A questo punto, sarebbe sufficiente provare che $r \in O(\log^k n)$.

Dimostriamo che se $k = \lfloor 16 \cdot \log^5 n \rfloor + 1$, allora si trova un r che va bene tale che $r \leq k$, oppure si fattorizza n come (n, r).

Dim. $Q = \prod_{i=1}^{[4\cdot\log^2 n]} n^i - 1$

Se $r \nmid Q$, allora $r \mid n^i - 1 \quad \forall i$

$n^i \not\equiv 1 \pmod r \quad \forall i \quad 1 \le i \le 4\cdot\log^2 n$

per $\exists r^*$ $n > 4\cdot\log^2 n$

Supponiamo che tutti gli interi $1, 2, \dots, k$ dividano Q. Allora:

$\Rightarrow \quad \mathrm{mcm}(1, 2, \dots, k) \mid Q$

$\Rightarrow \quad d_k \mid Q \quad \Rightarrow \quad Q \ge d_k > 2^k$

Si ha:

$$Q = \prod_{i=1}^{[4\cdot\log^2 n]} n^i - 1 < \prod_{i=1}^{[4\cdot\log^2 n]} n^i < \prod_{i=1}^{[4\cdot\log^2 n]} n^{(4\cdot\log^2 n)} = n^{[4\cdot\log^2 n]^2} < n^{(4\cdot\log^2 n)^2}$$

$$< n^{16\cdot\log^4 n} = 2^{16\cdot\log^5 n}$$

Se $1, 2, \dots, k \mid Q$, dunque, $2^k < Q < 2^{16\cdot\log^5 n}$.

Se $k > 16\cdot\log^5 n$, la disuguaglianza non vale, e quindi c'è un r tra 1 e k tale che $r \nmid \prod n^i - 1$, ovvero:

$\exists\, r \in \mathbb{N},\ 1 \le r \le [16\cdot\log^5 n] + 1 \ / \ r \nmid \prod_{i=1}^{[4\cdot\log^2 n]} n^i - 1$

Nel caso in cui risulti $(n, r) > 1$, allora si ha fattorizzazione n;

se invece $(n, r) = 1$, allora $n \in \mathbb{Z}_r^*$.

L'algoritmo restituisce in una risposta in un tempo logaritmico e dunque polinomiale.

(17.12.2010)

TECNICHE DI FATTORIZZAZIONE

- Metodo di Pollard α $p-1$:

  Per il Piccolo Teorema di Fermat, $a^{p-1} \equiv 1 \pmod p$, dunque $p \mid a^{p-1}-1$.

  Ovviamente se $p-1 \mid E$ si ha $a^E \equiv 1 \pmod p$, ovvero $p \mid a^E - 1$.

  Supponiamo di voler fattorizzare n e sia $p \mid n$.

  Se $p-1 \mid E$ allora $p \mid (a^E-1, n)$

  - Se non va bene $(a^E-1, n) = n$
  - ok se $1 < (a^E-1, n) < n$

  Come trovare E?

  - Per esempio, porre $E = k!$, $k = 2,3,\dots$
  - Se p non è grande e $p-1$ si fattorizza in parti piccole, $p-1 \mid k!$

  Definiamo un numero m B-smooth se $m = \prod p_i^{e_i}$ si fattorizza in maniera tale per cui $p_i^{e_i} \le B$.

  Sia $\mathcal{B}_B$ l'insieme dei numeri B-smooth per un dato B.

  Se $m \in B$, si calcola (a^m-1, n), e $p-1 = \prod p_i^{e_i}$ con $p_i^{e_i} \le B$.

  Il metodo non è efficiente nel caso, per esempio, dei numeri RSA, in cui $n = pq$ e $p-1$, $q-1$ non sono B-smooth per B "piccolo".

- Metodo $p+1$

  Sia n da fattorizzare. Sappiamo che $p \mid n$, $p \mid U_{p-(\frac{\Delta}{p})}$.

  Al solito $\Delta = h^2-4k$, $U_n(h,k) = W_n(0,1,h,k)$.

  Se $(\frac{\Delta}{p}) = -1$, allora $p \mid U_{p+1}$.

  Sappiamo che, se $m \mid n$, allora $U_m \mid U_n \quad ((a^E-1) \bmod n, n)$

  Si giunge a $p+1 = \prod p_i^{e_i}$, $p_i^{e_i} \le B$, ma all'inizio è necessario cercare Δ tale che $(\frac{\Delta}{n}) = -1 \Rightarrow \exists\, p \mid n : (\frac{\Delta}{p}) = -1$

- Metodo ρ

  Si basa sul risultato secondo cui, scelte 23 persone in maniera casuale, la probabilità che due di esse compiano gli anni lo stesso giorno è $> \frac{1}{2}$.

  In generale, se abbiamo un insieme di enti che si classificano in q classi, e prendiamo un insieme di enti di cardinalità $> \sqrt{q}$, la probabilità che due enti siano nella stessa classe è $> \frac{1}{2} \cdot c^{-1}$ con c molto vicino ad 1.

Utilizziamo questo risultato come ausilio per la fattorizzazione.
Se $p \mid n$, consideriamo le p classi di resto mod p.
Calcoliamo $x_1, x_2, \dots, x_j, x_m$, e consideriamo $(x_i - x_j, n)$.
Se m è $O(\sqrt{p})$, allora la probabilità che $\forall (i,j)$ esistano i, j tali che $i \neq j$, $x_i \equiv x_j \pmod p$, è $> \frac{1}{2}$.
Supponiamo di fabbricare una sequenza casuale ricorsiva $x_n = f(x_{n-1})$, a cominciare da un seme x_0.
Un esempio è dato da un random number generator in informatica, come $\begin{cases} x_0 = \text{seme} + a \\ x_n = x_{n-1}^2 + a \mod M \end{cases}$
Dopo un certo numero di passi ci si ricondurà ad un ciclo: $x_i = x_j$ con $j = i + kT \pmod p$
In particolare esisterà s tale per cui $x_s = x_{2s} \pmod p$.
Possiamo operare nel seguente modo:

$f(x_0) = x_1$ $\quad$ $x_2 = f(x_1) = f^2(x_0)$

$x_1 \to x_2 \to x_3 \to \dots \to x_m$ $\quad$ $x_2 \to x_4 \to x_6 \to \dots \to x_{2m}$

Una volta trovato s, si ha che $x_{2s} - x_s \mid n$ e si può fattorizzare. Grazie al risultato iniziale, s si troverà in un tempo conveniente.

- Metodo della base di Dixon

Il metodo classico consiste nel trovare due quadrati x^2, y^2, tali per cui $x^2 \equiv y^2 \pmod n \Rightarrow n \mid (x-y)(x+y)$
e $x \not\equiv \pm y \pmod n \Rightarrow \begin{cases} n \nmid x-y \\ n \nmid x+y \end{cases}$. In tal caso $(n, x-y)$ e $(n, x+y)$ sono fattori propri.
Sia ancora $\mathcal{B}$ l'insieme dei numeri B-smooth.

[Diciamo che a è un B-numero se:
$b = a^2 \mod n$ è B-smooth, cioè $b = \prod_{i=1}^{t} p_i^{e_i}$ $\quad p_i^{e_i} \leq B$

Supponiamo che $a_1, a_2, \dots, a_i, \dots$ siano B-numeri.
Allora $b_i = a_i^2 \mod n = \prod_{j=1}^{t} p_j^{\alpha_{ij}}$
Creiamo $v_i = (\dots, \alpha_{ij} \bmod 2, \dots)$ vettore di t componenti:
$v_i \in \mathbb{Z}_2^t$
Supponiamo di aver trovato s B-numeri $a_1, a_2, \dots, a_s$ tali che i vettori $v_1, v_2, \dots, v_s$ sono linearmente dipendenti in $\mathbb{Z}_2^t$.

Ciò accade certamente se $s > t$, poiché lo spazio ha dimensione t.
Senza restrizioni possiamo supporre, essendo in $\mathbb{Z}_2$, $\sum_{i=1}^{s} v_i = 0$ su $\mathbb{Z}_2$.
Sarà: $\sum_{i=1}^{s} v_i = (\ldots, \sum_{i=1}^{s} a_{ij}, \ldots) = 0$

$v_i = (\ldots, a_{is}, \ldots)$ in $\mathbb{Z}_2$

il che implica che $\sum_{i=1}^{s} a_{ij}$ sia pari.

Vediamo ora cosa si può dire a proposito del prodotto. Si ha:

$$\prod_{i=1}^{s} b_i = \prod_{i=1}^{s} \prod_{j=1}^{t} p_j^{a_{ij}} = \prod_{j=1}^{t} p_j^{\sum_{i=1}^{s} a_{ij}} = z^2 \quad \text{con } z \text{ intero.}$$

Allora:

$$z^2 = \prod_{i=1}^{s} b_i \equiv \prod_{i=1}^{s} a_i^2 = \left(\prod_{i=1}^{s} a_i\right)^2 \pmod{n}$$

Dunque $z^2 \equiv a^2 \pmod{n}$, e $(n, z-a)$, $n(z+a)$ sono fattori propri.

CURVE ELLITTICHE

Consideriamo una cubica nella forma standard $y^2 = x^3 + ax + b$, non singolare, ovvero tale per cui, passando a coordinate omogenee ed essendo $x_2^2 x_0 = x_1^3 + a \cdot x_1 \cdot x_0^2 + b \cdot x_0^3$, non esiste alcun punto che verifichi contemporaneamente $\frac{\partial F}{\partial x_0} = 0$, $\frac{\partial F}{\partial x_1} = 0$, $\frac{\partial F}{\partial x_2} = 0$, se F è $x_2^2 x_0 - x_1^3 - a \cdot x_1 \cdot x_0^2 - b \cdot x_0^3 = 0$.

Prendiamo un campo k. Definiamo l'insieme dei punti k-razionali come $E(k) = \{(x,y) : y^2 = ax^3 + ax + b, (x,y) \in k^2\}$. Si può dimostrare che questo insieme ha una struttura di gruppo rispetto all'operazione che definiremo ora.

Definiamo ora l'operazione di corda tangente. Sia O un punto qualsiasi appartenente alla curva ellittica E. Se $P, Q \in E$, si traccia la corda e si definisce come $P * Q$ il terzo punto (che esiste ed è unico) di intersezione della corda con E. A questo punto si uniscono O e $P * Q$ e si chiama $P + Q$ il punto di intersezione della retta con la curva distinto da O e $P * Q$.

Se $P = Q$, si prende la retta tangente, invece che la corda.

Si dimostra che l'operazione è commutativa, associativa, esistono elemento neutro e inverso, e pertanto si ha la struttura di gruppo.

Prendiamo $O = Y_\infty$, punto all'infinito dell'asse y, di coordinate proiettive $(x_1, x_2, x_0) = (0, 1, 0)$. Allora graficamente si trova subito che, se $P * Q = (x, y)$, allora $P + Q = (x, -y)$.

Vediamo ora di determinare, sotto tale condizione su 0, le coordinate di $P * Q$, sapendo che $P = (x_1, y_1)$ e $Q = (x_2, y_2)$.

- Sia $x_1 \neq x_2$ $(\Rightarrow P_1 \neq P_2)$.

Allora dei semplici calcoli di geometria analitica ci portano a:

$$\frac{y - y_1}{y_2 - y_1} = \frac{x - x_1}{x_2 - x_1} \longrightarrow y = y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$$

$$\begin{cases} y = y_1 + m(x - x_1) \\ y^2 = x^3 + ax + b \end{cases} \qquad m = \frac{y_2 - y_1}{x_2 - x_1}$$

$$(y_1 + m(x - x_1))^2 - x^3 - ax - b = 0 \longrightarrow (x_1 - x)(x_2 - x)(x_3 - x) = 0$$

$$\dots + m^2 x^2 + \dots - x^3 - ax - b = 0 \qquad \dots + (x_1 + x_2 + x_3)x^2 + \dots = 0$$

Per il principio di identità dei polinomi dovrà essere:

$$m^2 = x_1 + x_2 + x_3 \Rightarrow \begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= y_1 + m(x_3 - x_1) \end{aligned}$$

dunque $P * Q = (m^2 - x_1 - x_2,\ y_1 + m(x_3 - x_1))$, e

$P + Q = (m^2 - x_1 - x_2,\ -y_1 - m(x_3 - x_1))$

- Se invece $x_1 = x_2$:
  - in un caso $y_2 = -y_1$, ma allora $P_1 = -P_2$ e $P_1 + P_2 = 0$;
  - nell'altro $y_2 = y_1$, allora $P_1 = P_2$.

Dal teorema della funzione implicita la tangente a P_1 ha coefficiente angolare $m = -\frac{\partial F / \partial x}{\partial F / \partial y}$.

Calcolando:

$$\frac{\partial F}{\partial x} = -3x^2 - a \qquad \frac{\partial F}{\partial y} = 2y \qquad m = \frac{3x^2 + a}{2y}$$

dunque:

$$m = \frac{3x_1^2 + a}{2y_1} \qquad x_3 = m^2 - 2x_1 \qquad y_3 = y_1 + m(x_3 - x_1)$$

$P+Q$ è $(x_3, -y_3)$

(21.12.2010)

$(E, +)$ è un gruppo abeliano, di elemento neutro $0 = y_\infty$, e di inverso generico $-(x, y) = (x, -y)$

Se si vogliono utilizzare coordinate affini, poichè il punto 0 è all'infinito, sarà necessario implementare a parte i casi che coinvolgono 0.

```
if (A == 0) return (A);
if (B == 0) return (B);
if (a2 == -b2) return (0).
```

Teor. $\#E_q(f(x)) = 1 + \sum_{x \in GF(q)} (\theta(f(x)) + 1)$

dove θ è il carattere quadratico di $GF(q)$, ovvero:

- $\theta(0) = 0$.
- $\theta(a) = 1$ se a è un quadrato;
- $\theta(a) = -1$ se a non è un quadrato.

Si noti che, se $q = p$, allora $\theta(a) = \left(\frac{a}{p}\right)$.

Dim. L'1 conta 0.

Supponiamo ora $f(x) \neq 0$. Se $f(x)$ è un quadrato in $\mathbb{K} = GF(q)$ allora $\theta(f(x)) = 1$ e nella somma c'è un contributo di 2; del resto la $y^2 = f(x)$ ha due soluzioni $\pm a$ quindi in effetti ci sono due punti in E: (x, a), $(x, -a) \in E$.

Se $f(x)$ non è un quadrato, allora $\theta(f(x)) = -1$ e nella somma c'è un contributo di 0, e infatti la $y^2 = f(x)$ non possiede in tal caso soluzioni.

Supponiamo ora che gli $f(x)$ siano equidistribuiti, e che dunque nella metà dei casi $\theta(f(x)) = 1$, e nell'altra metà $\theta(f(x)) = -1$.

Nel caso ci sarebbero $\frac{1}{2}(q-1)$ quadrati e $\frac{1}{2}(q-1)$ non quadrati, oltre che lo 0.

Si avrebbe pertanto $1 + 2 \cdot \frac{q-1}{2} + 0 \cdot \frac{q-1}{2} = 1 + q - 1 = q$, e perciò

$\#E_q(f(x)) = q + 1$

In generale, si può dimostrare avere $\#E_q(f(x)) = q + 1 + \varepsilon$, con $|\varepsilon| \leq 2\sqrt{q}$ (Hasse). Pertanto:

$$q + 1 - 2\sqrt{q} \leq \#E_q(f(x)) \leq q + 1 + 2\sqrt{q}$$

$$(\sqrt{q} - 1)^2 \leq \#E_q(f(x)) \leq (\sqrt{q} + 1)^2$$

che definisce un intervallo $I_q = [(\sqrt{q}-1)^2, (\sqrt{q}+1)^2]$

Un altro risultato attribuito a Deuring afferma che, $\forall n \in I_p$ primo, $\exists\, E_p(f(x)) : \#E_p(f(x)) = N$.

Un esempio può essere dato dal seguente set:

$\mathbb{K} = \mathbb{Z}_5$ $\quad E_5 \not\ni (-1,-1)$ $\quad y^2 = x^3 - x - 1$

$$\#E_5(-1,-1) = 1 + \sum_{x \in \mathbb{Z}_5} \left(\left(\frac{f(x)}{5}\right) + 1\right)$$

$x = 0$	$f(0) = -1$	$y^2 = -1 = 4$	$y = \pm 2$	$(0,2), (0,-2)$
$x = 1$	$f(1) = -1$	"	"	$(1,2), (1,-2)$
$x = 2$	$f(2) = 5 = 0$	$y^2 = 0$	$y = 0$	$(2,0)$ doppio
$x = 3$	$f(3) = 23 = 3$	$\left(\frac{3}{5}\right) = 1$		non ci sono punti
$x = 4$	$f(4) = 59 = 4$	$\left(\frac{59}{5}\right) = \left(\frac{4}{5}\right) = 1$		$(4,2), (4,3)$

In questo caso, Hasse ci dice che $I_5 = [(\sqrt{5}-1)^2, (\sqrt{5}+1)^2] = [2, 10]$, e infatti $\#E_5(-1,-1) = 8$, mentre Deuring che esiste una curva per ogni $N \in [2,10]$ tale per cui sia N la cardinalità, in questo caso esse esplicitamente sono:

- $x^3 + 2x$ — 2
- $x^3 + 4x + 2$ — 3
- $x^3 + x$ — 4
- $x^3 + 3x + 2$ — 5
- $x^3 + 1$ — 6
- $x^3 + 2x + 1$ — 7
- $x^3 + 4x + 4$ — 8
- $x^3 + x + 1$ — 9
- $x^3 + 3x$ — 10

Sia ora R anello. Definiamo:

$E_R(f(x)) = \{(x,y) : y^2 = f(x)\} \cup \{0\}$ $\qquad f(x) = x^3 + ax + b.$

La somma dipende da $\begin{cases} m = (y_2 - y_1)\cdot(x_2 - x_1)^{-1} & \text{punti diversi} \quad x_1 \neq x_2 \\ m = (3x_1^2 + a)\cdot(2y_1)^{-1} & \text{2P} \qquad\qquad y_1 \neq 0 \end{cases}$

Quindi + è definita in $E_2(f(x))$ sempre, tranne i casi in cui $x_1 \neq x_2$ ma $x_2 - x_1 \notin R^*$, e $y_1 \neq 0$ ma $y_1 \notin R^*$

Se R non è un campo, $R^* \neq R - \{0\}$, e quindi la + non è ovunque definita. Dove è definita "funziona tutto", cioè $(A + B) + C = A + (B + C)$ se le somme sono definite.

Se in $E_R(f(x))$ non si può calcolare $A + B$, la situazione può essere comunque di nostro interesse.

<u>killian</u>

$E_n(a,b)$ $\qquad p \mid n$

$\pi : E_n(a,b) \longrightarrow E_p(a,b)$ $\qquad$ riduce modulo p

Se $y^2 = ax^3 + bx + c \mod n$

$y^2 = ax^3 + bx + c \mod p$

Esempio:

$p = 5,\ q = 7 \qquad E_5(-1,1) = 8$ punti

$E_7(-1,-1) = \{0, (3,3), (3,4), (5,0)\}$

$\#E_5 = 8$

$\#E_7 = 4$

Verrebbe da chiedersi se $\#E_{35} = \#E_5 \cdot \#E_7 = 8 \cdot 4 = 32$, in analogia a come, per esempio, c'è una biezione tra $\mathbb{Z}_{35}$ e $\mathbb{Z}_5 \times \mathbb{Z}_7$ data dal teorema cinese del resto.
La risposta è negativa, ma vale un risultato simile, infatti è possibile mettere in biezione $E_{35}(f(x)) - 0$ e $(E_5 f(x) - 0) \times (E_7 f(x) - 0)$, e così in generale per p, q qualsiasi.

Vediamo ora come sia possibile calcolare tP, $t \in \mathbb{N}$, per duplicazioni successive

Sia $E_{35} = (-1, -1)$, $P = (24, 17)$.

$Q = 2P = (24, 17) + (24, 17) = (26, 7) = (5, 0)$

$2Q$ non esiste, poiché $y_1 = 7$ e 7 non ha inverso in $\mathbb{Z}_{35}$.

Dunque l'algoritmo restituisce 7.

Questo pone le basi per l'algoritmo ECM.

ALGORITMO ECM (per fattorizzare n)

① si sceglie un limite B (esempio 10 000);

② si trovano $E_n(a,b)$ e $(x,y) \in E_n(a,b)$

random $x, y, a \in [0, n-1]$

$b = y^2 - x^3 - ax \mod n$

$g = (4a^3 + 27b^2)\ n$

se $g > 1$ e $g < n$ ha fattorizzato n se $g = 0$ goto

allora $g \neq 0$ $E = E_n(a,b)$ $P(x,y) \in E_n(a,b)$

③ Calcolo i multipli di $P(x,y)$ così:

for $1 \leq i \leq \pi(B)$

se $p_i^{a_i} \leq B$

for $1 \leq j \leq a_i$

$P = p_i P$

STOP se fallisce il calcolo, si ha trovato un fattore

④ se fallisce, goto 1

ALGORITMO ECPP (primalità)

① random $a, b \in [1, N-1]$

si verifica che $(4a^3 + 27b^2, N)$

② calcolo $m = |E_N(a,b)|$

si applica Atkin, Elkies $O(\log(p)^5)$

Se l'algoritmo non funziona correttamente STOP (N non è primo)

Se l'algoritmo dà un risultato fuori da I_n STOP, non è primo

③ Cerco q probabilmente primo (isprime) tale per cui

$m = kq$, $N > q > (N^{1/4} + 1)^2$

Se fallisce, goto ①

④ Random $x \in [1, N-1]$ cerco $Q = x^3 + ax + b$ tale che $\left(\frac{Q}{N}\right) \neq -1$.

Se $\left(\frac{Q}{N}\right) = 0$ si ha fattorizzato N STOP

Allora $\left(\frac{Q}{N}\right) = 1$ Calcolo y : $y^2 = Q \mod N$ come se N fosse primo.

Se il calcolo non si può eseguire, o dà un risultato sbagliato, STOP (N non è primo)

Altrimenti $(x, y) \in E_N(a, b)$, $P = (x, y)$

⑤ Calcolo $U = \frac{m}{q} P = kP$

Se $U = 0$ goto ④. Supponiamo $U \neq 0$.

Calcolo $V = qU = mP = |E_n(a,b)|\, P$

Se $V \neq 0$, allora N è certamente composto.

Altrimenti "q primo $\Rightarrow$ N primo"

Per giustificare quest'ultima affermazione, siano $qU = 0$, $U \neq 0$, q primo.

Dimostriamo che n è primo.

Prendiamo $p \mid N$, p primo. $qU = 0$ in $E_p(a,b)$, poichè $qU = 0$ in $E_N(a,b)$.

Se q è primo poichè $U \neq 0$:

per $_{E_p(a,b)}$ $U = q$ $\qquad q \leq |E_p(a,b)| \leq (\sqrt{p}+1)^2$

Poichè valgono:

$(\sqrt{p}+1)^2 \geq q > (\sqrt[4]{N} + 1)^2$

$\sqrt{p} + 1 > \sqrt[4]{N} + 1$

$\sqrt{p} > \sqrt[4]{N}$

$p > \sqrt{N}$

Ne discende il certificato di primalità che consiste nell'elenco dei $q_1, q_2, \dots, q_s$ e delle relative curve.

$(a_1, b_1), (a_2, b_2), \dots, (a_s, b_s)$ $\qquad m_1, m_2, \dots, m_s$

(13.01.2011)

$E: y^2 = x^3 + ax + b$

$E(\mathbb{K})$: se $a, b \in \mathbb{K}$

Se $\mathbb{K} = GF(q)$, allora $E(\mathbb{K}) = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$, con $d_1 | d_2$ e $d_1 | q-1$.

Dati k intero e $P \in \mathbb{K}$, noto $Q = kP$, è difficile ricavarne uno dei due conoscendo l'altro.

- Immersione del messaggio nella curva $E(\mathbb{K})$

  Il messaggio è un intero $\boxed{m}$ $\longleftrightarrow$ blocco del testo

  Il problema consiste nel come immergere m in E : $m \xrightarrow{?} E$

  Il metodo utilizzato principalmente è di tipo probabilistico.

  Si fissa $\boxed{k}$, e si fa variare j, $0 \le j \le k-1$, fino a che $x = km + j$ è tale per cui $x^3 + ax + b$ è un quadrato, cioè $(x, y) \in E$ dove $x = km + j$ e $y^2 = x^3 + ax + b$.

  $m \longleftrightarrow (km + j = x, \sqrt{x^3 + ax + b})$

  Il ricevente ha $km + j$, e calcola $\left[\frac{km+j}{k}\right] = \left[m + \frac{j}{k}\right] = m \quad \left(\frac{j}{k} < 1\right)$

- Diffie - Hellman (scambio delle chiavi)

  E pubblica, $P \in E$

  $A \xrightarrow{aP} B$ (a random) (baP)

  $A \xleftarrow{bP} B$ (abP) (b random)

- Massey - Omura

  $K = \mathbb{Z}_p$

  $A \xrightarrow{e_A P} B$

  – calcola $e_A d_A$ $\quad e_B, e_D \quad e_B e_D = 1 \mod |E|$

  $e_A d_A = 1 \mod |E|$ $\quad A \xleftarrow{e_B e_A P} B$

  e A riceve $e_A P$ $\quad A \xrightarrow{d_A e_B e_A P = e_B P} B$

  si calcola $d_A e_A P = P$ $\quad B$ riceve $P = d_B e_D P \mod |E|$

  – Richiede autenticazione, altrimenti C può infiltrarsi mandando $e_C e_A P$.

- RSA ellittico

  (A) $n = pq$

  sceglie a, b che determinano E

  A ha due curve $\begin{cases} E_p \\ E_q \end{cases}$ A calcola $\begin{matrix} |E_p| \\ |E_q| \end{matrix}$

  A prende e_A : $(e_A, |E_p|) = 1$, $(e_A, |E_q|) = 1$

  calcola $d_p = e_A^{-1} \mod |E_p|$, $d_q = e_A^{-1} \mod |E_q|$

  (A) pubblica $\boxed{n, a, b, e_A}$

B vuole inviare un messaggio m ad A

B considera E modulo n $\quad y^2 = x^3 + ax + b$

$m \longrightarrow P \in E$

$B \xrightarrow{e_A P} A$

A riceve $e_A P \in E \mod n$

$e_A P \mod p \in E$ in p

" in q

$d_p e_A P \pmod p = S$ è P su $E \mod p$

$d_q e_A P \pmod q = T$ " $\mod q$

A usa TCR e trova $P = S \mod p$, $P = T \mod q$.

- El Gamal

A pubblica E, $P \in E$, $r_A P$, dove r_A intero random segreto.

$B \xrightarrow{q} A$ calcola k random; B manda ad A

$(kP,\ kr_A P + Q)$, $Q \in E$

operazione su E

A calcola $r_A kP$ e poi ricava Q facendo $kr_A P + Q$

- Menezes Van Storm $E \mod p$

il messaggio è una coppia di interi $(m_1, m_2) = M \quad m_1, m_2 < p$

A pubblica $E \mod p$, $P \in E$, $r_P P$

B vuole inviare un messaggio che trasforma in una coppia $(m_1, m_2) = M$

B manda $(kP,\ kr_A P + M)$, con la somma per componenti:

$(x, y) + M = (x + m_1,\ y + m_2)$; $kr_A P \in E$, $kr_A P = (x, y) \in E$

Le curve ellittiche intervengano anche in problemi di altro tipo.

Sia il classico problema delle palle di cannone di Eulero, dove la pila più alta è costituita da una sola palla, quella immediatamente sotto da 4, quella ancora sotto da 9, e così via

Se l'altezza è x, il numero delle palle è $\sum_{k=1}^{x} k^2 = \frac{1}{6} x (x+1)(2x+1)$

Si cerca per quali x il numero delle palle sia un quadrato.

Il problema consiste nel trovare i punti a coordinate intere della curva ellittica $y^2 = \frac{x^3}{3} + \frac{x^2}{2} + \frac{x}{6}$.

Per il teorema di Siegel, tali punti sono in numero finito.

Soluzioni banali sono $\{(-1, 0),\ (0, 0) = P,\ (1, 1) = Q,\ (1, -1)\}$.

Si verifica che $P + 2Q = (24, 70)$ che è la soluzione cercata;

si prova che, oltre alla simmetrica $(24, -70)$, non ci sono altre soluzioni non banali.

Sia $E(\mathbb{Q}) = \{(x,y) : x,y \in \mathbb{Q},\ y^2 = x^3 + ax + b\}$

Mordell dimostrò che $E(\mathbb{Q})$ è finitamente generato.

Sia infatti $E(\mathbb{Q})_{tor} \triangleq \{\text{elementi di } E(\mathbb{Q}) \text{ di periodo finito}\}$

$$E(\mathbb{Q})_{tor} = \begin{cases} \mathbb{Z}_n & 1 \le n \le 10 \text{ oppure } n = 12 \\ \mathbb{Z}_2 \times \mathbb{Z}_{2n} & 1 \le n \le 4 \end{cases}$$

Si ha $E(\mathbb{Q}) / E(\mathbb{Q})_{tor} \cong \mathbb{Z}^r$, e r si definisce rango di $E(\mathbb{Q})$.

Rango r significa che $\exists\, r$ punti razionali $P_1, P_2, \dots, P_r \in E(\mathbb{Q})$ non di torsione tali che ogni $S \in E(\mathbb{Q})$ si scriva come $S = \sum_{i=1}^{r} n_i P_i$, con $n_i \in \mathbb{Z}$.

Dato r intero > 0 esiste una curva di rango r?

In particolare, esistono curve di rango grande quanto si vuole?

Nel 2006, Noam Elkies, famoso per avere trovato una cinquina di interi tali per cui $x_5^4 = \sum_{i=1}^{4} x_i^4$, ha trovato una curva di rango $r = 28$. Non si sa rispondere, a livello teorico, se esistano o meno curve di rango arbitrariamente grande.

Non è nemmeno noto se, dato r, per valori bassi o comunque di cui è conosciuta l'esistenza di almeno una curva, esistano o meno infinite curve di tale rango.

Tuttavia si possiedono dei risultati parziali, per esempio se $r = 1$ si sa che l'esistenza di infinite curve è equivalente alla congettura di Birch e Swinnerton-Dyer.

In particolare, data E, si associa ad e:

$$L(E,s) = \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}, \quad s \in \mathbb{C}$$

che converge se $\mathrm{Re}(s) > 3/2$

$$a_p = p - \#E_p$$

$L(E,s)$ si estende ad una funzione analitica in tutto $\mathbb{C}$.

Tale congettura afferma che rango di $E > 0 \iff L(E,1) = 0$.

Definiamo ora un numero come congruente se è area di un triangolo razionale rettangolo, ovvero tale per cui sia i lati che l'area sono razionali.

$n = 6$ è banalmente congruente $(3, 4, 5)$; nel 1225 Fibonacci dimostrò che lo sono anche $n = 5$ $\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$ ed $n = 7$.

~~Fattoria~~ Congetturò anche che 1 fosse non congruente, affermazione provata da Fermat nel 1650.

Sono equivalenti:

(i) • n è congruente;

(ii) • $\exists\, x \in \mathbb{Q}$ / $x-n$, x, $x+n$ sono quadrati in $\mathbb{Q}$.

(i) implica (ii) in quanto, per definizione di congruenza, $n = \frac{ab}{2}$. Poniamo $x = \left(\frac{c}{2}\right)^2$ e abbiamo rispettivamente:

$$x - n = \frac{c^2}{4} - \frac{ab}{2} = \frac{(a-b)^2}{4} \qquad x+n = \frac{c^2}{4} + \frac{ab}{2} = \frac{(a+b)^2}{4}$$

D'altro canto (ii) implica (i): se $x-n$, x, $x+n$ sono quadrati in $\mathbb{Q}$:

$$c = 2\sqrt{x} \qquad a = \sqrt{x+n} - \sqrt{x-n} \qquad b = \sqrt{x+n} + \sqrt{x-n} \in \mathbb{Q}$$

con $a^2 + b^2 = c^2$, $n = \frac{ab}{2}$.

Un legame naturale si ha con le terne pitagoriche:

$a^2 + b^2 = c^2$ si parametrizza con $a = v^2 - v^2$, $b = 2uv$, $c = u^2 + v^2$

dove $(u,v) = 1$, $u > v$, $2 \nmid u - v$.

È possibile utilizzare la parametrizzazione per compilare una tabella:

u	v	a	b	c	nt^2	n
2	1	3	4	5	6	6
⋮	⋮	⋮	⋮	⋮	⋮	⋮
7	2	45	28	53	630	70
7	4	33	56	65	924	231

Elkies trovò che $n = 157$ è congruente, ma con u e v numeri di 24 cifre.

Il 22 settembre 2009 è stato dichiarato che erano stati trovati tutti i numeri congruenti fino a 10^{12}.

Un importante risultato che mette in relazione terne pitagoriche e numeri congruenti da una parte, e curve ellittiche dall'altra, è che esiste una biezione tra:

$\{(a,b,c) \in \mathbb{Q}^3 : a^2+b^2+c^2,\ \frac{ab}{2} = n\}$ e $\{(x,y) \in \mathbb{Q}^2 : y^2 = x^3 - n^2x \text{ con } y \neq 0\}$

data da:

$$f(a,b,c) = \left(-\frac{nb}{a+c},\ \frac{2n^2}{a+c}\right) \qquad g(x,y) = \left(\frac{n^2-x^2}{y},\ -\frac{2xn}{y},\ \frac{n^2+x^2}{y}\right)$$

Se E_n è la curva $y^2 = x^3 - n^2x$, allora $E_n(\mathbb{Q})_{tor} = \{0, (0,0), (n,0), (-n,0)\}$

$(x,y) \in E_n(\mathbb{Q})$ e $y \neq 0$ $\quad (x,y) \notin E_n(\mathbb{Q})_{tor}$ per $(x,y) = \infty \Rightarrow r \geq 1$

(14.01.2011)

Ci si chiede ora se esista un algoritmo che permetta di stabilire se un numero sia congruente oppure meno.

Un primo risultato è stato pubblicato da Tunnell sulle Inventiones nel 1983.

Prop. n square free è congruente se è soltanto se:

- se n è pari, $\#\{(a,b,c) \in \mathbb{Z}^3 : 4a^2+b^2+8c^2 = \frac{n}{2} \text{ con } c \text{ pari}\} =$
$= \#\{(a,b,c) \in \mathbb{Z}^3 : 4a^2+b^2+8c^2 = \frac{n}{2} \text{ con } c \text{ dispari}\}$
- se n è dispari, $\#\{(a,b,c) \in \mathbb{Z}^3 : 2a^2+b^2+8c^2 = n \text{ con } c \text{ pari}\}$
$= \#\{(a,b,c) \in \mathbb{Z}^3 : 2a^2+b^2+8c^2 = n \text{ con } c \text{ dispari}\}$

Tunnell ha provato che vale $\Rightarrow$, mentre per quanto riguarda $\Leftarrow$ ha provato condizionatamente che vale supposta vera la congettura di Birch e Swinnerton-Dyer.

In particolare, se si trovassero dei valori per cui non vale, si negherebbe la congettura, il che è "molto improbabile".

Il metodo può essere dunque utilizzato come probabilistico.

Articoli interessanti su tale tematica sono stati proposti da Izadi e da Arxiv (30.12.2010, Congruent numbers via the Pell equation)

Il primo di questi inizia con l'osservazione che, se (a,b,c) è una terna pitagorica, allora lo sono anche:

- $(2ac, b^2, a^2+c^2)$ e in particolare acb^2 è cong. $\Rightarrow$ ac è cong.
- $(2bc, a^2, b^2+c^2)$ " bca^2 " $\Rightarrow$ bc "
- $(2ab, b^2-a^2, c^2)$

Sono dunque congruenti anche b^2-a^2, a^2+b^2, b^2+c^2, $\frac{ab}{2}$.

Inoltre, parametrizzando al solito (a,b,c) come:

$$a = s^2-t^2, \quad b = 2st, \quad c = s^2+t^2 \qquad s>t>0, \ (s,t)=1, \ 2 \nmid s-t$$

risulta che sono congruenti:

$$A = st(s^2-t^2) \qquad B = \frac{st}{2}(s^2+t^2) \qquad C = s^4-t^4$$

In particolare, prendendo $t=1$, risultano congruenti $\forall k>0$:

$$A_1 = k(k^2-1) \qquad B_1 = 2k(k^2+1) \qquad C_1 = k^4-1$$

Ancora più nello specifico, $k(k+1)(k-1)$ è congruente, per cui il prodotto di due primi gemelli è sempre parte di un numero congruente, e se uno dei tre è un quadrato allora il prodotto di gemelli è congruente:

$3 \cdot 4 \cdot 5$ è congruente, 60 è congruente, 15 è congruente.

Oss. $(x^2-1, 2x, x^2+1)$ sono una terna pitagorica.
$\forall x$, è congruente il numero $x(x^2-1)$.
Considerata ora l'equazione di Pell $x^2-dy^2=1$,
che ha infinite soluzioni, si consideri (x,y) una di queste.
Allora $x^2-1 = dy^2 \Rightarrow x(x^2-1) = xdy^2$ è congruente $\Rightarrow xd$ è congruente.

FRAZIONI CONTINUE

Introduciamo il nuovo argomento incominciando dal definire la mappa di Gauss su $\mathbb{R}$:

$$\begin{cases} \text{se } \alpha \in \mathbb{Z}, & G(\alpha) = 0 \\ \text{se } \alpha \notin \mathbb{Z}, & G(\alpha) = \dfrac{1}{\{\alpha\}} = \dfrac{1}{\alpha - \lfloor \alpha \rfloor} \end{cases}$$

Consideriamo questa mappa reiterata in modo tale da generare una successione $\alpha_n = G^n(\alpha) : \alpha_0 = \alpha, \alpha_1, \dots, \alpha_n$.

Come agisce questa mappa sui razionali?

Sia $\frac{a}{b} = \frac{r_0}{r_1} \in \mathbb{Q}$, $G\left(\frac{r_0}{r_1}\right) = \dfrac{1}{\left\{\frac{r_0}{r_1}\right\}}$. Applicando l'algoritmo di Euclide:

$$r_0 = a_0 r_1 + r_2$$

$$\frac{r_0}{r_1} = a_0 + \frac{r_2}{r_1} \qquad a_0 = \left[\frac{r_0}{r_1}\right] \qquad \frac{r_2}{r_1} = \left\{\frac{r_0}{r_1}\right\} \qquad G\left(\frac{r_0}{r_1}\right) = \frac{r_1}{r_2}$$

$$r_{k-1} = a_{k-1} r_k + r_{k+1} \qquad G\left(\frac{r_{k-1}}{r_k}\right) = \frac{r_k}{r_{k+1}} = G^k\left(\frac{r_0}{r_1}\right)$$

Le orbite dei razionali sotto l'azione di G sono dunque finite, in quanto l'algoritmo di Euclide prima o poi termina e la mappa si stabilizza a zero.

Se α è irrazionale:

$$G(\alpha) = \frac{1}{\{\alpha\}} = \frac{1}{\alpha - \lfloor \alpha \rfloor} = G(\alpha_0) = \frac{1}{\alpha_0 - \lfloor \alpha_0 \rfloor}$$

$$a_0 = \lfloor \alpha_0 \rfloor \qquad \alpha_0 = a_0 + \frac{1}{\alpha_1}$$

$$a_k = \lfloor \alpha_k \rfloor \qquad \alpha_k = a_k + \frac{1}{\alpha_{k+1}} \qquad \text{in generale}$$

$$\alpha = \alpha_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots\, a_{k+1} + \frac{1}{\alpha_k}}}} = [a_0, a_1, \dots, a_{k-1}, \alpha_k]$$

Esempio:

$$\frac{63}{59} = \frac{r_0}{r_1} \qquad r_0 = 63,\ r_1 = 59;\quad r_2 = 4,\ r_3 = 3,\ r_4 = 1,\ r_5 = 0$$
$$a_0 = 1,\ a_1 = 14,\ a_2 = 1,\ a_3 = 3$$

$$63 = 1 \cdot 59 + 4$$
$$59 = 14 \cdot 4 + 3 \qquad \frac{63}{59} = [1, 14, 1, 3]$$
$$4 = 1 \cdot 3 + 1$$
$$3 = 3 \cdot 1 + 0$$

$$G\left(\frac{63}{59}\right) = \frac{59}{4} = \alpha_1 \qquad a_1 = 14 = \lfloor \alpha_1 \rfloor$$
$$G\left(\frac{59}{4}\right) = \frac{4}{3} = \alpha_2 \qquad \alpha_2 = 1 = \lfloor \alpha_2 \rfloor$$
$$G\left(\frac{4}{3}\right) = 3 = \alpha_3 \qquad \alpha_3 = 3 = \lfloor \alpha_3 \rfloor$$
$$G(3) = 0 = \alpha_4$$

$$O\left(\frac{63}{59}\right) = \left\{\frac{63}{59}, \frac{59}{4}, \frac{4}{3}, 3, 0\right\}$$

La scrittura è unica a meno di una modifica alla fine:

$\frac{a}{b} = [a_0, a_1, \dots, a_n]$ ($n+1$) termini

- $a_n > 1$: $\frac{a}{b} = [a_0, a_1, \dots, a_n - 1, 1]$ ($n+2$) termini
- $a_n = 1$: $\frac{a}{b} = [a_0, a_1, \dots, a_{n-1} + 1]$ n termini

Metodo ricorsivo di Eulero:

considerando la notazione $[a_0, a_1, \dots, a_n] = \frac{p_n}{q_n}$, ponendo:

$p_0 = a_0$ $\qquad q_0 = 1$

$p_1 = a_0 a_1 + 1$ $\qquad q_1 = a_1$

$p_k = a_k p_{k-1} + p_{k-2}$ $\qquad q_k = a_k q_{k-1} + q_{k-2}$

allora vale sempre tale notazione.

Dim.

$$[a_0] = a_0 = \frac{a_0}{1} = \frac{p_0}{q_0}$$

$$[a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}$$

Supponiamo ora vera tale asserzione fino alla lunghezza $n+1$ e proviamola per $n+2$:

$$[a_0, a_1, \dots, a_n, a_{n+1}] = \left[a_0, a_1, \dots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right]$$

Per ipotesi induttiva:

$$\frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n+1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}} := \frac{N}{D}$$

$$N = \frac{a_n a_{n+1} p_{n-1} + p_{n-1} + p_{n-2} a_{n+1}}{a_{n+1}} = \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}}$$

$$= \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1}}$$

$$D = \frac{a_{n+1} q_n + q_{n-1}}{a_{n+1}}$$

$$\frac{N}{D} = \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1} q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}$$

il che prova la nostra tesi.

Prop. La successione dei q_k è strettamente crescente perchè $q_k = a_k q_{k-1} + q_{k-2}$, ma $a_k \geq 1$ per $k > 0$, dunque $q_k \geq q_{k-1} + q_{k-2} > q_{k-1}$.

Prop $p_k q_{k-1} + q_k p_{k-1} = (-1)^{k-1}$

Dim. Per induzione:

$K = 1$, $p_1 q_0 - q_1 p_0 = (a_0 a_1 + 1) - a_1 a_0 = 1 = (-1)^0$

Supponiamo ora vero per $\bar{k}$ e proviamolo per $\bar{k}+1$:

$$p_{\bar{k}+1} q_{\bar{k}} - q_{\bar{k}+1} p_{\bar{k}} = (a_{\bar{k}+1} p_{\bar{k}} + p_{\bar{k}-1}) q_{\bar{k}} - (a_{\bar{k}+1} q_{\bar{k}} + q_{\bar{k}-1}) p_{\bar{k}} =$$
$$= p_{\bar{k}-1} q_{\bar{k}} - q_{\bar{k}-1} p_{\bar{k}} = -(p_{\bar{k}} q_{\bar{k}-1} - p_{\bar{k}-1} q_{\bar{k}}) = -(-1)^{\bar{k}-1} = (-1)^{\bar{k}}$$

Def. convergente $C_k = \frac{p_k}{q_k}$

$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}} \qquad C_k - C_{k-2} = \frac{a_k \cdot (-1)^k}{q_k q_{k-2}}$$

$$C_k - C_{k-1} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{p_k q_{k-1} - p_{k-1} q_k}{q_{k-1} q_k} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

$$C_k - C_{k-2} = \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - p_{k-2} q_k}{q_{k-2} q_k} = \frac{(a_k p_{k+1} + p_{k+2}) - \dots}{q_{k-2} q_k}$$
$$= \frac{a_k p_{k-1} q_{k-2} - a_k p_{k-2} q_{k-1}}{q_{k-2} q_k} = \frac{a_k (p_{k-1} q_{k-2} - p_{k-2} q_{k-1})}{q_{k-2} q_k} = \frac{(-1)^k a_k}{q_k q_{k-2}}$$

sfruttando la proprietà dimostrata prima.

Se k è dispari $C_k - C_{k-2} < 0 \Rightarrow C_k < C_{k-2}$

$$C_{2k+1} < \dots < C_5 < C_3 < C_1$$

se k è pari $C_0 < C_2 < C_4 < \dots < C_{2k}$

Prop. $\forall k, j \quad C_{2k+1} > C_{2j}$

infatti $k \geq j \quad C_{2k+1} > C_{2k} \geq C_{2j}$

$k < j \quad C_{2k+1} > C_{2j+1} > C_{2j}$

Ricapitolando:

- $\alpha = [a_0, a_1, \dots]$ genera una sequenza di razionali C_k;
- i risultati sull'ordine portano a $C_0, C_2, \dots, C_{2k}, \dots, C_{2k+1}, \dots, C_3, C_1$

Valgono pertanto:

- $\exists \lim_{k \to \infty} C_{2k} = \sup \{C_{2k}\} = \alpha_1$
- $\exists \lim_{k \to \infty} C_{2k+1} = \inf \{C_{2k+1}\} = \alpha_2$
- $C_0 < C_{2k} < \dots < \alpha_1 \leq \alpha_2 < \dots < C_{2k+1} < C_1$

Dimostriamo ora che $\alpha_1 = \alpha_2$ ed esiste pertanto effettivamente un limite unico.

Si ha $\alpha_2 - \alpha_1 \leq C_{2k-1} - C_{2k} = \frac{p_{2k-1}}{q_{2k-1}} - \frac{p_{2k}}{q_{2k}} = \frac{p_{2k-1} q_{2k} - q_{2k-1} p_{2k}}{q_{2k-1} q_{2k}}$

$$= \frac{1}{q_{2k} q_{2k-1}}$$

q_k è strettamente crescente, $\lim q_k \to \infty$, $\alpha_2 = \alpha_1$, c.v.d.

Il limite $\lim_{k\to\infty} c_k$ esiste, pertanto.

Dimostriamo ora che non è razionale.

Per assurdo infatti sia $\lim c_k = \frac{a}{b}$. Si avrebbe:

$$c_{2k} < \frac{a}{b} < c_{2k+1}$$

$$0 < \frac{a}{b} - c_{2k} < c_{2k+1} - c_{2k}$$

$$0 < \frac{aq_{2k} - bp_{2k}}{bq_{2k}} < \frac{1}{q_{2k}\, q_{2k+1}} \qquad \forall k$$

$$0 < aq_{2k} - bq_{2k} < \frac{b}{q_{2k+1}} \qquad \forall k$$

assurdo poichè per k sufficientemente grande $\frac{b}{q_{2k+1}} < 1$, ma $aq_{2k} - bq_{2k}$ è intero e non può essere strettamente compreso tra 0 e 1.

(20.01.2011)

Abbiamo visto che, dato:

- α irrazionale
- $G(\beta) = \frac{1}{\{\beta\}}$
- $\alpha_0 = \alpha$
- $\alpha_n = G(\alpha_{n-1})$
- $a_n = \lfloor \alpha_n \rfloor$

allora: $\alpha = [a_0, a_1, \dots, a_{n-1}, \alpha_n]$

$$[a_0, a_1, \dots, a_{n-1}, a_n] = c_n = \frac{p_n}{q_n}$$

Dimostriamo ora che $L := \lim_{k\to\infty} c_k = \alpha$.

Si ha: $\alpha = [a_0, a_1, \dots, a_k, \alpha_{k+1}] = \frac{\alpha_{k+1}\cdot p_k + p_{k-1}}{\alpha_{k+1}\cdot q_k + q_{k-1}}$, da cui:

$$|\alpha - c_k| = \left| \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}} - \frac{p_k}{q_k} \right| = \left| \frac{q_k p_{k-1} - p_k q_{k-1}}{q_k(\alpha_{k+1} q_k + q_{k-1})} \right| = \frac{1}{q_k(\alpha_{k+1} q_k + q_{k-1})}$$

$$< \frac{1}{q_k \cdot q_{k+1}}$$

L'espressione in frazione continua di α irrazionale è unica.

Supponiamo infatti che ne esistano due distinte, ovvero:

$\alpha = [a_0, a_1, \dots]$ $\qquad$ $\alpha = [b_0, b_1, \dots]$

$a_0 = \lfloor \alpha \rfloor$ $\qquad$ $b_0 = \lfloor \alpha \rfloor$

$$a_0 = b_0$$

$$[a_0, a_1, \dots] = [a_0, b_1, \dots]$$

$$a_0 + \frac{1}{[a_1, \dots]} = a_0 + \frac{1}{[b_1, \dots]}$$

$$[a_1, \dots] = [b_1, \dots]$$

e si continua in maniera analoga, provando che $a_i = b_i \ \forall i$.

Proviamo ora che ad ogni passo la convergenza migliora

$$\alpha = [a_0, a_1, \dots, a_{k+1}, a_{k+2}] = \frac{\alpha_{k+2} p_{k+1} + p_k}{\alpha_{k+1} q_{k+1} + q_k}$$

$$\alpha(\alpha_{k+2} q_{k+1} + q_k) = \alpha_{k+2} p_{k+1} + p_k$$

$$\alpha \alpha_{k+2} q_{k+1} + \alpha q_k = \alpha_{k+2} p_{k+1} + p_k$$

$$\alpha \alpha_{k+2} q_{k+1} - \alpha_{k+2} p_{k+1} = -\alpha q_k + p_k$$

$$\alpha q_{k+1} - p_{k+1} = -\frac{1}{\alpha_{k+2}} (\alpha q_k - p_k)$$

$$\left|\left(\alpha - \frac{p_{k+1}}{q_{k+1}}\right)\right| = \left| -\frac{q_k}{a_{k+2} q_{k+1}} \right| \cdot \left| \alpha - \frac{p_k}{q_k} \right|$$

$$\left| \alpha - \frac{p_{k+1}}{q_{k+1}} \right| < \left| \alpha - \frac{p_k}{q_k} \right|$$

$$\frac{p_k}{q_k} < \alpha < \frac{p_{k+1}}{q_{k+1}}$$

$$\left| \alpha - \frac{p_k}{q_k} \right| < \left| \frac{p_k}{q_k} - \frac{p_{k+1}}{q_{k+1}} \right|$$

Prop. a, b interi $\quad a, b > 0 \quad (a, b) = 1$

$$|b\alpha - a| < |\alpha \cdot q_n - p_n| \implies b \geq q_{n+1} \qquad \odot$$

Dim. Supponiamo per assurdo che esistano tali a, b per cui:

$$|b\alpha - a| \underset{(1)}{<} |\alpha \cdot q_n - p_n| \quad \text{e} \quad b \underset{(2)}{<} q_{n+1}$$

Questo significherà che:

$$\begin{cases} x \cdot q_n + y \cdot q_{n+1} = b & (3) \\ x \cdot p_n + y \cdot p_{n+1} = a & (4) \end{cases}$$

Poiché $\begin{vmatrix} q_n & q_{n+1} \\ p_n & p_{n+1} \end{vmatrix} = \pm 1$, applicando Cramer si riscontra immediatamente come sia x che y debbano essere interi.

Mostriamo che $x \neq 0$. Se infatti fosse $x = 0$, sarebbe $y \cdot q_{n+1} = b$; poiché $q_{n+1} > 0$, $b > 0$, dovrà essere $y > 0$, ma $b < q_{n+1}$, dunque $y < 1$. Si ha $0 < y < 1$, assurdo.

Analogamente, se fosse $y = 0$, allora $x q_n = b$, $x p_n = a$. Dalla (1) sarebbe $|\alpha x q_n - x p_n| < |\alpha q_n - p_n|$, e poiché $|\alpha x q_n - x p_n| = |x| \cdot |\alpha q_n - p_n|$, e $|x| \geq 1$, seguirebbe $|\alpha b - a| \geq |\alpha q_n - p_n|$, contro l'ipotesi. Dunque $y \neq 0$.

Mostriamo anche che x, y hanno segno opposto.

Se $y < 0$, allora, con $x q_n = b - y q_{n+1}$, si giunge a $x q_n > 0 \implies x > 0$.

Se invece $y > 0$, allora $b < q_{n+1}$, $b < y \cdot q_{n+1}$; dalla (3) $x q_n = b - y q_{n+1} < 0$, da cui $x < 0$.

Poichè $(\alpha q_n - p_n)$ e $(\alpha q_{n+1} - p_{n+1})$ hanno segno opposto, segue che $x(\alpha q_n - p_n)$ e $y(\alpha q_{n+1} - p_{n+1})$ hanno lo stesso segno.

$$|\alpha b - a| = |(x q_n + y q_{n+1})\alpha - (x p_n + y p_{n+1})| = |\alpha x q_n + \alpha y q_{n+1} - x p_n - y p_{n+1}|$$
$$= |x(\alpha \cdot q_n - p_n) + y \cdot (\alpha \cdot q_{n+1} - p_{n+1})|$$
$$= |x| \cdot |\alpha q_n - p_n| + |y| \cdot |\alpha q_{n+1} - p_{n+1}|$$

Questo implica che $|\alpha b - a| \geq |\alpha q_n - p_n|$, contro la (1).

- L'importanza di questo risultato sta nel fatto che implica che i C_k siano le migliori approssimazioni, ovvero che:

$$\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{p_n}{q_n}\right| \Rightarrow b > q_n$$

Dimostriamo anche questo fatto per assurdo. Supponiamo infatti vera l'ipotesi, e sia la tesi $b \leq q_n$ per alcuni valori dei parametri. Moltiplicando a sinistra per b e a destra per q_n si otterrebbe:

$$|\alpha b - a| < |\alpha q_n - p_n|$$

allora $b \geq q_{n+1} > q_n$ per il risultato precedente, assurdo.

- Un risultato correlato afferma che:

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2} \Rightarrow \frac{a}{b} \text{ è un convergente}$$

Proviamo anche questo risultato per assurdo.

Supponiamo che siano $\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$, e che $\frac{a}{b}$ non sia un convergente.

Poichè $\frac{a}{b} \in \{C_k\}$, $\exists\, k \mid q_k < b < q_{k+1}$

$$\frac{a}{b} \neq \frac{p_k}{q_k} \Rightarrow a q_k - b p_k \neq 0 \Rightarrow |a q_k - b p_k| \geq 1$$

Da $b < q_{k+1}$ e da $\odot$ segue che:

$$|\alpha q_k - p_k| \leq |\alpha b - a| = b \cdot \left|\alpha - \frac{a}{b}\right| < \frac{1}{2b}$$

$$\frac{1}{b q_k} \leq \frac{|a q_k - b p_k|}{b q_k} = \left|\frac{a}{b} - \frac{p_k}{q_k}\right| \leq \left|\frac{a}{b} - \alpha\right| + \left|\alpha - \frac{p_k}{q_{k+1}}\right| < \frac{1}{2b^2} + \frac{1}{2b q_k}$$

$$\frac{1}{q_k} < \frac{1}{2b} + \frac{1}{2q_k} \Rightarrow \frac{1}{2q_k} < \frac{1}{2b} \Rightarrow q_k > b$$

assurdo poiché $q_k < b < q_{k+1}$

- Un interessante risultato lega le matrici 2×2 con le frazioni continue.

$$\prod_{i=0}^{n} \begin{bmatrix} a_i & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix}$$

Poichè le matrici a sinistra sono simmetriche, coincidono con le loro trasposte, ed essendo il prodotto delle trasposte in ordine inverso la trasposta del prodotto:

$$\prod_{i=0}^{n} \begin{bmatrix} a_{n-i} & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{bmatrix}$$

Vediamo un esempio. Se lo sviluppo finito di un razionale è $[2,1,3,4]$:

k	a_k	p_k	q_k
0	2	2	1
1	1	3	1
2	3	11	4
3	4	47	17

Se lo sviluppo è alla rovescia, $[4,3,1,2]$:

k	a_k	p_k	q_k
0	4	4	1
1	3	13	3
2	1	17	4
3	2	47	11

Si osservi che p_{n-1} e q_n sono scambiati nei due schemi.

Tutto questo vale però supposto $a_0 \neq 0$. Se $a_0 = 0$:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \prod_{i=1}^{n} \begin{bmatrix} a_i & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix}$$

$$\prod_{i=0}^{n-1} \begin{bmatrix} a_{n-i} & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{bmatrix}$$

$$\prod_{i=0}^{n-1} \begin{bmatrix} a_{n-i} & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1}$$

$$\prod_{i=0}^{n-1} \begin{bmatrix} a_{n-i} & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} q_n & p_n \\ q_{n-1} & p_{n-1} \end{bmatrix}$$

Rivolgiamo la nostra attenzione ora allo sviluppo parziale di numeri notevoli. Per esempio, $\pi = [3, 7, 15, 1, 292, \dots]$

k	a_k	p_k	q_k
0	3	3	1
1	7	22	7
2	15	333	106
3	1	355	113
4	292	103993	33102

$$c_1 = \frac{22}{7} \qquad |c_k - \alpha| < \frac{1}{q_k q_{k+1}} = \frac{1}{106 \cdot 7} > \left|\pi - \frac{22}{7}\right|$$

$$c_3 = \frac{355}{113} \qquad \left|\pi - \frac{355}{113}\right| < \frac{1}{113 \cdot 33102} < 10^{-6}$$

Denotiamo con $[a_0, \dots, a_n, \overline{a_{n+1}, \dots, a_m}]$ uno sviluppo periodico.

Consideriamo $[\bar{a}] = \beta$. Possiamo scrivere:

$$\beta = [\bar{a}] = [a, \bar{a}] = a + \frac{1}{\bar{a}} = a + \frac{1}{\beta}$$

$$\beta^2 - a\beta - 1 = 0$$

$$\beta = \frac{a \pm \sqrt{a^2+4}}{2} \qquad \beta > 0 \Rightarrow \beta = \frac{a + \sqrt{a^2+4}}{2}$$

Se β è zero di $x^2 - ax - 1$, allora $\beta = [a, a, a, \dots,] = [a]$

In particolare, se $a = 1$, si ottiene $\phi = [1, 1, 1, \dots]$

(21.01.2011)

Sia d non quadrato.

$\mathbb{Q}(\sqrt{d}) = \mathbb{Q}\left(\frac{a+b\sqrt{d}}{c}\right)$ a,b,c interi

Si tratta di uno spazio vettoriale su $\mathbb{Q}$ di base $\{1, \sqrt{d}\}$

Se $\alpha \in \mathbb{Q}(\sqrt{d})$, allora $\alpha = u + v\sqrt{d}$, $u, v \in \mathbb{Q}$

Se α è irrazionale, allora α' coniugato algebrico di α è $\alpha' = u - v\sqrt{d}$

α e α' sono le due radici del polinomio $x^2 - 2ux + (u^2 - dv^2)$, detto polinomio minimo.

Definiamo ora:

- $Tr(\alpha) = 2u = \alpha + \alpha'$ (additività)
- $N(\alpha) = \alpha\alpha' = u^2 - dv^2$ (moltiplicatività)

Si ha $N(\alpha)\,N(\beta) = N(\alpha\beta)$, infatti se $\beta = s + t\sqrt{d}$:

$$(u^2 - dv^2)(s^2 - dt^2) = N((us + vtd) + (ut + vs)\sqrt{d})$$
$$= (us + vtd)^2 - d(ut + vs)^2$$

$\alpha^0, \alpha, \alpha^2, \ldots = (\alpha^n)$ ricorre con $x^2 - Tr(\alpha)x + N(\alpha)$

$\alpha^n = Tr(\alpha)\cdot\alpha^{n-1} - N(\alpha)\cdot\alpha^{n-1}$

Poiché $\mathbb{Q}(\sqrt{d})$ è un campo, il quoziente di $\frac{u+v\sqrt{d}}{s+t\sqrt{d}}$, se non è razionale, è una irrazionalità quadratica $h + k\sqrt{d}$.

Esempio:

$\alpha_0 = \alpha = \sqrt{a^2+1}$

Calcoliamo la frazione continua:

$a_0 = [\alpha] = a$ $\qquad \alpha_1 = \frac{1}{\{\alpha_0\}} = \frac{1}{\sqrt{a^2+1} - a} = \sqrt{a^2+1} + a$

$a_1 = [\alpha_1] = 2a$

$a_2 = [\alpha_1] = 2a$ $\qquad \alpha_2 = \frac{1}{\sqrt{a^2+1} + a - 2a} = \frac{1}{\sqrt{a^2+1} - a} = \alpha_1$

I calcoli si ripetono tali quali e dunque lo sviluppo è $[a, \overline{2a}]$

Poiché $[\overline{b}] = \beta$ è zero di $x^2 - bx - 1$:

$[a, \overline{b}] = [a, b, \overline{b}] = [a, b, \beta] = \frac{\beta p_2 - p_1}{\beta q_2 - q_1}$ è una irrazionalità quadratica

Si giunge ad un importante risultato, dovuto in parte ad Eulero e in parte a Lagrange.

Teor. α è una irrazionalità quadratica $\iff$ il suo sviluppo è periodico

Dim. Eulero $\Longleftarrow$

Supponiamo $\alpha = [a_0, a_1, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+m}}] = [a_0, \ldots, a_n, \beta] = \frac{p_n\beta + p_{n-1}}{q_n\beta + q_{n-1}}$

$\beta = [\overline{a_{n+1}, \ldots, a_{n+m}}] = [a_{n+1}, \ldots, a_{n+m}, \beta]$

$= \frac{s\beta + t}{u\beta + v}$

In entrambi i casi si giunge ad avere un'irrazionalità quadratica.

ALGORITMO DI LAGRANGE

Partiamo con $x = \frac{P_0+\sqrt{D}}{Q_0}$, con le ipotesi che $Q_0 \neq 0$, $Q_0 \in \mathbb{Z}$, $P_0 \in \mathbb{Z}$, $D > 0$ non quadrato, $Q_0 \mid D - P_0^2$.

L'ipotesi non è restrittiva.

Infatti data $x = \frac{a+b\sqrt{D}}{c}$, $c \neq 0$, $c \in \mathbb{Z}$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $b > 0$, $D > 0$ non quadrato

$$x = \frac{a\cdot|c| + \sqrt{b^2 D c^2}}{c\cdot|c|} = \frac{P_0+\sqrt{D}}{Q_0} \quad \text{con } Q_0 = c\cdot|c| \;\Big|\; b^2Dc^2 - a^2c^2$$

Assegnati P_0 e Q_0, l'algoritmo è del tipo:

$$\begin{cases} x_0 = x \\ x_k = \frac{P_k+\sqrt{D}}{Q_k} \qquad a_k = [x_k] \end{cases}$$

$$P_{k+1} = a_k Q_k - P_k$$

$$Q_{k+1} = (D - P_{k+1}^2) / Q_k$$

Ad ogni passo P_k e Q_k sono interi, $Q_k \neq 0$.

$Q_k \mid D - P_k^2$ $\qquad x = [a_0, a_1, \dots]$

Infatti, per $k=0$ le ipotesi sono verificate.

Supponiamo ora che siano vere al passo k e proviamole per $k+1$.

P_{k+1} è intero, $Q_{k+1} \neq 0$ poichè D non è un quadrato.

$Q_{k+1} \mid D - P_{k+1}^2$; $D - P_{k+1}^2 = D - (a_k Q_k - P_k)^2$

$$= D - a_k^2 Q_k^2 - P_k^2 + 2 a_k Q_k P_k$$

Sappiamo che $Q_k \mid D - P_k^2$, e allora $Q_k \mid D - P_{k+1}^2$.

Dunque Q_{k+1} è effettivamente intero.

Si ha poi:

$$x_k - a_k = \frac{P_k+\sqrt{D}}{Q_k} - a_k = \frac{P_k+\sqrt{D} - a_k Q_k}{Q_k} = \frac{-P_{k+1}+\sqrt{D}}{Q_k} = \frac{D - P_{k+1}^2}{Q_k(P_{k+1}+\sqrt{D})}$$

$$= \frac{Q_{k+1}}{P_{k+1}+\sqrt{D}} = \frac{1}{x_{k+1}}$$

$$x_{k+1} = \frac{1}{x_k - a_k} = \frac{1}{\{x_k\}} = G(x_k)$$

e dunque si calcolano effettivamente gli sviluppi parziali (quozienti) in frazione continua.

Oss. L'algoritmo richiede soltanto aritmetica razionale, e quindi aritmetica di interi in multiprecisione.

Infatti, se ρ è irrazionale, e m è intero, $\lfloor \rho/m \rfloor = \lfloor \lfloor \rho \rfloor / m \rfloor$,

allora possiamo scrivere:

$$a_k = \left\lfloor \frac{P_k+\sqrt{D}}{Q_k} \right\rfloor = \left\lfloor \frac{P_k + [\sqrt{D}]}{Q_k} \right\rfloor = \left\lfloor \frac{P_k+s}{Q_k} \right\rfloor \quad \text{ponendo } \sqrt{D} = s$$

Dimostriamo ora che lo sviluppo è periodico.

Sia $x = \frac{x_k p_{k-1} + p_{k-2}}{x_k q_{k-1} + q_{k-2}}$. Passando al coniugato $x' = \frac{x_k' p_{k-1} + p_{k-2}}{x_k' q_{k-1} + q_{k-2}}$,

Svolgiamo una serie di calcoli:

$$x' x_k' q_{k-1} + x' q_{k-2} = x_k' p_{k-1} + p_{k-2}$$

$$x_k' (x' q_{k-1} - p_{k-1}) = p_{k-2} - x' \cdot q_{k-2}$$

$$x_k' = \frac{p_{k-2} - x' \cdot q_{k-2}}{-p_{k-1} + x' \cdot q_{k-1}} = -\frac{q_{k-2}}{q_{k-1}} \cdot \frac{x' - \frac{p_{k-2}}{q_{k-2}}}{x' - \frac{p_{k-1}}{q_{k-1}}} = -\frac{q_{k-2}}{q_{k-1}} \cdot \frac{x' - c_{k-2}}{x' - c_{k-1}}$$

Poiché $\lim_{k \to \infty} \frac{x' - c_{k-2}}{x' - c_{k-1}} = 1$, tale quantità è definitivamente positiva,

ovvero $\exists n_0 \; \forall k > n_0 \; / \; p_k > 0$.

$\forall k > n_0$, dunque, $x_k < 0$.

$\forall k > 0$, $x_k > 1$

$\forall k > n_0 \qquad 0 < x_k - x_k' = \frac{2\sqrt{D}}{q_k}$

$\forall k > n_0 \qquad q_k > 0$

Richiamando dall'algoritmo:

1) $p_{k+1} = a_k q_k - p_k$

2) $q_{k+1} = (D - p_{k+1}^2) / q_k$

e usando la 2) $D - p_{k+1}^2 = q_k q_{k+1} > 0 \quad \forall k > n_0$

$$\forall k > n_0 \quad p_{k+1}^2 < D \Rightarrow |p_{k+1}| < \sqrt{D}$$

$$p_{k+2} = a_{k+1} q_{k+1} - p_{k+1}$$

$$q_{k+1} = \frac{p_{k+1} + p_{k+2}}{a_{k+1}}$$

$$q_{k+1} = |q_{k+1}| = |\dots| \leq \frac{|p_{k+1}| + |p_{k+2}|}{a_{k+1}} \Rightarrow q_{k+1} < 2\sqrt{D}$$

Si troveranno ad un certo punto $(p_k, q_k) = (p_{k'}, q_{k'})$, $k' > k$, e tutto si ripeterà.

RISULTATO FONDAMENTALE

$$x = \frac{x_k p_{k-1} + p_{k-2}}{x_k q_{k-1} + q_{k-2}} \qquad x_k = \frac{p_k + \sqrt{D}}{q_k}$$

$$x = \underbrace{\frac{\frac{p_k + \sqrt{D}}{q_k} p_{k-1} + p_{k-2}}{\text{analogo}}}_{\text{analogo}} = \frac{\frac{p_k p_{k-1} + \sqrt{D} p_{k-1} + q_k p_{k-2}}{q_k}}{\text{analogo}}$$

$$= \frac{p_k p_{k-1} + \sqrt{D} p_{k-1} + q_k p_{k-2}}{p_k q_{k-1} + \sqrt{D} q_{k-1} + q_k q_{k-2}}$$

Consideriamo $x_0 = \sqrt{D}$, ovvero $p_0 = 0$, $q_0 = 1$

⇒ Esistono $P_1, P_2, \dots, P_r \in E(\mathbb{Q})$ t.c. $S = \mathbb{Z}\cdot P_i$ con $S \neq E(\mathbb{Q})_{tor}$

... rango infinito, ∃ curve di rango r?
Esistono curve di rango grande a piacere? } → BOH!

2006: $r = 28$, Noam Elkies

∃! ∞ curve di rango 1 ½? Sì se la congettura di Birch e Swinnerton-Dyer è vera.

CONG:

$$L(E,s) = \prod_{p \mid 2\Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} \qquad s \in \mathbb{C},\ \mathrm{Re}(s) > 3/2$$

$$1 + a_p = p - \#E_p$$

si estende ad una funzione analitica in tutto $\mathbb{C}$

rango $E = 0 \iff L(E,1) = 0$

Numeri congruenti

n è detto congruente se è area di un tr. rettangolo razionale (= i cui lati hanno area razionale)

Fibonacci (1225): 5 è congruente

5 è area di $\left(3/2, \frac{20}{3}, 41/6\right) = \left(9/6, \frac{40}{6}, 41/6\right)$

1 non è congruente (Fermat)

Fatto: sono equivalenti: • n è congruente • $\exists x \in \mathbb{Q}$ t.c. $x-n$, x, $x+n$ sono congruenti.

Dim: "⇐": $c = 2\sqrt{x}$ $\quad a = \sqrt{x+n} - \sqrt{x-n}$ $\quad b = \sqrt{x+n} + \sqrt{x-n}$ ☐

È sufficiente considerare i n. congruenti privi di quadrati
$n = 157$ è congruente: x e y hanno 24 cifre!!

Esiste una bijezione tra

$$\{(a,b,c) \in \mathbb{Q}^3 : a^2 + b^2 = c^2,\ \tfrac{ab}{2} = n\} \longleftrightarrow \{(x,y) \in \mathbb{Q}^2 \mid y^2 = x^3 - n^2 x,\ y \neq 0\}$$

$$(a,b,c) \longmapsto \left(-\frac{nb}{a+c},\ \frac{2n^2}{a+c}\right)$$

$$\left(\frac{n^2-x^2}{y},\ -\frac{2xn}{y},\ \frac{n^2+x^2}{y}\right) \longleftarrow (x,y)$$

$E(\mathbb{Q})_{tor} = \{0, (0,0), (n,0), (-n,0)\}$ Dunque se $(x,y) \in E_n(\mathbb{Q})$ e $y \neq 0$, rango $(E_n) \geq 1$

4C

PROP: Ogni sviluppo è in f. continua, $L = \alpha$, con $L = \lim_k C_k$

Dim: $\alpha = [a_0, \dots, a_{k+1}] = \dfrac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}}$

$$|\alpha - C_k| = \frac{|q_k p_{k-1} - p_k q_{k-1}|}{q_k (a_{k+1} q_k + q_{k-1})} = \frac{1}{q_k (\dots)} < \frac{1}{q_k q_{k-1}} \to 0$$

Sono: $a_{k+1} = [\alpha_{k+1}] < \alpha_{k+1} < a_{k+1} \Rightarrow$ denom $> q_k (a_{k+1} q_k + q_{k-1}) = q_k q_{k+1}$ D

L'espressione in f.c. di α è unica.
Supponi $\alpha = [a_0, \dots] = \alpha = [b_0, b_1, \dots] \Rightarrow a_0 = b_0$

$$\hookrightarrow a_0 + \frac{1}{[a_1, \dots]} = b_0 + \frac{1}{[b_1, \dots]} \Rightarrow a_1 = b_1 \text{ etc.}$$

Ad ogni passo le convergenti migliorano

$$\alpha = \frac{a_{k+2} p_{k+1} + p_k}{a_{k+2} q_{k+1} + q_k} \to \alpha (a_{k+2} q_{k+1} + q_k) = a_{k+2} p_{k+1} + p_k$$

$$\alpha - \frac{p_{k+1}}{q_{k+1}} = -\frac{q_k}{a_{k+2} q_{k+1}} \left(\alpha - \frac{p_k}{q_k} \right) \quad \text{con: } \begin{matrix} a_{k+2} \geq 1 \\ q_{k+1} > q_k \end{matrix} \to \left| \frac{q_k}{a_{k+2} q_{k+1}} \right| < 1$$

$q_{k+1} = a_{k+1} q_k + q_{k-1}$ → a_{k+1} grande ⇒ q_{k+1} grande ⇒ buona approx.

a, b interi; $a, b > 0$; $(a, b) = 1$

Prop: $|b\alpha - a| < |\alpha q_n - p_n| \to b \geq q_{n+1}$

Dim. Per assurdo: $|\alpha b - a| < |\alpha q_n - p_n|$ e $b < q_{n+1}$. $\begin{cases} x q_n + y q_{n+1} = b \\ x p_n + y p_{n+1} = a \end{cases}$ → $\det(\dots) = q_n p_{n+1} - p_n q_{n+1} = \pm 1$

Le sol sono intere: se $x \neq 0$, allora $y q_{n+1} = b$ con $y \geq 0$, assurdo.

Se $y = 0$, $\begin{cases} x p_n = a \\ x q_n = b \end{cases}$ → $|\alpha x q_n - x p_n| < |\alpha q_n - p_n| \Rightarrow |x| < 1$ più $x \neq 0$, no no!

$|x| \geq 1$

Quindi, $xy < 0$: se $y < 0$, $x > 0$. se $y > 0$, poi $b \geq q_{n+1}$ ...

ma: $\dfrac{p_n}{q_n} < \alpha < \dfrac{p_{n+1}}{q_{n+1}}$ ⇒ $(\alpha q_n - p_n) < (\alpha q_{n+1} - p_{n+1})$ sono discordi

$x < 0$ $\quad$ $y > 0$ $\quad$ concordi

$|\alpha b - a| = |x (\alpha q_n - p_n)| + |y (\alpha q_{n+1} - p_{n+1})|$ assurdo

STATICK, f.c. finisce D

$\exists$ C_k vanno le ridotte approx. con (molta) distanza.

Bisogna: $|\alpha - \frac{a}{b}| < |\alpha - \frac{p_n}{q_n}| \Rightarrow b > q_n$

Dim: P.a. $b \leq q_n$. Avrei che $|b\alpha - a| < |q_n \alpha - p_n| \Rightarrow b \geq q_{n+1} > q_n$ assurdo! □

Prop: $|\alpha - a/b| < 1/2b^2 \Rightarrow a/b$ è una convergente

Dim: P.A: $a/b \notin C_k$, $\exists\, k$ t.c. $q_k \leq b < q_{k+1}$. Studio $|aq_k - bp_k| \geq 1$.

Siccome $b < q_{k+1}$ vale $|\alpha q_k - p_k| \leq |\alpha b - a| = b|\alpha - a/b| < \frac{1}{2b}$

$$\frac{1}{bq_k} \leq \frac{|aq_k - bp_k|}{bq_k} = \left|\frac{a}{b} - \frac{p_k}{q_k}\right| < \frac{1}{2bq_k} + \frac{1}{2bq_k}$$

$$\frac{1}{q_k} < \frac{1}{2b} + \frac{1}{2q_k} \quad \text{da cui } q_k > b, \text{ no!} \qquad \square$$

Matrici 2×2 e $[\,,\dots,]$

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \dots \cdot \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \quad \text{trasposto} \quad \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix}$$

$[a_0, \dots, a_n] = \frac{p_n}{q_n}$ $\qquad [a_n, \dots, a_0] = \frac{p_n}{p_{n-1}}$ $\qquad (\text{se } a_0 \neq 0)$

Es $[2,1,3,4]$: $\quad 47/17$

n	a_n	p_n	q_n
0	2	2	1
1	1	3	1
2	3	11	4
3	4	47	17

$[4,3,1,2] = 47/11$

n	a_n	p_n	q_n
0	4	4	1
1	3	13	3
2	1	17	4
3	2	47	11

Se $a_0 = 0$: $\quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \dots \cdot \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$ $\quad T: \quad \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix}$

$$\Rightarrow \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} q_n & p_n \\ q_{n-1} & p_{n-1} \end{pmatrix} \qquad \text{Enp: } [a_n, \dots, a_1] = \frac{q_n}{q_{n-1}}$$

Es: $\pi = [3, 7, 15, 1, 292]$

k	a_k	p_k	q_k
0	3	3	1
1	7	22	7
2	15	333	106
3	1	355	113
4	292	103993	33102

$$\left|\pi - \frac{22}{7}\right| < \frac{1}{7 \cdot 106} < \frac{1}{742} \qquad \left|\pi - \frac{355}{113}\right| < \frac{1}{113 \cdot 33102} < 10^{-6}$$

Notazione: $[a_0, \dots, a_n, \overline{a_{n+1}, \dots, a_{n+k}}]$ f.c. periodica

$\beta = [\overline{a}]$ = invariante, e $\beta = [a, \overline{a}] \Rightarrow a + \frac{1}{[\overline{a}]}$ $\Rightarrow$ $\beta = a + \frac{1}{\beta}$ $\Rightarrow$ $\beta^2 = a\beta + 1$

$\rightsquigarrow \beta = \frac{a + \sqrt{a^2+4}}{2}$

Dunque le succ. di p_n e q_n ricorrono come $x^2 - ax - 1$

Ad es., $\varphi = [\overline{1}]$ e $|p_n| < |q_n|$ sono i n. di Fibonacci (ma va?)

[21.I]

Siccome le norme di $\mathbb{Z}[\sqrt{d}]$ è moltiplicativa, si ha che se $\alpha = u + v\sqrt{d}$, $\beta = s + t\sqrt{d}$

$$(u^2 - v^2 d)(s^2 - t^2 d) = (us + vtd)^2 - d(ut + vs)^2$$

Svolta: α ricorre come $x^2 - T(\alpha)x + N(\alpha)$

Es: $d = \sqrt{a^2+1}$ in f.c. $\quad a_0 = a \qquad \alpha_1 = \frac{1}{\sqrt{a^2+1} - a} = \frac{\sqrt{a^2+1} + a}{1} \qquad a_1 = 2a$

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{\sqrt{a^2+1} - a} = \alpha_1 \qquad \alpha = [\overline{a, 2a}]$$

In generale: $[\overline{a, b}] = [\overline{a, b, b}] \qquad \beta = \frac{\beta p_2 - p_1}{\beta q_2 - q_1}$

TEOR (LEGRO): α è irraz. quadratica $\Leftrightarrow$ il suo sviluppo è periodico

DIM: "$\Leftarrow$": $\alpha = [a_0, \dots, a_n, \overline{a_{n+1}, \dots, a_{n+k}}] \qquad \beta = [\overline{a_{n+1}, \dots, a_{n+k}}] = [a_{n+1}, \dots, a_{n+k}, \beta] = \frac{s\beta + t}{u\beta + v}$

$\rightsquigarrow \beta$ è quadratico

$\alpha = [a_0, \dots, a_n, \beta] = \frac{p_n \beta + p_{n-1}}{q_n \beta + q_{n-1}} \rightsquigarrow \alpha$ è quad. $\square$

ALGORITMO DI LAGRANGE

Partiamo con $x = \frac{P_0 + \sqrt{D}}{Q_0}$ $Q_0 \neq 0$, D non quadrato, $Q_0 \mid D - P_0^2$

x è un numero alg. di $\mathbb{Q}(\sqrt{D})$: basta moltiplicare per (denom.)^2

$$\begin{cases} x_0 = x; \quad x_k = \frac{P_k + \sqrt{D}}{Q_k} \\ a_k = \lfloor x_k \rfloor \end{cases} \qquad \text{con} \quad \begin{aligned} P_{k+1} &= a_k Q_k - P_k \\ Q_{k+1} &= (D - P_{k+1}^2)/Q_k \end{aligned}$$

CLAIM: P_k, Q_k sono interi, $Q_k \neq 0$ e $Q_k \mid D - P_k^2$. Svolta $x = [a_0, a_1, \dots]$

Per induz: ok $k=0$. Valgono per k. Per $k+1$?

$D - (P_{k+1})^2 = D - a_k^2 Q_k^2 - P_k^2 + 2a_k P_k Q_k$ è multiplo di Q_k $\rightsquigarrow Q_{k+1}$ è intero.

$$\frac{D - P_{k+1}^2}{Q_{k+1}} = \frac{D - P_k^2 - a_k^2 Q_k^2 - P_k^2 + 2a_k P_k Q_k}{(D - P_{k+1}^2)/Q_k} = Q_k \text{ è intero.}$$

$$x_k - a_k = \frac{-P_{k+1} + \sqrt{D}}{Q_k} = \frac{1}{x_{k+1}} \quad \Rightarrow \quad x_{k+1} = \frac{1}{\{x_k\}} = G(x_k) \quad \Rightarrow \quad x = [a_0, a_1, \dots]$$

AC

Oss: l'algoritmo richiede aritm. razionale soltanto: infatti, se $p \in \mathbb{R}-\mathbb{Q}$ e $m \in \mathbb{Z}$,
$[p/m] = [[p]/m]$, da cui

$$[x_n] = \left[\frac{P_n + \sqrt{D}}{Q_n}\right] = \left[\frac{P_n + [\sqrt{D}]}{Q_n}\right]$$

CLAIM: La scrittura è periodica

$$x = \frac{x_n P_{n-1} + P_{n-2}}{x_n q_{n-1} + q_{n-2}} \quad \text{coniug.} \quad x' = \dots \Rightarrow x_n' = -\frac{q_{n-2}}{q_{n-1}} \cdot \frac{x' - P_{n-2}/q_{n-2}}{x' - \frac{P_{n-1}}{q_{n-1}}} = -\frac{q_{n-2}}{q_{n-2}} \cdot \frac{x' - C_{n-2}}{x' - C_{n-1}}$$

Siccome i $C_n \to x$, $x_n' = \text{def.} < 0$, $\forall\, x_n > 1 \Rightarrow 0 < x_n - x_n' = \frac{2\sqrt{D}}{Q_n} \Rightarrow$ i Q_n sono def. positivi.
Per la def. $D - P_{n+1}^2 = Q_n Q_{n+1} \Rightarrow P_{n+1}^2 < D$
$\Rightarrow |a_{n+1}| = \left|\frac{P_{n+1} + P_{n+2}}{Q_{n+1}}\right| \le 2\sqrt{D}$ ↳ definitivamente, Q_n e P_n possono assumere un # finito di valori → $\exists$ ripetizione → periodicità.

Viceversa: $x = \frac{x_n P_{n-1} + P_{n-2}}{x_n q_{n-1} + q_{n-2}} \leftarrow x_n = \frac{P_n + \sqrt{D}}{Q_n} \Rightarrow x = \frac{P_n p_{n-1} + \sqrt{D} p_{n-1} + Q_n p_{n-2}}{q_n}$
con $x = \sqrt{D}$

$$P_n q_{n-1} \sqrt{D} + D q_{n-1} + Q_n q_{n-2} \sqrt{D} = P_n p_{n-1} + \sqrt{D} p_{n-1} + Q_n p_{n-2}$$

Uguaglio i coeff: $\begin{cases} P_n q_{n-1} + Q_n q_{n-2} = p_{n-1} \\ P_n p_{n-1} + Q_n p_{n-2} = D q_{n-1} \end{cases} \rightarrow Q_n = \frac{D q_{n-1}^2 - p_{n-1}^2}{q_{n-1} p_{n-2} - q_{n-2} p_{n-1}}$

$p_{n-1}^2 - D q_{n-1}^2 = Q_n (-1)^n$ ⇝ Shanks, metodo di fattorizzazione (c/n. Riesel, Prime numbers ...)

Se N non quadrato $\Rightarrow Q_n (-1)^n \neq$ quadrato mod N

Esempio: $d = 19$ $\quad x = \sqrt{19}$

n	0	1	2	3	4	5	6	7	8	9	...
a_n	4	2	1	3	1	2	8	2	1	3	...
P_n	0	4	2	3	3	2	4	4			
Q_n	1	3	5	2	5	3	1	3			

Oss: si ha che $\sqrt{D} = [a_0, \overline{a_1, \dots, a_1, 2a_0}]$ e $a_1, \dots, a_n$ è polindromo

Se $a_n = 2a_0$, $P_n = P_1$ e $Q_n = Q_0 = 1$

$\Rightarrow$ ho trovato una sol. di $x^2 - Ny^2 = (-1)^n$ $\qquad p_{n-1}^2 - N q_{n-1}^2 = (-1)^n$

$d = 7$
$x = \sqrt{29}$

n	0	1	2	3	4	5	6	7
a_n	5	2	1	1	2	10	2	1
P_n	0	5	3	2	3	5	5	3
Q_n	1	4	5	5	4	1	4	5

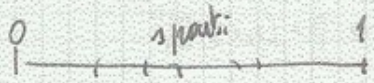
Eq. Pell $x^2 - dy^2 = 1$ d non quadrato

Lemma: $\forall s \in \mathbb{N}\ \exists\, t, v \in \mathbb{Z}$

$$|t - v\sqrt{d}| < 1/s \leq \frac{1}{|v|}$$

Dim: Dato $s \neq 0$ associo $0 \leq v \leq s$ e $t := \lceil v\sqrt{d} \rceil$

$$0 < t - v\sqrt{d} < 1$$



Ci sono $s+1$ v_i e t_i in s parti $\Rightarrow$ $0 < t_i - v_i\sqrt{d} < 1$ e

$\Rightarrow$ ci sono i, j t.c.

$$0 < \underbrace{(t_i - t_j)}_{\parallel T} - \underbrace{(v_i - v_j)}_{\parallel v} \sqrt{d} < 1/s$$

e $|v| \leq s$ da cui la tesi. □

Lemma 2: $\forall s$ $S = \{(t,v) \,/\, |t - v\sqrt{d}| < 1/|v|\}$. ~~Per il Lemma~~ S è infinito

Dim: Per ass: se fosse finito, esisterebbe il minimo. Esiste $M > 0$ t.c. $\frac{1}{M} < \min S$

Ma se prendo $s = M$ e non < 1, ho contraddizione. □

Teor: L'eq. di Pell ha sempre una soluzione non banale.

Dim: Sia $(t,v) \in S$. $|t + v\sqrt{d}| \leq |t - v\sqrt{d}| + |2v\sqrt{d}| < \frac{1}{|v|} + 2|v| \cdot \sqrt{d}$

$$|t^2 - v^2 d| = |t - v\sqrt{d}|\,|t + v\sqrt{d}| \leq \frac{1}{|v|} \cdot \left(\frac{1}{|v|} + 2|v|\sqrt{d}\right) = \frac{1}{v^2} + 2\sqrt{d} \leq 1 + 2\sqrt{d}$$

(S è un # finito di val. distinti che può assumere $\Rightarrow$ $\exists\, k$ t.c. $t^2 - v^2 d = k$ per ∞ (t,v).

$\Rightarrow \infty$ (t,v) nella stessa classe mod k. $\Rightarrow$ $t_1^2 - v_1^2 d = N(\ ) = k$

$t_1 = t_2$, $v_1 = v_2 \bmod k$, $t_1 \neq \pm t_2$
$v_1 \neq v_2$

$$N(\text{prodotto}) = k^2$$

$$(t_1 t_2 \pm v_1 v_2 d)^2 - d\,(\underbrace{v_1 t_2 \pm v_2 t_1}_{\parallel (v \cdot k)^2 \text{ b mod } k})^2 = k^2$$

$$k^2 \,|\, (\quad)^2 \quad \text{e} \quad k \,|\, v \cdot k \quad \Rightarrow \quad \left(\frac{t_1 t_2 - v_1 v_2 d}{k},\ \frac{v_1 t_2 - v_2 t_1}{k}\right) \text{ sol. di Pell.}$$

È banale? $v_1 t_2 - t_1 v_2 = 0$ $\Rightarrow$ ho che $t_1 = \pm t_2$, $v_1 = \pm v_2$, impos. □

Barbeau: Pell equations | $(t_1^2 - v_1^2 d)(t_2^2 - v_2^2 d) = t_1 t_2$ Ac

TEOR: $p^2 - dq^2 = 1 \Rightarrow p/q$ è una conv. a $\sqrt{d}$

Dim: $(p - q\sqrt{d})(p+q\sqrt{d}) = 1 \Rightarrow p - q\sqrt{d} > 0 \Rightarrow p > q\sqrt{d}$ Dunque

$$p - q\sqrt{d} = \frac{1}{p+\sqrt{d}\cdot q} < \frac{1}{2q\sqrt{d}} < \frac{1}{2q^2} \Rightarrow \left|p/q - \sqrt{d}\right| < \frac{1}{2q^2}$$

Per un lemma di prima, ciò dice che è una convergente con $\sqrt{d} < \frac{p_k}{q_k} \Rightarrow k =$ dispari □

TEOR: $\exists$ sol fondamentale (x_1, y_1) t.c. ogni altra si ottiene come potenza, nel modo che

$N(x_1 + y_1\sqrt{d}) = 1$ β sol, $\beta > 0 + 0\sqrt{d} \Rightarrow \beta = (x_1 + y_1\sqrt{d})^n$

Sia α come al corollario di sopra; $\alpha = x_1 + y_1\sqrt{d} < \alpha' = \alpha^{-1}$

$\forall \beta > 1 \Rightarrow \exists n$ t.c. $\alpha^n < \beta < \alpha^{n+1}$ $\Rightarrow$ moltiplico per $(\alpha')^n$:

Mi manipolo

$$1 < (\alpha')^n \beta < \alpha$$

$$A + B\sqrt{d} \quad < \quad A - B\sqrt{d} > 0$$

$\Rightarrow 2A > 0 \Rightarrow A > 0$; $A + B\sqrt{d} > 1$, $A - B\sqrt{d} < 1 \Rightarrow B > 0$.

Ora: $A + B\sqrt{d} = \gamma$ è sol $< \alpha \Rightarrow \beta$ è una potenza □

Se ho: $p_{n-1}^2 - d q_{n-1}^2 = Q_n (-1)^n$

$Q_n = 1$ solo per i multipli del periodo L: $n L$ $\exists$ pari (p_{L-1}, q_{L-1})

dispari: (p_{2L-1}, q_{2L-1})

- Ricordiamo delle soluzioni $\cdot p + q\sqrt{d}$, $N(\,) = 1$. $\Rightarrow$ si comporta come $x^2 - 2px + 1$

- Il lemma di Archimede

4 colori: B N NP B N = □ N + P = Δ ora ho $X^2 - D y^2 = 1$

$D = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 323 (2 \cdot 1650)^2$

$\Rightarrow L = 203254$ e le 2 mine ho 206545

- Il problema "il periodo L di $\sqrt{d}$ è pari?" sembra $\notin$ NP (!)

F. di Rédei: $(x + \sqrt{d})^n = N_n(x,d) + D_n(x,d)\sqrt{d}$ N, D pol. $Q_n = \frac{N_n}{D_n}$

$N_n = W_n(1, x, 2x, x^2 - d)$

$x \odot y = \frac{d + xy}{x + y}$

Fatt: $Q_n(d, Q_m(d,z)) = Q_{nm}(d,z)$

$Q_{n+m}(d,z) = Q_n(d, z \odot Q_m(d,z))$

$z^{\odot n} = Q_n(d,z)$

• f.c d zeri di ax^2+bx+c; $d = \left[\frac{a}{a}, \frac{b}{a}\right]$

f/z, $\sqrt{d} = \left[z, \frac{zb}{d-z^2}, zz\right]$ c.s. convergenti verso le $\sqrt{}$ di Pelli: $Q_n(d,z) \to \sqrt{d}$.

Se scelgo come z, ottengo successione famosa: $\begin{cases} x_0 = z \\ x_n = \frac{x_{n-1} + d}{2x_n^2} \end{cases}$ (Newton)

$Q_{2^n}(d,z) = x_n$ (Padi, Hitkin, Scanta...)

• Successioni ricorrenti

$a_n = [x_n]$ $\quad x_{n+1} = G(y_n)$ $\quad x_0, y_0$ in.

$b_n = [y_n]$ $\quad y_{n+1} = \frac{G(y_n)}{G(x_n)}$

$x_{n+1} = \frac{1}{1-[y_n]}$, $y_{n+1} = \frac{x_n - [x_n]}{y_n - [y_n]}$

Per 2 spazi particolari: $[\{a_0, a_1 \dots\}, \{b_0, b_1 \dots\}] = [\left(\frac{A_n}{C_n}, \frac{B_n}{C_n}\right)]$

con ricorrenze

Quelle proprietà conservano a un. unicità.
Date una un. adatta α, $\exists!$ β t.c. $[\alpha, \beta] = [\{-\}, \{\dots -\}]$ Boh?

$$\left[\left\{z, \frac{zb}{d}, \frac{3^{\cdot}db}{z^2d^2}, 3a, \frac{2a}{b}\right\}, \{0, \dots\}\right] \to \left(\sqrt[3]{d^2}, \sqrt[3]{b}\right)$$

FINE

tC