Primes is in P

Ester Dalvit

7 luglio 2004

Cos'è *Primes*? Cos'è *P*?

Primes è il problema della primalità, cioè determinare se un dato numero naturale n è primo oppure composto. Questo problema ha una facile soluzione: dividere il numero dato per tutti i primi p che sono minori di n (o meglio, della radice quadrata di n) e vedere se il risultato è intero. Se questo avviene almeno una volta, n è composto, altrimenti n è un numero primo. Tuttavia questo algoritmo richiede un tempo che cresce esponenzialmente al crescere della lunghezza di n, cioè del numero di bit necessari per rappresentarlo, ovvero $\log n$. Il tempo viene espresso come numero di operazioni elementari.

Un algoritmo deterministico è tale che il suo comportamento può essere previsto in base al dato iniziale, ovvero esso dà lo stesso risultato ogni volta che viene applicato a uno stesso dato. L'algoritmo deterministico si contrappone a quello probabilistico, il quale dà un risultato che con una piccola probabilità può non essere corretto.

P è una classe di problemi decisionali (per i quali si può rispondere "sì" o "no") che possono essere risolti con un algoritmo deterministico in un tempo polinomiale nella lunghezza dell'input del problema.

Esistono diversi test di primalità molto efficienti, probabilistici e/o condizionali (cioè basati sull'assunzione che sia valida l'ipotesi di Riemann, una congettura sulla distribuzione dei numeri primi). L'algoritmo AKS (dalle iniziali dei tre ricercatori che lo hanno trovato, Agrawal, Kayal e Saxena) che deriva dal teorema qui presentato, ha suscitato grande interesse perchè è il primo riguardante la primalità che sia deterministico e non condizionale.

Ciò significa appunto che *"Primes is in P"*.

Il risultato

Teorema. *Sia n un intero maggiore di 1. Sia r un primo che soddisfa le condizioni seguenti:*

1. *n non è divisibile per alcun primo $\leq r$*
2. *l'ordine di $n \pmod r$ è maggiore di $(\log n/\log 2)^2$*
3. *per $0 \leq j < r-1$ si ha $(X+j)^n = X^n+j$ nell'anello $(\mathbf{Z}/n\mathbf{Z})[X]/(X^r-1)$*

Allora n è potenza di un primo.

La dimostrazione

Se $n = 2$, non esiste r che soddisfa l'ipotesi 1. Dunque $n > 2$.

$$\operatorname{ord}_r n > \left(\frac{\log n}{\log 2}\right)^2 > 1$$

L'ordine di n modulo r è maggiore di 1, quindi $n \not\equiv 1 \pmod r$.
Perciò esiste p primo tale che $p \mid n$ e $p \not\equiv 1 \pmod r$.

Consideriamo l'anello

$$A = \mathbf{F}_p[X] \Big/ \left(\frac{X^r-1}{X-1}\right)$$

Per ogni k primo con r definiamo $\alpha_k : \mathbf{F}_p[X] \longrightarrow \mathbf{F}_p[X]$ ponendo $\alpha(X) = X^k$.

Fissiamo k. Si ha il diagramma

$$\begin{array}{ccc} \mathbf{F}_p[X] & \xrightarrow{\alpha} & \mathbf{F}_p[X] \\ {\scriptstyle\pi}\downarrow & \overset{\sigma}{\searrow} & \downarrow{\scriptstyle\pi} \\ A & \xrightarrow{\delta} & A \end{array}$$

dove π manda $X \in \mathbf{F}_p[X]$ nella sua classe di resto modulo $\frac{X^r-1}{X-1}$.

Dobbiamo mostrare che esiste una mappa δ che fa commutare il diagramma. Cioè deve essere $\delta \circ \pi = \sigma = \pi \circ \alpha$.

$\pi\left(\frac{X^r-1}{X-1}\right) = 0$ dunque $\delta\left(\pi\left(\frac{X^r-1}{X-1}\right)\right) = 0$. Allora deve essere $\frac{X^r-1}{X-1} \in \ker(\sigma)$.

$$\sigma\left(\frac{X^r-1}{X-1}\right) = \pi\ \left(\alpha\left(\frac{X^r-1}{X-1}\right)\right) = \pi\left(\frac{X^{kr}-1}{X^k-1}\right)$$

Osservazione. *Siano $a, b, c \in \mathbf{Z}$. Allora se $a \mid b$ si ha $X^a - 1 \mid X^b - 1$.*

Dimostrazione. È noto che

$$Y^c - 1 = (Y-1)(Y^{c-1} + Y^{c-2} + ... + 1)$$

Ponendo $Y = X^a$ e $ac = b$ si ottiene

$$X^b - 1 = (X^a - 1)(X^{a(c-1)} + ... + 1)$$

cioè $X^a - 1 \mid X^b - 1$. □

Più in generale, vale il seguente

Teorema. $X^a - 1 \mid X^b - 1 \quad \Longleftrightarrow \quad a \mid b$

Dimostrazione. Dividiamo b per a con resto; si trovano così $r, q \in \mathbf{Z}$ tali che

$$\begin{cases} b = aq + r \\ 0 \leq r < a \end{cases}$$

Dalla prima equazione si ottiene

$$X^b - 1 = X^{aq+r} - 1 \equiv X^r - 1 \pmod{X^a - 1}$$

Allora

$$X^a - 1 \mid X^b - 1 \quad \Longleftrightarrow \quad X^r - 1 \equiv 0 \quad \Longleftrightarrow \quad r = 0 \quad \Longleftrightarrow \quad a \mid b$$

□

$$\pi\left(\frac{X^{kr}-1}{X^k-1}\right) = 0 \qquad \Longleftrightarrow \qquad \frac{X^{kr}-1}{X^k-1} = g(X)\frac{X^r-1}{X-1}$$

$$\Longleftrightarrow \qquad X^{kr} - 1 = g(X)\frac{(X^r-1)(X^k-1)}{X-1}$$

La frazione $\frac{(X^r-1)(X^k-1)}{X-1}$ è un polinomio, perchè il denominatore divide il numeratore.
$(r,k)=1$, dunque $(X^r-1, X^k-1) = X-1$. Inoltre poichè $X^r-1 \mid X^{kr}-1$ e $X^k-1 \mid X^{kr}-1$, si ha

$$\frac{(X^r-1)(X^k-1)}{X-1} \quad \Big| \quad X^{kr}-1$$

Dunque

$$\pi\left(\frac{X^{kr}-1}{X^k-1}\right) = 0 \qquad \text{cioè} \qquad \frac{X^r-1}{X-1} \in \ker(\sigma)$$

Dimostriamo ora che δ è biiettiva. Se δ è suriettiva, allora è biiettiva per il principio dei cassetti.

Per dimostrare la suriettività di σ, basta mostrare che nell'immagine c'è X.
Poichè $(r,k)=1$, esistono $a, b \in \mathbf{Z}^+$ tali che:

- $-ar+bk=1$ cioè $bk = 1+ar$ per cui $X^{bk} = X\ X^{ar} \equiv X \pmod{\frac{X^r-1}{X-1}}$. Cioè X^b viene mandato in X dall'applicazione $X \mapsto X^k$.
- $ar-bk=1$ cioè $ar = 1+bk$ per cui $X\ X^{bk} = X^{ar} \equiv 1 \pmod{\frac{X^r-1}{X-1}}$. Cioè X ha inverso X^{bk}. Dunque $(X^{-b})^k = (X^{-a})^r X \equiv X \pmod{\frac{X^r-1}{X-1}}$. Cioè X^{-b} viene mandato in X.

Dunque ogni applicazione $\delta_k : A \longrightarrow A$ con $(k,r)=1$ è un automorfismo.

Teorema. *Sia $(G, \circ)$ un gruppo con la sua operazione e $(S, *)$ un insieme su cui è definita un'operazione binaria. Sia $\varphi : G \longrightarrow S$ una mappa suriettiva che conservi le operazioni, cioè $\varphi(a \circ b) = \varphi(a) * \varphi(b)$ dove $a, b \in G$.*
Allora $(S, *)$ è un gruppo.

Dimostrazione. Siano $A, B, C \in S$; allora esistono $a, b, c \in G$ tali che $A = \varphi(a)$, $B = \varphi(b)$ e $C = \varphi(c)$.

- S è chiuso rispetto a $*$.
  $A * B = \varphi(a) * \varphi(b) = \varphi(a \circ b) \in S$ perchè $a \circ b \in G$.

- Esistenza dell'elemento neutro.
  In G esiste l'elemento neutro 1_G tale che $1_G \circ g = g \circ 1_G = g$ per ogni $g \in G$. Dunque

$$\begin{array}{rcccl} \varphi(1_G \circ g) & = & \varphi(g \circ 1_G) & = & \varphi(g) \\ \varphi(1_G) * \varphi(g) & = & \varphi(g) * \varphi(1_G) & = & \varphi(g) \end{array}$$

  Allora $\varphi(1_G)$ è l'elemento neutro in S.

- Vale la proprietà associativa.

$$A * (B * C) = \varphi(a) * (\varphi(b) * \varphi(c)) = \varphi(a) * \varphi(b \circ c) = \varphi(a \circ (b \circ c))$$
$$(A * B) * C = (\varphi(a) * \varphi(b)) * \varphi(c) = \varphi(a \circ b) * \varphi(c) = \varphi((a \circ b) \circ c)$$

  Ma $a \circ (b \circ c) = (a \circ b) \circ c$ perchè in G vale la proprietà associativa, dunque

$$A * (B * C) = \varphi(a \circ (b \circ c)) = \varphi((a \circ b) \circ c) = (A * B) * C$$

- Ogni $A \in S$ ha inverso.
  In G esiste l'inverso di a, a^{-1}, tale che $a \circ a^{-1} = a^{-1} \circ a = 1_G$. Allora

$$\varphi(1_G) = \varphi(a \circ a^{-1}) = \varphi(a^{-1} \circ a)$$
$$1_S = A * \varphi(a^{-1}) = \varphi(a^{-1}) * A$$

  $\varphi(a^{-1})$ è l'inverso di A.

Dunque $(S, *)$ è un gruppo. □

Osservazione. *Se φ è biiettiva, è un isomorfismo tra G e S.*

Sia Δ l'insieme formato dagli automorfismi δ_k.
In A vale $X^r = 1$, dunque $\delta_k = \delta_{k+r\mathbf{Z}}$. Inoltre poichè $(k, r) = 1$, k non può essere nè 0 nè r. Allora $\Delta = \{\delta_{k+r\mathbf{Z}} : 0 < k < r\}$.

Per il teorema appena dimostrato, ponendo $G = \mathbf{Z}/r\mathbf{Z}^*$ rispetto alla moltiplicazione, $S = \Delta$ rispetto alla composizione e $\varphi(k) = \delta_k$ per $k \in \mathbf{Z}/r\mathbf{Z}^*$, si ottiene che Δ è un gruppo.
Poichè δ_k è biiettiva, è un isomorfismo, dunque Δ è isomorfo a $(\mathbf{Z}/r\mathbf{Z})^*$.

Consideriamo questi due automorfismi di Δ:
φ dato da $\varphi(X) = X^p$ (l'automorfismo di Frobenius)
σ dato da $\sigma(X) = X^n$

Sia Γ il sottogruppo ciclico di Δ generato da φ e σ. $\Gamma = \langle \varphi, \sigma \rangle$.
Cioè un elemento $\gamma \in \Gamma$ è $X \mapsto X^{p^a n^b}$ con a, b interi.

Sia ζ una radice primitiva r-esima dell'unità in $\overline{\mathbf{F}}_p$. Cioè r è il più piccolo intero positivo tale che $\zeta^r \equiv 1 \pmod{p}$.

Dobbiamo mostrare che esiste. Esiste sicuramente una radice r-esima dell'unità perchè in $\overline{\mathbf{F}}_p$ tutti i polinomi di grado i hanno i radici, contate con la loro molteplicità.

$$(X-1)^r = X^r - rX^{r-1} + \ldots - 1 \equiv 0 \Longrightarrow r \equiv 0$$

Ma $r \equiv 0$ se e solo se $p \mid r$, che non è vero perchè $(r, p) = 1$. Allora deve essere $(X^r - 1) \not\equiv (X-1)^r \pmod{p}$. L'unica radice del secondo polinomio è l'unità, dunque il primo polinomio ha almeno una radice diversa da 1.

Sia $a \neq 1$ una radice r-esima dell'unità. Se non è una radice primitiva, esiste b tale che $b \mid r$ e $a^b \equiv 1$. Ma r è primo dunque o $b = 1$ (allora $a = 1$, contraddizione) o $b = r$. Dunque a ha periodo r.

Allora esiste ζ radice primitiva r-esima dell'unità in $\overline{\mathbf{F}}_p$.

Teorema. *Sia K un campo, $K[X]$ l'anello dei polinomi e $K[\alpha]$ un'estensione di K. Allora esiste un unico morfismo di anelli*

$$\phi : K[X] \longrightarrow K[\alpha]$$

tale che:
(1) per ogni $a \in K$, $\phi(a) = a$
(2) $\phi(x) = \alpha$.
Questo morfismo è la valutazione $f(X) \mapsto f(\alpha)$.

Dimostrazione. (Unicità) Sia $f = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$; allora, poichè ϕ deve essere un morfismo, avremo

$$\begin{aligned} \phi(f) &= \phi(a_0 + a_1 X + \cdots + a_n X^n) \\ &= \phi(a_0) + \phi(a_1)\phi(X) + \cdots + \phi(a_n)\phi(X^n) \\ &= a_0 + a_1\alpha + \cdots + a_n\alpha^n \end{aligned}$$

e quindi ϕ è univocamente determinato.

(Esistenza) L'applicazione ϕ definita dalla formula appena scritta è un morfismo poichè conserva le operazioni: $\phi(f)\phi(g) = \phi(fg)$. □

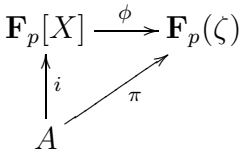
Definiamo l'applicazione

$$\pi : A \longrightarrow \mathbf{F}_p(\zeta)$$

ponendo $\pi(X) = \zeta$.

π è suriettiva ed è un morfismo di anelli.

Infatti, detta i l'inclusione, si ha il diagramma



Per il teorema precedente, ponendo $K = \mathbf{F}_p[X]$ e $\alpha = \zeta$, ϕ è un morfismo, dunque anche $\pi = \phi \circ i$ è un morfismo.

Consideriamo questo sottogruppo di A^*

$$G = \{a \in A^* : \sigma(a) = a^n\}$$

È un sottogruppo:

- G è chiuso: se $a, b \in G$ è $\sigma(a) = a^n$ e $\sigma(b) = b^n$, dunque $\sigma(ab) = (ab)^n$ cioè $ab \in G$.
- esiste l'elemento neutro: $1 \in G$ perchè $1 = \sigma(1) = 1^n$.
- esiste l'inverso.
  Vogliamo mostrare che se $a \in G$ e $(k, r) = 1$, allora $a^k \in G$. Così, poichè G è finito, esiste $i \in \mathbf{Z}$ tale che $a^i = 1$, dunque esiste l'inverso di a.
  Sia δ_k un automorfismo di Δ; esiste perchè $(k, r) = 1$. Sia $\sigma = \delta_n$.
  Allora $\delta_k \delta_n = \delta_n \delta_k = \delta_{nk}$ perchè $(n, r) = 1$.
  Per verificare che $a^k \in G$, bisogna mostrare che $\delta_n(a^k) = (a^k)^n$.

  $$\delta_n(a^k) = \delta_n(\delta_k(a)) = \delta_k(\delta_n(a))$$

  $$(a^k)^n = (a^n)^k = \delta_k(a^n)$$

  Allora $\delta_n(a^k) = (a^k)^n \iff \delta_k(\delta_n(a)) = \delta_k(a^n)$, che è vera perchè $a \in G \Longrightarrow \delta_n(a) = a^n$.

L'immagine di G, $H = \pi(G)$ è un sottogruppo di $\mathbf{F}_p(\zeta)^*$.

Infatti c'è una mappa π dal gruppo G all'insieme H che conserva le operazioni, H è un gruppo. π ristretto a G è un morfismo suriettivo.

$$\begin{array}{ccc} G & \subset & A^* \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ H & \subset & \mathbf{F}_p(\zeta)^* \end{array}$$

Definizione. *Sia d un intero ≥ 1. $\varphi(d)$, detta funzione di Eulero, dà il numero di interi x con $0 < x < d$ tali che $(x, d) = 1$ o, in altre parole, il numero di elementi la cui immagine in $\mathbf{Z}/d\mathbf{Z}$ è un generatore di questo gruppo.*

Proposizione. *Sia $n \geq 1$ un intero. Allora*

$$\sum_{d|n} \varphi(d) = n$$

Dimostrazione. Se d divide n, sia C_d l'unico sottogruppo di $\mathbf{Z}/n\mathbf{Z}$ di ordine d e sia Φ_d l'insieme dei generatori di C_d. Poichè ogni elemento di $\mathbf{Z}/n\mathbf{Z}$ genera uno dei C_d, il gruppo $\mathbf{Z}/n\mathbf{Z}$ è unione disgiunta dei Φ_d. Si ha

$$n = \#\,\mathbf{Z}/n\mathbf{Z} = \sum_{d|n} \#\,\Phi_d = \sum_{d|n} \varphi(d) \qquad \square$$

Proposizione. *Sia H un gruppo finito di ordine n. Supponiamo che, per ogni d che divide n, l'insieme degli $x \in H$ tali che $x^d = 1$ abbia al massimo d elementi. Allora H è ciclico.*

Dimostrazione. Sia d un divisore di n. Se esiste un elemento $x \in H$ di periodo d, il sottogruppo $(x) = \{1, x, \ldots, x^{d-1}\}$ generato da x è ciclico ed ha ordine d. Dall'ipotesi segue che tutti gli $y \in H$ tali che $y^d = 1$ appartengono a (x). In particolare tutti gli elementi di H di periodo d generano (x); essi sono in numero di $\varphi(d)$.
Dunque il numero di elementi di H di periodo d è 0 o $\varphi(d)$. Se fosse 0 per un valore di d, la formula

$$n = \sum_{d|n} \varphi(d)$$

mostrerebbe che il numero di elementi di H è minore di n, che è contro l'ipotesi.

In particolare, esiste un elemento $x \in H$ di periodo n e H coincide con il gruppo ciclico (x). $\square$

Teorema. *Il gruppo moltiplicativo* $\mathbf{F}_q^*$ *di un campo finito* $\mathbf{F}_q$ *è ciclico ed ha ordine* $q-1$.

Dimostrazione. L'equazione $x^d = 1$ ha grado d, dunque ha al massimo d soluzioni in $\mathbf{F}_q$. Applicando la seconda proposizione a $H = \mathbf{F}_q^*$ e $n = q-1$, si ottiene la tesi. □

Osservazione. *Più in generale, questa dimostrazione prova che ogni sottogruppo finito del gruppo moltiplicativo di un campo è ciclico.*

H è un gruppo ciclico perchè sottogruppo di $\mathbf{F}_p(\zeta)^*$, che è ciclico per il teorema appena visto.

Sia $\gamma \in \Gamma = \langle \varphi, \sigma \rangle$. Allora γ agisce su un elemento g di G elevandolo alla potenza $e_\gamma = p^a n^b$ con $a, b \in \mathbf{Z}$

$$\gamma(g) = g^{p^a n^b} = g^{e_\gamma}$$

Sia $\exp(G)$ il minimo comune multiplo dei periodi degli elementi di G.

Sia $a \in G$; indichando con $|a|$ il periodo di a, si ha

$$|a| = |\sigma(a)| = |a^n| = \frac{|a|}{(|a|, n)}$$

dove l'ultima uguaglianza si ottiene dalla proposizione.

Proposizione. *Sia* G *un gruppo finito. Sia* $a \in G$ *un elemento di periodo* r. *Allora* $|a^n| = \frac{r}{(r,n)}$.

Dimostrazione. Sia $k = |a^n|$, cioè k è il più piccolo intero positivo tale che $a^{nk} = (a^n)^k = 1 = a^0$. Allora $nk \equiv 0 \pmod{r}$, cioè r divide nk.

Allora $\frac{r}{(r,n)} \mid k$ cioè esiste $t \in \mathbf{Z}$ tale che $k = t\frac{r}{(r,n)}$. Il più piccolo di questi k si ha per $t = 1$. Dunque $k = \frac{r}{(r,n)}$. □

Dunque $(|a|, n) = 1$ e anche $(\exp(G), n) = 1$. Allora, poichè $e_\gamma = p^a n^b$ e p divide n, si ha $(e_\gamma, \exp(G)) = 1$.

La mappa

$$\Gamma \longrightarrow (\mathbf{Z}/\exp(G)\mathbf{Z})^*$$

data da $\gamma \mapsto e_\gamma$ modulo $\exp(G)$ conserva l'operazione, dunque è un omomorfismo di gruppi.

Poichè H è ciclico, il suo ordine s divide $\exp(G)$.
Si ha quindi l'omomorfismo

$$\Gamma \longrightarrow (\mathbf{Z}/s\mathbf{Z})^*$$

che mappa φ e σ nelle classi di resto modulo s.

A questo punto, vediamo che succede se n è primo. Si ha $n = p$ e quindi $\varphi = \sigma$.

Teorema. *Se n è primo, $f(x^n) = f(x)^n \pmod n$.*

Dimostrazione. Sia $f = a_0 + a_1 x + \cdots + a_d x^d$. Il coefficiente di x^i nel polinomio $f(x)^n$ è

$$a'_i = \sum_{\substack{i_0+i_1+\ldots+i_d=n \\ i_1+2i_2+\ldots+di_d=i}} a_0^{i_0} \cdots a_d^{i_d} \frac{n!}{i_0! \cdots i_d!}$$

a'_i è sempre divisibile per n, a meno che esista j tale che $i_j = n$. In questo caso $i = ji_j = jn$, dunque $a'_i = a_j^n \frac{n!}{n!} = a_j^n \equiv a_j$ perchè n è primo.
Dunque $f(x^n) = f(x)^n \pmod n$ perchè per ogni i i coefficienti di x^i sono uguali. □

Per il teorema, $G = A^*$, quindi $H = \mathbf{F}_p(\zeta)^*$
Sia f il periodo di n modulo r. Quindi $\Gamma = \langle\varphi\rangle$ ha ordine f.
H ha ordine $s = p^f - 1 = n^{\#\Gamma} - 1$

Anche se n non è primo, si può dimostrare che $s > n^{[\sqrt{\#\Gamma}\,]}$ (vedi il *Lemma* nella sezione seguente).

Sia $\psi = \sigma\varphi^{-1}$. L'omomorfismo $\Gamma \longrightarrow (\mathbf{Z}/s\mathbf{Z})^*$ manda ψ in $\frac{n}{p} := q$.
Consideriamo i prodotti $\varphi^i\psi^j$ per $0 \le i, j \le [\sqrt{\#\Gamma}]$, dove [ ] indica la parte intera. Dunque $\varphi^i\psi^j = \varphi^i\sigma^j\varphi^{-j}$.
Poichè $\sqrt{\#\Gamma} < 1 + [\sqrt{\#\Gamma}]$, si ha

$$\#\Gamma < (1 + [\sqrt{\#\Gamma}])^2 = \#(\varphi^i\psi^j)$$

Infatti $1 + [\sqrt{\#\Gamma}]$ è il numero di valori che possono assumere i e j.

Perciò esistono due coppie distinte (i, j) e (i', j') tali che $\varphi^i\psi^j$ e $\varphi^{i'}\psi^{j'}$ sono lo stesso elemento in Γ.

Quindi le loro immagini p^iq^j e $p^{i'}q^{j'}$ sono uguali in $(\mathbf{Z}/s\mathbf{Z})^*$.

$$p^iq^j \leq n^{\max(i,j)} \leq n^{[\sqrt{\#\Gamma}]} < s$$

dove la prima disuguaglianza si ottiene da $p \leq n$ perchè $p \mid n$, $q \leq n$ perchè $q = \frac{n}{p}$ e $i, j \geq 0$.

Nello stesso modo si dimostra

$$p^{i'}q^{j'} < s$$

Dunque $p^iq^j = p^{i'}q^{j'}$ in $\mathbf{Z}$ (e non solo in $\mathbf{Z}/s\mathbf{Z}$).

Poichè $(i, j) \neq (i', j')$,

$$p^i\frac{n^j}{p^j} = p^{i'}\frac{n^{j'}}{p^{j'}}$$

Dunque

$$p^{i-i'} = \left(\frac{n}{p}\right)^{j'-j}$$

cioè il secondo membro è una potenza di p; dunque n deve essere una potenza di p. Questo prova il teorema.

Lemma

Nelle ipotesi del teorema e secondo le definizioni date nella dimostrazione, si ha

$$s > n^{[\sqrt{\#\Gamma}\,]}$$

Dimostrazione. Poichè $p \not\equiv 1 \pmod{r}$, r non divide $p - 1$.

Scomponiamo $X^r - 1$ nei suoi fattori irriducibili.

$$X^r - 1 = (X - 1)f_1(X) \cdots f_l(X)$$

L'unica radice di $X^r - 1$ in $\mathbf{F}_p[X]$ è 1; non ve ne sono altre perchè r non divide $p-1$, dunque non ci sono elementi di periodo r (o di periodo divisore di r, visto che r è primo).

Allora i fattori irriducibili di $\frac{X^r-1}{X-1}$ in $\mathbf{F}_p[X]$ hanno almeno grado 2 e quindi non possono dividere nessun polinomio di grado 1. Dunque $X+j$ per $0 \leq j < r-1$ sono unità in A.

Per ipotesi questi polinomi sono contenuti in G. Inoltre essi sono tutti distinti modulo p perchè $p > r$.

Poichè G è chiuso rispetto al prodotto, per ogni $J \subset I = \{0, 1, \ldots, r-2\}$ il polinomio

$$f_J = \prod_{j \in J} (X + j)$$

appartiene a G. Questi polinomi sono tutti distinti in $\mathbf{F}_p[X]$ perchè i loro zeri sono diversi.

I loro gradi sono $\leq r-1$ dunque essi sono distinti anche modulo $\frac{X^r-1}{X-1}$ cioè in A.

L'unico problema potrebbe nascere nel caso si avesse $f_I \equiv f_\emptyset \pmod{\frac{X^r-1}{X-1}}$ cioè se

$$\begin{aligned} f_I - f_\emptyset = \prod_{j \in I} (X+j) - 1 &= \frac{X^r - 1}{X - 1} \quad \text{nell'anello } \mathbf{F}_p[X] \\ X(\ldots) - 1 &= X^{r-1} + \cdots + X + 1 \end{aligned}$$

Eguagliando le unità si ottiene -1=1 in $\mathbf{F}_p[X]$ cioè $p = 2$. Allora $p = 2 \mid n$, ma non esiste nessun primo $r < 2$. Questo contraddice le ipotesi del teorema. Dunque il caso $f_I \equiv f_\emptyset \pmod{\frac{X^r-1}{X-1}}$ non si verifica.

Il numero di sottoinsiemi J di I è 2^{r-1} dunque $\# G \geq 2^{r-1}$.

Componendo π con gli automorfismi in Δ, si ottiene, per ogni $k \in (\mathbf{Z}/r\mathbf{Z})^*$, l'omomorfismo di anelli

$$\pi_k = \pi \circ \delta_k : A \longrightarrow \mathbf{F}_p(\zeta)$$

dato da $X \mapsto \zeta^k$.

Poichè se $a \in G$ allora $\delta_k(a) = a^k \in G$, si ha che $\delta_k(G) = G$ per ogni k coprimo con r, cioè Δ conserva G. Allora ogni π_k mappa G in H, sottogruppo di $\mathbf{F}_p(\zeta)^*$.

Consideriamo l'omomorfismo α dato dalla composizione

$$G \hookrightarrow A^* \xrightarrow{(\pi_k)_{k \in C}} \prod_{k \in C} \mathbf{F}_p(\zeta)^*$$

dove C è un sottoinsieme del sottogruppo generato da p e n in $(\mathbf{Z}/r\mathbf{Z})^*$. Cioè se $c \in C$, esistono $a, b \in \mathbf{Z}$ tali che $c \equiv p^a n^b \pmod{r}$.

$\#\,\alpha(G) \leq s^{\#\,C}$ perchè $\#\,\pi_k(G) = \#\,H = s$.

Mostriamo che α è iniettiva, così sarà $\#\,G \leq \#\,\alpha(G) \leq s^{\#\,C}$.
Sia $a \in G$ e $\pi_k(a) = 1$ per qualche $k \in (\mathbf{Z}/r\mathbf{Z})^*$. Mostriamo che $a = 1$.

$$\pi_{kn}(a) = \pi_k(\sigma(a)) = \pi_k(a^n) = \pi_k(a)^n = 1$$

$$\pi_{kp}(a) = \pi_k(\varphi(a)) = \pi_k(a^p) = \pi_k(a)^p = 1$$

Dunque se $\pi_k(a) = 1$ per ogni $k \in C$, allora vale per ogni k coprimo con r.
Consideriamo $a - 1 \in A$ come polinomio $h(X)$ modulo $\frac{X^r-1}{X-1}$. Allora per ogni k primo con r vale $h(\zeta^k) = \pi_k(h) = \pi_k(a-1) = \pi_k(a) - 1 = 0$.
Dunque $h(X) = h(\pi_k^{-1}(\zeta^k)) = 0$. Perciò $a = 1$.

Poichè $\#\,C = [\Delta : \Gamma]$, si ha $2^{r-1} \leq \#\,G \leq s^{\#\,C} = s^{[\Delta:\Gamma]}$. Dunque

$$s \geq 2^{\frac{r-1}{[\Delta:\Gamma]}}$$

Inoltre, dal momento che $\#\,\Gamma[\Delta : \Gamma] = \#\,\Delta = r - 1$, vale

$$s \geq 2^{\frac{r-1}{[\Delta:\Gamma]}} = 2^{\#\,\Gamma}$$

L'ordine di $\sigma \in \Gamma$ è $\mathrm{ord}_r\, n > (\log n/\log 2)^2$ per ipotesi. Dunque

$$\#\,\Gamma \geq \mathrm{ord}\,\sigma > \left(\frac{\log n}{\log 2}\right)^2$$

$$\sqrt{\#\,\Gamma} > \frac{\log n}{\log 2} = \log_2 n$$

$$2^{\sqrt{\#\Gamma}} >= 2^{\log_2 n} = n$$

Quindi

$$2^{\#\,\Gamma} > n^{\sqrt{\#\Gamma}}$$

$$s \geq 2^{\#\,\Gamma} > n^{\sqrt{\#\,\Gamma}} \geq n^{[\sqrt{\#\,\Gamma}\,]}$$

□

Algoritmo e analisi dei tempi

Algoritmo. *Sia dato $n > 1$.*
(i) Controlla che n non sia potenza propria di un intero.
(ii) Provando per $r = 2, 3, \ldots,$ determina il più piccolo primo r che non divide n nè alcuno dei numeri $n^i - 1$ per $1 \leq i \leq (\log n/\log 2)^2$.
(iii) Controlla che n non abbia divisori primi propri $\leq r$.
(iv) Per $0 \leq j < r - 1$ controlla che $(X + j)^n = X^n + j$ nell'anello $(\mathbf{Z}/n\mathbf{Z})[X]/(X^r - 1)$.
Se n non passa il test, è composto; se lo passa, è primo.

Dimostrazione. Se n è primo, passa il test *(iv)* per il piccolo teorema di Fermat.

Viceversa, supponiamo che n passi il test per qualche primo r.
Poichè n ha passato il test *(iii)*, o è primo, oppure non ha divisori primi $\leq r$. Questo soddisfa l'ipotesi (1) del teorema. Poichè r non divide i $n^i - 1$ per $1 \leq i \leq (\log n/\log 2)^2$, l'ordine di n modulo r è maggiore di $(\log n/\log 2)^2$. Questo soddisfa l'ipotesi (2) del teorema.
Il superamento del test *(iv)* soddisfa l'ipotesi (3) del teorema.
Dunque n è potenza di un primo. Poichè n ha passato il test *(i)*, è primo. □

Riportiamo brevemente i risultati di analisi dei tempi per questo algoritmo.

Il primo test viene effettuato controllando che $n^{1/m} \notin \mathbf{Z}$ per tutti gli interi $2 \leq m \leq \log n/\log 2$. Questo si può fare in un tempo $\mathrm{O}((\log n)^4)$.

Il secondo test non richiede più di $r\,\mathrm{O}((\log n)^2)$ moltiplicazioni modulo un intero $\leq r$. Per questo servono al massimo $\mathrm{O}(r(\log r \log n)^2)$ operazioni elementari.

Il terzo test richiede al massimo un tempo $\mathrm{O}(r(\log n)^2)$.

Per effettuare l'ultimo test sono necessarie $r\,\mathrm{O}(\log n)$ moltiplicazioni nell'anello $(\mathbf{Z}/n\mathbf{Z})[X]/(X^r - 1)$. Se l'algoritmo che viene utilizzato per moltiplicare due elementi di lunghezza t richiede al massimo $\mathrm{O}(t^\mu)$ operazioni elementari, allora il quarto test viene svolto in un tempo massimo $\mathrm{O}((r \log n)^{1+\mu})$.

Poichè $\mu \geq 1$ e $r > \mathrm{ord}_r\, n > (\log n/\log 2)^2$, il terzo test richiede la parte più rilevante del tempo necessario all'algoritmo.

Riferimenti bibliografici

[1] M. Agrawal, N. Kayal, N. Saxena, *Primes is in P*, IIT Kanpur, Preprint of August 8, 2002, http://www.cse.iitk.ac.in/news/primality.html.

[2] J.P. Serre, *A course in Arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer, New York, 1973.