

TEORIA DEI NUMERI 1 (MEDIUM)

Titolo nota

05/09/2011

$q(x)$ ha grado $n \Rightarrow q$ non ha più di n radici

α è radice di $q \Leftrightarrow q(\alpha) = 0$

$$\Leftrightarrow x - \alpha \mid q(x) \quad q(x) = (x - \alpha) r(x)$$

• $q(x) = r(x) \quad \forall x \in \mathbb{Z}_p \not\Rightarrow q = r$ come polinomi

$$x^p - x = 0 \quad \forall x \in \mathbb{Z}_p$$

• $f(a) = 1 \quad f(x) = 0 \quad x \not\equiv 0 \pmod{p}$

$$1 - x^{p-1} \quad 1 - (x - \alpha)^{p-1}$$

• $\text{ord}_p(\alpha) = \min \left\{ k > 0 : \alpha^k \equiv 1 \pmod{p} \right\}$

$$\text{ord} \mid \varphi(p) = p - 1$$

$$\text{ord}(\alpha b) \quad \text{ord}(\alpha) \quad \text{ord}(b)$$

$$b = \alpha = (-1)$$

$$(ab)^k \equiv 1 \pmod{p}$$

$$\alpha^{k \cdot \text{ord}(b)} \cdot b^{k \cdot \text{ord}(b)} \equiv 1 \pmod{p}$$

$$\text{ord}_p(\alpha) \mid k \cdot \text{ord}(b)$$

$$\frac{\text{o}(\alpha)}{(\text{o}(\alpha), \text{o}(b))} \mid k \quad \frac{\text{o}(b)}{(\text{o}(\alpha), \text{o}(b))} \mid k$$

$$\left[\frac{\text{o}(\alpha)}{(\text{o}(\alpha), \text{o}(b))}, \frac{\text{o}(b)}{(\text{o}(\alpha), \text{o}(b))} \right] \mid k$$

$$\frac{1}{(\text{o}(\alpha), \text{o}(b))} \quad \left[\text{o}(\alpha), \text{o}(b) \right] \mid \text{o}(\alpha b) \mid [\text{o}(\alpha), \text{o}(b)]$$

$$(\alpha b)^{[\text{o}(\alpha), \text{o}(b)]} \equiv 1 \pmod{p}$$

• Modulo p esiste un generatore

$$\exists g \text{ t.c. } \text{ord}_p(g) = p-1$$

$$\{g^0, g^1, \dots, g^{p-2}\} = \{1, 2, \dots, p-1\}$$

$$\{m \mid \exists x : \text{ord}_p(x) = m\}$$

$$\begin{matrix} m_1 & m_2 \\ x_1 & x_2 \end{matrix}$$

$$m_1 = 9 \cdot 2$$

$$m_2 = 3 \cdot 4$$

$$\begin{aligned} x_1^2 &\text{ ha ordine 9} \\ x_2^3 &\text{ ha ordine 4} \end{aligned} \quad \left. \begin{array}{l} \text{ha ordine 9} \\ \text{ha ordine 36} \end{array} \right\} x_1^2 x_2^3$$

M = massimo degli ordini mod p .

$q(x) = x^M - 1$. Che radici ha?

$\alpha \in \mathbb{Z}_p^*$ $\text{ord}_p(\alpha) \nmid M$ (per assurdo)

$M < [\circ(\alpha), M]$ è insieme ordini

$$\alpha^M \equiv 1 \pmod{p} \Rightarrow q(\alpha) = 0$$

$$M = \deg q(x) \geq p-1$$

Esiste g : $\text{ord}_p(g) = M = p-1$

Oss $\text{ord}(g^k)$ se $(k, p-1) = 1$?

$$g^{km} \equiv 1 \pmod{p} \Leftrightarrow p-1 \mid km$$

$$\Leftrightarrow p-1 \mid m$$

$\text{ord}(g^k) = p-1$ Ci sono $\varphi(p-1)$ gener.

• $q(x)$ polinomio di grado $\leq p-2$

Allora $\sum_{i=0}^{p-1} q(i) \equiv 0 \pmod{p}$.

$$q(x) = x^m \quad (\text{basta per questi:})$$

$\sum_{i=0}^{p-1} i^m$ non contribuisce (se $m > 0$)

$$\sum_{i=1}^{p-1} q(i) = \sum_{j=0}^{p-2} q(g^j) =$$

$$= \sum_{j=0}^{p-2} g^{mj} = \frac{g^{m(p-1)} - 1}{g^m - 1} \pmod{p}$$

$$\equiv_0$$

Se $m < p-1$, $g^m - 1 \not\equiv 0 \pmod{p}$

Dim. altern.

$$f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$$

$$i \mapsto \alpha \cdot i \quad \alpha \neq 0 \pmod{p}$$

$$\underbrace{\sum_{i=0}^{p-1} i^m}_{S} = \sum_{i=0}^{p-1} (\alpha i)^m \equiv \alpha^m \sum_{i=0}^{p-1} i^m$$

$$S \equiv \alpha^m \cdot S \pmod{p}$$

$$\alpha^m \neq 1 \Rightarrow S \cdot (\alpha^m - 1) \equiv 0 \pmod{p}$$

$$\Downarrow$$

$$S \equiv 0 \pmod{p}$$

α = generatore

$\alpha^m - 1$ non puo' essere sempre 0, perche'
altrimenti $x^m - 1$ avrebbe troppe radici

• Frazioni mod p: funzionano

$$\frac{a}{b} \equiv ab^{-1}$$

$$\frac{a}{b} + \frac{c}{d} \equiv \frac{ad+bc}{bd} \pmod{p}$$

Mo qualcosa Trovare tutti gli m che sono
(2005/4)

coprimi con tutti i numeri della forma $2^n + 3^n + 6^n - 1$

$$(2^n + 3^n + 6^n - 1, p) = 1$$

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$$

$$p \mid \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1$$

$$x^{p-1} = 1 \Rightarrow x^{p-2} \equiv 1/x \pmod{p}$$

$$n = p-2$$

$$2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 = 0 \pmod{p}$$

$$\boxed{m=1}$$

Attenzione: non dividere per 0 vuol dire
non dividere per multipli di p ($\Rightarrow p=2,3$
~~a mano!~~)

"SOLLEVAMENTO, o, HENSEL

$q(x) \in \mathbb{Z}[x]$ polinomio a coeff. interi

Mod p ha certe radici x_1, \dots, x_r

Se $q'(x_i) \not\equiv 0 \pmod{p}$, allora il numero di soluzioni mod p^n non dipende da n

$$q(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_0 x^0$$

$$q'(x) = n \cdot \alpha_n x^{n-1} + (n-1) \alpha_{n-1} x^{n-2} + \dots + \alpha_1 x^0 + \dots$$

$$q(x_i) \equiv 0 \pmod{p^n}$$

Cerchiamo le radici mod p^{n+1} .

$$q(\alpha) \equiv 0 \pmod{p^{n+1}} \Rightarrow q(\alpha) \equiv 0 \pmod{p^n}$$

$$\alpha \equiv x_i \pmod{p^n}$$

$$\alpha \equiv x_i + k \cdot p^n \pmod{p^{n+1}}$$

$$q(x_i + k \cdot p^n) \equiv$$

$$(x_i + k \cdot p^n)^m \equiv x_i^m + x_i^{m-1} \cdot m \cdot k \cdot p^n$$

$$+ p^{2m} (\dots) \equiv$$

$$= x_i^m + (m x_i^{m-1})(k \cdot p^n) \pmod{p^{n+1}}$$



$$0 \equiv q(x_i + k \cdot p^n) \equiv \underbrace{q(x_i)}_{\alpha} + \underbrace{q'(x_i) \cdot k \cdot p^n}_{\alpha \cdot p^n} \pmod{p^{n+1}}$$

$$\Leftrightarrow -\alpha \cdot p^n \equiv q'(x_i) \cdot k \cdot p^n \pmod{p^{n+1}}$$

$$\Leftrightarrow -\alpha \equiv q'(x_i) \cdot k \pmod{p}$$

$$\Leftrightarrow k \equiv -\alpha \cdot (q'(x_i))^{-1} \pmod{p}$$

$$x^2 \equiv \alpha \pmod{p^n}$$

$$q(x) = x^2 - \alpha \quad q'(x) = 2x \quad q'(x) \neq 0 \quad (\text{se } p \neq 2)$$

$$x^2 \equiv 1 \pmod{8}$$

ESERCIZI

$n \nmid 2^n - 1$ $n \neq 1$. Per assurdo $n \dots$

$$p \mid n \quad 2^n \equiv 1 \pmod{p}$$

$$\begin{aligned} \text{ord}_p(2) &\mid n \\ &\mid \varphi(p) = p-1 \end{aligned}$$

$$\mid (n, p-1) = 1$$

$p = p_1 \cup \dots \cup p_k$ PICCOLO PRIMO DI n

$$\text{ord}_p(2) = 1 \quad 2^1 \equiv 1 \pmod{p} \quad \text{ASSURDO}$$

$$a > b > 0 \text{ interi coprimi} \Rightarrow n \mid \varphi(\overbrace{a^n - b^n}^M)$$

Se sapessimo costruire x t.c- $\text{ord}_M(x) = n$
avremmo vinto.

$$b = 1 \pmod{a^n - 1}$$

$$a^m \equiv 1 \pmod{a^n - 1}$$

$$\begin{aligned} a^{n-1} &\mid a^{m-1} \Rightarrow a^{m-1} \geq a^{n-1} \\ &\Rightarrow m \geq n \end{aligned}$$

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

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

$$(a/b)^n \equiv 1 \pmod{a^n - b^n}$$

$$(a^n - b^n, b) = (a^n, b) = 1$$

$$\left(\frac{a}{b}\right)^k \equiv 1 \quad (a^n - b^n)$$

$$a^k - b^k \equiv 0 \quad (a^n - b^n)$$

$$a^k - b^k = (a - b)(a^{k-1} + \dots + b^{k-1})$$

$a^k - b^k$ è crescente al variare di k

$\Rightarrow k \geq n$ e fine.

$$n < p \leq \frac{4n+2}{3}, \quad p \text{ primo}$$

Allora $p \mid \sum_{i=0}^n \binom{n}{i}^4$

$$n = p-1 \quad \binom{p-1}{i} \equiv \frac{(p-1)(p-2)\cdots(p-i)}{i!} \\ \equiv (-1)^i \frac{i!}{i!} \equiv (-1)^i \pmod{p}$$

$$n = p-2 \quad \binom{p-2}{i} \equiv \frac{(p-2)(p-3)\cdots(p-1-i)}{i!} \\ \equiv (-1)^i \frac{\cancel{2} \cdot \cancel{3} \cdots \cancel{(i+1)}}{\cancel{1} \cdot \cancel{2} \cdots \cancel{i}} \\ \equiv (-1)^i \frac{3 \cdot 4 \cdots (i+2)}{1 \cdot 2 \cdot 3 \cdots i} \equiv (-1)^i \frac{(i+1)(i+2)}{2}$$

$$n = p-k \quad \binom{p-k}{i} \equiv (-1)^i \frac{(i+k-1)(i+k-2)\cdots(k)}{i!} \\ \equiv (-1)^i \binom{i+k-1}{i} \equiv (-1)^i \binom{i+k-1}{k-1}$$

$$\binom{n}{i}^4 \equiv q(i) \quad \text{con } q \text{ polin di grado } 4(p-n-1)$$

$$\sum_{j=0}^{p-1} q(j) \equiv 0 \pmod{p} \quad i \geq p-k+1 = n+1$$

$$\sum_{j=0}^n q(j) \quad 4(p-n-1) < p-1$$

$$3p < 4n+3 \\ p < \frac{4n+3}{3}$$

VALUTAZIONI P-ADICHE

$$p \mid n \quad p^k \parallel n \quad p^k \mid n \text{ ma } p^{k+1} \nmid n$$

$$k = v_p(n) \quad v_p(a \cdot b) = v_p(a) + v_p(b)$$

$$v_p(a+b) \geq \min \{ v_p(a), v_p(b) \}$$

$$\text{ed } e^- = \infty \quad v_p(a) \neq v_p(b)$$

$$v_p(a) > v_p(b)$$

$$b = p^{v_p(b)} \cdot r$$

$$a = p^{v_p(b)} \cdot p^{v_p(a) - v_p(b)} \cdot q$$

$$a+b = p^{v_p(b)} \cdot \underbrace{\left(r + q \cdot p^{v_p(a) - v_p(b)} \right)}_{\not\equiv 0 \pmod{p}}$$

p primo dispari, $p \nmid x-y$, \checkmark Allora

$$v_p(x^m - y^m) = v_p(x-y) + v_p(m)$$

Per induzione sul numero di fattori primi di n .

$$n = q \quad x-y = kp$$

$$\begin{aligned} x^q - y^q &= (y+kp)^q - y^q = \\ q \neq p &= y^q + y^{q-1} \cdot kpq + (kp)^2 \cdot \dots - y^q \end{aligned}$$

$$v_p(y^{q-1} kpq) < v_p(\text{il resto})$$

$$v_p(x^q - y^q) = v_p(kp) = v_p(x-y)$$

$$q=p \quad = \cancel{y^p} + kp^2 y^{p-1} + (kp)^2 p \cdot \dots + (kp)^{p-yp}$$

$$v_p(k^2 p^3) > v_p(kp^2)$$

$$v_p((kp)^p) > v_p(kp^2)$$

$$v_p(x^p - y^p) = v_p(kp^2) =$$

$$= v_p(kp) + 1$$

$$= v_p(x-y) + v_p(p)$$

$$v_p(x^{mq} - y^{mq}) = v_p((x^m)^q - (y^q)^q) =$$

$$= v_p(x^m - y^q) + v_p(q) =$$

$$= v_p(x-y) + \underbrace{v_p(m) + v_p(q)}$$

$$V_p(mq)$$

$$x^n + y^n = x^n - (-y)^n$$

E se $p=2$?

Se $q \mid x-y$ ($2 \nmid x$) va tutto bene

Se $2 \mid x-y$ ma n è pari, $n=2^k \cdot d$

$$V_2(x^n - y^n) = V_2(x^{2^k} - y^{2^k})$$

$$= V_2((x^2)^{2^{k-1}} - (y^2)^{2^{k-1}}) =$$

$$= V_2(x^2 - y^2) + k-1$$

$$= V_2(x^2 - y^2) + V_2(n) - 1$$

\mathbb{Z}_p^* e' ciclico.

\mathbb{Z}_n^* e' ciclico: per quali n ?

$$|\mathbb{Z}_n^*| = \varphi(n)$$

$$g \in \mathbb{Z}_n^* \text{ t.c. } \text{ord}_n(g) = \varphi(n)$$

$$x \in \mathbb{Z}_n^* \quad x^m \equiv 1 \pmod{n}$$

$$(*) \quad \left\{ \begin{array}{l} x^m \equiv 1 \pmod{p_1^{a_1}} \\ \vdots \\ x^m \equiv 1 \pmod{p_k^{a_k}} \end{array} \right.$$

m e' divisibile per l'ordine di x mod $p_i^{a_i}$ V.

Se prendo $m = \text{lcm}(\varphi(p_1^{a_1}), \dots, \varphi(p_k^{a_k}))$

ritroviamo ho $(*)$

Cercavamo $m = \varphi(n)$. Abbiamo trovato

$$\begin{aligned} \varphi(n) &| [\varphi(p_1^{a_1}), \dots, \varphi(p_k^{a_k})] \\ &\Downarrow \\ \varphi(p_1^{a_1}) \cdots \varphi(p_k^{a_k}) \end{aligned}$$

Ma la φ e' "sempre" pari ($\varphi(1), \varphi(2)$)

Caso 1) c'e' un solo primo nella fatt. di n

Caso 2) c'e' un 2 ed un p^k

Attenzione: $\varphi(2^9)$ è pari anche lui ($9 \geq 2$)

\mathbb{Z}_n^* ciclici $\Rightarrow n = p^k, 2p^k$

$\mathbb{Z}_{2^k}^*$: è ciclico? Solo $\mathbb{Z}_2, \mathbb{Z}_4$

g genera $\mathbb{Z}_{2^k}^*$. $g^2 \equiv 1 \pmod{8}$

$$v_2(g^{2^t} - 1) = v_2(g^2 - 1) + t - 1$$

Essere un generatore vuol dire $g^{2^{k-2}} \not\equiv 1 \pmod{2^k}$

$$t = k-2 \text{ da } v_2(g^{2^{k-2}} - 1) = k-3+3 = k$$

$$g^{2^{k-2}} \equiv 1 \pmod{2^k}$$

Massimo degli ordini? 2^{k-2} , realizzato da 5

$$5^{2^{k-3}} \not\equiv 1 \pmod{2^k} \text{ ma } 5^{2^{k-2}} \equiv 1$$

Induz. su k . $k=3$ OK

$$5^{2^{k-2}} = A \cdot 2^k + 1 \text{ con } A \text{ dispari}$$

$$5^{2^{k-1}} = (A \cdot 2^k + 1)^2 = A^2 \cdot 2^{2k} + A \cdot 2^{k+1} + 1$$

$$= 2^{k+1}(A + \text{pari}) + 1$$

$\{5^m\}$ sono metà degli elementi di $\mathbb{Z}_{2^k}^*$

Ogni elemento di $\mathbb{Z}_{2^k}^*$ si scrive come $\pm 5^m$.

Se invece p è un primo dispari $\mathbb{Z}_{p^n}^*$ è a.c.

g genera \mathbb{Z}_p^*

$$\text{ord}_{p^2}(g) = ?$$

$$g^m \equiv 1 \pmod{p^2} \Rightarrow g^m \equiv 1 \pmod{p}$$

$$\Rightarrow (p-1) \mid m \mid \varphi(p^2) = p(p-1)$$

Cosa accade se l'ordine è $p-1$?

$$p^2 \mid g^{p-1} - 1$$

$$\begin{aligned} (g+p)^{p-1} - 1 &= (g^{p-1} - 1) + g^{p-2} \cdot p \pmod{p^2} \\ &\equiv p \cdot g^{p-2} \not\equiv 0 \pmod{p^2} \end{aligned}$$

Induzione su n (esponente di p)

Sia g un generatore modulo p^2

$$\begin{aligned} n &\leq v_p(g^{(p-1)p^t} - 1) = v_p((g^{p-1})^{p^t} - 1) \\ &= v_p(g^{p-1} - 1) + v_p(p^t) \\ &= 1 + t \end{aligned}$$

$$t \geq n-1 \Rightarrow (p-1) \cdot p^t \geq (p-1) \cdot p^{n-1} = \varphi(p^n)$$

$$n^2 \mid 2^m + 1 \quad n=1, \quad n=3$$

$$p = P.P.P. \text{ di } n. \quad p \mid n^2 \mid 2^m + 1 \Rightarrow 2^m \equiv -1 \pmod{p}$$

$$\Rightarrow 2^{2n} \equiv 1 \pmod{p}$$

$$2^{p-1} \equiv 1 \pmod{p} \Rightarrow \text{ord}_p(2) \mid (2m, p-1) = 2$$

$$\text{ord}_p(2) = 2 \Rightarrow 2^2 \equiv 1 \pmod{p} \Rightarrow p = 3$$

$$n = 3m. \quad 3m^2 \mid 8^m + 1$$

$$q = P.P.P \text{ di } m. \quad 8^{2m} \equiv 1 \pmod{q}$$

$$\text{ord}_q(8) \mid (2m, q-1) = 2$$

$$q \mid 8^2 - 1 = 63 \quad q = 3, 7$$

$$\text{Può essere } q = 7? \quad \text{No} \quad 7 \mid 8^m + 1$$

$$\text{Quindi } q = 3. \quad V_3(n^2) \leq V_3(8^m + 1)$$

$$\begin{aligned} &= 2V_3(m) \\ &= 2[V_3(m) + 1] \\ &= V_3(8+1) + V_3(m) \end{aligned}$$

$$2V_3(m) \leq V_3(m) \quad V_3(m) \leq 0$$

ASSURDO se $m \neq 1$

(IMO 2000) Dire se esiste n : $n \mid 2^n + 1$ e
 n ha esattamente 2000 fattori primi distinti

$$n \mid 2^n + 1 \mid 2^{nd} + 1$$

$$(n, d) = 1 \text{ con } d \mid 2^n + 1$$

$$\Rightarrow nd \mid 2^n + 1 \mid 2^{nd} + 1$$

Saremmo contenti di avere $n = 3^k$

$$3^k \mid \underbrace{2^{3^k} + 1}_{\alpha_k} \quad v_3(2^{3^k} + 1) =$$

$$= v_3(2+1) + v_3(3^k) = k+1$$

$$v_3(2^{3^{k+1}} + 1) = v_3(2^{3^k} + 1) + 1$$

Passando da 3^k a 3^{k+1} , $\alpha_{k+1} \sim \alpha_k^3$ ed ha

solo un fattore 3 in più.

$$\begin{aligned} v_p(2^{3^{k+1}} + 1) &= v_p((2^{3^k})^3 + 1) = \\ &= v_p(2^{3^k} + 1) + v_p(3) \\ &\quad \underbrace{\text{o, per } p \neq 3} \end{aligned}$$

$$2^{3^k} + 1 \mid 2^{3^{k+1}} + 1 \quad (\text{i fattori primi di } \alpha_k$$

si trovano tutti anche in α_{k+1})

Trovare (a, b) con $a > 1, b > 1$ t.c.

$$b^a \mid a^b - 1$$

$p = p_1 p_2 p_3$ che divide b .

$$a^b \equiv 1 \pmod{p}$$

Se p è di pari valo

$$\alpha v_p(b) = v_p(b^a) \leq v_p(a^{b-1}) =$$

$$= v_p(a-1) + v_p(b)$$

$$v_p(b) \cdot (a-1) \leq v_p(a-1)$$

$$\frac{v_p(b)}{a-1}$$

ASSURDO ($\Rightarrow p$ non era
di pari)

$$\alpha v_2(b) \leq v_2(a^2-1) + v_2(b) - 1$$

$$(a-1)v_2(b) \leq v_2(a+1) + v_2(a-1) - 1$$

$$\frac{v_2(b)}{a-1}$$

$$a \leq v_2(a^2-1)$$

$$2^a \leq a^2 - 1 \Rightarrow a \leq 3$$

$$a = 3.$$

$$b^3 \mid 3^b - 1$$

$$b = 2c$$

$$8c^3 \mid g^c - 1$$

$q = p \cdot p \cdot p$ che divide c

$$g^c \equiv 1 \pmod{q}$$

$$\text{ord}_q(g) \mid (c, q-1) = 1$$

$$\Rightarrow q \mid g-1 = 8, \text{ cioè } c \text{ è } \underline{\text{pari}} \quad \underline{\text{No}}$$

RESIDU QUADRATICI E NON

$a \in \mathbb{Z}_p^*$ t.c. $x^2 \equiv a \pmod{p}$ si risolva

Def. $\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{se } a \text{ e' un res. q-mod p} \\ 0, & \text{se } p \mid a \\ -1, & \text{se } a \text{ non e' un residuo} \end{cases}$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$$

"Criterio di Eulero"

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

Se a e' un quadrato, $a \equiv x^2$, $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$

$$q(x) = x^{\frac{p-1}{2}} - 1 \quad f : x \mapsto x^2$$

$$f(x) = f(y) \Leftrightarrow x \equiv \pm y \pmod{p}$$

$$x^2 - y^2 \equiv 0 \pmod{p} \Leftrightarrow (x+y)(x-y) \equiv 0 \pmod{p}$$

Quadrati = RADICI DI $Q(x)$

$$(x^{\frac{p-1}{2}})^2 \equiv x^{p-1} \equiv 1 \pmod{p}$$

$$x^{\frac{p-1}{2}} = +1, -1$$

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

$$\left(g^K\right)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Leftrightarrow p-1 \mid K \left(\frac{p-1}{2}\right)$$

$\Rightarrow K$ e' pari

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \text{ quindi } -1 \in \mathbb{R.Q.} \Leftrightarrow p \equiv 1 \pmod{4}$$

ed in tal caso $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p}$

$$(p-1)! \equiv -1 \pmod{p}$$

Se $p \equiv 3 \pmod{4}$ e $\left(\frac{a}{p}\right) = 1$, allora

(una) radice di a e' $a^{\frac{p+1}{4}}$

$$\left(a^{\frac{p+1}{4}}\right)^2 \stackrel{?}{=} a$$

$$\left(a^{\frac{p+1}{4}}\right)^4 \stackrel{?}{=} a^2$$

m

OK

$$a^{\frac{p+1}{2}} = a^2$$

$$\text{Quindi } \left(a^{\frac{p+1}{4}}\right)^2 \equiv \pm a.$$

Siccome $p \equiv 3 \pmod{4}$, $\left(\frac{-1}{p}\right) = -1$, cioè esattamente uno tra a e $-a$ e' un quadrato, e perciò era proprio $+a$ (perché LHS è un quadrato).

Reciprocità quadratiche

p, q primi dispari distinti.

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Se almeno uno tra p, q e' $\equiv 1 \pmod{4}$, allora p è residuo mod q ($\Rightarrow q$ residuo mod p)

Viceversa, se $p \equiv q \equiv 3 \pmod{4}$, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$.

Lemma (Gauss) Sia $n \not\equiv 0 \pmod{p}$, $p \neq 2$

$$A = \left\{ [kn]_p < p/2 \mid k = 1, \dots, \frac{p-1}{2} \right\}$$

$$B = \left\{ [kn]_p > p/2 \mid k = 1, \dots, \frac{p-1}{2} \right\}$$

$$m = |B| \quad \left(\frac{n}{p}\right) = (-1)^m$$

$$b \in B \quad p - b \stackrel{\text{?}}{=} a \quad (\Rightarrow) \quad a + b = p$$

$$n(k_1 + k_2) \not\equiv p$$

$$|(p - B) \cup A| = \frac{p-1}{2}$$

$$\left\{ 1, \dots, \frac{p-1}{2} \right\}$$

$$\prod_{i=1}^{\frac{p-1}{2}} i \equiv \left(\prod_{a \in A} a \right) \left(\prod_{b \in B} (p-b) \right) \pmod{p}$$

$$\equiv \left(\prod_{a \in A} a \right) (-1)^{|B|} \cdot \left(\prod_{b \in B} b \right)$$

$$\equiv \left(\prod_{i=1}^{\frac{p-1}{2}} (im) \right) (-1)^{|B|}$$

$$\equiv n^{\frac{p-1}{2}} \cdot \prod_{i=1}^{\frac{p-1}{2}} i \cdot (-1)^m \pmod{p}$$

$$1 \equiv n^{\frac{p-1}{2}} \cdot (-1)^m \pmod{p}$$

$$(-1)^m \equiv \left(\frac{n}{p}\right) \pmod{p}$$

$$\left(\frac{2}{p}\right)$$

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1$$

Considera $\left\{ [2k]_{p^2/2} \mid k=1, \dots, \frac{p-1}{2}\right\}$

$$= \left\{ 2k > p/2 \mid k = \right\}$$

Risultato: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Sia $i = \sqrt{-1} \pmod{p}$. $2 = \frac{(1+i)^2}{i} = \frac{1-i+2i}{i} = 2$

$$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} \equiv \left[\frac{(1+i)^2}{i}\right]^{\frac{p-1}{2}} \equiv \frac{(1+i)^{p-1}}{i^{\frac{p-1}{2}}} \equiv \frac{(1+i)^p}{(1+i)i^{\frac{p-1}{2}}}$$

$$\equiv \frac{1+i^p}{(1+i)i^{\frac{p-1}{2}}} \pmod{p}$$

$a = \text{somma elementi } A, b = \dots \text{ di } B$

$$1 + 2 + \dots + \frac{p-1}{2} = \underbrace{a}_{\substack{\text{somma} \\ \text{elementi } A}} + \underbrace{mp - b}_{\substack{\text{somma} \\ \text{elementi } B}}$$

$$n + 2n + 3n + \dots + \left(\frac{p-1}{2}\right)n = a + b + \sum_{k=1}^{\frac{p-1}{2}} p \left\lfloor \frac{kn}{p} \right\rfloor$$

$$(n-1) \left(1 + \dots + \frac{p-1}{2}\right) = 2b - mp + \sum_{k=1}^{\frac{p-1}{2}} p \left\lfloor \frac{kn}{p} \right\rfloor$$

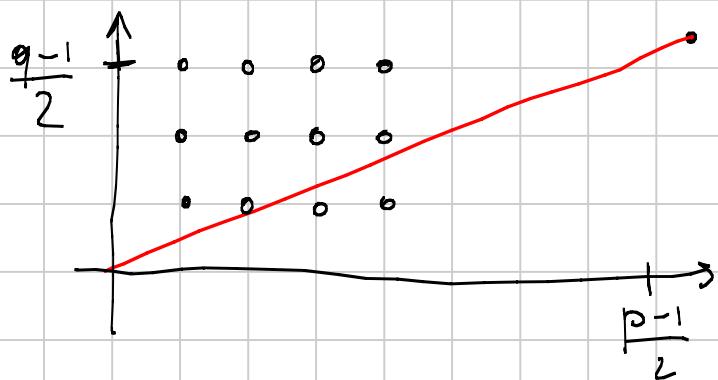
n disp.

\Rightarrow

$$m \cdot p \equiv \sum_{k=1}^{\frac{p-1}{2}} p \left\lfloor \frac{k \cdot n}{p} \right\rfloor \pmod{2}$$

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{k \cdot n}{p} \right\rfloor \quad (2)$$

$$\left(\frac{p}{q} \right) \left(\frac{q}{p} \right) = (-1)^{m_1} (-1)^{m_2} = (-1)^{\sum_k \left\lfloor \frac{k \cdot q}{p} \right\rfloor + \sum_l \left\lfloor \frac{k \cdot p}{q} \right\rfloor}$$



$$y = \frac{q}{p}x$$

$$(-1)^{\frac{(p-1)(q-1)}{4}}$$

Simbolo di Jacobi $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{\alpha_1} \cdots \left(\frac{m}{p_k}\right)^{\alpha_k}$$

$$\left(\frac{m}{n}\right) = -1$$

↓ P

Vale ancora la recipr. quadr.

m non è quadr. mod n

Ese $a \equiv b \pmod{2}$. $2^a - 1 \nmid 3^b - 1$
 $(a \neq 1)$

a e' pari $3 \mid 2^a - 1 \mid 3^b - 1$ ASSURDO

a e' dispari. $3^b - 1 \equiv 0 \pmod{2^a - 1}$

$$\Rightarrow 3^{b+1} \equiv 3 \pmod{2^a - 1}$$

$$\begin{aligned} 1 &= \left(\frac{3}{2^a - 1}\right) = (-1)^{\frac{2(2^a-2)}{4}} \left(\frac{2^a - 1}{3}\right) \\ &= -\left(\frac{2^a - 1}{3}\right) = -\left(\frac{(-1)^a - 1}{3}\right) \end{aligned}$$

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

ASSURDO

$$\left(\frac{n}{p}\right) = 1 \quad \forall p \Rightarrow n \text{ e' un quadrato}$$

$$n = p_1 \cdots p_k$$

$$1 = \left(\frac{n}{p}\right) = \left(\frac{p}{p_1}\right) \left(\frac{p}{p_2}\right) \cdots \left(\frac{p}{p_k}\right) = -1$$

$\uparrow \quad \uparrow \quad \cdots \quad \uparrow$
 $p \equiv 1 \pmod{4} \quad -1 \quad 1 \quad \cdots \quad 1$

Scegliamo q un non-residuo mod p_1 e scriviamo

$$\left\{ \begin{array}{l} p \equiv q \pmod{p_1} \\ p \equiv 1 \pmod{p_2} \\ \vdots \\ p \equiv 1 \pmod{p_k} \\ p \equiv 1 \pmod{4} \end{array} \right.$$

Modo 1: c'è un teorema (Dirichlet) che dice che
p esiste.

$$a \cdot n + b \quad \text{con} \quad (a, b) = 1$$

Modo 2: simboli di Jacobi + pensateci
(idea: scegli p soluzione del sistema
anche se non è primo)

Residui d-esimi, $d \mid p-1$

o.c.: $x^d = a$ ha soluz.

$$x^d \equiv y^d \pmod{p} \Rightarrow \left(\frac{x}{y}\right)^d \equiv 1 \pmod{p}$$

$$x^d - 1 \mid x^{p-1} - 1 = (x-1)(x-2) \cdots (x-(p-1))$$

Quindi $x^d - 1$ ha esattamente d soluz.

$$f(x) = x^d : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$$

La cardinalità dell'immagine è $\frac{p-1}{d}$

\Rightarrow i residui d-esimi sono $\frac{p-1}{d}$

In generale sono $\frac{p-1}{(d, p-1)}$; in particolare,

se $(d, p-1) = 1$, f è surgettiva (e quindi iniettiva)