TEORIA DEI NUMERI 1

Titolo nota 06/09/2010

a INTERO $\quad n > 1$ INTERO

$(a,n) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$

$\mathrm{ord}_n(a) := \min k > 0$ t.c. $a^k \equiv 1 \pmod{n}$

$\langle a \rangle = \{ a^i \mid i \in \mathbb{Z} \} \subseteq \mathbb{Z}_n$

$o(\langle a \rangle) = \mathrm{ord}_n(a)$

$a^m \equiv 1 \pmod{n} \iff \mathrm{ord}_n(a) \mid m$

$m = k\,\mathrm{ord}(a) + r \qquad a^m \equiv a^r$

$\mathrm{ord}_n(a) \mid \phi(n)$

$a, b \qquad (a,n) = 1 \qquad (b,n) = 1$

$\mathrm{ord}(ab)$?

$J = \mathrm{ord}_n(a)$

$K = \mathrm{ord}_n(b)$

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

$a^{mJ} b^{mJ} \equiv 1 \pmod{n}$

$b^{mJ} \equiv 1 \Rightarrow K \mid mJ$

$\frac{K}{(K,J)} \mid m \cdot \frac{J}{(K,J)}$ $\qquad \left(\frac{K}{(K,J)}, \frac{J}{(K,J)}\right) = 1$

$\Downarrow$

$\frac{K}{(K,J)} \mid m \qquad \frac{J}{(K,J)} \mid m$

$\frac{KJ}{(K,J)^2} \mid m \qquad \frac{KJ}{(K,J)^2} = \frac{mcm}{MCD} \mid ord(ab)$

$ord(ab) \mid mcm(ord(a), ord(b))$

$m = mcm \quad J \mid m \quad K \mid m$

$a^m b^m \equiv 1 \cdot 1 \equiv 1$

$\frac{mcm(ord(a), ord(b))}{MCD(ord(a), ord(b))} \mid ord(ab) \mid mcm$ sé

$(ord(a), ord(b)) = 1 \Rightarrow ord(ab) = ord(a)\,ord(b)$

$a, b \in \mathbb{Z}_n^* \quad \exists c : ord(c) = mcm(ord\,a, ord\,b)$

$\mathbb{Z}_n^*$ g el di ord. massimo

$a \in \mathbb{Z}_n^* \quad \exists\, c = mcm(ord(a), ord(b))$

$\text{ord}(a) \mid \text{ord}(g)$ $\Leftarrow$ $\text{ord}(g) = k$

$\forall a,\ \text{ord}(a) \nmid k \iff a^k \equiv 1 \pmod n$

$\mathbb{Z}_p^*$ ciclici

$p(X)$ $\quad p(a) = 0$ $\quad a \in \mathbb{R}$ $\quad p(X) = (X-a)q(X) + k$

$\deg p = d$ $\quad p(X) = (X-a_1)\cdots(X-a_d)$

$p(X)$ ha al + d radici

$p(X) - \prod (X-a_i)$ è pol grado $\le d-1$

[vero in $\mathbb{Z}_p$ $\quad a \neq 0,\ b \neq 0 \Rightarrow ab \neq 0$

$\mathbb{Z}_8$ $\quad x^2 - 1 \equiv 0 \pmod 8$

$\mathbb{Z}_p$ $\quad g$ ord max $\quad \text{ord}_p(g) = k$

$\forall x \in \mathbb{Z}_p^* \quad x^k \equiv 1 \pmod p$

$p-1$ radici $\quad k \ge p-1 \quad \text{ord}(g) \ge p-1$

$=$

$\Rightarrow$ g è generatore

$a = g^m$ $\quad \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$

$$\sum_{i=0}^{p-1} i^m \pmod p \qquad n < p-1$$

$$\text{se } n \neq 0: \quad \sum_{i=1}^{p-1} i^n \equiv \sum_{j=1}^{p-1} (g^j)^n \equiv \sum_{j=1}^{p-1} (g^n)^j \equiv \frac{(1-g^{np})}{1-g^n} \equiv$$

$$\equiv \frac{g^n - g^{np}}{1-g^n} \equiv 0$$

$p-1 \nmid n \qquad \sum_{i=0}^{p-1} i^n \equiv 0 \qquad$ ALTRIMENTI $\sum_{i=0}^{p-1} i^{k(p-1)} \equiv -1 \ (p)$

$$f : \mathbb{Z}_p \to \mathbb{Z}_p \qquad i \to a \cdot i \qquad a \neq 0$$

$$\sum_{i=0}^{p-1} i^n \equiv \sum_{i=0}^{p-1} (ai)^n \equiv a^n \cdot \sum_{i=0}^{p-1} i^n$$

($n < p-1 \qquad X^n - 1$ al più n radici

$\exists\, a \in \mathbb{Z}_p^* : a^n \neq 1$)

$$(a^n - 1) \sum_{i=0}^{p-1} i^n \equiv 0 \iff \sum_{i=0}^{p-1} i^n \equiv 0$$

ESERCIZIO!

$\forall\, p$: $\quad p \mid z^{n^3+1} - z^{n^2+1} + z^{n+1}$ almeno un n.

$p \neq 2, 3, 5 \qquad z^{p-1} \equiv z^{3(p-1)} \equiv z^{5(p-1)} \equiv 1 \bmod p$

$$D = \{ p \mid \exists n : p \mid 2^{n^3+1} - 3^{n^2+1} + 5^{n+1} \}$$

$$P = \prod_{p \in D} (p-1)$$

$n = 4kP$

$p \neq 2,3,5 \quad p \in P$

$$2^{n^3+1} - 3^{n^2+1} + 5^{n+1} \equiv 2 - 3 + 5 \equiv 6 \not\equiv 0$$

$$2^{n^3+1} - 3^{n^2+1} + 5^{n+1} = 2^a 3^b 5^c \qquad a \leq 1 \quad b = 0 \quad c = 0$$

mod 4 ||

$$0 - 3 + 5 \equiv 2 \mod 4$$

mod 3

$$\equiv 2 + 5 \equiv 7 \not\equiv 0$$

$$2 - 3 \equiv -1 \not\equiv 0$$

$$\left| 2^{(4kP)^3+1} - 3^{(4kP)^2+1} + 5^{4kP+1} \right| \leq 2$$

$n \nmid 2^n - 1 \qquad n > 1$

$\operatorname{ord}_n(2) \mid n$

$\exists n \quad n \mid 2^n - 1$

$\operatorname{ord}_n(2) \mid n$

$\operatorname{ord}_n(2) \mid \phi(n)$

p PIÙ PICCOLO PRIMO T.C. $p \mid n$

$p \mid n \mid 2^n - 1 \qquad p \mid 2^n - 1$

$\operatorname{ord}_p(2) \mid n \quad \Rightarrow \quad \operatorname{ord}_p(2) \mid (n, p-1) = 1$

$\operatorname{ord}_p(2) \mid p-1$

$p \mid 2 - 1$ ASSURDO

$a > b > 0$ INTERI $(a, b) = 1$

$n \mid \phi(a^n - b^n)$

$a \in \mathbb{Z}_m \qquad m = a^n - b^n$

$n \mid \operatorname{ord}(a) \Rightarrow n \mid \phi(m)$

$x = \frac{a}{b} \mod m \qquad a, b$ COPRIMI

$\exists\, s, k \qquad sa + kb = 1$

$(b, m) = 1 \quad \exists\, s, k: \quad sb + km = 1 \quad sb \equiv 1 \pmod m$

$\frac{a}{b} + \frac{p}{q} = \frac{aq + bp}{bq}$

$\left(\frac{a}{b}\right)^k = 1 \; ? \qquad a^k \equiv b^k \qquad m \mid a^k - b^k$

$0 < k < n \qquad 0 < a^k - b^k < m \qquad m = a^n - b^n$

$\mathrm{ord}\left(\frac{a}{p}\right) = n \qquad n \mid \phi(a^n - b^n)$

$n^{exp} \mid \phi(a^n - b^n)$

~~$n < p \leq 4n+2$~~ $\qquad p \mid \sum_{i=0}^{n} \binom{n}{i}^4$

$p \mid \sum_{i=0}^{p-1} i^n \qquad n < p-1 \qquad g(x) \quad \deg(g) < p-1$

$\mid \sum_{i=0}^{p-1} g(i)$

BINOMIALE $\in$ POL. IN i

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

$\frac{(p-1)\cdot\ldots\cdot(p-k)}{k!} \equiv \frac{(-1)}{1}\cdot\frac{(-2)}{2}\cdot\ldots\cdot\frac{(-k)}{k} \equiv (-1)^k$

$\frac{\binom{n}{i}}{\binom{p-1}{n}} \equiv \frac{\frac{n!}{i!(n-i)!}}{\frac{(p-1)!}{n!(p-1-n)!}} = \frac{n!}{(p-1)!}\cdot\frac{(p-1-n)!}{(n-i)!}$

$n = p-2$

$\frac{n!}{(p-1)!}(p-i-1)\cdot(p-i-2)\cdot\ldots\cdot(p-i-n+1)$

$$\sum_{i=0}^{n} \binom{n}{i}^4 \equiv \sum_{i=0}^{n} \frac{\binom{n}{i}^4}{\binom{p-1}{i}^4} \qquad \binom{p-1}{n}^4 \equiv 1 \mod p$$

$$\equiv \sum_{i=0}^{n} \left\{ \frac{n!}{(p-1)!} \left[(p-i-1)(p-i-2)\cdots(p-i-n) \right] \right\}^4$$

$$n < i \leq p-i \qquad \text{III} \sum_{i=0}^{p-1}$$

$\deg(q(x)) < p-1$

$4(n-1) < p-1$ $\qquad r = p-n$

$4(p-n-1) < p-1$ $\qquad Hp: p \leq \frac{4n+2}{3}$

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

$\subset \vee D$

~~////~~

VALUTAZIONI p-ADICA

$a \neq 0$ $\qquad p$ PRIMO

$k \in \mathbb{N}$ $\qquad k = v_p(a)$

$p^k \mid a$ $\qquad p^k \| a$

$p^{k+1} \nmid a$

$$v_p(ab) = v_p(a) + v_p(b)$$

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

$v_p(a) \neq v_p(b) \qquad v_p(a+b) = \min$

$a \equiv 1 \mod p \qquad a = kp^{\alpha} + 1$

$v_p(a^n - 1) \qquad (k, p) = 1$

$\alpha = v_p(a-1)$

$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \dots + 1)$

$\dots$

$1 + 1 \dots + 1 = n \neq 0 \pmod{p}$

$(n, p) = 1$

ALLORA $v_p(a^n - 1) = v_p(a-1)$

p PRIMO DISP.

$v_p(a^p - 1)$?

$a = k \cdot p^{\alpha} + 1$

$a^p - 1 = (kp^{\alpha} + 1)^p - 1 = \sum_{i=1}^{p} k^i p^{\alpha i} \binom{p}{i}$

$= kp^{\alpha} \cdot p + kp^{2\alpha} \cdot \binom{p}{2} + n \cdot p^{3\alpha} =$

FTB

$k p^{\alpha+1} \pmod{p^{\alpha+2}}$ $\qquad p^{\alpha+1} \parallel a^p - 1$

$$v_p(a^p - 1) = v_p(a-1) + 1$$

EX: $4 \mid a-1$ $\qquad v_p(a^2-1) = v_p(a-1) + 1$

$$v_p(a^n - 1) = v_p(a-1) + v_p(n)$$

$a \equiv 1 \pmod{p^\alpha}$
p d. sp
app. $p=2$ $4 \mid a-1$

LEMMA

I PRIMO DISP.

g GEN IN $\mathbb{Z}_p^*$

HOPE: g GEN $\mathbb{Z}_{p^k}^*$

g GEN IN $\mathbb{Z}_{p^k}^*$ $k \geq 2$ $\iff$ g GEN $\mathbb{Z}_p^*$ $v_p(g^{p-1} - 1) = 1$

$p^k \mid g^n - 1 \Rightarrow p \mid g^n - 1$ $\qquad p-1 \mid n$

$n = m(p-1)$ $\qquad g^{p-1} = a$ $\qquad v_p(a-1) = 1$

$p^k \mid [g^{p-1}]^m - 1$ $\qquad p^k \mid a^m - 1$

$p^k \mid a^m - 1 \iff v_p(a^m - 1) \geq k$

$v_p(a-1) + v_p(m) \geq k$

$v_p(m) \geq k-1 \quad (p-1)p^{k-1} \mid m(p-1) = \text{ord}(g)$

$\text{ord}(g) = m(p-1) \quad g$ GENERA!

$\Longrightarrow$

g GEN in $\mathbb{Z}_{p^k}^*$ $\quad$ g GEN in $\mathbb{Z}_p^*$

$v_p(g^{p-1}-1) = 1$

$\forall (a,p)=1$: $g^{\text{ord}} \equiv a \pmod{p^k}$

$\forall (a,p)=1$: $g^n \equiv a \pmod{p}$

$v_p(g^{p-1}-1) \geq 2$

$p^k \mid g^{(p-1)p^{k-2}} - 1 \qquad \text{ord}(g) < (p-1)p^{k-1}$

1) g GEN mod p^2

$\Updownarrow$

g GEN mod p^k $\forall k$

2) $\boxed{g \text{ GEN mod } p}$

$-g$ GEN mod p^2

oppure

$-g+p$ GEN $\mod p^2$

g GEN $\mod p^2 \iff g$ GEN $\mod p$

e' $v_p(g^{p-1}-1)=1$

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

$g+p$ GEN $\mod p$ se $v_p((g+p)^{p-1}-1)=1$ ho $v_{IN}=0$

$p^2 \mid (g+p)^{p-1}-1$

$\Downarrow$

$p^2 \mid \left[(g+p)^{p-1}-1\right] - \left[g^{p-1}-1\right]$

$\| \sum_{i=1}^{p-1} p^i g^{p-1-i}\binom{p-1}{i} \equiv p g^{p-2}\binom{p-1}{2} \not\equiv 0 \mod p^2$

ASSURDO. g opp. $g+p$ GENERA $\mod p^2$

SEGUE CHE, PRESO p PRIMO DISPARI, $\mathbb{Z}_{p^k}^*$ E' CICLICA, OVVERO C'E' UN GENERATORE

$\mathbb{Z}_{2^k}^*$

$4 \mid a-1$ $\qquad$ $\boxed{v_2(a^n-1) = v_2(a-1) + v_2(n)}$

$n \geq 3$ $\qquad$ $\mathrm{Ord}_{2^n}(5)$???

"min" k t.c. $v_2(5^k-1) \geq n$

$5 \equiv 1 \pmod 4$ $\qquad$ $5 \equiv 1 \pmod 4$

$v_2(5-1) = 2$

$v_2(5^k-1) = v_2(k) + v_2(5-1) = v_2(k) + 2$

$v_2(k) + 2 \geq n$

PIÙ PICCOLO $k > 0$ PER CUI SUCCEDE ??

$2^{n-2} \mid k$ $\qquad$ $k = 2^{n-2}$

$\mathrm{ord}_{2^n}(5) = 2^{n-2}$

$|\mathbb{Z}_{2^n}^*| = 2^{n-1}$ $\qquad$ $k \in \{1, \dots, 2^{n-2}\}$

$\boxed{\pm 5^k}$ $\qquad$ $5^k \not\equiv \pm 5^j \pmod{2^n}$

ALLORA $k = j$ $\qquad$ ↑ è UN PIÙ

$5^k \equiv 5^j \Rightarrow 5^{k-j} \equiv 1 \quad |k-j| < \mathrm{ord}(5)$

$k-j = 0$

$5^k \equiv -5^j \pmod{2^n}$

$\Downarrow$

$5^k \equiv -5^j \pmod 8$

$5^{k-j} \equiv -1 \pmod 8$

$5 \quad 1G \equiv 1 \quad 5 \quad 1$

$\pm 5^k \quad 2^{n-1}$ numeri tutti diversi

Preso $a \in \mathbb{Z}_{2^n}^*$ $\exists k$ t.c. $a \equiv 5^k \vee a \equiv -5^k$

ORDINE massimo: c'è sempre el di ord massimo

in $\mathbb{Z}_{2^n}^*$ tutti ordine è almeno 2^{n-2}

$\mathrm{ord}(5) \geq 2^{n-2}$

$\mathrm{ord}_{2^n}(g) = 2^{n-1} \qquad g = \boxed{\pm 5^k}$

$g^{2^{n-2}} \equiv (\pm 5^k)^{2^{n-2}} \equiv 5^{k \cdot 2^{n-2}} \equiv 1 \mod 2^n$

TEOREMA RADICI PRIMITIVE $\mathbb{Z}_{p^k}^*$

p_i : $p_i^{k_i} \| n$ $\quad g_i \equiv GEN \bmod p_i^{k_i}$

$g_i \equiv 1 \bmod p_j^{k_j} \quad j \neq i$

2 CASI A CASI p^k DISPARI CASI

MOD $2 \cdot p^k$

$g \equiv 1 \bmod 2 \qquad g \equiv GEN \bmod p^k$

$$\boxed{ord_{2p^k}(g) = mcm\left(ord_2(g),\ ord_{p^k}(g)\right) = \phi(p^k) = \phi(2p^k)}$$

$(a,b)=1$

$$\boxed{ord_{ab}(g) = mcm\left(ord_a(g),\ ord_b(g)\right)}$$

$(a,b) \qquad \phi(ab) = \phi(a)\,\phi(b)$

$\phi(2p^k) = \phi(2)\cdot\phi(p^k) = \phi(p^k)$

DATO $n = \prod_{i=1}^{r} p_i^{k_i} \cdot 2^k$ QUALE È IL MINIMO

m TALE CHE $a^m \equiv 1 \pmod n$ $\forall (a,n)=1$?

$ord_n(a) = mcm\left(ord_{p_1^{k_1}} a, \dots, ord_{p_r^{k_r}} a, ord_{2^k} a\right)$

$| \ mcm\left(\phi(p_1^{k_1}), \dots, \phi(p_r^{k_r}), 2^{k-2}\right)$

se $8 \mid n$ oppure se $\exists\, p \neq q$ primi dispari

$pq \nmid n$ allora vale $m^{\lambda} < \phi(n)$

$$\phi(n) = \prod \phi(p_i^{k_i}) \cdot 2^{k-1}$$

$$mcm\left(\phi(p_1^{k_1}), \dots, 2^{k-2}\right) \leq \prod \phi(p_i^{k_i}) \cdot 2^{k-2}$$

$$< \prod \phi(p_i^{k_i}) \cdot 2^{k-1}$$

se $8 \mid n \Rightarrow$ no CBN (mod 8 no CBN)

$\exists\, p \neq q$ disp prim. $pq \mid n$

$4p \qquad a^{p-1} \equiv 1 \pmod{p}$

$$\equiv 1 \pmod{4}$$

$$a^{mcm(p-1,\, q-1)} \equiv 1$$

$$mcm(p-1, q-1) < (p-1)(q-1)$$

- Dato k trovare un tale che 2^n ha un blocco di esattamente k termini consecutivi in base 10

$2^n = 1572500000006$

3^n 3 è un generatore modulo 5^N

k $\boxed{n = 2^{k+1} \cdot 5^k}$

$3^n \equiv 1 \pmod{5^{k+1}}$

$3^n \equiv 1 \pmod{2^{k+1}}$

$3^n \equiv m \cdot 2^{k+1} + 1$

$1\,5\,4 \ldots \underbrace{0\,0\,0\,0\,0}_{k \text{ zeri}}\,1$

$5^{k+1} \nmid n$

$3^n \not\equiv 1 \pmod{5^{k+2}}$

$\Leftarrow$ $n^2 \mid 2^n + 1$ $\quad n = 3$ risolve

$3^2 \mid 2^3 + 1$

p più piccolo primo che divide n

$p^2 \mid 2^n + 1 \mid 2^{2n} - 1$

$\text{ord}_p(2) \mid 2n \qquad \text{ord}_p(2) \mid p-1$

$(p-1, 2n) = 2 \qquad (p-1, n) = 1$

$\text{ord}_p(2) \mid 2$

$p \mid 2^2 - 1 \qquad p = 3$

$n = 3^k m \qquad (m, 3) = 1$

$3^{2k} \cdot m^2 \mid 2^{3^k \cdot m} + 1 \Rightarrow 3^{2k} \mid 2^{3^k \cdot 2m} - 1$

$(m, 3)$ COPRIMI

$3^{2k} \mid 4^{3^k \cdot m} - 1 \qquad v_3(4^{3^k m} - 1) =$

$= v_3(4-1) + v_3(3^k m) =$

$2k \leq 1 + k \qquad 1 + k$

$k \leq 1$

$n = 3m \qquad (3, m) = 1$

$9 \mid m^2 \mid 2^{3m} + 1 = 8^m + 1$

P PIÙ PICCOLO PRIMO

$p^2 \mid 8^m + 1 \mid 8^{2m} - 1 = 64^m - 1$

$\text{ord}_p 64 \mid m \qquad \text{ord}_p(64) \mid p-1$

$(m, p-1) = 1 \qquad \operatorname{ord}_p(6h) = 1$

$p \mid 6 \} \qquad p = 3 \qquad No!$

$p = 7$

$p = 7 \quad No!$

$p^2 \mid g^m + 1$

$g^m + 1 \equiv (1)^m + 1 \equiv 2 \not\equiv 0 \mod 7$

$h = 3$ è L'UNICA SOLUZIONE.

Dato un intero $n > 1$ e a INTERO

a è RESIDUO QUADRATICO mod n

se $\exists\, m \in \mathbb{Z} : \; n \mid m^2 - a$

SIMBOLO DI LEGENDRE:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & \text{se } p \nmid a \text{ è } a \text{ è RESIDUO } a. \\ -1 & \text{se } p \nmid a \text{ è } a \text{ non è RESIDUO } a. \end{cases}$$

$a \equiv g^k \pmod p$

$k = 2n \qquad a \equiv g^{2n} \equiv (g^n)^2 \pmod p$

$a \equiv g^{2n+1} \qquad a \equiv x^2 \pmod p$

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

$$g^{2n+1} \overset{\frac{p-1}{2}}{=} (g^{2n})^{\frac{p-1}{2}} (g)^{\frac{p-1}{2}} \equiv (g^{p-1})^n g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod p$$

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

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

$$R \cdot R = R \qquad NR \cdot NR = R \qquad R \cdot NR = NR$$

o R. Q. $\quad g^k$ res $\iff k$ è PARI

$\frac{p-1}{2}$ RESIDUI PRIMI CON p $(\neq 0)$

p PRIMO DISP.

a RES. MOD p $\qquad a \equiv g^k \pmod{p^k}$

$\Downarrow$

a RES MOD p^N $\qquad a \equiv g^n \pmod p$

g GEN MOD p^N $\qquad \Downarrow$

$a \equiv (g^m)^2 \bmod p^N$ $\qquad n$ PARI $n = 2m$

$n \geq 3$ QUALI RESIDUI (DISPARI) CI SONO mod 2^n

$a^2 \equiv 1 \pmod 8$ AL PIÙ 2^{n-3}

5 ha ord 2^{n-2}

$5^2, 5^4, \ldots, 5^{2^{n-2}}$ TUTTI RESIDUI DISPARI

SONO 2^{n-3}

a R.Q. mod 2^n $(n \geq 3) \iff a \equiv 1 \pmod 8$

$n = \prod p_i^{k_i} \cdot 2^k$ $\quad (a, n) = 1$

a R.Q. $\iff \forall i \left(\frac{a}{p_i}\right) = 1$ se $k = 2$ $a \equiv 1 \pmod 4$

se $k \geq 3$ $a \equiv 1 \pmod 8$

$n \mid x^2 - a$ e $m \mid n \Rightarrow m \mid x^2 - a$

QUANDO -1 È R.Q mod p?

$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \cdot \begin{cases} = 1 & \text{se } 4 \mid p-1 \\ = -1 & \text{se } p \equiv 3 \pmod 4 \end{cases}$

LEMMA DI GAUSS

p PRIMO DISPARI, (a, p) INTERO

$A = \left\{ ai \mid 1 \leq i \leq \frac{p-1}{2} \right\} \subseteq \mathbb{Z}_p^*$

PRESO a_i $\exists!$ $1 \leq b_i \leq \frac{p-1}{2}$ $\quad a_i \equiv \pm b_i \pmod p$

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

$f : \left\{1, \ldots, \frac{p-1}{2}\right\} \to \{-1, 1\}$

$a_i \equiv f(i)\, b_i \pmod p$

$$\left(\frac{a}{p}\right) = (-1)^n \qquad n = \#\{ i \mid \ell(i) = -1 \}$$

$i \neq j \quad b_i \neq b_j \quad b_i = b_j \quad ai \equiv \pm aj \pmod p$

$a(i \pm j) \equiv 0 \pmod p$ $\quad p = 2$ INT. DIV.

$i \pm j = 0 \Rightarrow i = j$ $\quad 1 \le b_i \le \frac{p-1}{2}$

$$\prod_{i=1}^{\frac{p-1}{2}} ai \equiv \prod_{i=1}^{\frac{p-1}{2}} b_i \, \ell(i) = (-1)^{\sum \ell(i)} \cdot \prod b_i \equiv (-1)^n \cdot \left(\frac{p-1}{2}\right)! \pmod p$$

$$\prod_{i=1}^{\frac{p-1}{2}} ai \equiv \prod_{i=1}^{\frac{p-1}{2}} a \cdot \prod_{i=1}^{\frac{p-1}{2}} i \equiv a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod p$$

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

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

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

---

2 $\quad$ p

$\{ 2, 4, \dots, p-1 \}$ $\qquad \{ 1, \dots, \frac{p-1}{2} \}$

$\{ \frac{p+1}{2}, \dots, p-1 \}$

$p \equiv 1 \pmod 8$

$\{ 2, 4, \dots, \frac{p-1}{2} \}$ $\qquad \{ \frac{p-1}{2} + 2, \dots, p-1 \}$

$$\frac{\left(\frac{p-1}{2}\right)}{2} \equiv \frac{p-1}{4} \pmod 2$$ è R.Q

2 è RES $\Leftrightarrow p \equiv \pm 1 \pmod 8$

RECIPROCITÀ QUADRATICA

$p \neq q$ PRIMI DISPARI

VALE

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

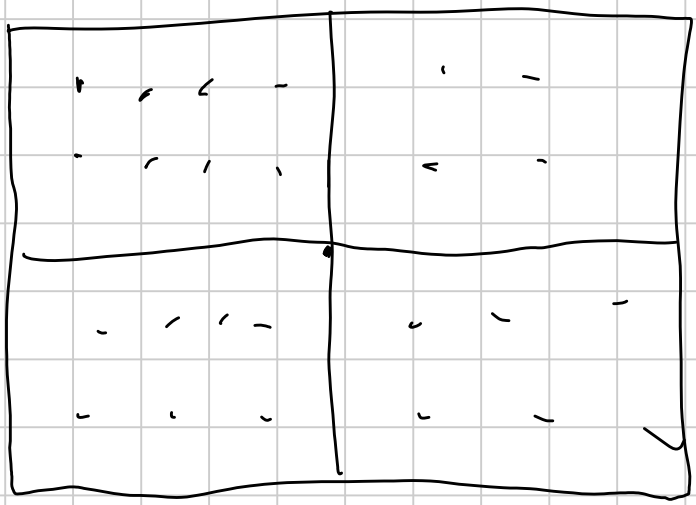
modulo quali primi 5 è R.Q.?

$$\left(\frac{5}{q}\right)\left(\frac{q}{5}\right) = (-1)^{2\cdot\frac{q-1}{2}} = 1$$

5 è res. mod q sse q è res mod 5, cioè $q \equiv \pm 1 \pmod 5$

$p = 2a+1$

$q = 2b+1$



$$S = [-a, a] \times [-b, b] \cap \mathbb{N}^2$$

$$S = \{ (x, y) \mid x, y \in \mathbb{Z},\ |x| \le a,\ |y| \le b \}$$

$$\left(\frac{p}{q}\right) = \#\left\{ 1 \le i \le \frac{p-1}{2} \mid pi \in \left\{ -\frac{q-1}{2}, -\frac{q-1}{2}+1, \dots, -1 \right\} \text{ in } \mathbb{Z}_q \right\}$$

$$k : \left\{ 1, \dots, \frac{pq-1}{2} \right\} \to S$$

$$f(n) = (x, y) \qquad n \equiv x \bmod p, \quad n \equiv y \bmod q$$

$$P = k\left(\left\{ 1, \dots, \frac{pq-1}{2} \right\}\right)$$

$$v = \#\{ (x, 0) \mid x < 0,\ (x, 0) \in P \}$$

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

$$\frac{p-1}{2} \cdot q \le \frac{pq-1}{2} < \frac{p+1}{2} \cdot q$$

$$-\frac{q}{2} \le -\frac{1}{2}$$

$$\frac{q}{2} \ge \frac{1}{2}$$

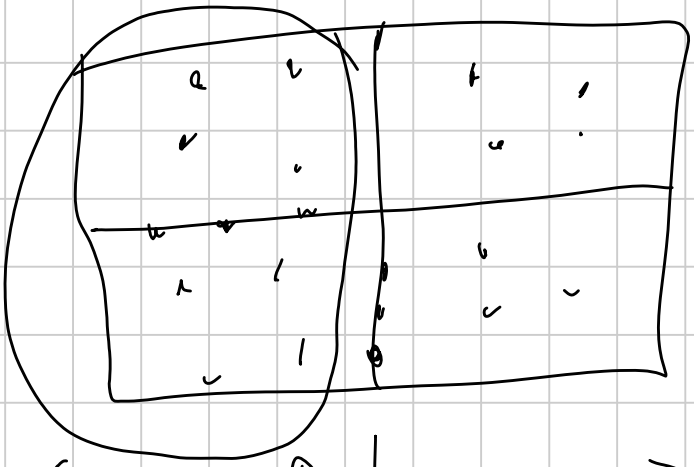
$$s \equiv x \bmod p \qquad s = kq$$

$$kq \qquad \boxed{q, 2q, \dots, \frac{p-1}{2} \cdot q}$$

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

$$v = \#\{ (0, y) \mid y < 0,\ (0, y) \in P \}$$

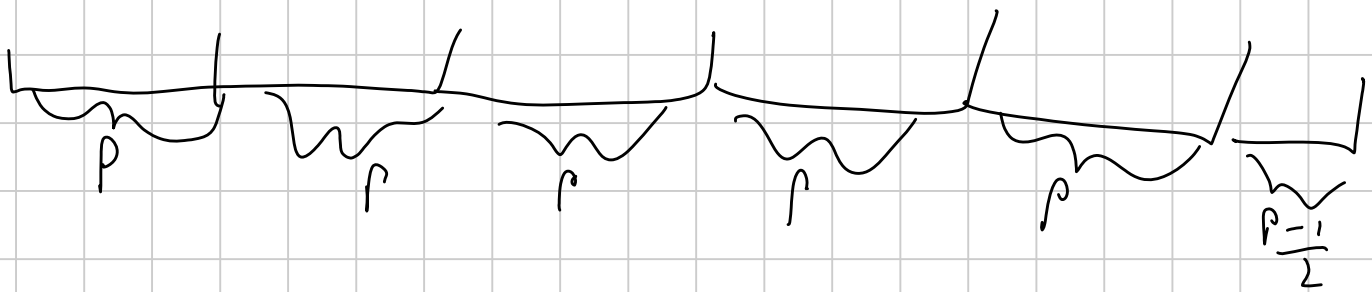
$$\left(\frac{p}{q}\right) = (-1)^v$$



$A = \{(x,y) \in P \mid x < 0\}$

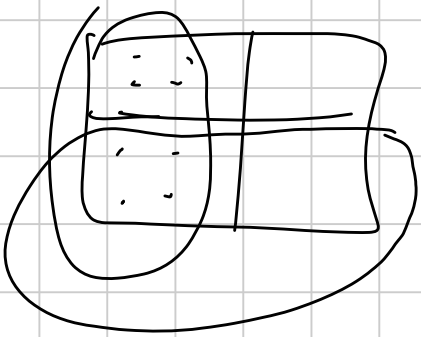
I NUMERI i TRA 1 e $\frac{pq-1}{2} = p \cdot \frac{q-1}{2} + \frac{p-1}{2}$

TALI CHE $i \in \{-\frac{p-1}{2}, \dots, -1\}$ in $\mathbb{Z}_p$



$|A| = \frac{p-1}{2} \cdot \frac{q-1}{2} = ab$

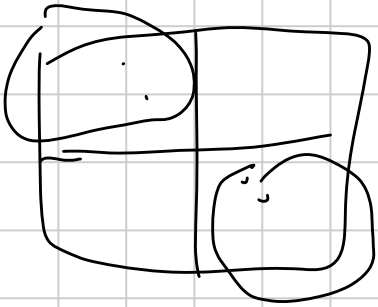
$B = \{(x,y) \in P \mid y < 0\}$



$|B| = ab$

$C = \{(x,y) \in P \mid (x>0 \text{ e } y<0) \text{ opp. } (x<0 \text{ e } y>0)\}$

$(x,y) \notin Imm(f) \iff (-x,-y) \notin Imm f$



$f : \{-\frac{pq-1}{2}, \dots, \frac{pq-1}{2}\} \xrightarrow{SURG} S$

$f^{-1}(x,y) > 0$

$f^{-1}(x,y) = -f^{-1}(-x,-y)$

$C = \{(x,y) \in P \mid xy < 0\}$

$D = \{(x,y) \in S \mid xy < 0\}$

$[(x,y), (-x,-y)] \to$ COPPIE DI QUESTO TIPO PARTIZIONANO D,

UNO SOLO DI QUESTI CE L'È IN C

$|C| = \frac{|D|}{2}$

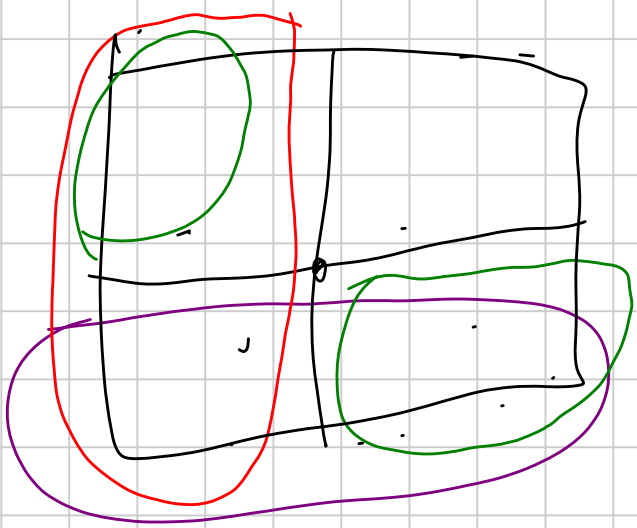
$\{1, \dots, a\} \times \{-b, \dots, -1\} \cup \{-a, \dots, -1\} \times \{1, \dots, b\}$

$|D| = 2 \cdot ab \qquad |C| = ab$

$|A| = |B| = |C|$

$|A| + |B| + |C| =$

$= |A \cap B| + 2|B \cap C| + 2|A \cap C| + U + V$



$$3a\ell = 2|A\cap B| + 2|B\cap C| + 2|A\cap C| + u + v$$

$$a\ell \equiv u+v \pmod 2$$

$$(-1)^{a\ell} = (-1)^u \cdot (-1)^v = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)$$

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

ESERCIZI:

- $x^2 = y^3 + 7 \qquad x, y \in \mathbb{N}$

mod 4 $\qquad x^2 \equiv 0, 1 \pmod 4$

$x^2 \equiv 0 \qquad y^3 + 7 \equiv 0 \pmod 4 \qquad y^3 \equiv +1 \pmod 4 \qquad y \equiv 1 \pmod 4$

$x^2 \equiv 1 \qquad y^3 \equiv 2 \pmod 4$

$y \equiv 1 \pmod 4$

$$\boxed{\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}}$$

$p \mid x^2 + y^2 \qquad (x, y) = 1$

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

$4 \mid p \equiv 1 \pmod 4$

$x^2 + 1 = y^3 + 8$

$(y+2) \mid y^3 + 8 \Rightarrow y+2 \mid x^2+1$

$p \mid y+2 \Rightarrow p \equiv 1 \pmod 4$

$y+2 = \prod p_i^{k_i} \equiv \prod 1^{k_i} \equiv 1 \pmod 4$

- Sia n intero positivo dispari.

Se n è r.q modulo ogni primo $\Rightarrow$ è un quad.

$n = \prod p_i^{d_i}$ SE n NON È UN QUADRATO ALLORA d_i DISPARI

q PRIMO $\equiv 1 \pmod 4$ $\equiv a \pmod{p_1}$

SIA a UN N.R. mod p_1 $\forall n \neq 1$ $\equiv 1 \pmod{p_i}$

$q \equiv m \pmod{4\prod p_i}$ $(m, 4\prod p_i) = 1$

m P $(m, P) = 1$ $\exists \infty$ q : $q \equiv m \pmod P$

$q \equiv m \pmod{4 \prod p_i}$

$q = \prod p_i^{a_i}$

$\exists i$ T.C. $\left(\frac{n}{p_i}\right) = -1$

$\prod \left(\frac{n}{p_i}\right)^{a_i} = -1$

$\left(\frac{m}{n}\right) = \prod \left(\frac{m}{p_i}\right)^{a_i}$ n non PRIMO

$\left(\frac{m}{n}\right) = 1 \iff m$ è RQ mod n

m è RES, $\Rightarrow \left(\frac{m}{n}\right) = 1$

m, n int. disp. coprimi

$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}$

$q \equiv m \pmod{4\prod p_i}$

$\Downarrow$ $\left(\frac{n}{q}\right) = -1$ $\exists p \mid q$ t.c. $\left(\frac{n}{p}\right) = -1$

n è N.R per almeno primo

RESIDUI d-esimi

a è res. d-esimo mod p

se $a \equiv x^d \pmod p$ ha soluzioni

$a \equiv g^k \pmod p$ $\quad (d, p-1) \mid k$

$g^1, \dots, g^{p-1}$ $\quad (d, p-1)$

$\frac{p-1}{(d, p-1)}$ è il num di res. d-esimi.

$X^{p-1} - 1$ CON SOLAMENTE $p-1$ RADICI

$X^{p-1} - 1 \equiv \prod_{i=1}^{p-1} (X - i) \pmod p$

$-1 \equiv \prod_{i=1}^{p-1} (-i) \equiv (p-1)! \pmod p$

$\prod_{i<j} ij \equiv 0 \pmod p$

$d \mid p-1$

$x^d - 1 \mid x^{p-1} - 1$

$$x^d - 1 = \prod_{i=1}^{d} (x - a_i)$$

$d \mid p-1$, ci sono esattamente d radici d-esime dell'unità

$$\sum_{d \mid n} \phi(d) = n$$

$$\psi(d) = \#\{ x \in \mathbb{Z}_p^* \mid \mathrm{ord}_p(x) = d \}$$

$$\psi(d) \overset{!!}{=} \phi(d) \qquad \forall d \mid p-1$$

Vuoto) $d = 1$ ✓

$n \mid p-1$

$$\sum_{d \mid n} \psi(d) = n$$

$x^n - 1$

RAGGRUPPA PER LORO

QUANTI DI HA

$$\sum_{d \mid n} \psi(d) = \sum_{\substack{d \mid n \\ d < n}} \psi(d) + \psi(n) = \sum_{\substack{d \mid n \\ d < n}} \phi(d) + \psi(n)$$

$$\sum_{\substack{d \mid n \\ d < n}} \phi(d) + \psi(n) = n = \sum_{d \mid n} \phi(d)$$

$$\psi(n) = \phi(n) \qquad \forall n \mid p-1$$

$n = p-1 \qquad \psi(p-1) = \phi(p-1) > 0$

x^d funz. $\mathbb{Z}_p^* \to \mathbb{Z}_p^*$

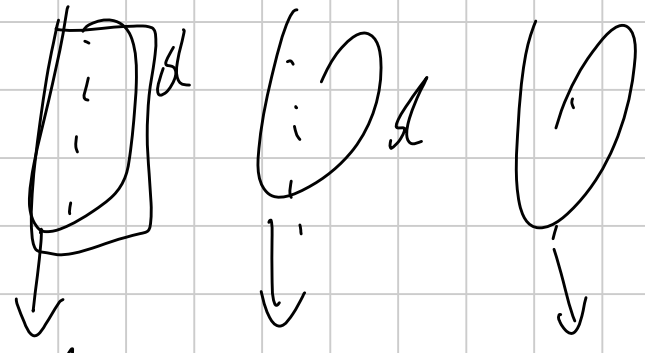
ESATTAMENTE d el vanno in 1.

a RR d-esimo

$a = d^{ol}$

$x = dy$

$x: x^d = a$ $\qquad d^d y^d = a \iff y^d = 1$



$p-1$ el $\mathbb{Z}_p^*$

$\frac{p-1}{d}$ BLOCCHETTI VA d el.

d el vanno in 1

IV

~~X~~ rest. $\frac{p-1}{d}$-esimo $\Rightarrow x^{ol} = 1$ $\qquad x = y^{\frac{p-1}{d}}$

$x^{ol} = y^{p-1} = 1$

sono d

$x^d = 1 \iff x$ resi $\frac{p-1}{d}$-esimo

$n = \frac{p-1}{d}$ $\qquad (n \mid p-1)$

$x^{\frac{p-1}{n}} \equiv 1 \pmod p \iff x$ res n-esimo

$n = 2$ $\qquad x$ R.Q. sse $x^{\frac{p-1}{2}} \equiv 1 \pmod p$

ESERCIZI

$x^2 + 4 = y^5$ ASSURDO mod p PER QUALCHE PRIMO

$\frac{p-1}{(d, p-1)}$ CONVIENE CHE $d \mid p-1$

$(5, p-1) = 1$

$p \equiv 1 \pmod 2$

$\equiv 1 \pmod 5$

$p \equiv 11$ $\quad y^5 \in \{-1, 0, +1\}$

$(p-a)^2 \equiv a^2 \pmod p$

$x^2 \equiv y^5 + 7$ $\quad 6 \quad 7 \quad 8$ $\quad 0, 1, 4, 9, 5, 7$

ASSURDO $\pmod{11}$

Preso p PRIMO, $\exists q$ TALE CHE p NON È UN RES. p-esimo mod q.

$\boxed{p \mid q-1}$ ALTRIMENTI TUTTI SONO RES p-esimi

$p \mid \mathrm{ord}_q(p)$

$p^{\frac{q-1}{p}} \not\equiv 1 \pmod q$

q: $\mathrm{ord}_q(p) = p$

$q \mid p^p - 1$ $\quad q \nmid p-1$ $\quad q \mid \boxed{\frac{p^p - 1}{p-1}}$

$q \mid \frac{p^p-1}{p-1}$ $\quad p^p \equiv 1$ $\quad p \equiv 1 \ (q)$?

$\left(\frac{a^p-1}{a-1}, a-1\right) \mid p$ $\quad \left(\frac{p^p-1}{p-1}, p-1\right) = 1$

$\text{ord}_q(p) = p$

$p^{\frac{q-1}{p}} \not\equiv 1 \pmod q$ $\quad p \nmid \frac{q-1}{p}$ cioè $p^2 \nmid q-1$

$\exists\, q : \ q \mid \frac{p^p-1}{p-1}$ $\quad q \not\equiv 1 \pmod{p^2}$

$q \mid \frac{p^p-1}{p-1}$ SIANO $\equiv 1 \pmod{p^2}$

$$\frac{p^p-1}{p-1} = \prod_{i=1}^{k} q_i^{a_i} \equiv \prod_{i=1}^{k} 1^{a_i} \equiv 1 \pmod{p^2}$$

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

$p^2 \nmid \frac{p^p-1}{p-1} - 1$

$p^2 \mid \frac{p^p-p}{p-1} = p \cdot \boxed{\frac{p^{p-1}-1}{p-1}}$

$\exists\, q : \ p \,\|\, q-1$

$\text{ord}_q(p) = p$ $\quad p$ NON res. p-esimo