TEORIA DEI NUMERI 2

Titolo nota 08/09/2010

EQ DIOFANTEE.

$\frac{1}{m} + \frac{1}{n} = \frac{1}{p}$ p PRIMO in $\mathbb{N}^+$

$np + mp = mn$ $\quad mn - nf - mp + p^2 = p^2$

$(m-p)(n-p) = p^2$

DISCESA

$f(x_1, \dots, x_n) = 0$

SUPPORRE $a_1, \dots, a_n$ SOL + PICCOLA

TROVARNE UNA MINORE

VIETA - JUMPING

$f(x,y) = 0$ $\quad f$ COEFF. INTERI
POL DI 2° GRADO SIMM.

$a, b \quad a \geq b$

$f(x,b) = 0$ $\quad$ CONOSCIAMO UNA SOL. $x = a$

$\exists$ UN'ALTRA SOL. a'

SE $a > a' \Rightarrow$ ASSURDO

ESERCIZIO:

$(4ab-1) \mid (4a^2-1)^2 \Rightarrow a=b$

$(\alpha, \beta$ + PICCOLA SOL. $\alpha > \beta)$

MOD $4ab-1$ $\quad 4a \equiv \frac{1}{b} \pmod{4ab-1}$

$(4ab-1) \mid (4a^2-1)^2 \Leftrightarrow \left(a \cdot \frac{1}{b} - 1\right)^2 \equiv 0 \pmod{4ab-1}$

$(b, 4ab-1) = 1$ $\quad \Downarrow$

$(a-b)^2 \equiv 0 \pmod{4ab-1}$

$(a-b)^2 - K(4ab-1) = 0 \qquad K \in \mathbb{Z}$ RISOLVO

α, β LA + PICCOLA SOLUZIONE $\alpha > \beta$

$x^2 - 2x\beta + \beta^2 - 4K\beta x + K = 0 \qquad \alpha, \gamma$

$\alpha > \frac{\text{SOMMA RADICI}}{2} \qquad \alpha > \gamma$

$\alpha > \sqrt{\text{PROD RADICI}}$

$\alpha\gamma = K + \beta^2$

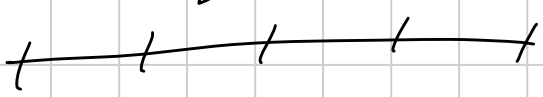
$\alpha^2 \geq K + \beta^2$ $\qquad$ $(\alpha - \beta)^2 \geq K(4\alpha\beta - 1)$

$\alpha \geq (\beta + c)$ $\qquad$ $c^2 \geq K(4(\beta+c)\beta - 1)$

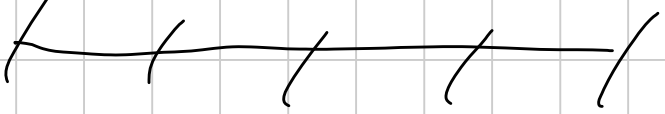
$\beta^2 + 2\beta c + c^2 > K + \beta^2$

$c^2 \geq K(4\alpha\beta - 1) > K$

$c \geq 0$



$x^4 + y^4 = z^4$ $\qquad$ $(x, y, z) \in \mathbb{N}^3$



RIDURRE MOD. p

$f(x_1, \dots, x_n) = 0$ $\qquad$ $x_n \in \mathbb{N}$

$\equiv 0 \pmod p$

$x^2 - 3y^2 = 17$ $\qquad$ x, y INTERI

HA SOL MOD p $\forall p \neq 3$

È POSS. CHE UNA CERTA EQ HA SOL MODULO p, MA DIVENTA NON MOD p^4

$x^3 + 2x + 1 = 2^n \quad x \equiv 5 \pmod 8$

$\forall n \ \exists x : \ 2^n \mid x^3 + 2x + 1$?

LEMMA DI HENSEL:

$f(x)$ POL HA RAD mod $p^n \ \forall n$?

SIA f UN POL COEFF. INTERI.

SE $\exists \ x_1 \in \mathbb{Z}$:

- $f(x_1) \equiv 0 \pmod p$
- $f'(x_1) \not\equiv 0 \pmod p$

$f(x) = \sum a_n x^n$

$f'(x) = \sum a_n n x^{n-1}$

ALLORA $\exists$ SUCC. x_n :

- $p^n \mid f(x_n)$
- $x_{n+1} \equiv x_n \pmod{p^n}$

PASSO BASE: SÍ

INDUZIONE:

$f(x_n) = p^n \cdot k \qquad x_n \equiv x \pmod p$

$f'(x_1) \not\equiv 0 \pmod{p}$

SCRIVIAMO GENERICO

$x_n + m \cdot p^n$

$f(x_n + m \cdot p^n) \equiv f(x_n) + m \cdot p^n f'(x_n) \pmod{p^{n+1}}$

INCISO

$\varphi(x)$ $\deg \varphi = d$

$$q(x) = \sum_{i=0}^{d} \frac{f^{(i)}(x_0)}{i!} (x - x_0)^i$$

$$q(x_0 + m \cdot n) = \sum_{i=0}^{d} \frac{f^{(i)}(x_0)}{i!} (mn)^i \equiv \sum_{i=0}^{r} \frac{f^{(i)}(x_0)}{r!} (mn)^i (\dots)$$

$$f(x + m \cdot p^n) = \sum_{i=0}^{d} a_i (x + m \cdot p^n)^i \equiv \sum a_i x^i + \left(\sum a_i x^{i-1} \cdot i \right) m p^n$$

$$f(x) + f'(x) \cdot m p^n \equiv$$

$$f(x_n + m \cdot p^n) \equiv f(x_n) + m \cdot p^n \cdot f'(x_n) \pmod{p^{n+1}}$$

$f(x_n) = k \cdot p^n$

$0 \equiv k \cdot p^n + m p^n \cdot f'(x_n) \quad (p^{n+1})$

$p \mid k + m f'(x_n)$

$f'(x_n) \not\equiv 0 \quad (p)$

$m \equiv -\frac{k}{f'(x_n)} \pmod p$

$x_{n+1} \doteq x_n + m \cdot p^n$

- $p \mid f(x_1)$
- $p \nmid f'(x_1)$

LEMMA PIÙ GENERALE:

$\boxed{v_p(f(x_1)) > 2 v_p(f'(x_1))}$

POL IN PIÙ VARIABILI:

LE FISSO TUTTE TRANNE 1

APPLICO IL LEMMA IN 1 VARIABILE

$n \geq 3$ QUALI RK. Q. mod 2^n

$\Downarrow$

$Q \equiv 1 \pmod 8$

$x^2 \equiv a \pmod 8$ $\quad x = 1$

$x^2 - a \xrightarrow{\text{deriv}} 2x$

$v_2(x^2-a) \geq 2\, v_2(2x)$, ?

≥ 2 $\quad$ 1

$x^3 + 2x + 1 = 2^n$ $\quad x = 0$

$n = p_1$

$x = 1$

$1 + 2 + 1 = 2^2$

$n = 2^k$ È L'UNICA SPERANZA!

$\forall\, n \geq k$

$x^3 + 2x + 1 \equiv 0 \pmod{2^k}$

$k = 1$

$x^3 + 2x + 1 \equiv 0 \pmod 2$

$x = 1$

$3x^2 + 2$ $\quad x = 1$

$\rightarrow 5$

$\Rightarrow$ C'È SOL mod 2^n

POLINOMI

TEST DELLA DERIVATA:

$f \in \mathbb{Q}[X]$

X^2+1 $\qquad f(X) = \prod q_i^{\alpha_i}(X)$

q_i IRR.

TH FATTORIZZAZIONE UNICA A MENO DI UNITÀ

q IRR. $\qquad q(X) \mid a(X)\,b(X)$

$\Rightarrow q(X) \mid a(X) \vee q(X) \mid b(X)$

$q(X) = (q(X), e(X)) \cdot (q(X), b(X))$

DIVISIONE EUCLIDEE

VI DEFINISCE mcd

BÉZOUT:

DATI $p(x), q(x) \in \mathbb{Q}[x]$, $a(x), b(x) \in \mathbb{Q}[x]$

$a(x)p(x) + b(x)q(x) = MCD(p(x), q(x))$

TEST DELLA DERIVATA:

$f(x)$ HA FATTORI DOPPI

$\Updownarrow$

$(f(x), f'(x)) \neq 1$

VALE ANCHE IN $\mathbb{Z}_p[x]$

(COEFF. mod p)

α RADICE DOPPIA $\Leftrightarrow f'(\alpha) = 0 \pmod p$

ESERCIZIO:

$f(x) \in \mathbb{Z}[x]$ IRRIDUCIBILE

$\exists$ INF. $n \in \mathbb{N}$:

$f(n)$ NON È UN QUAD. PERFETTO

$\deg f' < \deg f$ $\quad (f(x), f'(x)) = 1$

$a, b \in \mathbb{Q}[x]$

$a(x) f(x) + b(x) f'(x) = 1$

$m, n \in \mathbb{Z}[x]$

$m(x) f(x) + n(x) f'(x) = c \neq 0$

$p \nmid c \Rightarrow p \mid f(x) \Rightarrow p \nmid f'(x)$

$\exists \infty\ p : \exists n \in \mathbb{N} : p \mid f(n)$

$\forall p : \exists n : p \mid f(n)$ ma $p \nmid c \Rightarrow p \nmid f'(n)$

$p^2 \mid f(n)$

$f(n+p) \equiv f(n) + p \cdot f'(n) \pmod{p^2}$

$p \mid f(n+p)$

$\Rightarrow$ ASSURDO

$p^2 \nmid f(n+p)$

Adatto $f(x)$ IRR. $\exists \infty\ p : \exists n : p \nmid f(n)$

TECNICA DI STRINGERE TRA 2 QUAD.

$a \in \mathbb{N}$

$a^2 < b < (a+1)^2 \Rightarrow b$ NON È UN QUADRATO.

$$f(x) = x^{2n} + a_1 x^{2n-1} + \dots + a_{2n}$$

$\exists\, q(x) \in \mathbb{Q}(x) \quad \deg(q) = n$

$$\deg(f(x) - q^2(x)) < n$$

$$q = x^n + \frac{a_1}{2} x^{n-1} + \dots$$

$\exists\, m > 0 : \quad m\, q(x) \in \mathbb{Z}[x]$

$$\deg(m^2 f(x) - m^2 q^2(x)) < n \qquad \deg(q) = n$$

$$(m\,q(x) - 1)^2 < m^2 f(x) < (m\,q(x) + 1)^2$$

$$(m^2 q^2(x) - m^2 f(x)) - 2m\,q(x) + 1 < 0$$

$$m^2 f(x) = [m\,q(x)]^2 \qquad f(x) = q^2(x) \quad \forall\, x > N$$

$\Rightarrow f(x) = q^2(x)$ < 0 MÉ POI $\forall x > N$

$p(x), q(x) \quad \forall x \in \mathbb{R} \quad p(x) = q(x) \rightarrow$ lo stesso polinomio

$X^p \quad X \quad \mathbb{Z}_p$

COMBINATORIAL NULLSTELLENSATZ

$f(x_1, \dots, x_n)$

$\deg(f) = d$

$\exists$ monomio $x_1^{d_1} \cdots x_n^{d_n} \quad \sum d_i = d$

coefficiente $\neq 0$

$\Rightarrow$ se lo posso scegliere

la variabile x_i in $d_i + 1$ modi

per ogni, riesco a trovare n-upla in cui $f(x_1, \dots, x_n) \neq 0$

$S_i : \quad |S_i| = d_{i+1}$

$\exists (x_1, \dots, x_n) \in S_1 \times \dots \times S_n : f(x_1, \dots, x_n) \neq 0$

DIMOSTRAZIONE:

SUPP. $\forall\ S_i$: A si annulla $S_1 \times \dots \times S_n$

X_1 $\qquad f(X_1, \dots, X_n) = P_{x_2, x_3, \dots, x_n}(X)$

$\{a_1, a_2, \dots, a_d\} = S_1$

$(X-a_1)(X-a_2)\cdots(X-a_d) = 0 \quad \forall X \in S_1$

$g_{x_2,\dots,x_n}(X) \equiv f(X_1, \dots, X_n) \pmod{P_{x_2,\dots,x_n}(X)}$

$\deg(g) < d+1 \Rightarrow \deg(g) \le d$

$X y^2 + x^2 y \qquad S_x = \{1, 2\}$

$(X-1)(X-2) \qquad x^2 = 3x - 2 \qquad \forall X \in S_x$ IL VALORE DEL POL NON CAMBIA

$\Updownarrow$

$\prod (X - a_i) = 0$

$\deg_x(g) \le d$

$g(X_1, \dots, X_n) \equiv f(X_1, \dots, X_n) \quad \forall x_i \in S_i$

$X_1^{d_1} \cdots X_n^{d_n}$ ha sempre coeff $\neq 0$

$X_2^{d_2} \cdots X_n^{d_n}$ in $g_{x_1}(x_2, \dots, x_n)$

$p(x_1) : x_2^{d_2} \cdots x_n^{d_n}$

$\deg(p) = d_1$ $\quad |S| = \delta_1 + 1$

$\exists\, a \in S_1 : p(a) \neq 0$

$g(a, x_2, \dots, x_n) \in \mathbb{K}[x_2, \dots, x_n]$

non solo $\deg(x_i) \leq d_i$

ma per ogni x_i allo stesso modo,

così ci si semplifica la vita

$g = f \quad \forall x_1, \dots, x_n \in S_1 \times \cdots \times S_n$

$\deg(x_i) \leq d_i$:

$x_2^{d_2} \cdots x_n^{d_n}$ ha grado $\leq \delta_1$

$\exists\, a_2, \dots, a_n : g(a, a_2, \dots, a_n) \neq 0$

$a_i \in S_i \Rightarrow f(a, a_2, \dots, a_n) = g(a, \dots a_n) \neq 0$

COROLLARIO:

Th Chevalley – Warning:

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \dots \\ f_k(x_1, \dots, x_n) = 0 \end{cases} \qquad \sum_{i=1}^{k} \deg(f_i) < n$$

$\Downarrow$

se c'è una soluzione allora ce n'è un'altra (in $\mathbb{Z}_p$) $\quad S_i = \mathbb{Z}_p$

Sec. prima $= 0$ se $\forall i \; x_i \neq a_i$

Se $x_i = a_i \; \forall i$ vuol dire 1 ✓

$$\prod_{j} \frac{(x_j - 1)(x_j - 2) \cdots (x_j - (a_j - 1)) \cdot (x_j - (a_j + 1)) \cdots (x_j - p)}{(a_j - 1) \cdots (a_j - p)}$$

$$\prod_{i=1}^{k} \left(1 - f_i^{p-1}(x_1, \dots, x_n)\right) - \prod_{j=1}^{n} \left(\prod_{\substack{a \in \mathbb{Z}_p \\ a \neq a_j}} \frac{x_j - a}{a_j - a}\right)$$

Γ

$(p-1) \sum \deg(f_i) < (p-1) n$

$x_1^{p-1} \cdots x_n^{p-1}$

$\exists\, a_1, \dots, a_n : \varphi(a_1, \dots, a_n) \neq 0$

$\Rightarrow$ È UN'ALTRA SOLUZIONE!!

COROLLARIO:

TH CAUCHY-DAVENPORT

$A \subseteq \mathbb{Z}_p \qquad B \subseteq \mathbb{Z}_p$

$A = \{1, p+1, \dots, np+1\} \qquad |A| = 1$

$A + B = \{a + b \mid a \in A, b \in B\} \subseteq \mathbb{Z}_p$

$A = \{ x^2 \mid x \in \mathbb{Z}_p \}$ $\quad |A| = \frac{p-1}{2} + 1$

$A = B$

$A + B = \{ x^2 + y^2 \mid x, y \in \mathbb{Z}_p \}$

$|A+B| \geq |A| + |B| - 1$

OPPURE $\quad A + B = \mathbb{Z}_p$

LAVORO $\quad |A| + |B| - 1 \geq \mathbb{Z}_p \Rightarrow A + B = \mathbb{Z}_p$

se $\quad |A| + |B| - 1 < \mathbb{Z}_p \Rightarrow |A+B| \geq |A| + |B| - 1$

$\exists\ C : \quad |C| = |A| + |B| - 2$ $\qquad |A| = m$

$|B| = n$

$A + B \subseteq C$

$\Phi(x, y) = \prod_{c \in C} (x + y - c)$

grado $m + n - 2$

$x^{m-1} y^{n-1}$ $\qquad (m-1) + (n-1)$

$x \in A \quad y \notin B$

$\therefore x + y \notin C$

$p \nmid \binom{n+m-2}{m-1} \geq \frac{(n+m-2) \cdots (n)}{(m-1) \cdots 1}$

$n, m < p \qquad n+m < 2p$

$n+m-1 \leq p$

$p \nmid \binom{n+m-2}{m-1}$ ABVIAMO VINTO!

$|A+B| \geq n+m-1$

$n+m-1 > p$

$\emptyset \subsetneq A, \quad E \subsetneq B: \ |\emptyset| + |E| - 1 = p$

$|D+E| \geq p \Rightarrow \mathbb{Z}_p \subseteq D+E \subseteq A+B$

$A+B = \mathbb{Z}_p$

$|A_1 + A_2 + \dots + A_n| \geq |A_1| + \dots + |A_n| - n + 1$

opp. $\mathbb{Z}_p = A_1 + \dots + A_n$

$|A_1 + \dots + A_n| \geq |A_1 + \dots + A_{n-1}| + |A_n| - 1$

$\geq |A_1| + \dots + |A_{n-1}| - (n-1) + 1 + |A_n| - 1 =$

$|A_1| + \dots + |A_n| - n + 1$

ESERCIZIO:

$$\sum_{i=1}^{n} a_i x_i^{d_i} = c \qquad a_i \in \mathbb{Z}$$

$p \nmid a_i \quad \forall i \qquad \sum \frac{1}{d_i} \geq 1$

ALLORA C'È SOL. MOD p!

$$A_i = \{ a_i x_i^{d_i} \mid x_i \in \mathbb{Z}_p \}$$

$$|A_i| \geq \frac{p-1}{d_i} + 1$$

$c \in A_1 + A_2 + \dots + A_n$

$$|A_1 + \dots + A_n| \geq \sum |A_i| - n + 1 \geq$$

$$\geq \sum \left(\frac{p-1}{d_i} + 1 \right) - n + 1 = \sum \frac{p-1}{d_i} + \sum 1 - n + 1 =$$

$$= (p-1) \sum \frac{1}{d_i} + 1 \geq p - 1 + 1 = p$$

$\mathbb{Z}_p = A_1 + \dots + A_n$

$x^2 - 3y^2 = 1$? $p = 3$

$x_1^d + \dots + x_d^d \equiv 0 \pmod p$

HA SEMPRE SOLUZIONE!

$a_1, \dots, a_{2p+1} \in \mathbb{Z}$

NE ESISTONO p LA CUI SOMMA

È MULTIPLA DI p.

POLINOMI CICLOTOMICI

$$\Phi_n(x) = \prod_{(k,n)=1} (x - \omega^k) \qquad \omega = e^{\frac{2\pi i}{n}}$$

$\deg \Phi_n = \phi(n)$

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x) \Rightarrow \boxed{\sum \phi(d) = n}$$

$\Phi_n(x) \in \mathbb{Z}[x]$

CONSIDERARLI MODULO p!

AD ESEMPIO, $p \nmid n$ $\quad \exists m : n^m \equiv 1$

$f(x) = x^n - 1$ $\quad (nx^{n-1})x m - (x^n - 1) \equiv 1 \pmod p$

$\Phi_n(a)$ $\quad p \mid \Phi_n(a)$ $\quad p \nmid n$

$x^n - 1$ $\quad p \nmid \Phi_d(a)$ $\quad \forall d \mid n$, $d < n$

$(f(x), f'(x)) = 1 \Rightarrow f(x)$ 无 [重根, 否则 $p \mid n$]

$f(x) = \boxed{P(x)}\,\boxed{Q(x)}$ ← 从0到

$(x-a) \cdot P_1(x)$ $\quad (x-a)^2 \mid f(x)$

$\Phi_n(x) \cdot \Phi_d(x) \mid x^n - 1$

$(x-a) \mid \Phi_n(x) \Leftrightarrow \Phi_n(a) = 0$

$(x-a) \nmid \Phi_d(x) \Leftrightarrow \Phi_n(a) \neq 0$

$\forall d < n$, $d \mid n$ $\quad \Phi_d(a) \not\equiv 0 \pmod p$

$m < n$, $m \mid n$ $\quad \boxed{x^m - 1 = \prod_{d \mid m} \Phi_d(x)}$

$a^m - 1 = \prod_{d \mid m} \Phi_d(a) \not\equiv 0 \pmod p$

$m \mid n$, $m < n$ $\quad a^m \not\equiv 1 \pmod p$

$\Phi_n(X) \mid X^n - 1$

$p \mid \Phi_n(a) \Rightarrow p \mid a^n - 1$

$p \mid \Phi_n(a) \mid a^n - 1$

$p \nmid n$ e $p \mid \Phi_n(a) \Rightarrow \operatorname{ord}_p(a) = n$

$\operatorname{ord}_p(a) = n$

$p \mid \Phi_d(a) \cdot d \mid n$

$p \mid a^n - 1$

SUPP. $d < n$ $p \mid \Phi_d(a) \mid a^d - 1$ NO!

$p \mid \Phi_n(a)$

$(p, n) = 1$ ALLORA $p \mid \Phi_n(a) \iff \operatorname{ord}_p(a) = n$

$n = p - 1$

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

$\Phi_{p-1}(X) \mid X^{p-1} - 1$

↖ SI FATT. IN FATT. LINEARI

ESISTONO $\phi(p-1)$ RADICI DI QUEST POL.

VISTO CHE $p \nmid p-1$

a DIA UNA RADICE $\iff \operatorname{ord}_p(a) = p-1$

$\iff a$ È UN GENERATORE

$p \mid n \qquad n = mp$

$p \mid \Phi_m(a)$

$m \mid n \qquad X^m - 1 \mid X^n - 1$

$$\frac{X^n-1}{X^m-1} = \frac{\prod_{d \mid n} \Phi_d(X)}{\prod_{d \mid m} \Phi_d(X)} = \prod_{\substack{d \mid n \\ d \nmid m}} \Phi_d(X)$$

$\Phi_n(X) \mid \dfrac{X^n-1}{X^m-1}$

$\Phi_n(a) \mid \dfrac{a^{mp}-1}{a^m-1}$

$a^p - b^p$ HA FATTORE PRIMO NUOVO RISP A $a-b$

$p \mid (a^m)^p - 1 \qquad (a^m)^p \equiv a^m \Rightarrow p \mid a^m - 1$

$v_p(a^{mp}-1) = 1 + v_p(a^m-1)$ p DISP.

$v_2(a^{m2}-1) = v_p(a^m-1) + v_p(a+1)$ $p=2$

$p \mid \Phi_n(a) \quad \therefore p \mid a^n - 1$.

$n = \mathrm{ord}_p(a) \cdot p^r \cdot d$ $\quad (d, n) = 1$

$d \neq 1$

$p \mid n \quad p \mid \Phi_n(a) \quad p \mid a^n - 1$

$\Phi_n(a) \mid \dfrac{a^n - 1}{a^{\frac{n}{d}} - 1}$

$e^{\frac{n}{d}} \equiv 1 \pmod p$

$\mathrm{ord}_{p(a)} \mid \frac{n}{d}$

$\dfrac{e^d - 1}{e - 1}$ $\quad (d, p) = 1$, $e \equiv 1 \pmod p$

$d = 1$ $\quad p \mid \Phi_n(a)$

$n = p^r \mathrm{ord}_p(a)$

$\Phi_n(a) \qquad \Phi_n(a) \mid \dfrac{a^n - 1}{a^{\frac{n}{p}} - 1}$

n DISPARI

$(\Phi_n(a), n) \mid p$

p = max primo che divide

$p \mid \Phi_n(a) \qquad \left(\dfrac{\Phi_n(a)}{p}, n\right) = 1$

$a, n \quad |INTERI| \geq 3$ $\quad$ n non pot. di 2

Th ZSIGMONDY

p = massimo primo che $\nmid n$

$$|\Phi_n(a)| = \prod_{(i,n)=1} |(a - \omega^i)| \geq \prod_{(i,n)} 2 = 2^{\phi(n)}$$

$p \nmid \Phi_n(a)$ $\quad q \nmid n$ $\quad \operatorname{ord}_q(a) = n$

$q \mid \Phi_n(a)$

$p \mid \Phi_n(a)$ $\qquad \left(\frac{\Phi_n(a)}{p}, n\right) = 1$

$|\Phi_n(a)| > 2^{\varphi(n)} \geq n$

$\left|\frac{\Phi_n(a)}{p}\right| > 1 \Rightarrow \exists q : q \mid \frac{\Phi_n(a)}{p}$

$\Rightarrow q \nmid n$

$\operatorname{ord}_q(a) = n$

$a, n \geq 3$ $\qquad n \neq 2^r$

$\exists\, q$ PRIMO T.C. $\operatorname{ord}_q(a) = n$

$\forall n \in \mathbb{Z}^+ \exists\, \infty$ primi $\equiv 1 \pmod n$

$n \mid m$ T.C. $m \geq 3$ m non è pari

$m = 3n$

$$P = \prod_{\substack{p \equiv 1 \,(m) \\ p \text{ PRIMO}}} p$$

$\exists q : \operatorname{ord}_q(P) = m$

$m \mid q-1 \Rightarrow q \equiv 1 \pmod{m}$ $\quad q \mid P$

ASSURDO !

$\operatorname{ord}_p(a) \geq n \Rightarrow p \equiv 1 \pmod{n}$
