Teoria dei Numeri

Note Title 9/3/2016

Livoleito
BrOOtal

RIEPILOGO

WILSON p PRIMO $\rightarrow (p-1)! \equiv -1 \ (p)$

EULERO $(n,x)=1$ $\quad x^{\varphi(n)} \equiv 1 \ (n)$

$ord_n(x) \mid \varphi(n)$

LTE

SIA $p>2$ PRIMO E SIANO a,b INTERI TALI CHE

$(a,p)=1$ $\quad (b,p)=1$ E $p \mid a-b$

$$\nu_p(a^n - b^n) = \nu_p(a-b) + \nu_p(n)$$

$\nu_p(x)$ = "NUMERO DI FATTORI p CHE COMPAIONO IN x"

$$x = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \qquad \nu_{p_j}(x) = \alpha_j$$

$\nu_p(a^n - b^n)$

SUGGERIMENTO: PROVIAMO CON n PRIMO E POI CERCHIAMO DI GENERALIZZARE

i) $n = q$ primo $\neq p$

$$v_p(a^q - b^q) = v_p(a-b) + \underbrace{v_p(q)}_{\| \; 0}$$

$p \nmid q$

$v_p(a^q - b^q) = v_p(a-b)$ È VERO

SE $\dfrac{a^q - b^q}{a-b}$ NON È UN MULTIPLO DI p

$\underbrace{a^{q-1} + a^{q-2}b + \dots + ab^{q-2} + b^{q-1}}_{q \text{ TERMINI}}$

SONO TUTTI $\equiv$ MOD p

PERCHÉ $a \equiv b \; (p)$

$$a \equiv b \ (p)$$

$$a^{q-1} \equiv a^{q-2} \cdot a \equiv a^{q-2} \cdot b \ (p)$$

$$a^{q-i-1} \cdot b^i \equiv a^{q-1} \ (p)$$

$$a^{q-1} + \dots + b^{q-1} \equiv q \cdot a^{q-1} \ (p)$$

$$\not\equiv 0 \ (p)$$

$$a^{q-1} \not\equiv 0 \ (p) \Leftarrow p \nmid a$$

$$q \not\equiv 0 \ (p) \Leftarrow q \neq p$$

$$\frac{a^q - b^q}{a-b} \not\equiv 0 \ (p) \rightarrow v_p\left(\frac{a^q - b^q}{a-b}\right) = 0$$

$$v_p(a^q - b^q) = v_p(a-b) \qquad \square$$

ii) $n = p$

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

FARE IL RAPPORTO; VIENE MA È UN PO' LABORIOSO

Hp. $p \mid a-b$ $\Leftarrow$ $\boxed{a = b + kp}$

(SPESSO RITORNA)

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

$$v_p((b+kp)^p - b^p) = v_p(kp) + 1$$

$(b+kp)^p$ → SVILUPPIAMO

$$(b+kp)^p - b^p =$$

LUI DÀ LA VALUTAZIONE NE p-ADICA =

$$b^p + \boxed{\binom{p}{1} \cdot b^{p-1} \cdot kp} + \binom{p}{2} \cdot b^{p-2} \cdot (kp)^2 + \dots + b^1 (kp)^{p-1} \binom{p}{p-1} + (kp)^p - b^p =$$

$$= \sum_{i=1}^{p} \binom{p}{i} \cdot b^{p-i} \cdot (kp)^i$$

$\nu_p = 1$ SPESSO

TRANNE $i=p \to \nu_p = 0$

$\nu_p = 0$

$\nu_p =$ $i + i\,\nu_p(k)$

$1+i+i\,\nu_p(k)$ (SE $i \neq p$)

$p + p\,\nu_p(k)$ QUANDO $i=1$

Abbiamo $v_p(k)$ è minimo per $i=1$.

(Inoltre con $i=1$ è minore di $i=p$

$$2+v_p(k) < p+p v_p(k)$$

(Ricordiamo: $p>2$) $\rightarrow$ se $p=2$ è $v_2(k)=0$

$$2+v_p(k) = v_p\left((b+k)^p - b^p\right)$$

$$\| \cdot v$$

$$1+v_p(kp)$$

$$1+\left(\underbrace{v_p(k)}_{\|} + \underbrace{v_p(p)}_{\|}\right)$$

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

Vale per n primo

$n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \ldots \cdot q_k^{\alpha_k}$

$v_p\left(\frac{a}{b}\right) = v_p\left(\frac{(q_1^{\alpha_1} \cdot \ldots \cdot q_k^{\alpha_k})}{(q_1^{\alpha_1} \cdot \ldots \cdot q_k^{\alpha_k})}\right) =$

$= v_p(q_1) + v_p\left(\frac{(q_1^{(\alpha_1-1)} \cdot q_2^{\alpha_2} \cdot \ldots \cdot q_k^{\alpha_k})}{(q_1^{\alpha_1} \cdot \ldots \cdot q_k^{\alpha_k})}\right) =$

$= \ldots$ TRIANG $\ldots$ TUTTI

$= v_p(q_1) + \ldots + v_p(q_1) + \ldots$ VARI q_1

α_1

$v_p(n) + v_p(a-b)$

LTE CON IL 2 (a/b) DISPARI

$$v_2(a^n - b^n) = v_2(a-b)$$

SE n È DISPARI

$$v_2(a^n - b^n) = v_2(a^2 - b^2) + v_2(n) - 1$$

SE n È PARI

(SI FA UGUALE)

ESERCIZIO (PLIFORUM) DIMOSTRARE CHE ESISTONO INFINITI INTERI POSITIVI n TALI CHE $n^2 \mid 3^n + 2^n$

LTE CON $a=3$ $b=-2$

L'UNICO PRIMO CHE POSSO PRENDERE È 5

LEMMA DEL GUADAGNO DI UN PRIMO

$(a,b)=1$

SIA $p \geq 2$ PRIMO. ALLORA SPESSO

$\frac{a^p - b^p}{a-b}$ HA UN DIVISORE PRIMO CHE NON HA $a-b$

SE $p=2$ È FALSO MOLTISSIME VOLTE

$a+b$ $(3,1) \to 4$ E 2

$a+b = 2^k$ $a-b=2$

$(a,b)=1$ MA HANNO GLI STESSI FATTORI PRIMI

$p=3$ $a=2$ $b=-1$

$\frac{a^3 - b^3}{a-b} = 3$ $a-b=3$

LTE!

$a^p - b^p$ E $a-b$

SUPPONIAMO CHE NON ESISTA NESSUN PRIMO CHE DIVIDE a^p-b^p E NON $a-b$.

SIA q UN DIVISORE PRIMO DI $a-b$

ALLORA $v_q(a^p-b^p) = v_q(a-b) + v_q(p) =$

$= v_q(p(a-b))$

VERO SE $q \mid a-b$.

SE $q \nmid a-b$ E $q \neq p$

$q \nmid a^p-b^p$ PER IPOTESI $\rightarrow$ $v_q(a^p-b^p) \overset{?}{=} v_q(p(a-b)) \overset{?}{=} 0$

RESTA p: — SE $p \mid a-b$ (LTE)

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

| SE $p \nmid a-b \rightarrow p \nmid a^p-b^p$ (mod p $a^p-b^p \equiv a-b$)

$$v_p(a^p-b^p) = v_p(p(a-b))$$

RIEPILOGANDO

$$v_q(a^p-b^p) = v_q(p(a-b)) = v_q(a-b)$$

$$v_p(a^p-b^p) = \begin{cases} v_p(a-b) \\ v_p(p(a-b)) \end{cases}$$

$\forall q \neq p$ → $a^p-b^p \neq (a-b)$ PERCHÉ HANNO ESATTAMENTE GLI STESSI FATTORI PRIMI

$a-b=0$ (SE $(a,b)=1 \rightarrow a=b=1$)

$a^p-b^p = p(a-b)$

a^p-b^p E $a-b$ HANNO LO STESSO

SEGNO!

SE $a-b>0 \iff a>b \Leftrightarrow a^p>b^p \Leftrightarrow a^p-b^p>0$

a^p-b^p / $p(a-b)$

$(a-b)$

$a^{p-1}+a^{p-2}b+a^{p-3}b^2+\dots+b^{p-1}$

(1,0)

(1,-1)

1

ϕ

SE SONO TUTTI CONCORDI (OVVIO)

SE HANNO SEGNI OPPOSTI

$a^{p-2}(a-b)+a^{p-4}b^2(a-b)+\dots+$

$+b^{p-3}(a-b)+b^{p-1}$

ECCEZIONE CON p

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

$a=2 \quad b=-1 \quad p=3$

$n^2 \mid 2^n + 3^n$

PASSIAMO DA UNA SOLUZIONE ALL'ALTRA ATTRAVERSO IL LEMMA DEL GUADAGNO DI UN PRIMO.

$n=1$ ✓ $\quad 1 \mid 2^1 + 3^1$

$n=5$ ✓ $\quad 25 \mid 2^5 + 3^5$

$\| \quad 275 = 5^2 \cdot 11$

$11^2 \mid 2^{11} + 3^{11}$ NO!

$\|$

$2+3 \ (11)$

$55 \quad 2 \mid 2^{55} + 3^{55} = \checkmark \quad (2^5)^{11} + (3^5)^{11}$

$v_p\left(2^{55} + 3^{55}\right) = v_p(11) + v_p\left(2^5 + 3^5\right)$

$p = 5, 11$ $\qquad$ 11 $\qquad$ $5^2 \cdot 11$

SIA $a_0 = 1$, $a_1 = 5$ E DEFINIAMO

$a_{n+1} = p \cdot a_n$, DOVE p È UN

PRIMO CHE DIVIDE $3^{a_n} + 2^{a_n}$ MA NON

$3^{a_{n-1}} + 2^{a_{n-1}}$. TALE PRIMO ESISTE

PER IL LEMMA DI p PERCHÉ

$a_n = a_{n-1} \cdot q$, CON q PRIMO

VERIFICHIAMO PER INDUZIONE CHE LA a_i FUNZIONANO

$a_0 = 1$ ✓ $\quad 1^2 \mid 5$

$a_{n+1} = p \cdot a_n$

$a_{n+1}^2 \overset{?}{\mid} 3^{a_{n+1}} + 2^{a_{n+1}}$

$p^2 \cdot a_n^2 \mid 3^{p a_n} + 2$?

$p a_n$

$p a_n$

PERCHÉ $a_n^2 \mid 3^{a_n} + 2^{a_n}$

$\Big\} \; p a_n \quad p a_n$

$+2$

VERIFICHIAMO

CHE $(p, a_n) = 1$ PERCHÉ

$p \mid 3^{a_n} + 2^{a_n}$ MA NON $3^{a_{n-1}} + 2^{a_{n-1}}$

E $a_n = q \cdot a_{n-1}$

VOGLIAMO $a_n \mid 3^{a_{n-1}} + 2^{a_{n-1}}$

$\| \; q \cdot a_{n-1}$

PER INDUZIONE

NORMALMENTE: $(p_n, a_n) = 1$ PER INDUZIONE

BASE: $a_0 = 1$ P.I.: SOPRA

(1 MANCA $p^2 \mid 3^{a_{n+1}} + 2^{a_{n+1}} =$

$\Rightarrow 3^{pa_n} + 2^{pa_n}$

$v_p\left(3^{pa_n} + 2^{pa_n}\right) = v_p(p) + v_p\left(3^{a_n} + 2^{a_n}\right)$

$\geq 1 \qquad \geq 1$

$\mathbb{F}_p$ → PER QUANTI INTERI $n \in \{0, 1, \dots, (p-1)\}$ PUÒ ANNULLARSI?

UN POLINOMIO QUANTE RADICI $\bmod p$ PUÒ AVERE MODULO p?

$x+1$ IN CHE VALORI SI ANNULLA

SOLO IN -1,

$x+1 \equiv 0 \ (p) \Rightarrow x \equiv -1 \ (p)$

$$x^2+1 \equiv 0 \ (p)$$

TRE TIPI
- 0: $x^2+1 \equiv 0 \ (3)$
- 1: $x^2+1 \equiv 0 \ (2)$
- 2: $x^2+1 \equiv 0 \ (5)$

FATTO: SE $f(x)$ È UN POLINOMIO MONICO DI GRADO k HA AL PIÙ k RADICI MODULO p.

MOD 15: $x(x-1)(x-2)$

HA COME RADICI.

0, 1, 2, 5, 6, 7, 10, 11, 12

PERCHÉ È VERO IL FATTO?

IN $\mathbb{Z}$ I POLINOMI HANNO AL PIÙ k RADICI.

$$a \cdot b = 0 \rightarrow a = 0 \vee b = 0$$

$$a \cdot b \equiv 0 \ (p) \rightarrow a \equiv 0 \ (p) \vee b \equiv 0 \ (p)$$

$$3 \cdot 5 \equiv 0 \ (15) \not\Rightarrow 3 \equiv 0 \ (15) \vee 5 \equiv 0 \ (15)$$

SIA $f(x)$ UN POLINOMIO MONICO DI GRADO k E SUPPONIAMO CHE ABBIA $k+1$ RADICI.

PER INDUZIONE, SE $g(x)$ HA

GRADO $k-1$, HA AL PIÙ $k-1$ RADICI.

PASSO BASE: GRADO 0

1 NON HA RADICI MOD p.

PASSO INDUTTIVO.

$f(x)$ HA $\alpha_1, \dots, \alpha_{k-1}$ COME RADICI.

VORREMMO SCRIVERE $f(x) =$

$$g(x) \cdot (x - \alpha_1)$$

$f(x) = x^2 + 1 \qquad \alpha_1 = 2 \qquad p = 5$

$$x^2 + 1 = (x-2) \cdot g(x)$$

$$\downarrow$$

$$(x+2) =$$

$$x^2 - 4 \quad (5)$$

Polinomi modulo p

I coefficienti dei polinomi sono guardati modulo p.

Modulo 5: $x^6 - 3x^2 + 17x \equiv$

$\equiv x^6 + 2x^2 + 2x \pmod 5$

α è radice di f se $f(\alpha) \equiv 0 \pmod p$

Def. finale: $\alpha(x)$ e $\beta(x)$ sono uguali modulo p se i coefficienti sono uguali modulo p.

Oss. $x^5 \equiv x \pmod 5$ il pol.

$x^5 - 1 \overset{?}{\equiv} x - 1 \pmod 5$

$x^5 - 1 \equiv (x-1)^5 \quad (5) \rightarrow$ 5 RADICI

$x - 1 \quad (5) \rightarrow$ 1 SOLA RADICE

$x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1$

$f(x)$ E VOGLIAMO $f(x) = (x - \alpha_1) \cdot g(x)$ (p)

$f(\alpha_1) \equiv 0 \cdot p$ PER IPOTESI

IL POLINOMIO $f(x) - 0_p$ (NO) HA UNA INF. RADICE INTERA, IN $\mathbb{R}$.

PER RUFFINI $\boxed{f(x) - 0_p = (x - \alpha_1) \cdot g(x)}$ ($\deg g = k-1$)

VALE ANCHE MODULO p

$$f(x) \equiv (x - \alpha_1) \cdot g(x) \pmod{p}$$

α_1

$\alpha_2, \dots, \alpha_{k+1}$ → DISTINTI MOD p

$f(\alpha_2) \equiv 0 \pmod{p}$ ma $\not\equiv 0$

$$\equiv (\alpha_2 - \alpha_1) \cdot g(\alpha_2) \pmod{p}$$

$g(\alpha_2) \equiv 0 \pmod{p}$

ALLORA $g(x)$ HA k RADICI.

(E HA GRADO $k-1$)

QUALUNQUE POLINOMIO MOD p IN CUI IL TERMINE DI TESTA NON SIA CONSIDERATO NULLO

$$0 \cdot x \equiv 0 \pmod{p}$$

GRADO DI UN POLINOMIO MOD p:

IL GRADO DEL MONOMIO NON NULLO MOD p MAGGIORE

$$3x^2 + 2 \equiv 0 \quad (5)$$

$\updownarrow$ HA LE STESSE

$$2(3x^2 + 2) \equiv 2 \cdot 0 \quad (5)$$

$$x^2 + 4 \equiv 0 \quad (5)$$

PRENDIAMO TUTTI I POLINOMI MODULO p DI GRADO MINORE DI p.

QUELLI DI GRADO k SONO:

$$(p-1) \cdot p^k$$

$a_k x^k + \dots + a_0$

a_k: $p-1$

$a_{k-1}, \dots, a_0$: p mod l'uno

IN TOTALE $\sum_{i=0}^{p-1} (p-1)\cdot p^i = p^p - 1$

METTIAMOCI PURE LO 0 : p^p

PRENDIAMO $f(x)$ E $g(x)$ TRA QUESTI.
POSSONO COINCIDERE MODULO p
PER OGNI x INTERO?

SE $\underbrace{f(x) - g(x)}_{h(x)} \equiv 0 \pmod p \quad \forall x$ ~~$\neq$~~

$h(x)$ HA p RADICI MODULO p.

↳ HA GRADO $< p$ E NON È 0 SE $f \neq g$

$h(x)$ HA p RADICI: $h(x) \equiv x \cdot h_1(x) \equiv$

$x(x-1)\cdot h_2(x) \equiv x(x-1)(x-2)\cdot h_3(x) + \dots$

TRA I p^p POLINOMI NON CE NE SONO DUE CHE COINCIDONO IN OGNI INTERO MODULO p.

HO UNA FUNZIONE f DA $\{0,\dots,p-1\} \to \{0,\dots,p-1\}$ SONO p^p.

DATO CHE DUE POLINOMI DIVERSI SONO DUE FUNZIONI DIVERSE, ALLORA OGNI FUNZIONE È RAPPRESENTATA DA UN POLINOMIO, POICHÉ SONO NELLO STESSO NUMERO (FINITO).

$$f: \{0,\dots,p-1\} \to \{0,\dots,p-1\}$$

$$f(x) \equiv \sum_{i=0}^{p-1} \left(\left(1-(x-i)^{p-1}\right) \cdot f(i) \right)$$

SE $x \equiv i$ $\quad \left(1 - (x-i)^{p-1}\right) \equiv 1$

$x \not\equiv i$ $\quad \left(1 - \underbrace{(x-i)^{p-1}}_{\to 1}\right) \equiv 0$

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

HA $p-1$ RADICI

SONO DUE POLINOMI MONICI DI GRADO $p-1$ CON ESATTAMENTE LE STESSE $p-1$ RADICI

VALUTO IN 0: $-1 \equiv (-1)\cdot(-2)\cdot\dots\cdot(-(p-1)) \pmod p$

(T.N. UGUALI) $\quad (-1)^{p-1}\cdot(p-1)! \pmod p$

RADICI DI $x^k - 1$ MODULO p

1 SEMPRE

$x^{\frac{p-1}{2}} - 1$. AL MASSIMO $\frac{p-1}{2}$

SE $x = a^2 \ (p) \Rightarrow x^{\frac{p-1}{2}} \equiv a^{2 \cdot \frac{p-1}{2}} \equiv 1 \ (p)$

↳ sono $\frac{p-1}{2}$

ESCURSUS SUI RESIDUI QUADRATICI

(CHIAMIAMO x R.Q. SE $\exists \ a$ T.C. $a^2 \equiv x \ (p)$

I RESIDUI QUADRATICI $\neq 0$ SONO $\frac{p-1}{2}$.

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

SE $x^2 \equiv y^2 \ (p) \Rightarrow (x-y)(x+y) \equiv 0 \ (p)$

$\equiv 0$ $\quad$ $0 < x < p$

QUINDI

$1^2, 2^2, \dots \left(\frac{p-1}{2}\right)^2$ SONO DISTINTI MODULO p

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

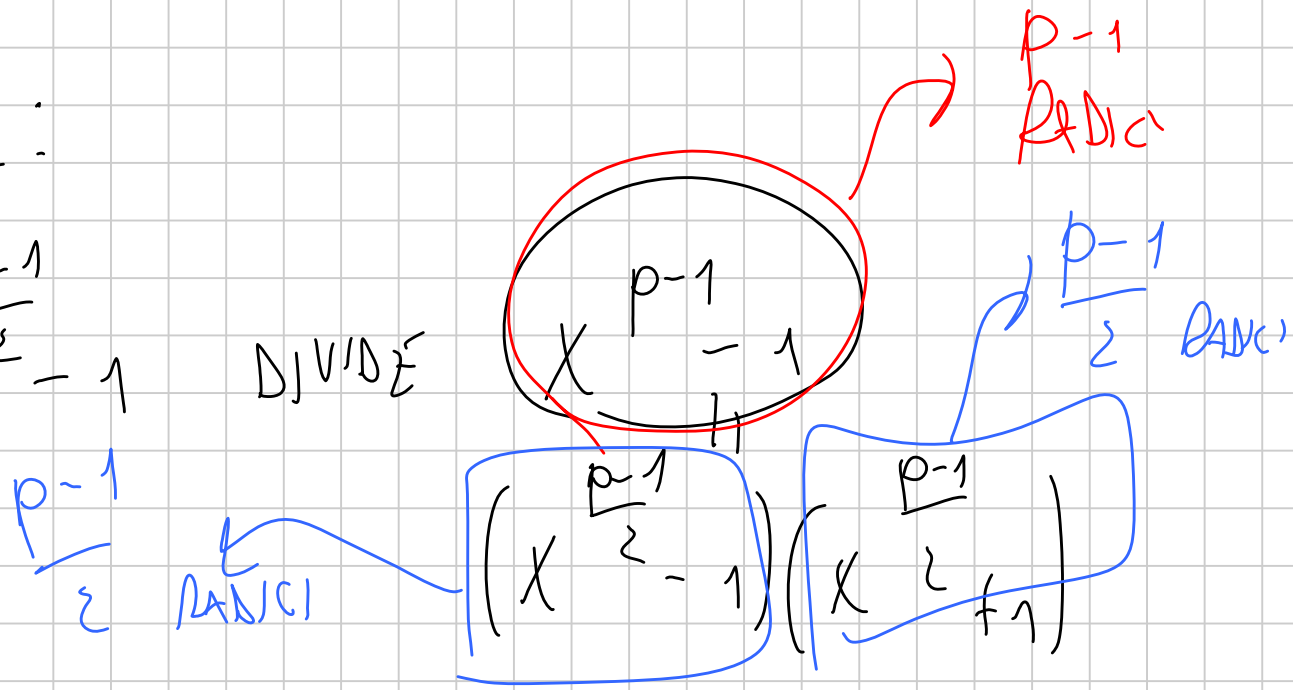
a^2

$X^{\frac{p-1}{2}} - 1$ HA AL MASSIMO $\frac{p-1}{2}$ RADICI E I R.Q. SONO SUE RADICI.

Modo 1: CI SONO $\frac{p-1}{2}$ R.Q. V

Modo 2:

$X^{\frac{p-1}{2}} - 1$ DIVIDE $X^{p-1} - 1$



CRITERIO DI EULERO:

a R.Q. $\Leftrightarrow$ $a^{\frac{p-1}{2}} \equiv 1 \ (p)$

a N.Q. $\Leftrightarrow$ $a^{\frac{p-1}{2}} \equiv -1 \ (p)$

AD ESEMPIO: QUANDO -1 È R.Q.

$$(-1)^{\frac{p-1}{2}} \equiv 1 \ (p) \iff p \equiv 1 \ (4)$$

$$\left(\frac{p-1}{2}\right)! \equiv \underbrace{\left(\left(\frac{p+1}{2}\right) \cdot \ldots \cdot (p-1)\right)}_{\left(\frac{p-1}{2}\right)! \cdot (-1)^{\frac{p-1}{2}}} \ (p)$$

$$1 \equiv -(p-1)$$
$$2 \equiv -(p-2)$$
$$\ldots \equiv -$$
$$\left(\frac{p-1}{2}\right) \equiv -\left(\frac{p+1}{2}\right)$$

SE $p \equiv 1 \ (4)$

$\frac{p-1}{2}$ — SONO PARI

PROP. DI TUTTI $(p-1)! \equiv -1 \ (p)$

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

$p = 13$

$\{1, 2, 3, 4, 5, 6\}$

$\{7, 8, 9, 10, 11, 12\}$

$(13-1) \equiv (-1) \cdot 1$
$(13-2) \equiv (-1) \cdot 2$
$(13-3) \equiv (-1) \cdot 3$
$\ldots$
$(13-6) \equiv (-1) \cdot 6$

$\cdot (-1)^6 = 1$

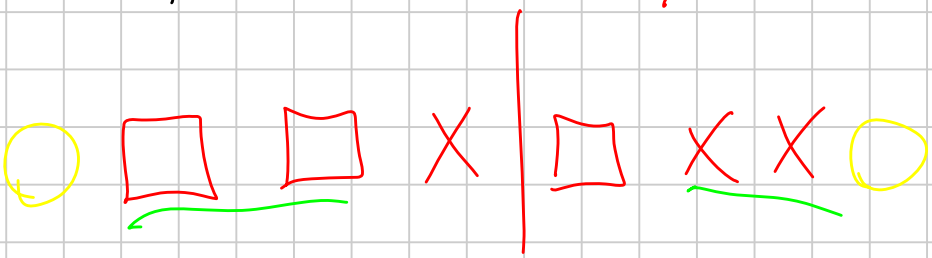
ESERCIZIO

- VEDIAMO (PER QUALI) QUANDO $(x^2+1)^{\frac{p-1}{2}} \equiv 1 \ (p)$

  x^2+1 È R.Q.

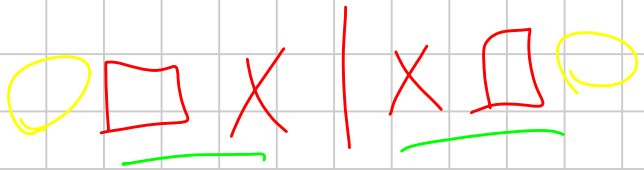
- È QUANDO 2 È R.Q. MODULO p

SE $p \equiv 3 \ (4)$ □ R.Q. X N.Q.



SIMMETRIA INVERSA

$p \equiv 1 \ (4)$



SIMMETRIA GIUSTA

PROVIAMO CONTARE QUANDO

$\sum_{\#\square (\Delta-1)}$ [□ + 1 = □] SE $p \equiv 3(4)$ SONO UGUALI

[X + 1 = X]

$\sum_{\#\Delta (\Delta-1)}$ [□ + 1 = X]

[X + 1 = □] SE $p \equiv 1(4)$ SONO UGUALI

QUANTI SONO $\square + 1 = \square$

$x^2 + 1 \equiv y^2 \ (p)$

È (CIRCA) 4 VOLTE

(SUPPONIAMO $x, y \neq 0$ — SE $x=0$ O $y=0$)

$(x-y)(x+y) \equiv -1 \ (p)$

a b

$ab \equiv -1 \ (p)$

$\frac{a+b}{2} \equiv x \ (p)$

$\frac{b-a}{2} \equiv y \ (p)$

$a \not\equiv b \ (p)$

$a \not\equiv -b \ (p)$

$a^2 \equiv -1 \ (p)$

$a^2 \equiv 1 \ (p)$

TOGLIAMO

$a \equiv i \ (p)$

$b \equiv i \ (p)$

$a \equiv -i \ (p)$ $b \equiv -i \ (p)$

$a \equiv 1 \ (p)$ $b \equiv -1 \ (p)$

$a \equiv -1 \ (p)$ $b \equiv 1 \ (p)$

$ab \equiv -1 \ (p)$

$ab \equiv -1 \pmod p$ SONO $p-1$:

$a \equiv -\frac{1}{b} \pmod p$ PER OGNI $b \neq 0$ C'È ESATTAMENTE UNA SOLUZIONE.

SOLUZIONI: $p-1$

SE $p \equiv 1 \pmod 4$ → $\frac{p-5}{4}$ BUONE

$p \equiv 3 \pmod 4$ → $\frac{p-3}{4}$ BUONE

$p \equiv 3 \pmod 4$

□ + 1 = □ $\frac{p-3}{4}$

△ + 1 = △ $\frac{p-3}{4}$

□ + 1 = △ $\frac{p+1}{4}$

△ + 1 = □ $\frac{p-3}{4}$

$p \equiv 1 \pmod 4$

□ + 1 = □ $\frac{p-5}{4}$

△ + 1 = △ $\frac{p-1}{4}$

□ + 1 = △ $\frac{p-1}{4}$

△ + 1 = □ $\frac{p-1}{4}$

2 è R.Q. $\Leftrightarrow \left(\frac{p+1}{2}\right)$ è R.Q.

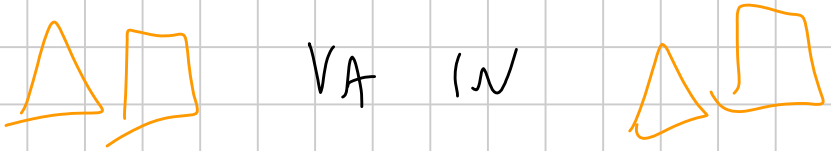
$$2^{\frac{p-1}{2}} \equiv 1 \ (p) \Leftrightarrow \left(\frac{p+1}{2}\right)^{\frac{p-1}{2}} \equiv 1 \ (p)$$

$$\text{Se} \quad \left(\frac{p+1}{2}\right)^{\frac{p-1}{2}} \equiv -1 \ (p)$$

$$-1 \equiv 2^{\frac{p-1}{2}} \cdot \left(\frac{p+1}{2}\right)^{\frac{p-1}{2}} \equiv 1^{\frac{p-1}{2}} \ (p)$$

7

In $p \equiv 3 \ (4)$



VA IN

$\left(\frac{p-1}{2}, \frac{p+1}{2}\right)$ È L'UNICA COPPIA FISSA:

È DEL TIPO DISPARI

ANALOGO PER $p \equiv 1 (4)$.

IN GENERALE

2 R.Q. $p \Leftrightarrow p \equiv \pm 1 (8)$

GENERATORI

IDENTITÀ

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

$\frac{1}{15}$ $\frac{2}{15}$ $\frac{3}{15}$ $\frac{4}{15}$ $\frac{5}{15}$ $\frac{6}{15}$ $\frac{7}{15}$ $\frac{8}{15}$ $\frac{9}{15}$ $\frac{10}{15}$ $\frac{11}{15}$

$\frac{12}{15}$ $\frac{13}{15}$ $\frac{14}{15}$ $\frac{15}{15}$

15 : 8

5 : 4

3 ; 2

1 : 1

LE FRAZIONI SONO n:

QUELLE CON DENOMINATORE

d SONO $\phi(d)$, OVVERO TUTTE QUELLE DEL TIPO $\frac{a}{d}$ CON $a<d$ E $(a,d)=1$

DELLE n FRAZIONI RESTANO FRAZIONI DEL TIPO $\frac{a}{d}$, CON $d \mid n$ E NE RESTANO $\varphi(d)$ ESATTAMENTE.

POLINOMI IN $\mathbb{Z}[x]$:

POLINOMI A COEFFICIENTI INTERI.

UN POLINOMIO MONICO $f(x)$ SI DICE IRRIDUCIBILE SE NON ESISTONO POLINOMI NON COSTANTI TALI CHE $f(x)=p(x)\cdot q(x)$

OGNI POLINOMIO MONICO A COEFFICIENTI INTERI È PRODOTTO DI IRRIDUCIBILI:

$$f(x)=f_1(x)\cdot f_2(x)=f_1(x)\cdot f_2(x)\cdot f_3(x)=\dots$$

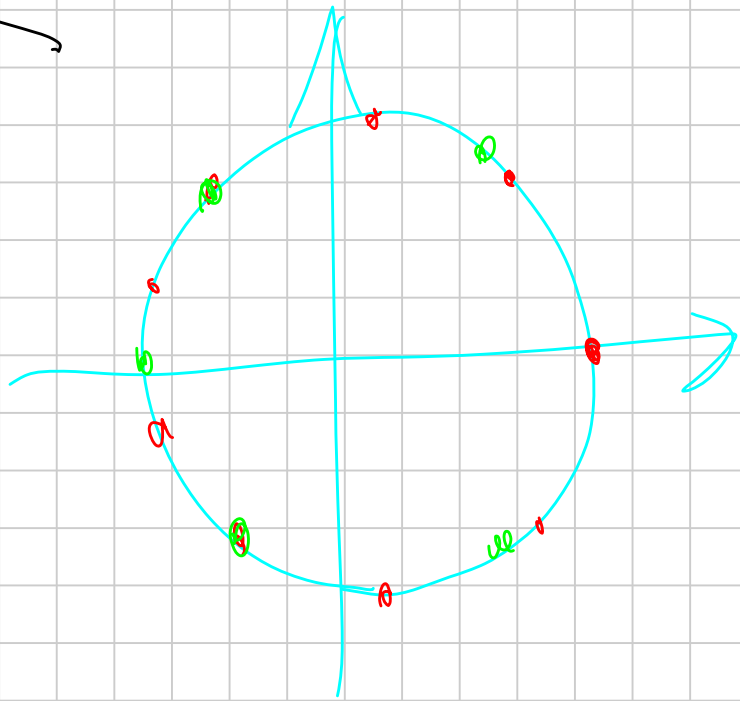
NON POSSO ANDARE AVANTI ALL'INFINITO

$x^n - 1 \mid x^m - 1$

$\rightarrow$ SE $n \mid m$ ALLORA

$m = kn$

$$x^m - 1 = x^{kn} - 1 = (x^n - 1)(x^{n(k-1)} + \dots + 1)$$



9 6

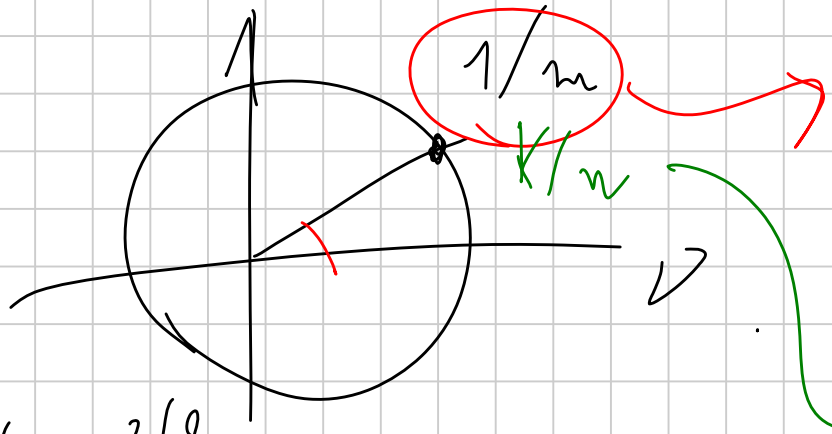
SE $n \nmid m$,

$\exists\, d$ t.c.

$d \mid n$ · $\frac{n}{m}$ NON È INTERO

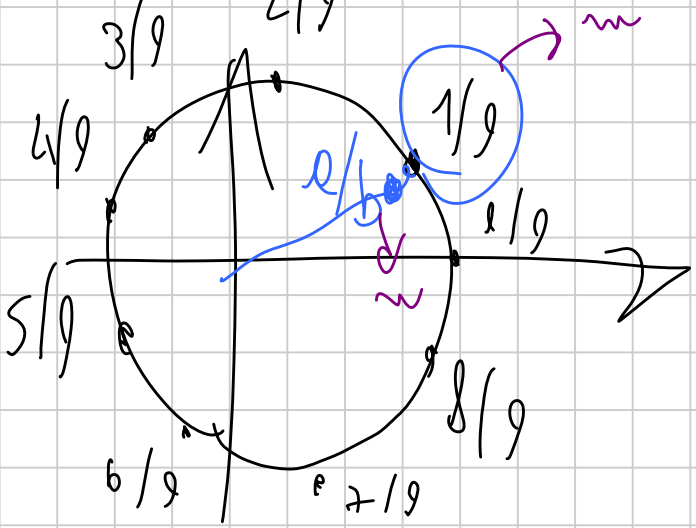
$d = 1$

SE $n \nmid m \rightarrow$ LA RADICE m-ESIMA PRIMITIVA "PIÙ VICINA" A 1 NON È RADICE DI $x^n - 1$



FA PARTE DELL'n-AGONO

$\Rightarrow n = km$



$$9 \cdot \frac{a}{b} = 1 \qquad b = 9 \cdot a$$

$$\left(X^m - 1,\ X^n - 1\right) = X^{(m,n)} - 1$$

PER INDUZIONE SU $|m \cdot n|$

SE $m > n$

$$\left(X^m - 1,\ X^n - 1\right) = \left(X^m - 1 - X^{m-n}\left(X^n - 1\right),\ X^n - 1\right) =$$

$$= \left(X^{m-n} - 1,\ X^n - 1\right) = X^{(m-n,n)} - 1 =$$

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

$$x^m - 1 = f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_k(x)$$

OGNI $x^n - 1$ CONTIENE UN POLINOMIO CHE LO DIVIDE NUOVO.

$\Phi(1)$

1: $x-1$ $\quad \Phi(2)$

2: $(x-1)(x+1)$

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

4: $(x-1)(x+1)(x^2+1)$

5: $(x-1)(x^4+x^3+x^2+x+1)$

6: $(x-1)(x+1)(x^2+x+1)(x^2-x+1)$

$\Phi(1)$ $\Phi(2)$ $\Phi(3)$ $\Phi(4)$ $\Phi(5)$ $\Phi(6)$

IN $x^n - 1$ CI SONO GLI IRRIDUCIBILI DEI DIVISORI d PER $x^d - 1$

SE $\Phi(K)$ STA IN $x^n - 1$ E $K \nmid n$ ALLORA APPARE PURE IN $x^{(n,K)} - 1$: ASSURD! $(n,K) < K$

PER INDUZIONE:

SUPPONIAMO $\deg\left|\Phi(k)\right| = \phi(k)$ $\forall k \le n-1$

$\Phi(n)$

NIENTE: OGNI POLINOMIO O È NUOVO, O STA IN $\Phi(d)$

$$X^n - 1 = \Phi(n) \cdot \left(\prod_{d<n,\, d\mid n} \Phi(d) \right)$$

OPPURE STA IN $\Phi(k)$ CON $k<n$:

ASSURDO

QUINDI $\deg\left(X^n-1\right| = n$

$$= \deg\left|\Phi(n)\right| + \deg\left|\prod_{d<n,\, d\mid n} \Phi(d)\right| =$$

$$= \deg\left|\Phi(n)\right| + \sum_{d\mid n,\, d<n} \varphi(d)$$

$$n - \varphi(n)$$

$$\Phi_n(x) = \prod_{(d,n)=1,\ d<n} \left(x - \omega^d\right)$$

CON ω RADICE PRIMITIVA n-ESIMA

PRENDIAMO $x^{p-1} - 1 \equiv 0 \ (p)$

HA p RADICI.

$\Phi_{p-1}(x) \equiv 0 \ (p)$

$\deg : \phi(p-1)$

$\Rightarrow$ HA $\phi(p-1)$ RADICI ≥ 1

Def. di $\Phi_n(x)$: PRODOTTO DEGLI IRRIDUCIBILI CHE DIVIDONO $x^n - 1$ MA NON $x^m - 1 \ \forall m < n$

SIA y UNA SUA RADICE.

$\Rightarrow \mathrm{ord}_p(y) = d \mid p-1$

y È RADICE DI $x^d - 1$

SE $d < p-1$, $\Phi_{p-1}(x) \cdot (x^d - 1)$ DIVIDE $x^{p-1} - 1$

↳ PRODOTTO DI ALTRI CICLOTOMICI

ASSURDO! $x^{p-1} - 1$ NON HA RADICI DOPPIE.

DUNQUE $\operatorname{ord}_p(g) = p-1$

$$\sum_{i=1}^{p-1} i^k \equiv \begin{cases} 0 & \text{SE } p-1 \nmid k \\ -1 & \text{SE } p-1 \mid k \end{cases}$$

$$\{1, \dots, p-1\} \longleftrightarrow \{g, 2g, \dots, g(p-1)\}$$

PERMUTAZIONE MODULO p

$$\sum_{i=1}^{p-1} i^k \equiv \sum_{j=1}^{p-1} (gj)^k \equiv g^k \sum_{i=1}^{p-1} i^k \pmod{p}$$

$$0 \equiv (g^k - 1) \cdot \sum_{i=1}^{p-1} i^k \pmod{p}$$

$g^k - 1 \neq 0$ (crossed out)

$\sum_{i=1}^{p-1} i^k \to \equiv 0 \pmod{p}$

SE $p-1 \nmid K \to y^K \not\equiv 1 \pmod p$ PERCHÉ $\operatorname{ord}_p(y) = p-1$

SE $p-1 \mid K \to i^K \equiv 1 \pmod p \to \sum_{i=1}^{p-1} 1 \equiv p-1 \pmod p$

CONTANO PER QUANTI (X, Y)

$$X^2 + 1 \equiv y^2 \pmod p$$

X^2+1 È $\square \iff (X^2+1)^{\frac{p-1}{2}} \equiv 1 \pmod p$

X^2+1 È $\triangle \iff (X^2+1)^{\frac{p-1}{2}} \equiv -1 \pmod p$

$X^2+1 \equiv 0 \pmod p \iff (X^2+1)^{\frac{p-1}{2}} \equiv 0 \pmod p$

$$\sum_{i=0}^{\frac{p-1}{2}} (i^2+1)^{\frac{p-1}{2}} \to \#\square - \#\triangle$$

$$\sum_{i=0}^{p-1} (i^2+1)^{\frac{p-1}{2}} = 2\sum_{i=1}^{\frac{p-1}{2}} (i^2+1)^{\frac{p-1}{2}} + 1$$

→ MEGLIO DI $p-1$

$$\sum_{i=0}^{p-1}\left(\sum_{j=0}^{\frac{p-1}{2}} i^{2j}\binom{\frac{p-1}{2}}{j}\right) = \sum_{j=0}^{\frac{p-1}{2}}\left(\sum_{i=0}^{p-1} i^{2j}\binom{\frac{p-1}{2}}{j}\right)$$

$$\sum_{i=0}^{p-1} i^{p-1}\binom{\frac{p-1}{2}}{\frac{p-1}{2}} \equiv -1 \ (p) \qquad \neq 0 \Leftrightarrow j = \frac{p-1}{2}$$

$$-1 \equiv \sum_{i=0}^{\frac{p-1}{2}} (1+i^2)^{\frac{p-1}{2}} \equiv 2\sum_{i=0}^{\frac{p-1}{2}} (i^2+1)^{\frac{p-1}{2}} + 1 \ (p)$$

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

$\rightarrow \#\square$

$\rightarrow \#\triangle$

$\rightarrow 0$ (se $p \equiv 1 \ (4)$)

- $p \equiv 1 \ (4)$ $\quad -1 \equiv \#\square - \#\triangle \ (p)$ $\quad \#\square + \#\triangle = \frac{p-3}{2}$

$$2\#\square \equiv \frac{p-5}{2} \ (p)$$

$$\#\square \equiv \frac{p-5}{4} \ (p) \rightarrow \#\square < p$$

$$\#\square = \frac{p-5}{4}$$

- $p \equiv 3(4)$ $\quad -1 = \#\square - \#\triangle$ (p) $\quad \#\square + \#\triangle = \frac{p-1}{2}$

$$\#\square \equiv \frac{p-3}{4} \quad (p)$$

$$\text{ou } \frac{p-3}{4}$$