Teoria dei Numeri 2 - Medium

Note Title 9/6/2017

(Bozza 6)

OGGI:

- LTE;
- GENERATORI E POLINOMI CICLOTOMICI;
- RESIDUI QUADRATICI;
- PELL / INTERI DI GAUSS / NIENTE.

LTE

PRELIMINARMENTE:

$v_p(n) = k$

↳ VALUTAZIONE p-ADICA

t.c. $p^k \mid n$ E $p^{k+1} \nmid n$

$v_p(n)$ È L'ESPONENTE DI p NELLA FATTORIZZAZIONE DI n. [ES. $v_3(87) = 1$]

LTE: p PRIMO DISPARI

$(a \not\equiv b)$ a, b INTERI NON MULTIPLI DI p

$a-b$ MULTIPLO DI p.

n INTERO POSITIVO.

Th. → $v_p(a^n - b^n) = v_p(a-b) + v_p(n)$

IDEA FONDAMENTALE: FACCIO IL CASO n PRIMO.

PERCHÉ? I.E.: $n = 60$ p

$$v_p(a^{60} - b^{60}) = v_p(a^{30} - b^{30}) + v_p(2) =$$

$$= v_p(a^{15} - b^{15}) + v_p(2) + v_p(2) =$$

$$= v_p(a^5 - b^5) + v_p(2) + v_p(2) + v_p(3) =$$

$$= v_p(a-b) + v_p(2) + v_p(2) + v_p(3) + v_p(5) =$$

$$= v_p(a-b) + v_p(60)$$

SE LO SO FARE CON n PRIMO LO SO FARE

CON OGNI n.

CONTROLLIAMO CHE IN OGNI SINGOLA UGUAGLIANZA SIANO RISPETTATE LE IPOTESI DI LTE

Hp. $p \mid a-b,\ p \nmid a,\ p \nmid b$

OCCHIO; SOPRA NON ABBIAMO SEMPRE APPLICATO LTE AD a E b, MOLTO SPESSO L'ABBIAMO USATO SU a^k E b^k

Hp. NUOVE $p \mid a^k - b^k$, $p \nmid a^k$, $p \nmid b^k$

OVVIA (da $p \nmid a^k$)

OVVIA PERCHÉ p PRIMO (da $p \nmid b^k$)

$p \mid a-b \mid a^k - b^k \rightarrow p \mid a^k - b^k$

QUINDI BASTA DAVVERO n PRIMO.

QUINDI DIMOSTRIAMOLO CON $n = q$

VOGLIAMO DIMOSTRARE CHE:

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

SCRIVIAMO $a = b + kp$ PERCHÉ $p \mid b - a$

E ANDIAMO A SVILUPPARE

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

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

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

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

NOI VOGLIAMO TROVARNE LA v_p

HA POCHI p DENTRO (MENO DEGLI ALTRI TERMINI)

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

$$v_p\left(\binom{q}{i}\cdot b^{q-i}\cdot (Kp)^i\right) =$$

$$= v_p\left(\binom{q}{i}\right) + v_p\left(b^{q-i}\right) + v_p\left((Kp)^i\right) =$$

$$= v_p\left(\binom{q}{i}\right) + (q-i)\,\underbrace{v_p(b)}_{=0} + i\,v_p(Kp) =$$

$$= v_p\left(\binom{q}{i}\right) + i\,v_p(Kp)$$

QUESTO CI DICE CHE:

SE $i > 1$:

$$v_p\left(\binom{q}{i}\cdot b^{q-i}\cdot (Kp)^i\right) > v_p\left(\binom{q}{1}\cdot b^{q-1}\cdot (Kp)\right)$$

PERCHÉ

$$v_p\left(\binom{q}{i}\right) + i\,v_p(Kp) \overset{\star}{\geq} v_p\left(\binom{q}{1}\right) + v_p(Kp)$$

C'È UN PROBLEMA: SE $p = q$

$$v_p\left(\binom{q}{1}\right) > v_p\left(\binom{q}{i}\right) \quad \text{A VOLTE}$$

CASO 1: $p \neq q$

$\longrightarrow \quad \nu_p\left(\binom{q}{1}\right) = 0.$

$\star \quad \nu_p\left(\binom{q}{i}\right) + i\,\nu_p(p^k) > \nu_p(p^k)$

VERA PER OGNI $i > 1$ PERCHÉ $\nu_p(p^k) > 0$

IN QUESTO CASO:

$$\nu_p\left(\sum_{i=1}^{q}\binom{q}{i}\cdot b^{q-i}\cdot (p^k)^i\right) =$$

$\downarrow$ TUTTI GLI ALTRI TERMINI DELLA Σ HANNO ν_p MAGGIORE

$$= \nu_p\left(\binom{q}{1}\cdot b^{q-1}\cdot (p^k)^1\right) = \nu_p(p^k) = \nu_p(a-b) \quad \checkmark$$

CASO 2: n PRIMO, $n \neq p$, A POSTO:

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

$\downarrow$

$= 0$

CASO $n = p$.

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

PRIMA $v_p\left(\binom{p}{1}\right) = 0$

IN GENERALE $v_p\left(\binom{p}{i}\right) = ?$ $\begin{cases} 0 \\ 1 \end{cases}$

PERCHÉ AL NUMERATORE C'È $p!$, CON AL MASSIMO UN p CHE COMPARE.

$p! \to v_p = 1$

$i!\,(p-i)! \to$ STESSO $v_p = 0$

↳ 2 SOLI CASI IN CUI È MULTIPLO DI p: $i = 0$ E $i = p$

(SENNÒ NON ARRIVO A p)

$$v_p\left(\binom{p}{i}\right) \begin{cases} 0 & \text{SE } i = 0, p \\ 1 & \text{ALTRIMENTI} \end{cases}$$

EURISTICAMENTE I TERMINI PROBLEMATICI SONO CON $i = 1, p$

$$v_p\left(\binom{p}{i} \cdot b^{p-i} \cdot (k_p)^i\right) \overset{?}{\geq} v_p\left(\binom{p}{1} b^{p-1} \cdot (k_p)\right)$$

LA VORREMO PER OGNI $i \geq 1$

$$v_p\left(\binom{p}{i}\right) + i\, v_p(k_p) \overset{?}{\geq} v_p\left(\binom{p}{1}\right) + v_p(k_p)$$

$v_p(k_p) > 0$; QUINDI $\quad i\, v_p(k_p) > v_p(k_p)$

$$v_p\left(\binom{p}{i}\right) \geq v_p\left(\binom{p}{1}\right) \qquad \forall\, 1 \leq i \leq p-1$$

PERCIÒ SE $i \neq p$ LA ✡ È VERA

RESTA $i = p$.

$$p\, v_p(k_p) > v_p\left(\binom{p}{1}\right) + v_p(k_p)$$

$$(p-1)\, v_p(k_p) > 1$$

MOTIVO PER CUI LTE NON VALE PER $p = 2$

VERA PER $p > 2$

PERCIÒ $v_p\left(\binom{p}{i} \cdot b^{p-i} \cdot (pk)^i\right) \geq v_p\left(\binom{p}{1} \cdot b^{p-1} \cdot (pk)\right)$

$\forall\, i > 1$

QUINDI:

$$v_p\left(\sum_{i=1}^{p} \binom{p}{i} \cdot b^{p-i} \cdot (pk)^i\right) = v_p\left(\binom{p}{1} \cdot b^{p-1} \cdot (pk)\right) =$$

$$= 1 + v_p(pk) = v_p(pk) + v_p(n)$$

□

È p CHE DEVE ESSERE DISPARI, n PUÒ ESSERE CHIUNQUE.

VALE UNA SPECIE DI LTE CON IL 2, OVVERO:

$2 \nmid a,\quad 2 \nmid b,\quad 4 \mid a - b$

$$\longrightarrow \quad v_2(a^n - b^n) = v_2(a-b) + v_2(n)$$

DIMOSTRATELO

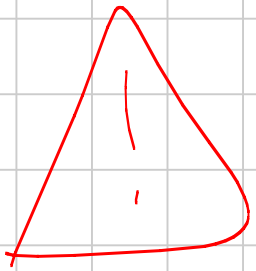
(HINT: È UGUALE)

Es. DIMOSTRARE CHE 2 È GENERATORE MODULO 3^n PER OGNI n INTERO POSITIVO

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

CONDIZIONE: VOGLIAMO TANTO k MULTIPLO DI $\varphi(3^n) = 2 \cdot 3^{n-1}$

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



$3 \nmid 2 - 1$!

NOTIAMO CHE:

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

$$k = 2j$$

$$2^{2j} \equiv 1 \pmod{3^n} \rightarrow 4^j \equiv 1 \pmod{3^n}$$

$$v_3(4^j - 1) = v_3(4-1) + v_3(j)$$

$$v_3(4^j - 1) \geq n \quad \Leftarrow \quad 3^n \mid 4^j - 1$$

$$2^{k''} - 1$$

$$v_3(4-1) = 1$$

$v_3(J) \geq n-1 \longrightarrow 3^{n-1} \mid J$

$2 \cdot 3^{n-1} \mid K$

$2^K \equiv 1 \pmod{3^n} \longrightarrow 2 \cdot 3^{n-1} \mid K$

$ord_{3^n}(2) \mid \varphi(3^n)$ MA $\varphi(3^n) \mid ord_{3^n}(2)$

QUINDI $ord_{3^n}(2) = \varphi(3^n)$

ESISTENZA DI UN GENERATORE

DEFINIAMO I POLINOMI CICLOTOMICI.

I POLINOMI CICLOTOMICI SONO I COMPONENTI IRRIDUCIBILI (NON VEDREMO QUESTO) DEGLI $X^n - 1$

n	$x^n - 1$	Scomposizione
1	$x-1$	$(x-1)$
2	x^2-1	$(x-1)(x+1)$
3	x^3-1	$(x-1)(x^2+x+1)$
4	x^4-1	$(x-1)(x+1)(x^2+1)$
5	x^5-1	$(x-1)(x^4+x^3+x^2+x+1)$
6	x^6-1	$(x-1)(x+1)(x^2+x+1)(x^2-x+1)$
7	x^7-1	$(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$
8	x^8-1	$(x-1)(x+1)(x^2+1)(x^4+1)$
9	x^9-1	$(x-1)(x^2+x+1)(x^6+x^3+1)$
10	$x^{10}-1$	$(x-1)(x+1)(x^4+x^3-x^2+x+1)(x^4-x^3+x^2-x+1)$

QUINDI QUESTO CI CONSENTE DI

DEFINIRE:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d \mid n} \Phi_d(x)}$$

↳ n-ESIMO CICLOTOMICO

L'IDEA È AVERE

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

CI SONO DEI GROSSI PROBLEMI:

① È UNA BUONA DEFINIZIONE? IL QUOZIENTE È UN POLINOMIO?

② È A COEFFICIENTI INTERI?

COSA SAPPIAMO BENE DI $x^n - 1$? LE RADICI.

UN CRITERIO PER CAPIRE QUANDO

$$\frac{p(x)}{q(x)}$$

È INTERO (COME POLINOMIO)?

LE RADICI DI q SONO TRA LE RADICI DI p (CON MOLTEPLICITÀ).

1 $x - 1$

2 $x + 1$

3 $x^2 + x + 1$

4 $x^2 + 1$

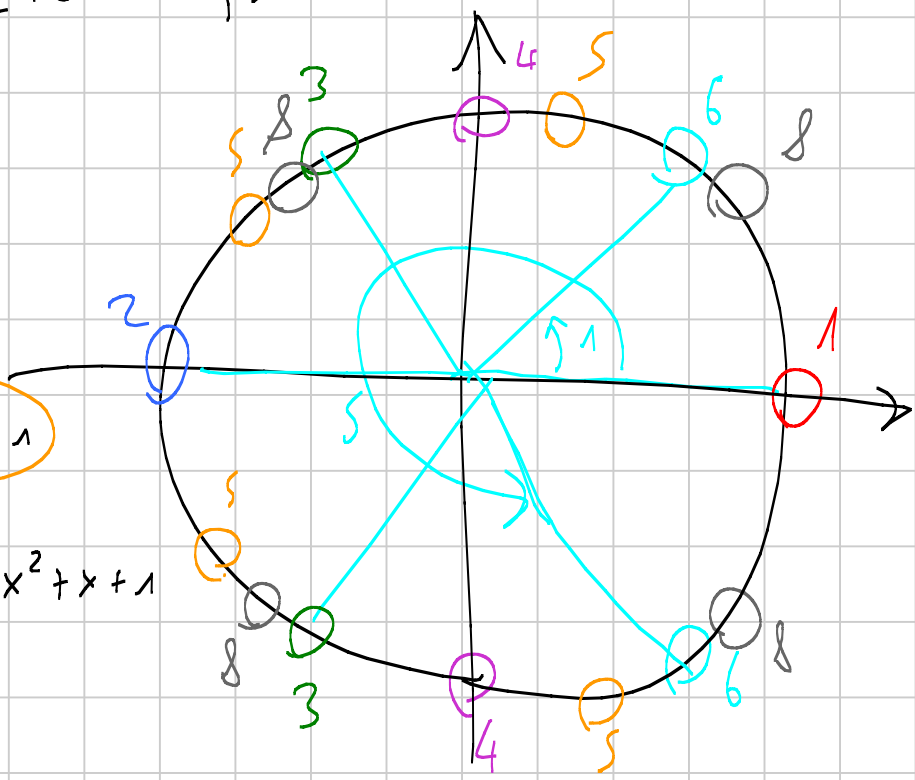
5 $x^4 + x^3 + x^2 + x + 1$

6 $x^2 - x + 1$

7 $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

8 $x^4 + 1$

9 $x^6 + x^3 + 1$



NOI SAPPIAMO (SPERIAMO) CHE LE RADICI DI $\prod_{d \mid n} \Phi_d(x)$ SONO LE RADICI n-ESIME DELL'UNITÀ.

SE LE RADICI DI $\Phi_n(x)$ FOSSERO

ESATTAMENTE QUELLE DELLA FORMA $\omega^d - 1$

CON ω RADICE PRIMITIVA (PIÙ A DESTRA)

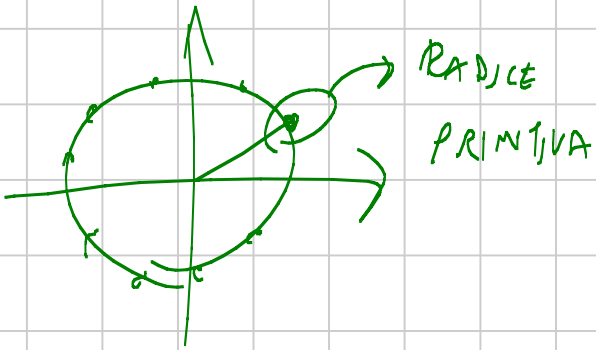
DI $x^n - 1$ E $(d, n) = 1$ SAREMMO FELICI

DIMOSTRIAMOLO PER INDUZIONE: (DEFINITI ATTRAVERSO ☆)

SUPPONIAMO PER IPOTESI INDUTTIVA CHE:

$\Phi_d(x)$ SIA UN POLINOMIO MONICO A COEFFICIENTI INTERI CON RADICI ω^j DOVE $(j, d) = 1$

E ω È LA RADICE PRIMITIVA DI $x^\phi - 1$



PASSO BASE:

$n = 1 \rightarrow X - 1$ HA SOLO 1 COME RADICE

$n = 2 \rightarrow X + 1$ HA SOLO -1 COME RADICE, PERCHÉ -1 È LA RADICE PRIMITIVA DI $X^2 - 1$

E LE RADICI SONO $(-1)^k$ CON $(k,2)=1$.

PASSO INDUTTIVO

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d<n}} \Phi_d(x)}$$

COSA VOGLIAMO FORTEMENTE? VORREMMO CHE OGNI RADICE DI $\prod_{\substack{d \mid n \\ d<n}} \Phi_d(x)$ FOSSE RADICE DI $x^n - 1$

QUESTO È VERO PERCHÉ:

$$x^d - 1 = \prod_{\tilde{d} \mid d} \Phi_{\tilde{d}}(x) \to \Phi_d(x) \mid x^d - 1$$

E $x^d - 1 \mid x^n - 1$, QUINDI $\Phi_d(x) \mid x^n - 1$, PERCIÒ LE RADICI DI $\Phi_d(x)$ SONO IN $x^n - 1$

MANCA QUALCOSA? ALCUNE RADICI POTREBBERO COMPARIRE PIÙ VOLTE.

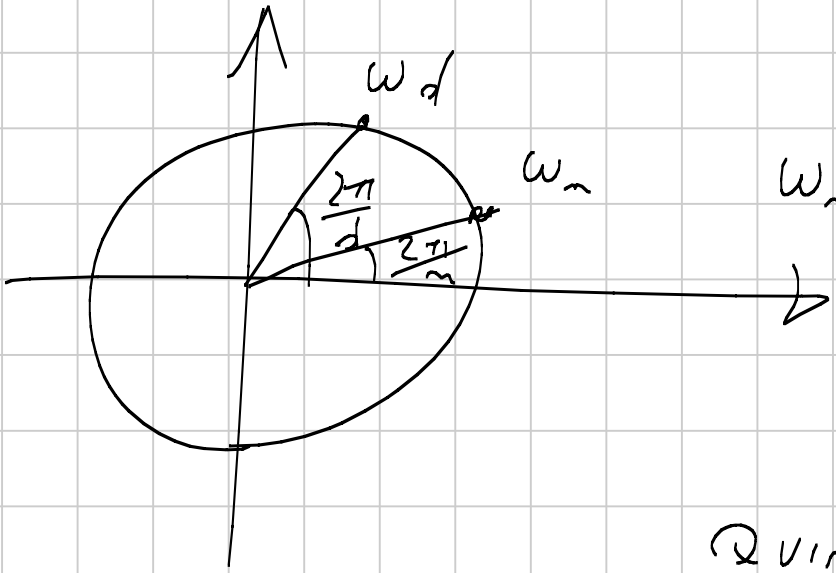
$$\frac{X^n - 1}{\prod_{\substack{d \mid n \\ d < n}} \Phi_d(X)}$$

LE RADICI DI $\Phi_d(X)$ SONO DELLA FORMA

$$\omega_d^t \quad \text{con} \quad (t,d) = 1$$

E ω_d RADICE PRIMITIVA DI $X^d - 1$

REL. FONDAMENTALE $\quad \omega_d = \omega_n^{\left(\frac{n}{d}\right)}$ → INTERO



$\omega_n^{(n/d)}$ FORMA UN ANGOLO DI

$$\frac{2\pi}{n} \cdot \frac{n}{d} = \frac{2\pi}{d},$$

QUINDI È ω_d

SE LE RADICI DI $\Phi_d(X)$ SONO

$$\omega_d^t \quad \text{con} \quad (t,d) = 1,$$

COME POSSIAMO ESPRIMERLE IN FUNZIONE DI ω_n?

$$\omega_n^{t \cdot \frac{n}{d}} \quad \text{con} \quad (t,d) = 1$$

CON d FISSATO, CHI SONO LE $\omega_n^{t \cdot \frac{n}{d}}$ CON $(t,d)=1$

ω_n^K → CARATTERIZZIAMOLO $= t \cdot \frac{n}{d}$

BUONA DEF.

$t \to t+d$

$\omega_n^K \to \omega_n^{K+n}$

$$\left(t \cdot \frac{n}{d}, n\right) = \frac{n}{d}$$

$$\to \quad \frac{n}{d} \mid t \cdot \frac{n}{d} \qquad \frac{n}{d} \mid n$$

$\leftarrow$ $(t,d)=1$ $\exists$ a, b t.c.

$$at - bd = 1$$

$$a \cdot t \cdot \frac{n}{d} - bd \cdot \frac{n}{d} = \frac{n}{d}$$

$$a \cdot \left(t \cdot \frac{n}{d}\right) - b \cdot n = \frac{n}{d}$$

SONO TUTTI?

SE $(K,n) = \frac{n}{d}$ $\to$ $K = J \cdot \frac{n}{d}$

$(j,d) \overset{?}{=} 1$

$$\left(\frac{k}{(n/d)}, \frac{n}{(n/d)}\right) =$$

PROP.

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1 \iff (j,d) = 1$$

ALTRO MODO: COMBINAZIONI LINEARI

SE $(k,n) = \frac{n}{d}$ → k È DELLA FORMA

$$j \cdot \frac{n}{d} \quad \text{con } (j,d) = 1$$

QUINDI LE $\omega_n^k = \omega_n^{j \cdot \frac{n}{d}}$ con $(j,d) = 1$

SONO ESATTAMENTE QUELLE CON $(k,n) = \frac{n}{d}$

$x^n - 1$ → NON HA RADICI DOPPIE PERCHÉ NE CONOSCIAMO GIÀ n DISTINTE

→ TUTTE QUELLE DEL TIPO ω_n^s

$\Phi_d(x)$ → TUTTE QUELLE DEL TIPO ω_n^s CON $(s,n) = \frac{n}{d}$

$d \mid n$

$d < n$

NON HA RADICI PER IPOTESI INDUTTIVE

CI SONO 2 MODI DI AVERE RADICI DOPPIE:

① $\Phi_d(x)$ HA RADICI DOPPIE (MA NON È VERO PER IP. INDUTTIVA: ABBIAMO ESATTAMENTE ω_d^k CON $(k,d)=1$) [OPPURE FAI IL CONTO]

② $\Phi_d(x)$ E $\Phi_J(x)$ HANNO UNA RADICE IN COMUNE CON $d \neq J$

ω_n^k CON $(k,n)=\frac{n}{d}$

ω_n^J CON $(J,n)=\frac{n}{J}$

SI VEDE GEOMETRICAMENTE, MA SE $\omega_n^J=\omega_n^k$ ALLORA $(k,n)=(J,n)$.

$$\Phi_n(x)=\frac{x^n-1}{\prod_{\substack{d\mid n\\ d<n}}\Phi_d(x)}$$

È MONICO E A COEFFICIENTI INTERI

NON HA RADICI DOPPIE E LE SUE RADICI SONO RADICI DI x^n-1

POLINOMIO MONICO A COEFFICIENTI INTERI

$$\overline{\Phi}_n(x) = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d < n}} \overline{\Phi}_d(x)} =$$

$$= \frac{\prod_{i=0}^{n-1} (x - \omega_n^i)}{\prod_{\substack{d \mid n \\ d < n}} \left(\prod_{(k,n)=\frac{n}{d}} (x - \omega_n^k) \right)}$$

$\overline{\Phi}_d(x)$

VISTO CHE d VARIA TRA I DIVISORI DI n DIVERSI DA n E (k,n) PUÒ ASSUMERE SOLO I VALORI CHE DIVIDONO n

$$\prod_{(k,n)\neq 1} (x - \omega_n^k)$$

$$\longrightarrow \frac{\prod_{(k,n) \text{ QUALSIASI}} (x - \omega_n^k)}{\prod_{(k,n)\neq 1} (x - \omega_n^k)}$$

$$\overline{\Phi}_n(x) = \prod_{(k,n)=1} (x - \omega_n^k)$$

□

Teorema

Ogni campo finito ammette un generatore.

Ricordiamo che:

posto $n = |K| - 1$

$$x^n - 1 = \prod_{z \neq 0} (x - z)$$

$$\prod_{d|n} \Phi_d(x)$$

$\Phi_d(x)$ è a coefficienti interi

E $\mathbb{Z}$ è mappabile in ogni campo:

perché $1 \in K$ e

ogni n si può mappare in $\underbrace{1+1+\dots+1}_{n \text{ volte}}$

È chiaro come un polinomio a coefficienti interi vada visto in $\mathbb{Z}_p$.

CONTIAMO QUANTI SONO GLI ELEMENTI DI ORDINE d.

d DIVIDE n

QUINDI:

$(X-1)$

ELEMENTI DI ORDINE 1 $\longrightarrow$ 1

ELEMENTI DI ORDINE 2 $\longrightarrow$ -1 $(X+1)$

ELEMENTI DI ORDINE 3 $\longrightarrow$ 2 ω, ω^2 (X^2+X+1)

RADICI DI X^3-1 CHE NON SONO RADICI DI $X-1$

(GLI ELEMENTI DI ORDINE 3 DI $\mathbb{H}_5$ QUANTI SONO?) ZERO! $3 \nmid 4$

L'ORDINE È SEMPRE DIVISORE DI $n = |K|-1$.

GLI ELEMENTI DI ORDINE 1 SONO LE RADICI DI $x-1$.

SE m DIVIDE n, GLI ELEMENTI DI ORDINE d t.c. $d \mid m$ SONO LE RADICI DI: (TUTTI GLI ELEMENTI IL CUI ORDINE DIVIDE m)

$x^m - 1$ (LE CUI RADICI SONO ESATTAMENTE QUELLE CON ORDINE DIVISORE DI m)

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

$\hookrightarrow$ n RADICI DISTINTE

ANCHE $x^m - 1$ HA m RADICI DISTINTE

(PERCHÉ $x-z$ È IRRIDUCIBILE)

$\leftarrow$ SE $\mathrm{ord}_{K^*}(z) \mid m \rightarrow z^m = 1$

E SONO PROPRIO m!

COSA ABBIAMO:

$$\prod_{\mathrm{ord}_{/K}(z)\,|\,m} (x - z) = x^m - 1$$

$\forall\, m \mid n$

CRUCIALE, SENNÒ $x^m - 1$ NON SI SCOMPORREBBE COME $\prod (x-z)$

POI HO $p_d(x) = \prod_{\mathrm{ord}_{/K}(z)=d} (x - z)$

$$\prod_{d\,|\,m} p_d(x) = x^m - 1 \qquad \forall\, m \mid n$$

QUINDI $p_d(x) = \overline{\Phi}_d(x)$ visto su $/K$

$\overline{\Phi}_d(x)$ HA LE RADICI CHE SONO ESATTAMENTE QUELLE CHE HANNO ORDINE d E SONO

$\left(\overline{\Phi}_d(x) \mid x^n - 1\right)$ (n RADICI DISTINTE)

$\deg(\overline{\Phi}_d) \; (= \varphi(d))$

Φ_d HA GRADO $\varphi(d)$ PERCHÉ LE SUE RADICI (IN $\mathbb{C}$) SONO:

$$\omega_d^k \quad \text{con} \quad (k,d)=1$$

$\longrightarrow$ SONO $\varphi(d)$

IN $\mathbb{C}$ ABBIAMO VISTO IL GRADO DI Φ_d

IN $\mathbb{K}$ Φ_d PASSA PERCHÉ A COEFFICIENTI INTERI E LE RELAZIONI SULLE RADICI (TRAMITE DECOMPONIBILITÀ) DERIVANO DALLA RELAZIONE

$$\Phi_d(x) \mid x^n - 1 = \prod_{z^n=1} (x-z)$$

VALE COMUNQUE $\prod_{d|n} \Phi_d(x) = x^n - 1$ PERCHÉ VALE SU $\mathbb{Z}[x]$

I.E.: MOD 3+

$$(x^2-3)(x^2+1) \qquad (x^2+1)^2 \quad (3+)$$

$$x^4 - 35x^2 - 36 \qquad (3-)$$

IN OGNI CAMPO $\underbrace{(1+1+\dots+1)}_{n \text{ VOLTE}} \underbrace{(1+1+\dots+1)}_{m \text{ VOLTE}} =$

$\underbrace{1+1+\dots+1}_{m \cdot n}$ VOLTE.

TORNANDO A PRIME, $\Phi_n(x)$ SU K HA $\varphi(n)$ RADICI.

MA $\Phi_n(x) = \prod_{\mathrm{ord}_K(z)=n} (x-z)$.

QUINDI CI SONO $\varphi(n)$ ELEMENTI DI K DI ORDINE n E OGNUNO DI LORO È UN GENERATORE.

LEMMA

SIA $\mathbb{K}$ UN CAMPO FINITO E SIA $n = |\mathbb{K}| - 1$, $s > 0$

ALLORA $\sum_{z \neq 0} z^s = 0 \iff n \nmid s$

PRENDIAMO UN GENERATORE g.

$$\sum_{z \neq 0} z^s = \sum_{i=0}^{n-1} (g^i)^s = \sum_{i=0}^{n-1} (g^s)^i = (*)$$

$$(*) = \frac{g^{sn} - 1}{g^s - 1}$$

$g^s \neq 1$

CASO 1: $g^s = 1 \iff n \mid s$

g HA $\mathrm{ORD}_{\mathbb{K}} = n$

IN QUESTO CASO $\sum_{i=0}^{n-1} (g^s)^i = n.$

IL PROBLEMA È CHE n INTERO PUÒ ESSERE $0 = \underbrace{1 + 1 + \dots + 1}_{n \text{ VOLTE}}$ NEL CAMPO

(INTERROGATEVI SULLA QUESTIONE)

COMUNQUE FA SEMPRE -1 ☆

CASO 2: $g^s \neq 1$

$$\frac{g^{sn}-1}{g^s-1} = \frac{1-1}{g^s-1} = 0$$

☆ PER I VOLENTEROSI, PER DIMOSTRARE UNA COSA SI PUÒ DIMOSTRARE:

- $\exists\, p$ PRIMO t.c. $\underbrace{1+1+\dots+1}_{p \text{ volte}} = 0 \ (|K|)$;
- $p \mid |K|$ PERCHÉ ESISTONO DELLE CLASSI DI PARTIZIONE DI K IN p ELEMENTI

(TROVATELE)

RESIDUI QUADRATICI

Su $\mathbb{Z}_p$.

INDICHIAMO CON $\left(\frac{a}{p}\right)$

- 0 SE $a \equiv 0$
- 1 SE $\exists\, t \not\equiv 0$ (p) t.c. $t^2 \equiv a$ (p)
- -1 ALTRIMENTI

a È R.Q. $\leftrightarrow \left(\frac{a}{p}\right) = 1$ o 0

---

p DISPARI

CRITERIO DI EULERO:

$$a^{\frac{p-1}{2}} \begin{cases} 1 & \text{SE } \left(\frac{a}{p}\right) = 1 \\ 0 & \text{SE } \left(\frac{a}{p}\right) = 0 \\ -1 & \text{SE } \left(\frac{a}{p}\right) = -1 \end{cases}$$

CASO $a \equiv 0$: $\left(\frac{a}{p}\right) = 0 \leftrightarrow a^{\frac{p-1}{2}} \equiv 0$ (p)

$\updownarrow$ $\qquad \updownarrow$

$a \equiv 0$ (p)

① GENERATORI (CONTO LESTISSIMO)

② POLINOMI:

$X^{p-1} - 1$ HA $p-1$ RADICI DISTINTE MODULO p

$$\downarrow$$

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

OGNI RESIDUO O È RADICE O DELL'ALTRO

$\frac{p-1}{2}$ RADICI DIST. MOD p

$\frac{p-1}{2}$ RADICI DIST. MOD p

SE a È RESIDUO QUADRATICO:

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

$\longrightarrow$ TUTTI I R.Q. STANNO TRA LE RADICI DI $X^{\frac{p-1}{2}} - 1$

SE I R.Q. FOSSERO $\frac{p-1}{2}$ E TUTTI CONTENUTI IN $X^{\frac{p-1}{2}} - 1$, ALLORA LE RADICI DI $X^{\frac{p-1}{2}} - 1$ SAREBBERO ESATTAMENTE I R.Q.

I R. Q. $\neq 0$ sono $\frac{p-1}{2}$.

MAPPA: $\{1, \dots, p-1\} \to \{1, \dots, p-1\}$

$x \ (p) \to x^2 \ (p)$

QUANDO $x^2 \equiv y^2 \ (p)$

$(x+y)(x-y) \equiv 0 \ (p)$ $\nearrow$ $x \equiv y \ (p)$

$\searrow$ $x \equiv -y \ (p)$

CIOÈ: (I.E. 13)

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓
1	4	−4	3	−1	−3
↑	↑	↑	↑	↑	↑
12	11	10	9	8	7

QUINDI SONO $\frac{p-1}{2}$: $x^2 \equiv y^2 \ (p) \iff x \equiv \pm y \ (p)$

(ANCHE PERCHÉ QUINDI

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

LEMMA DI GAUSS

SE $a \in \mathbb{Z}^{(p)}$ È UN INTERO MODULO p, CONSIDERIAMO I NUMERI:

VISTI MODULO p

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

(TUTTI TRA 1 E $p-1$)

E SIA $S = \left\{ i \mid [ia]_p > \frac{p}{2} \right\}$

T.E.: $p = 13$ $\quad a = 3$ $\quad \left(\frac{3}{13}\right) = 1$

3	6	9	12	15 ↓ 2	5

$$S = \{3, 4\}$$

Th. $\left(\frac{a}{p}\right) = (-1)^{|S|}$

a R.Q. $\Leftrightarrow$ $|S|$ PARI

CONSIDERIAMO:

$$a,\ 2a,\ 3a,\ \dots,\ \left(\frac{p-1}{2}\right)a$$

$$\forall x \in \mathbb{Z}_p \quad \exists!\ i \le \frac{p-1}{2} \text{ t.c. } ia \equiv \pm x \ (p)$$

$a, 2a, \dots, (p-1)a$ È UNA PERMUTAZIONE DI $\mathbb{Z}_p \setminus \{0\}$

SE MI FERMO A $\left(\frac{p-1}{2}\right)$:

TRA a E $(p-1)a$ NE PRENDO UNO;

TRA $2a$ E $(p-2)a$ NE PRENDO UNO;

...

HO UNA PERMUTAZIONE DA CUI TOLGO UN ELEMENTO PER OGNI COPPIA DI OPPOSTI.

$$\prod_{i=1}^{\frac{p-1}{2}} (a\,i) \equiv \prod_{i=1}^{\frac{p-1}{2}} (a\,i) \cdot \prod_{i=1}^{\frac{p-1}{2}} (a\,i) \equiv$$

$(a\,i)_p < \frac{p}{2}$ $\qquad$ $(a\,i)_p > \frac{p}{2}$

$$\equiv \prod_{i=1}^{\frac{p-1}{2}} (a\,i) \cdot \prod_{i=1}^{\frac{p-1}{2}} (p - a\,i) \cdot (-1) \equiv$$

$|S|$ VOLTE

$(a\,i)_p < \frac{p}{2}$ $\qquad$ $(a\,i)_p > \frac{p}{2}$] S È L'INSIEME DEGLI i CON QUESTA PROPRIETÀ

$$\equiv (-1)^{|S|} \cdot \prod_{i=1}^{\frac{p-1}{2}} (a\,i) \cdot \prod_{i=1}^{\frac{p-1}{2}} (p - a\,i)$$

$(a\,i)_p < \frac{p}{2}$ $\qquad$ $(a\,i)_p > \frac{p}{2}$

$< \frac{p}{2}$ $\qquad$ $\frac{p}{2}$

IN TOTALE I TERMINI SONO $\frac{p-1}{2}$: GLI DA 1 A $\frac{p-1}{2}$ O STANNO A SX O DX

GLI ELEMENTI SONO TUTTI DIVERSI:

$a\,i \equiv \pm X_i(p)$ MA GLI X_i SONO TUTTI DIVERSI

ABBIAMO VISTO PRIMA CHE

$\pm a, \pm 2a, \dots, \pm\left(\frac{p-1}{2}\right)a$

ERANO TUTTI DIVERSI, PERCIÒ

ANCHE GLI a_i E I $(p-a_i)$ SONO

TUTTI DIVERSI

ABBIAMO $\frac{p-1}{2}$ TERMINI $< \frac{p}{2}$ DIVERSI TRA

LORO: IL PRODOTTO FA $\left(\frac{p-1}{2}\right)!$

$$\prod_{i=1}^{\frac{p-1}{2}} (a_i) \equiv (-1)^{|S|} \cdot \left(\frac{p-1}{2}\right)! \quad (p)$$

$$\| \qquad \| \qquad \| \qquad \| \qquad \| \qquad \| \qquad \| \qquad \|$$

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

$$a^{\frac{p-1}{2}} \equiv (-1)^{|S|} \quad (p) \rightarrow \left(\frac{a}{p}\right) = (-1)^{|S|}$$

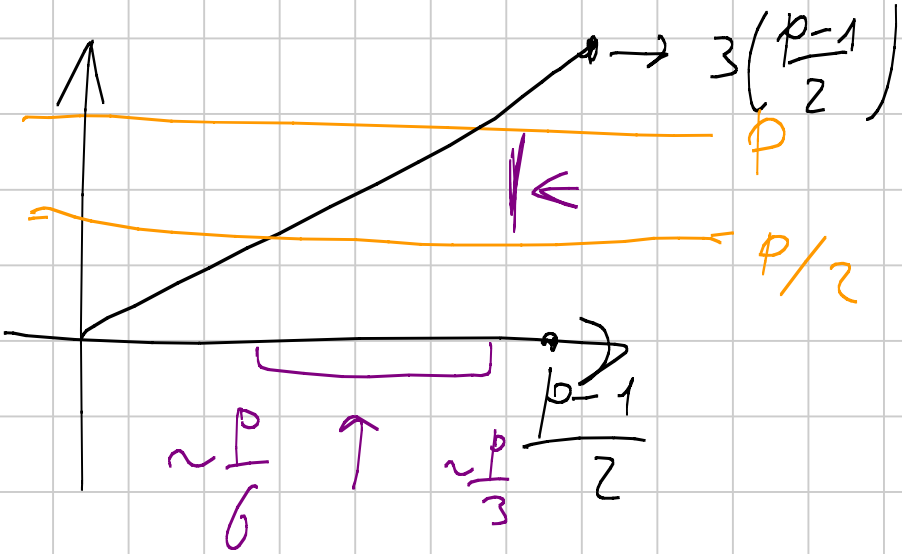
QUANDO $\left(\frac{3}{p}\right) = 1$?

(COMUNQUE A CASA PROVATE CON $\left(\frac{-3}{p}\right)$, VIENE UGUALE (COME METODO)

GUARDIAMO:

$3, 6, \dots, 3\left(\frac{p-1}{2}\right)$

QUALI SARANNO (mod p) IN $\left(\frac{p}{2}, p\right)$?



QUANDO $\frac{p}{2} < 3 \iff < p$ E IN REALTÀ BASTA,

PERCHÉ $\left(\frac{p-1}{2}\right) - 3 < p + \frac{p}{2}$

PERCIÒ ABBIAMO: $\frac{p}{6} < i < \frac{p}{3}$ QUINDI

$$|S| = \left\lfloor \frac{p}{3} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor \quad \forall p > 3$$

QUAL È IL MINIMO R T.C.:

$$\left\lfloor \frac{p+R}{3} \right\rfloor - \left\lfloor \frac{p+R}{6} \right\rfloor \equiv \left\lfloor \frac{p}{3} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor \ (2)$$

12! (FORSE)

$$\left\lfloor \frac{p+12}{3} \right\rfloor \equiv \left\lfloor \frac{p}{3} \right\rfloor \ (2)$$

$$\left\lfloor \frac{p}{3} \right\rfloor + 4 \qquad \left\lfloor \frac{p+12}{6} \right\rfloor \equiv \left\lfloor \frac{p}{6} \right\rfloor \ (2)$$

$\lfloor x+1 \rfloor = \lfloor x \rfloor + 1$

$$\left\lfloor \frac{p}{6} \right\rfloor + 2$$

PROVIAMO $p = 12K + J$

$\varphi(12)$

J: 1, 5, 7, 11

$$|S| = \left\lfloor \frac{12K+J}{3} \right\rfloor - \left\lfloor \frac{12K+J}{6} \right\rfloor =$$

$$= \left\lfloor \frac{J}{3} \right\rfloor - \left\lfloor \frac{J}{6} \right\rfloor \ (2)$$

$p \equiv 1 (12)$ $\quad 0-0 \quad \rightarrow \quad \left(\frac{3}{p}\right) = 1$

$p \equiv 5 (12)$ $\quad 1-0 \quad \rightarrow \quad \left(\frac{3}{p}\right) = -1$

$p \equiv 7 (12)$ $\quad 2-1 \quad \rightarrow \quad \left(\frac{3}{p}\right) = -1$

$p \equiv 11 (12)$ $\quad 3-1 \quad \rightarrow \quad \left(\frac{3}{p}\right) = 1$

Es. 1 $\quad \forall p > 1000 \quad \forall r \in \mathbb{Z}$

$\exists x, y$ t.c. $x^2 \equiv y^3 + r \ (p)$

Es. 2 $\quad \forall a > 1$

$\exists \infty \ q$ t.c. $v_2(a^{q-1} - 1)$ è DISPARI

---

① $\quad (y^3 + r)^{\frac{p-1}{2}}$ VORREMMO FOSSE 1 o o

PER ASSURDO: $\quad (y^3 + r)^{\frac{p-1}{2}} \equiv -1 \ (p) \quad \forall x \in \mathbb{Z}_p$

$$\sum_{x=0}^{p-1} \left(x^3 + k \right)^{\frac{p-1}{2}} \equiv 0 \pmod{p}$$

IDEA STANDARD SE UNO L'HA VISTA

BELLA PERCHÉ SAPPIAMO QUANTO FA $\sum x_i$

IN GENERALE SOMMARE SU TUTTE LE CASI DI RESTO NON È UNA BUONA IDEA

$$\sum_{x=0}^{p-1} \left(x^3 + k \right)^{\frac{p-1}{2}} = \sum_{y=0}^{p-1} \left(\sum_{i=0}^{\frac{p-1}{2}} y^{3i} \cdot k^{\left(\frac{p-1}{2} - i\right)} \cdot \binom{\frac{p-1}{2}}{i} \right) =$$

$$= \sum_{i=0}^{\frac{p-1}{2}} \left(\sum_{y=0}^{p-1} y^{3i} \cdot k^{\left(\frac{p-1}{2} - i\right)} \cdot \binom{\frac{p-1}{2}}{i} \right) =$$

PROBLEMA: $y=0$, $i=0$, $y^i = ?$

SE $y=0$ NELLO SVILUPPO $0^0 = 1$

$$\left(\sum_{i=0}^{\frac{p-1}{2}} k^{\left(\frac{p-1}{2} - i\right)} \cdot \binom{\frac{p-1}{2}}{i} \left(\sum_{y=0}^{p-1} y^{3i} \right) \right)$$

$(p) \to 0$

$i=0 \to 0$

i VARIA TRA 0 E $\frac{p-1}{2}$

SE $p-1 \nmid 3i \to 0$

SE NON È MULTIPLO DI $p-1$, VIENE 0

$p-1 \mid 3i, \quad 0 \le i \le \frac{p-1}{2}$

$i = 0$

$i = \frac{p-1}{3}$

QUINDI RESTA SOLO $i = \frac{p-1}{3}$

i DIVENTA SOLO $\frac{p-1}{3}$

SE $p \equiv 2 (3) \rightarrow 0$ (i NON C'È)

SE $p \equiv 1 (3)$

$$k^{\left(\frac{p-1}{6}\right)} \cdot \left(\frac{p-1}{2} \atop \frac{p-1}{3}\right) \cdot (-1) \equiv 0 \ (p) \qquad \left(\frac{p}{p}\right) \equiv 0 \ (p)$$

$\Downarrow$

$V \equiv 0 \ (p)$ ✓

$y^2 \equiv x^3 + 0 \ (p)$

$\downarrow$

$(1, 1)$

SE $p \equiv 2 \ (3)$?

$$y^2 \equiv x^3 + k \ (p)$$

$$y^2 - k \equiv x^3 \ (p)$$

↳ ASSUME TUTTI I VALORI

SE $p \equiv 2 \ (3)$, QUALI SONO I RESIDUI CUBICI?

SONO TUTTI, PERCHÉ IL NUMERO DI RESIDUI d-ESIMI È $\frac{p-1}{(p-1, d)}$

[DIMOSTRAZIONE]

$$x \equiv x^{2p-1} \ (p) \equiv \left(x^{\frac{2p-1}{3}}\right)^3 \ (p)$$

SE $(d, p-1) = 1$

$$x \equiv x^{(p-1)k+1} \equiv \left(x^{\frac{(p-1)k+1}{d}}\right)^d \ (p)$$

E SCELGO $(-)k$ INVERSO DI $(p-1)$ MODULO d