Teoria dei Numeri - 1

Note Title 04/02/2023

POLINOMI CICLOTOMICI

Def: $z \in \mathbb{C}$ è detto radice n-esima di 1 se per $n \in \mathbb{N}$ $z^n = 1$.

Def: z radice n-esima di 1 è detta primitiva se $z^n = 1$ e $z^k \neq 1$ $\forall k < n$.

OSS: $e^{\frac{2\pi i k}{n}}$ sono le radici n-esime.

Se $(k, n) = 1$ allora la radice è primitiva.

Def: L'n-esimo polinomio ciclotomico è il polinomio monico le cui radici sono tutte e sole le radici primitive (n-esime) di 1.

Ovvero $$\Phi_n(x) = \prod_{\substack{0 < k < n \\ (k,n)=1}} (x - e^{\frac{2\pi i k}{n}})$$

PROP:

- $\Phi_n(x) \in \mathbb{Z}[x]$
- $\Phi_n(x) \mid x^n - 1$ perché $x^n - 1$ ha tutte le radici di Φ_n.

ES: • $\Phi_1(x) = x - 1$ • $\Phi_2(x) = x + 1$

• $\Phi_3(x) = x^2 + x + 1 = \frac{x^3 - 1}{x - 1}$

• Se p è primo $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 =$

$= \frac{x^p - 1}{x - 1}$

OSS: $\deg \Phi_n(x) = \varphi(n)$

PROP: $\prod_{d|n} \Phi_d(x) = x^n - 1$

Infatti gli insiemi delle radici sono uguali

$$\bigcup_{d|n} \{ z \in \mathbb{C} \mid z \text{ è rad. prim. } d\text{-esima di } 1 \} = \{ z \in \mathbb{C} \mid z \text{ è radice } n\text{-esima di } 1 \}$$

GENERATORI MOD p^n

TEOREMA: $\forall$ p primo $\exists$ g generatore mod p,

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

DIM: $\forall n \quad \text{ord}_p(n) \mid p - 1$

$\mathbb{F}_p = \{ \text{classi di resto mod } p \} = \{ 0, 1, \dots, p-1 \pmod p \}$

$$\mathbb{F}_p \setminus \{0\} = \bigcup_{d \mid p-1} \{ n \in \mathbb{F}_p \mid \mathrm{ord}_p(n) = d \}$$

questa è un'unione disgiunta

G_d = numero di elementi di ordine d =

$$= |\{ n \in \mathbb{F}_p \mid \mathrm{ord}_p(n) = d \}|$$

$$\rightarrow \quad p-1 = \sum_{d \mid n} G_d$$

Se $\mathrm{ord}_p(n) = d \rightsquigarrow n^d - 1 \equiv 0 \ (p)$

In $\mathbb{F}_p$ il numero di radici di un polinomio è al più il grado del polinomio.

$\Longrightarrow$ Ci sono al più d elementi di ord. d.

$$x^d - 1 = \prod_{k \mid d} \Phi_k(x)$$

$\Phi_k(x) \mid x^k - 1$, se $k \neq d$ allora le radici di $\Phi_k(x)$ NON hanno ordine d (ma più piccolo)

Se n ha ordine d allora è radice di $x^d - 1$ ma non di $\Phi_k(x)$ per $k \mid d$ $k < d$, allora n è radice di $\Phi_d(x)$.

$$G_d \leq \deg \Phi_d = \varphi(d)$$

$$\Rightarrow \quad p-1 = \sum_{d \mid p-1} G_d \leq \sum_{d \mid p-1} \varphi(d) = p-1$$

↑ ESERCIZIO

$$\Longrightarrow \quad G_d = \varphi(d) \quad \Rightarrow \quad G_{p-1} = \varphi(p-1) > 0$$

$\Rightarrow$ esiste un elemento di ordine $p-1$!

TEOREMA: Dato p primo $\forall n \in \mathbb{N}$ $\exists g$ t.c. $\operatorname{ord}_{p^n}(g) = \varphi(p^n)$,

ovvero g è generatore mod p^n.

LEMMA: Dato p primo e $s \in \mathbb{N}$

$$(1+kp)^{p^s} \equiv 1 + kp^{s+1} \ (p^{s+2})$$

DIM: PASSO BASE: $s = 0$

$$1 + kp \equiv 1 + kp \ (p^2) \qquad \text{ok } \checkmark$$

PASSO INDUTTIVO: vogliamo $(1+kp)^{p^{s+1}} \equiv 1 + kp^{s+2} \ (p^{s+3})$

$$(1+kp)^{p^{s+1}} = \left((1+kp)^{p^s}\right)^p \equiv \left(1 + kp^{s+1} + hp^{s+2}\right)^p \pmod{p^{s+3}}$$

$$\equiv \left(1 + p^{s+1}(k+ph)\right)^p \equiv 1 + kp^{s+2} \qquad (p^{s+3})$$

$$\sum_{i=0}^{p} \binom{p}{i} \cdot p^{(s+1)i} \cdot (k+ph)^i$$

$\square$

Sappiamo che per $p^n = p$ c'è un generatore

Se $g \bmod p^n$ è un generatore mod p

$$p-1 \mid \operatorname{ord}_{p^n}(g) \mid (p-1)p^{n-1}$$

Vogliamo trovare g t.c. $g^{(p-1)p^{n-2}} \not\equiv 1 \ (p^n)$

$$g^{p-1} \equiv 1 \ (p) \implies g^{p-1} = 1 + kp$$

Vediamo $n=2$: Se $p \nmid k$ allora

g è un generatore

Se $p \mid k$ basta prendere $g+p$ e

ho un generatore

Usando il lemma, per n generico,

$$g^{p-1} = 1 + kp \qquad \text{con } k \not\equiv 0 \ (p)$$

$$(1+kp)^{p^{n-2}} \equiv 1 + kp^{n-1} \ (p^n)$$

$$\implies g^{(p-1)p^{n-2}} \not\equiv 1 \ (p^n), \text{ che è quello}$$

che volevamo.

Supponiamo che $g^{(p-1)p^k} \equiv 1 \ (p^n)$ per $k < n-2$,

allora $\left(g^{(p-1)p^k}\right)^{p^{n-2-k}} \equiv g^{(p-1)p^{n-2}}$

$$\equiv (1)^{p^{n-2-k}} \equiv 1$$

FATTO: Non tutti gli n ammettono un generatore mod n, vale solo per tutti quelli nella forma:

$$2,\ 4,\ p^n,\ 2p^n$$

LIFTING THE EXPONENT (LTE)

TEOREMA: p primo $p \neq 2$, $v_p(n)$ = il più grande k tale che $p^k \mid n$ ($p^k \| n$), allora dati $x, y \not\equiv 0 \pmod p$ $\quad p \mid x-y$, vale

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

valutazione p-adica

DIM: Posso assumere n primo, infatti se così non fosse potrei scrivere

$n = q \cdot m$, con q primo, e avrei

$$x^n - y^n = (x^m)^q - (y^m)^q$$

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

$v_p(a \cdot b) = v_p(a) + v_p(b)$

e induttivamente otterrei $\quad v_p(x-y) + v_p(m) + v_p(q) = v_p(x-y) + v_p(n)$

Sappiamo che $n = q^{\text{sia primo}}$. Abbiamo due casi:

$p \neq q$ $\qquad x \equiv y \ (p)$

$$x^q - y^q = (x-y)(x^{q-1} + x^{q-2}y + \ldots + y^{q-1})$$

$$x^{q-1} + \ldots + y^{q-1} \equiv \underbrace{x^{q-1} + x^{q-1} + \ldots + x^{q-1}}_{q \text{ volte}} \equiv q x^{q-1} \ (p)$$

ma $p \nmid x$ e $p \neq q \Rightarrow q x^{q-1} \not\equiv 0 \ (p)$

$$\Rightarrow v_p(x^q - y^q) = v_p(x-y) = v_p(x-y) + v_p(q)$$

$q = p$ $\qquad v_p(q) = 1$, quindi vogliamo mostrare che $v_p(x^{q-1} + x^{q-2}y + \ldots + y^{q-1}) = 1$

$x \equiv y \ (p) \Rightarrow x^{p-1} + \ldots + y^{p-1} \equiv$

$$\equiv \underbrace{x^{p-1} + \ldots + x^{p-1}}_{p \text{ volte}} \equiv p x^{p-1} \equiv 0 \ (p)$$

$$\Rightarrow v_p(x^{p-1} + \ldots + y^{p-1}) \geq 1$$

$y = x + kp$, perché $y \equiv x \ (p)$

$$\Rightarrow y^i = \sum_{j=0}^{i} \binom{i}{j} x^j \cdot k^{i-j} \cdot p^{i-j} \equiv x^i + i x^{i-1} kp \ (p^2)$$

$$x^{p-1} + x^{p-2}y + \ldots + y^{p-1} = \sum_{i=0}^{p-1} x^{p-1-i} \cdot y^i \equiv$$

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

$$\equiv x^{p-2} \sum_{i=0}^{p-1} (x + ikp) \equiv x^{p-2}\left(px + kp \cdot \frac{(p-1)p}{2}\right) \pmod{p^2}$$

$$\equiv p x^{p-1} \mod p^2$$

ma $p \nmid x \implies p x^{p-1} \not\equiv 0 \pmod{p^2}$

$\implies v_p(x^{p-1} + \dots + y^{p-1}) = 1$.

PROP: p primo $\neq 2$, n dispari, $x, y \not\equiv 0 \pmod p$, $p \mid x+y$, allora

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

PROP:
- Se $4 \mid x-y$ allora $2 \nmid x$
$$v_2(x^n - y^n) = v_2(x-y) + v_2(n)$$
- Se $2 \| x-y$ e $2 \mid n$ allora $2 \nmid x$
$$v_2(x^n - y^n) = v_2(x-y) + v_2(x+y) + v_2(n) - 1$$
- Se n è dispari $v_2(x^n - y^n) = v_2(x-y)$ $2 \nmid x$

ESERCIZIO: Sia $a \in \mathbb{N}$, $a \neq 0$, $a_n = 1 + a + \dots + a^{n-1}$, siano s, t interi t.c. $\forall p \mid s-t$ primo $p \mid a-1$. Mostrare che $\frac{a_s - a_t}{s-t}$ è intero.

SOL: $a_n = \frac{a^n - 1}{a - 1}$ WLOG $s > t$

$$\frac{a_s - a_t}{s - t} = \frac{a^s - 1 - a^t + 1}{(a-1)(s-t)} = \frac{a^s - a^t}{(a-1)(s-t)} =$$

$$= \frac{a^t(a^{s-t} - 1)}{(a-1)(s-t)}$$ questo è intero se

$(a-1)(s-t) \mid a^t(a^{s-t} - 1)$ che è equivalente

a dire che $\forall p$ primo $p \mid (a-1)(s-t)$

$$v_p(a^t(a^{s-t} - 1)) \geq v_p((a-1)(s-t))$$

$p \nmid a^t \Rightarrow$ $\hookrightarrow = v_p(a^{s-t} - 1) =$ $\Big\lceil$ $=$

$$= v_p(a^{s-t} - 1^{s-t}) = v_p(a-1) + v_p(s-t)$$

↑ posso usare LTE perché $p \mid a - 1$

Nel caso $p = 2$ basta vedere i vari casi...

ESERCIZIO: a dispari. Vogliamo trovare tutti gli a per cui $\frac{a^n + 1}{2}$ è un cubo $\forall n$.

SOL: Scegliamo n dispari. Se $\exists p$ primo

dispari t.c. $p \mid 2+1$

$v_p\left(\frac{2^n+1}{2}\right) = v_p\left(2^n+1\right) = v_p(2+1) + v_p(n)$ deve essere divisibile per 3.

Posso sempre scegliere un n per cui

$v_p(n) \not\equiv -v_p(2+1) \pmod 3$.

$\Longrightarrow \quad 2+1 = 2^k$.

$\frac{(2^k-1)^n+1}{2}$ è un cubo $\forall n$.

$(2^k-1)^n + 1 = 2x^3$.

Scelgo $n=2$ $\qquad (2^k-1)^2 + 1 = 2x^3$

$2^{2k} - 2^{k+1} + 2 = 2x^3$ $\qquad$ Se $k > 1$

$2^{2k-1} - 2^k + 1 = x^3$

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

$2^k(2^{k-1}-1)$

$x^2 + x + 1 \not\equiv 0 \ (2)$

$\Longrightarrow \quad 2^k \mid x-1$

$x^2+x+1 \mid 2^{k-1}-1$

$2^k \le x-1 < x^2+x+1 \le 2^{k-1}-1$ assurdo.

$\Rightarrow \quad k = 1 \qquad \Rightarrow \quad a = 1$.

TEOREMA (LEMMA DEL GUADAGNO DI UN PRIMO):

$x, y \in \mathbb{N}$, $x > y$, $n > 1$, $(x, y) = 1$,

allora $x^n - y^n$ ha un primo che non divide $x - y$, tranne i casi in cui $n = 2$ e $x + y = 2^k$.

DIM: Possiamo assumere che $n = q$ sia primo.

Dimostriamolo per assurdo. Se $q \neq 2$

Se $p \mid x^q - y^q \Rightarrow p \mid x - y$

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

Se $p \neq q \Rightarrow v_p(x^q - y^q) = v_p(x - y)$, ma se questo valesse $\forall q$ avrei $x^q - y^q = x - y$

$\Rightarrow$ deve esserci anche $p = q$.

$\Rightarrow q \mid x - y$.

$$v_q(x^q - y^q) = v_q(x - y) + 1$$

$$\Rightarrow \quad x^q - y^q = q(x - y)$$

$$\frac{x^q - y^q}{x - y} = q$$

$x > y$

$$x^{q-1} + x^{q-2}y + \dots + y^{q-1} = q$$

$$\Rightarrow \quad q y^{q-1} \geq q \qquad \Rightarrow \text{ assurdo!}$$

Se invece $q = 2$ $\qquad x^2 - y^2 = (x-y)(x+y)$

$p \mid x+y \Rightarrow p \mid x-y \Rightarrow p \mid 2x$ e $p \mid 2y$

$\Rightarrow p = 2$ (perché x e y sono coprimi)

$\Rightarrow x + y = 2^k$

Resta da vedere cosa succede per $n = 2^\alpha$ $(\alpha > 1)$

$$x^n - y^n = x^{2^\alpha} - y^{2^\alpha} = (x^2)^{2^{\alpha-1}} - (y^2)^{2^{\alpha-1}}$$

$x^2 - y^2 \equiv 0 \ (4)$ $\Rightarrow$ caso di LTE con $p = 2$

$$v_2(x^n - y^n) = v_2(x^2 - y^2) + \alpha - 1$$

$$x^n - y^n = 2^{\alpha-1}(x^2 - y^2)$$ (si finisca come nel caso $n = q$ dispari)

LEMMA DI HENSEL

LEMMA: Dato un polinomio $f(x) \in \mathbb{Z}[x]$ e detto S_ℓ il numero di soluzioni di $f(x)$ mod p^ℓ (per p primo), se $\forall$ soluzione mod p z abbiamo $f'(z) \not\equiv 0 (p)$, allora

$$S_\ell = S_1 \qquad \forall \ell \in \mathbb{N}.$$

DIM: Come prima cosa vogliamo sollevare una radice modulo p ad una radice modulo p^ℓ.

PASSO BASE: $f(z) \equiv 0 (p)$ per $\ell = 1$ è lei stessa.

PASSO INDUTTIVO: Supponiamo che $\exists\, z \in \mathbb{Z}/p^\ell\mathbb{Z}$ t.c. $f(z) \equiv 0 (p^\ell)$. Prendiamo un sollevamento $\tilde{z}$ di z, ovvero $\tilde{z} \in \mathbb{Z}/p^{\ell+1}\mathbb{Z}$ t.c. $\tilde{z} \equiv z (p^\ell)$

$$f(\tilde{z}) \equiv k p^\ell \pmod{p^{\ell+1}}$$

Se per caso $p \mid k$ allora abbiamo finito.

$$\tilde{z} + \alpha p^\ell \longrightarrow f(\tilde{z} + \alpha p^\ell)$$

$$(\tilde{z} + \alpha p^\ell)^i = \sum_{j=0}^{i} \binom{i}{j} \tilde{z}^j \cdot \alpha^{i-j} p^{\ell(i-j)} \equiv$$

$$\equiv \tilde{z}^i + i \cdot \alpha p^\ell \cdot \tilde{z}^{i-1} \quad (p^{\ell+1})$$

$$f(x) = \sum_{i=0}^{d} c_i x^i$$

$$f(\tilde{z} + \alpha p^l) \equiv \sum_{i=0}^{d} c_i (\tilde{z} + \alpha p^l)^i \equiv \sum_{i=0}^{d} \left(c_i \tilde{z}^i + c_i i \alpha p^l \tilde{z}^{i-1}\right) \pmod{p^{l+1}}$$

$$\equiv f(\tilde{z}) + \sum_{i=0}^{d} c_i \cdot i \cdot \alpha p^l \tilde{z}^{i-1} = f(\tilde{z}) + \alpha p^l f'(\tilde{z})$$

$$D(c_i \cdot \tilde{z}^i) = c_i \cdot i \cdot \tilde{z}^{i-1}$$

$$f(\tilde{z} + \alpha p^l) \equiv k p^l + \alpha p^l \cdot f'(\tilde{z}) \quad (p^{l+1})$$

Mi basta scegliere $\alpha \equiv -\frac{k}{f'(\tilde{z})} \pmod{p}$

e posso farlo perché $f'(\tilde{z}) \not\equiv 0 \pmod{p}$.

Data una soluzione $\pmod{p}$, mi resta da dimostrare che si "solleva" in modo unico a ogni step.

Ma la scelta di α era unica, quindi ho la tesi.

OSS: Il lemma di Hensel ci dice che le equazioni polinomio = potenza non sempre si possono risolvere con le congruenze

ES: $3^n = x^2 + 5$

$f(x) = x^2 + 5$ ha una radice mod 3,

perché -1 è un $\square$, inoltre

$f'(x) = 2x$ non fa 0 in questa radice

$\Longrightarrow$ x^2+5 ha soluzioni mod 3^h $\forall$ n

VERA SOL: GUARDARE MOD 8

$3^h \equiv \begin{cases} 1 \\ 3 \end{cases}$ $\qquad$ $x^2+5 \equiv \begin{cases} 5 \\ 6 \\ 1 \end{cases}$

$\Longrightarrow$ n è pari

$\Longrightarrow$ $3^{2m} = x^2 + 5$ $\qquad$ $(3^m - x)(3^m + x) = 5$

... ecc ...

TEOREMA DI WILSON

TEOREMA: dato p primo, $(p-1)! \equiv -1 \pmod p$

DIM: si osserva che $\forall$ $x \bmod p$ $\exists$ $x^{-1} \bmod p$

Questo suddivide le classi di resto mod p a coppie,

$\{2, 2^{-1}\}, \{3, 3^{-1}\}, \dots$

rimangono soli soletti solamente 1 e -1

Perché 1 e -1 sono gli unici che sono inversi di loro stessi. Infatti $x^{-1} = x \Rightarrow x^2 = 1$

$\Rightarrow x^2 - 1 = 0 \qquad (x-1)(x+1) = 0$.

$$(p-1)! \equiv \prod_{\substack{x \bmod p \\ x \neq 0}} x \equiv 1 \cdot -1 \equiv -1 \ (p).$$

↑ ogni numero si annulla con il suo inverso.

ESERCIZIO: Determinare tutti gli n interi positivi t.c.

$$2n+7 \mid (n!)^{2n} + 1$$

Se $p \mid 2n+7 \Rightarrow p \mid (n!)^{2n} + 1 \Rightarrow$

$\Rightarrow p \nmid n! \qquad p > n$

Se $2n+7$ <u>NON</u> è primo, ci sono due fattori $p > n$

$$2n+7 \geq (n+1)^2 = n^2 + 2n + 1$$

$$\Rightarrow \quad n^2 \leq 6 \quad \Rightarrow \quad n \leq 2$$

$\Rightarrow$ per $n > 2$ $\quad 2n+7$ è primo.

$$2n+7 = p \qquad (2n+6)! \equiv -1 \ (p)$$

$$(n!)^{2n} + 1$$

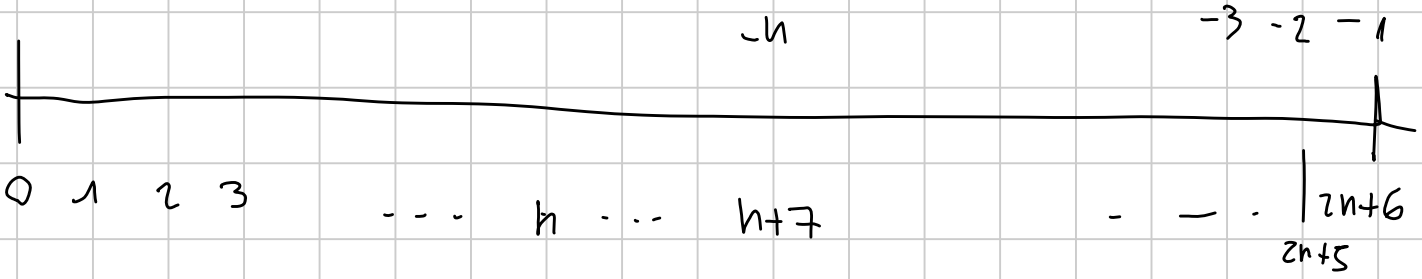
Se $p \mid (n!)^{2n} + 1$ allora

-1 è un $\square$ mod p $\Rightarrow$ $p \equiv 1 \ (4)$

$\Rightarrow$ n è dispari.

$$n! = \frac{(2n+6)!}{(n+1)\cdot\ldots\cdot(2n+6)} \equiv \frac{(2n+6)!}{(n+1)\cdot\ldots\cdot(n+6)\cdot(-1)(-2)\cdot\ldots\cdot(-n)} =$$

$$\equiv \frac{-1}{(n+1)\cdot\ldots\cdot(n+6)\cdot(-1)^n \cdot n!} \quad (p)$$



$$n! \equiv \frac{(-1)^{n+1}}{(n+1)\cdot\ldots\cdot(n+6)\cdot n!} \quad (\text{mod } p)$$

$$(n!)^2 \equiv \frac{1}{(n+1)\cdot\ldots\cdot(n+6)} \quad (\text{mod } p)$$

$$\equiv -(n+1)^{-2}(n+2)^{-2}(n+3)^{-2} \quad (p)$$

$$\equiv \frac{-64}{(2n+2)^2(2n+4)^2(2n+6)^2} \equiv \frac{-64}{(-5)^2\cdot(-3)^2\cdot(-1)^2} \equiv$$

$$\equiv -\frac{64}{225}$$

$$2n+7 \mid \left(\frac{64}{225}\right)^n - 1$$

$$2n+7 \mid 64^n - 225^n$$

$$2n+7 \mid (15^n - 8^n)(15^n + 8^n)$$

Ci basta $2n+7 \mid 15^n \pm 8^n$

↖ o + o −

$$p \mid 225^{\frac{p-7}{2}} - 64^{\frac{p-7}{2}} \qquad \frac{64}{225} = x$$

$$p \mid \left(\frac{64}{225}\right)^{\frac{p-7}{2}} - 1 \qquad \left(\frac{64}{225}\right)^{\frac{p-7}{2}} \equiv 1 \ (p)$$

$$ord_p(x) \mid \left(p-1, \frac{p-7}{2}\right) = (2n+6, n) = (6, n) =$$

$$= (n, 3)$$

$$ord_p(x) = \begin{cases} 1 \\ 3 \end{cases}$$

Se $ord_p(x) = 1$ $\quad p \mid 225 - 64 = 161$

Se $\operatorname{ord}_p(x) = 3$

$$p \mid 225^3 - 64^3 = (15^6 - 8^6) = (15^3 - 8^3)(15^3 + 8^3)$$

$$= \dots$$ si finisce.