Teoria dei Numeri - 1

Titolo nota 30/12/2011

POLINOMI CICLOTOMICI

Def: $z \in \mathbb{C}$ è detta radice n-esima dell'unità se per $n \in \mathbb{N}$ $z^n = 1$

Def: una radice n-esima è detta primitiva se

$$z^n = 1 \quad \text{e} \quad \forall k < n \quad z^k \neq 1$$

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

... PARTE ALLA LAVAGNA ...

GENERATORI MOD p^n

$\forall p$ primo $\exists g$ generatore mod p, ovvero $\exists g$ t.c $\text{ord}_p(g) = p-1$.

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

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

è un'unione disgiunta!

$$G_d = |\{a \in \mathbb{F}_p \mid \text{ord}_p(a) = d\}| \qquad p-1 = \sum_{d \mid p-1} G_d$$

Se $\text{ord}_p(a) = d \Rightarrow a^d - 1 \equiv 0 \ (p) \Rightarrow$

$\Rightarrow$ ϑ è radice di $x^d - 1$, ma $x^d - 1$ ha al più d radici in $\mathbb{F}_p$. Voglio dire che ϑ è radice di $\Phi_d(x)$; questo è vero perché $x^d - 1 = \Phi_d(x) \cdot \prod_{\substack{c \mid d \\ c < d}} \Phi_c(x)$, quindi se ϑ non fosse radice di $\Phi_d(x)$ $\exists\, c < d$ t.c. $\Phi_c(\vartheta) \equiv 0 \Rightarrow \vartheta^c - 1 \equiv 0 \Rightarrow$ assurdo perché d è l'ordine. $\Rightarrow$ ogni ϑ di ordine d è radice (in $\mathbb{F}_p$) di $\Phi_d(x)$.

$\Rightarrow$ $G_d \leq \varphi(d)$

(G_d: elementi di ord d; $\varphi(d)$: radici di Φ_d)

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

$\Rightarrow$ $G_d = \varphi(d)$ $\forall d$!!! $\Rightarrow$

$\Rightarrow$ in particolare $G_{p-1} = \varphi(p-1) > 0$

$\Rightarrow$ $\exists$ α generatore.

DIGRESSIONE: In $\mathbb{F}_p$ bisogna fare attenzione alla differenza fra funzione polinomiale e polinomio.

$f : \mathbb{F}_p \to \mathbb{F}_p$ t.c. $f(x) = x^p - x$ $\rightsquigarrow$

$\rightsquigarrow$ $f \equiv 0$ questo È la funzione 0.

tuttavia il polinomio $x^p - x$ NON È il polinomio nullo.

LEMMA: dato p primo

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

DIM: PER INDUZIONE

PASSO BASE: $s=0$ $\quad 1+kp \equiv 1+kp \ (p^2)$

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

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

$$\equiv (1+p^{s+1}(k+hp))^p \equiv 1+kp^{s+2} \ (p^{s+3})$$

perché ho $\sum_{i=0}^{p} \binom{p}{i} p^{(s+1)i} (k+hp)^i \equiv \uparrow$ □

TEOREMA: Dato p primo $\forall n \in \mathbb{N}$ $\exists g$ t.c.

$$\text{ord}_{p^n}(g) = \varphi(p^n) \quad \text{(generatore)}$$

DIM: Se g è un generatore mod p allora

$p-1 \mid \text{ord}_{p^n}(g) \mid (p-1)p^{n-1}$, ci basta trovare un g tale che $g^{(p-1)p^{n-2}} \not\equiv 1 \ (p^n)$.

Sappiamo che $g^{p-1} \equiv 1 \ (p) \Rightarrow g^{p-1} \equiv 1+kp \ (p^2)$

se $p \nmid k$ g è un generatore mod p^2

se invece $p \mid k$ prendo $g+p$, il suo ordine

è ancora multiplo di $p-1$.

$$(g+p)^{p-1} = \sum_{k=0}^{p-1} \binom{p-1}{k} p^k g^{p-1-k} \equiv g^{p-1} + (p-1)p\,g^{p-2} \equiv$$

$$\equiv 1 + (p-1)g^{p-2}p \ (p^2) \quad , \text{ ma } p \nmid g^{p-2}(p-1)$$

$\Longrightarrow$ $g+p$ è un generatore.

Abbiamo trovato che mod p^2 esiste sempre un generatore. Per il lemma, se $\exists$ un generatore mod p^2 allora $g^{p-1} \equiv 1 + kp \ (p^2)$

$\Longrightarrow \forall n \quad g^{(p-1)p^{n-2}} \equiv (1+kp)^{p^{n-2}} \equiv 1 + kp^{n-1} \ (p^n)$ (GEMMA),

ma $p \nmid k$ (g è gen.) $\Longrightarrow$ g è generatore mod p^n. $\square$

"OSS": Gli unici n per cui $\exists$ un generatore mod n sono $2, 4, p^k, 2p^k$ (p dispari primo).

LTE — LIFTING THE EXPONENT

TEOREMA: Sia p primo, $v_p(n)$ il più grande k per cui $p^k \mid n$ (si scrive $p^k \| n$), allora dati $x, y \not\equiv 0 \ (p)$, $p \mid x-y$, $p \neq 2$ vale

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

DIM: $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \dots + y^{n-1})$

Ci basta dimostrare che $v_p(n) = v_p(x^{n-1} + \dots + y^{n-1})$

Possiamo assumere che $n = q$ primo, perché mi basta scomporre in primi e iterare il ragionamento.

Abbiamo 2 casi:

$q \neq p$ $\quad x \equiv y \ (p) \Rightarrow x^{q-1} + \dots + y^{q-1} \equiv$

$\equiv x^{q-1} + x^{q-1} + \dots + x^{q-1} \equiv q x^{q-1} \not\equiv 0 \ (p)$

$\Rightarrow v_p\left(\frac{x^q - y^q}{x-y}\right) = v_p(q) = 0$ è ok!

$q = p$ Vorrei che $v_p(p) = 1 = v_p(x^{p-1} + \dots + y^{p-1})$

Sicuramente $v_p(x^{p-1} + \dots) \geq 1$ perché

$x^{p-1} + \dots + y^{p-1} \equiv p x^{p-1} \ (p) \equiv 0$

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

fa 0 se $i = p-1$

$x^{p-1} + \dots + y^{p-1} \equiv \sum_{i=0}^{p-1} x^i \left(x^{p-1-i} + kpi\, x^{p-2-i}\right) \equiv$

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

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

OSS: $p = 2$ non funziona per via di lui

PROP: Se n è dispari e $p \mid x+y$ $\quad p \nmid x$

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

DIM: $x^n+y^n = x^n-(-y)^n$ ... come prima.

PROP: • Se $4 \mid x-y$ allora

$$v_2(x^n-y^n) = v_2(x-y)+v_2(n)$$

• Se $2 \parallel x-y$ e $2 \mid n$ allora

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

• Se n è dispari $v_2(x^n-y^n) = v_2(x-y)$

ESERCIZIO 1 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: $a_s = \frac{a^s-1}{a-1}$, $a_t = \frac{a^t-1}{a-1}$, quindi

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

mi basta che $\forall p \mid s-t$

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

$=$ ← LTE □

ESERCIZIO: Determinare il più grande $k \in \mathbb{Z}$ tale che $2017^k \mid 2016^{2017^{2018}} + 2018^{2017^{2016}} + 2017^{2016^{2015}}$

SOL: Se le ipotesi fossero rispettate

$$v_{2017}\left(2016^{2017^{2018}} + 2018^{2017^{2016}}\right) =$$

$$v_{2017}\left(2016^{2017^2} + 2018\right) + 2016$$

Le ipotesi sono rispettate se $2017 \mid 2016^{2017^2} + 2018 \equiv$

$\equiv (-1)^{2017^2} + 1 \equiv 0 \ (2017)$ OK.

$2017 = p$

$2016 = p - 1 \longrightarrow -2016p^2 = -(1-p)p^2$ ma

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

$\implies 2016^{2017^2} + 2018 \equiv -1 + 2018 \equiv 2017 \ (2017^2)$

$\implies k = 2016 + 1 = 2017.$

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: casi in cui $n = 2$ $x + y = 2^k$.

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

Se la tesi fosse falsa avrei, per $q \neq 2$,

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

$v_p(q) = \begin{cases} 0 & q \neq p \\ 1 & q = p \end{cases}$, quindi se $q \nmid x - y$

$x^q - y^q = x - y$ assurdo per $q \neq 1$.

se $q \mid x - y$ allora $x^q - y^q = q(x - y)$

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

assurdo.

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

$(x+y, x-y) \mid 2y$ e $\mid 2x \Rightarrow (x+y, x-y) \mid 2$.

$\Rightarrow$ se in $x+y$ non ci sono primi "nuovi" allora

$x+y = 2^k$.

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

in questo caso $4 \mid x^2 - y^2$, quindi

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

Sono nel caso q dispari! (o quasi)

(ripercorro lo stesso ragionamento di prima).

TEOREMA DI ZSIGMONDY:

$x, y \in \mathbb{N}$ $\quad x > y$ $\quad n > 1$, allora $x^n - y^n$

contiene un primo che non è contenuto in

tutti i $x^k - y^k$ per $k < n$ .....

tranne nei seguenti casi:

- $n = 2$, $x = 3$, $y = 1$
- $x + y = 2^k$

LEMMA DI HENSEL

LEMMA: Dato un polinomio $f(x) \in \mathbb{Z}[x]$ detto S_ℓ il numero di soluzioni di $f(x)$ modulo p^ℓ (per p primo), se $\forall$ soluzione mod p z, $f'(z) \not\equiv 0 \ (p)$, ho che $S_\ell = S_1 \quad \forall \ell \in \mathbb{N}$

DIM: Mostriamo prima che data una soluzione mod p questa si può "sollevare" ad una soluzione mod p^n

PASSO BASE: $f(z) \equiv 0 \ (p)$

PASSO INDUTTIVO: So che $\exists z \in \mathbb{Z}/p^n\mathbb{Z}$ t.c. $f(z) \equiv 0 \ (p^n)$

$\Rightarrow$ sia $\tilde{z}$ un "sollevamento di z in $\mathbb{Z}/p^{n+1}\mathbb{Z}$, ovvero tale che $\overline{\tilde{z}} = z$ (proiezione su $\mathbb{Z}/p^n\mathbb{Z}$), allora $f(\tilde{z}) \equiv k p^n \ (p^{n+1})$. Se $p \mid k$ allora $\tilde{z}$ è una soluzione mod p^{n+1}, altrimenti prendo $\tilde{z} + \alpha p^n$, allora $f(\tilde{z} + \alpha p^n)$ cos'è?

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

$$\Rightarrow \quad f(\tilde{z} + \alpha p^n) = \sum_{i=0}^{\deg f} a_i \underbrace{(\tilde{z}^i}_{①} + \underbrace{i\tilde{z}^{i-1} \cdot \alpha p^n)}_{②} \equiv$$

(coefficienti)

$$\equiv \overbrace{kp^n}^{0} + \overbrace{\alpha p^n \cdot f'(\tilde{z})}^{0} = p^n(k + \alpha f'(\tilde{z}))$$

α lo posso scegliere, prendo $\alpha \equiv -\frac{k}{f'(z)}$ (p)

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

Inoltre, per come scelgo α data z radice mod p^n $\exists!$ $\tilde{z}$ tale che $f(\tilde{z}) \equiv 0 (p^{n+1})$ e $\tilde{z} = z$.

Definisco una funzione $\psi_n : S_n \to S_{n+1}$ t.c. (pensati come insiemi)

$z \mapsto \tilde{z}$ (è ben definita per unicità di α)

se mostro che ψ_n è biiettiva ho la tesi.

se $z_1 \neq z_2$ allora $\tilde{z}_1 \neq \tilde{z}_2$ perché $\tilde{z}_1 = z_1 \neq z_2 = \tilde{z}_2$,

$\Rightarrow$ è iniettiva. Inoltre $\forall$ w radice mod p^{n+1}

$\bar{w}$ è radice mod p^n $\Rightarrow$ $w = \tilde{\bar{w}}$ $\Rightarrow$ ψ_n è suriettiva $\square$

COSA CI DICE HENSEL?

Le equazioni polinomio = potenza

NON si possono risolvere con le congruenze

ES: $3^n = x^2 + 5$ x^2+5 ha una radice mod 3 che è 1 e $2x$ in 1 non fa 0 mod 3,

$\Rightarrow$ ha sol. mod 3^n $\forall n$

SOL: mod 8 $\quad 3^n \equiv \begin{cases} 1 \\ 3 \end{cases}$ $\qquad x^2+5 \equiv \begin{cases} 5 \\ 1 \\ 6 \end{cases}$

$\Rightarrow$ n pari $\Rightarrow$ $3^n - x^2 = 5$ - - - -

e si finisce.

ESERCIZIO) Mostrare che $\forall n \in \mathbb{N}$ $\exists m \in \mathbb{N}$ t.c. $7^n \mid 5^m + 3^m - 1$