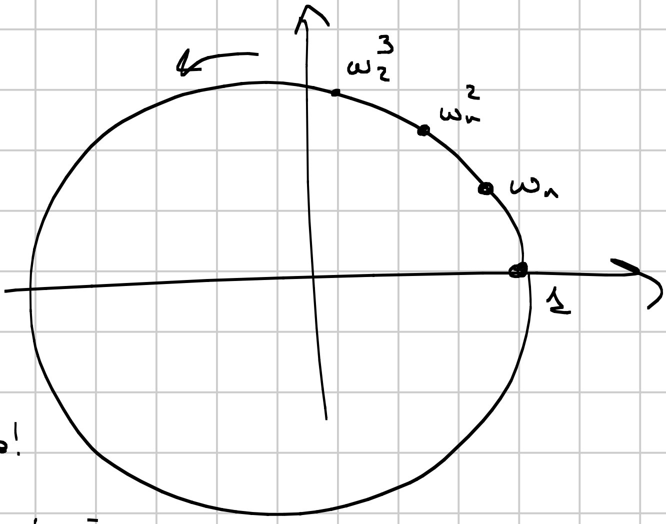
N1 MEDIUM - NUMERI PRIMI [Gallo]

Note Title 04/09/2022

→ Polinomi ciclotomici
⇒ generatori mod p, p^n
→ LTE e guadagno di un primo
→ Hensel

Polinomi Ciclotomici

le radici n-esime dell'unità $x^n - 1$



$\omega_n = e^{i\frac{2\pi}{n}}$

$\omega_n^k = e^{i\frac{2\pi}{n}k}$

PRIMITIVE: sono le radici n-esime "di ordine n" (tipo 1 no! se $n>1$)
o -1 non lo è

→ Quante sono? $\varphi(n)$

$e^{i\frac{2\pi}{n}k}$ ← questa è primitiva se e solo se $(n,k)=1$

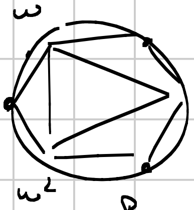
N-ESIMO POLINOMIO CICLOTOMICO

$$\Phi_N(x) = \prod_{(k,n)=1} \left(x - e^{i\frac{2\pi}{n}k}\right)$$

il polinomio che ha come radici le rad. prim. di 1.

$\Phi_2(x) = x+1$

$\Phi_3(x) = x^2+x+1$



$\Phi_6(x) = x^2 - x + 1$

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \_\_\_ + x + 1 = \frac{x^p - 1}{x-1}$$

- $\deg \Phi_n(x) = \varphi(n)$
- Φ_n hanno tutti coeff. interi

- sono tutti irriducibili $\quad \Phi_p(x+1)$ è p-eisenstein
- Φ_n e Φ_m sono coprimi $\forall m \neq n$
- $\boxed{x^n-1 = \prod_{d|n} \Phi_d(n)}$ $\rightsquigarrow$ $n = \sum_{d|n} \varphi(d)$

  $\downarrow$ inversione di Möbius
- $\Phi_n(x) = \prod_{d|n} (x^d-1)^{\mu(\frac{n}{d})}$

con $\mu(m) = \begin{cases} 0 & \text{se } m \text{ non è sq-free} \\ 1 & \text{se } m \text{ ha \#pari di f. primi} \\ -1 & \text{altrimenti} \end{cases}$

Problema 1. Esistono infiniti interi positivi n t.c. n^2+n+1 non ha fattori primi $> \sqrt{n}$. !

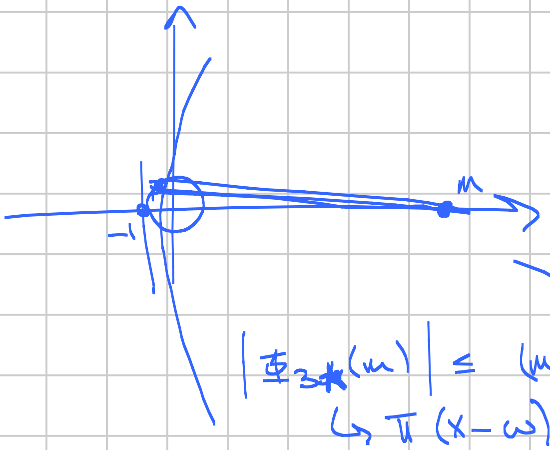
$$\Phi_3(n) = n^2+n+1 = \frac{n^3-1}{n-1}$$

!! se fattorizziamo in molti fattori

Prendo $n = m^k$.

$$\Phi_3(m^k) = \frac{m^{3k}-1}{m^k-1} \overset{\text{formula}}{=} \frac{\prod_{d|3k} \Phi_d(m)}{\prod_{j|k} \Phi_j(m)} \overset{(k,3)=1}{=} \prod_{d|k} \Phi_{3d}(m)$$

ⓘ vorrei $\le m^{k/2}$



$$|\Phi_{3k}(m)| \le (m+1)^{\varphi(3k)}$$

$\hookrightarrow \prod (x-\omega)$

$|x-\omega| \le m+1$

$\exists k$ intero

$$(m+1)^{\underbrace{\frac{2\varphi(k)}{k}}} \overset{?}{\le} m^{1/2}$$

$\downarrow$

$\frac{\varphi(k)}{k}$ va vicino a 0 quanto voglio

Generatori mod p

$\exists\, g \in \{1, 2, 3, —, p-1\}$ tc $\text{ord}_p(g) = p-1$

è come dire: $\exists\, g$ tc $\{g^1, g^2, —, g^{p-1}\} = \{1, 2, 3, — p-1\}$ mod p

g lo chiamo GENERATORE $\quad \mathbb{Z}/8\mathbb{Z} \ [1^2 = 3^2 = 5^2 = 7^2]$

⇝ Anche mod p^n dispari esiste un generatore

$\exists$ generatore mod n $\iff n = 2, 4, p^n, 2p^n$.

→ Polinomi mod p $\quad \mathbb{F}_p[x]$ c'è la div. euclidea

- $x^{p-1} - 1 = (x-1)(x-2) — (x-(p-1))$
- $\Psi_d(x) = \prod (x-k)$ sui k di ordine esattamente d

$$\longrightarrow \quad x^{p-1} - 1 = \prod_{d \mid p-1} \Psi_d(x)$$ come prima

- Gli elementi mod p di ordine $d \mid p-1$ sono esattamente $\varphi(d)$

  ⌐ per induzione su d

$$x^d - 1 = \Psi_d(x) \cdot \prod_{\substack{k \mid d,\\ k<d}} \Psi_k(x)$$

per hp. ind

$$d = \boxed{?} + \sum_{\substack{k \mid d\\ k<d}} \varphi(k)$$

$$? = \deg \Psi_d = d - \sum_{\substack{k \mid d\\ k<d}} \varphi(k) = \varphi(d)$$

Problema 2. n intero pos., p primo con $p > n+1$ $\quad n < p-1$

$$p \mid 1^n + 2^n + 3^n + \_\_\_ + (p-1)^n$$

$$= (g^1)^n + (g^2)^n + (g^3)^n + \_\_\_ + (1)^n \quad \text{mod } p$$

$$= \frac{(g^n)^{p-1} - 1}{g^n - 1} \equiv 0 \quad \text{mod } p$$

Residui k-esimi

→ i residui quadratici mod p sono $\frac{p-1}{2}$

$$\{(g^1)^k, (g^2)^k, (g^3)^k, — , (g^{p-1})^k\} \subsetneq \{1, 2, 3, —, p-1\}$$

$$= \{ g^k, g^{2k}, g^{3k}, — g^{k(p-1)} \}$$

è come chiedersi $\{k, 2k, —, k(p-1)\}$ mod p-1

Quando ottengo tutto? | Quando i residui k-esimi sono tutti?

Quando $(k, p-1) = 1$

Quanti sono i residui k-esimi? $\boxed{\frac{p-1}{(k,p-1)}}$

Problema 3. [BMO 2014] Trovare tutte le $(a,b,c,d) \in \mathbb{Z}^4$ di numeri interi tc

$2 \cdot 19 \cdot 53$

$$2014 = \frac{a^3+2b^3}{c^3+2d^3}$$

$\boxed{(c^3+2d^3)\, 2014 = (a^3+2b^3)}$ → mod 2 : a pari

$0 \equiv a^3 + 2b^3$ mod 19

ab^{-1}

$(ab^{-1})^3 = -2$ mod 19

i residui cubici sono $\frac{18}{(18,3)} = 6$

$(-2)^6 = +64 = 7$ mod 19 è un residuo cubico?

⟹ -2 NON È UN RESIDUO CUBICO

$(-2)^6 = (g^a)^6$ se $6a = 0$ mod 18 allora $a \equiv 0$ mod 3

Criterio di Eulero

[In generale a è residuo k-esimo mod p ⟺ $a^{\frac{p-1}{(k,p-1)}} \equiv 1$ mod p]

$a \equiv b \equiv 0$ mod 19 → DISCESA INFINITA

LTE Lemma. "Lifting the exponent"

p primo dispari, a, b interi t.c.

i. $p \mid a-b$ ←

ii. $p \nmid a$, $p \nmid b$ ←

allora

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

$v_p(n)$ è il più grande esponente di p che divide n

- Se n è dispari, vale con il $+$ ⤴ (posso $b \mapsto -b$)
- Con $p=2$:
  - Se $4 \mid a-b$ tutto invariato
  - Se $2 \| a-b$ $[v_2(a-b)=1]$ allora

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

Dimostrazione

- $\boxed{(n,p)=1}$

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \_\_\_ + b^{n-1}\right)$$

lo guardo mod p

$a^{n-1} + a^{n-2}b + \_\_ + b^{n-1} \equiv 0 \mod p$

$(ab^{-1})^{n-1} + \_\_\_\_ + 1 \equiv 0 \mod p$ ← $a \equiv b \mod p$

$n \not\equiv 0 \mod p$

- $\boxed{n=p}$ Vogliamo mostr. $v_p(a^p - b^p) = v_p(a-b) + 1$

$a-b = \alpha \cdot p^k$ con $(\alpha,p)=1$ e $k = v_p(a-b)$

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

$$= [b - p^k \cdot \alpha]^p - b^p$$

$$= \left[\cancel{b^p} - \binom{p}{1} \cdot b^{p-1} \boxed{p^k} \cdot \alpha + \underbrace{\binom{p}{2} b^{p-2} p^{2k} \alpha^2 - \dots}_{\text{ha } v_p \geq 2k+1}\right] - \cancel{b^p}$$

$\frac{p(p-1)}{2}$

$$\equiv \boxed{p^{k+1}} \cdot (b^{p-1} \cdot \alpha) + \underbrace{p^{2k+1}(\_\_\_)}$$

$$\equiv \boxed{p^{k+1} \cdot b^{p-1} \cdot \alpha} \mod p^{2k+1}$$

$$v_p(a^n - b^n) = \boxed{k} + \boxed{1}$$
$$= v_p(a-b) + v_p(p)$$

- Gli altri n: $n = \alpha \cdot p^k$ con $(\alpha,p)=1$ $\quad a^n - b^n = (a^{p^k})^\alpha - (b^{p^k})^\alpha$

$p \mid a-b \implies p \mid a^{p^k} - b^{p^k}$

$$v_p(a^n - b^n) = v_p(a^{p^k} - b^{p^k})$$ per I caso

$$= v_p\left((a^{p^{k-1}})^p - (b^{p^{k-1}})^p\right)$$

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

"Bootstrap"/ Induzione

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

Problema 4. Trovare il più grande k tc

$$2017^k \mid 2016^{2017^{2018}} + 2018^{2017^{2016}} + \cancel{2017^{2016^{2018}}}$$

$$(-1)^{disp} + (1) + 0 \equiv 0 \mod 2017 \qquad k \geq 1$$

→ p è primo = 2017

$2017^{2016^{2018}}$ lo possiamo ignorare se $k \leq 2016^{2018}$

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

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

LTE

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

$$= \qquad + 2016$$

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

$$\equiv$$

$$\varphi(2017^2) = 2017 \cdot 2016$$

$$2017^2 = 2017 \cdot 2016 + 2017$$

$$\varphi(p^n) = p^{n-1}(p-1)$$

$\neq 0$

USO LTE DI NUOVO

$$v_{2017}\left(2016^{2017} + 1\right)$$

Problema 5. (Russia 1996) Trovare tutti gli $n>0$ t.c. $\exists\,(x,y)\in\mathbb{N}_{>0}$ t.c.

$(x,y)=1$

$$3^n = x^{\boxed{k}} + y^k = (x+y)(\_\_\_\_)$$

← Anche lei è una pot di 3; $=3^{n-m}$

$\boxed{k \text{ DISPARI}}$: guardo mod 3, se k è pari $x^k \equiv 1 \mod 3$

$\Longrightarrow x^k+y^k \equiv 2 \mod 3$ ↯

$\longrightarrow x \equiv -y \mod 3$: $\boxed{(x+y)} \mid x^k+y^k$

è una potenza di 3, $\boxed{x+y=3^m}$

LTE $\longrightarrow$ $n = v_3(x^k+y^k) = v_3(x+y)+v_3(k) = m + \boxed{v_3(k)}$

- m grosso; $m>1$, $9 \mid x+y$

dis. tra le medie

$$x^k+y^k \boxed{\geq} 2\left(\frac{x+y}{2}\right)^k =$$

alg.

$$= (x+y)\cdot\left(\frac{x+y}{2}\right)^{k-1}$$

def.

$$= 3^m\cdot\left(\frac{x+y}{2}\right)^{k-1}$$

$k-1 \geq v_3(k)$

$v_3 \sim \log_3$

$$> 3^m\cdot 3^{k-1}$$

$$\geq 3^{m+v_3(k)}$$

$\longrightarrow n > m+v_3(k) = n$ ASSURDO

- $\boxed{m=1}$ $x+y=3$ $2^k+1=3^n$

$$k = v_2(2^k) = v_2(3^n-1) = v_2(\cancel{3-1}) + v_2(\cancel{3+1}) + v_2(n) - \cancel{1}$$

1 2

$$k = v_2(n)+2$$

$$\boxed{2^{v_2(n)+2}+1} = \boxed{3^n}$$

lui poco

cresce troppo

INDUZIONE