

Struttura moltiplicativa di $(\mathbb{Z}/p\mathbb{Z})^\times$:

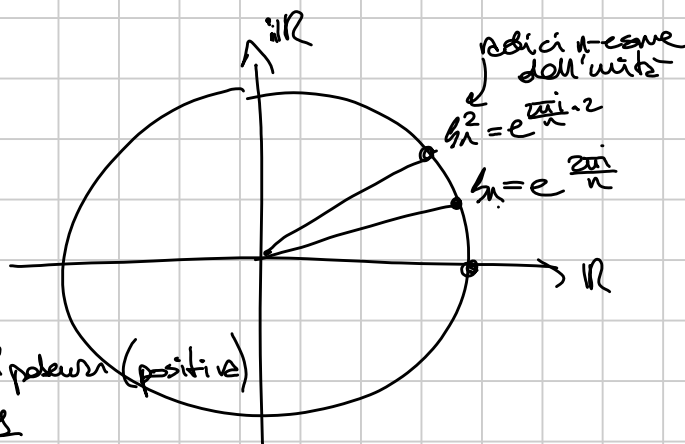
- generatore modulo p^n
- polinomi ciclotomici
- CRT, quadrato di un primo
- Lemma di Hensel

$\mathbb{Z}/N\mathbb{Z} = \{ \text{classi di resto modulo } N \}$

Polinomi Ciclotomici

Def Una radice n -esima di 1

si dice primitiva se ha ordine esattamente n



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

$\frac{k \cdot 2\pi i}{n}$ è intero $\iff n \mid k \cdot n$

Oss! le radici primitive n -esime di 1 sono $\phi(n)$.

$(a^k)^n$

Def $\Phi_n(x)$ il polinomio a coeff complessi che ha per zeri le radici n -esime primitive dell'unità!

$$\Phi_n(x) = \prod (x - \zeta)$$

ζ è radice n -esima di 1

lmo $\Phi_n(x) \mid x^n - 1$ • $\deg \Phi_n(x) = \phi(n)$

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

$n = \sum \phi(d)$

• $\Phi_n(x)$ ha coefficienti interi e è irriducibile su $\mathbb{Q}$ (su $\mathbb{Z}$)

$$\begin{aligned} x^8 - 1 &= (x^4 - 1)(x^4 + 1) \\ &= (x^2 - 1)(x^2 + 1)(x^4 + 1) \\ &= (x - 1)(x + 1)(x^2 + 1)(x^4 + 1) \end{aligned}$$

$\uparrow \quad \uparrow \quad \uparrow \quad \uparrow$

GENERATORI MODULO p^k

Quando $\mathbb{Z}/p\mathbb{Z}$. Ricordo che se $a \in \mathbb{Z}/p\mathbb{Z}$ e $a \neq 0 \pmod p$,
esiste $b \in \mathbb{Z}/p\mathbb{Z}$ t.c. $ab = 1 \pmod p$

$\text{ord}_p(a) =$ il più piccolo intero positivo n t.c. $a^n = 1 \pmod p$

FATTO. Esiste un elemento $a \in \mathbb{Z}/p\mathbb{Z}$ t.c. $\text{ord}_p(a) = p-1$. (qui è il massimo possibile per il piccolo teo di Fermat $a^p = a \pmod p$)

$\Leftrightarrow \{a, a^2, \dots, a^{p-1}\} = (\mathbb{Z}/p\mathbb{Z})^\times$

$\Leftrightarrow$ Gli elementi di ordine $d \mid p-1$ sono esattamente $\phi(d)$.

Dim

Guardo il polinomio $x^{p-1} - 1$ a coefficienti in $\mathbb{Z}/p\mathbb{Z}$

Oss! I polinomi mod p hanno le prop seguenti:

il numero di radici di $P(x)$ è al più $\deg P$
(se $P(a)=0$, allora $P(x) = (x-a)Q(x)$)
(se $P(b)=0$, allora $P(x) = (x-b)Q(x)$)
 $P = Q \cdot R \quad P(b) = Q(b)R(b)$

$$x^{p-1} - 1 = (x-1)(x-2) \dots (x-(p-1))$$

$$= \prod_{d \mid p-1} \Psi_d(x)$$

$\Psi_d(x)$ = il polinomio che ha per zeri gli elementi di $\mathbb{Z}/p\mathbb{Z}^\times$ di ordine esattamente d

• Dovrò mostrare che $\Psi_d(x)$ ha grado $\phi(d)$

Osservo che $\Psi_d(x) \mid x^d - 1$.

Osservo che $\Psi_2(x)$ ha grado 1.

Induzione! ← N da $N \mid p-1$ ← Suppongo che $\deg \Psi_d = \phi(d)$ per ogni $d < N$
e poi guardo $x^N - 1 = \prod_{d \mid N} \Psi_d(x)$

$$N = \deg(x^N - 1) = \deg \Psi_N + \sum_{\substack{d \mid N \\ d < N}} \deg \Psi_d$$

$$\deg \Psi_N = N - \sum_{\substack{d \mid N, d < N}} \deg(\Psi_d) = \phi(N)$$

(per la formula $n = \sum_{d \mid n} \phi(d)$)

Dim 2

• $x^{p-1} = \prod_{d|p-1} \Phi_d(x)$ come polinomi a coefficienti in $\mathbb{Z}$

$\downarrow$ riduco mod p
 $x^{p-1} \equiv \prod_{d|p-1} \Phi_d(x)$
 $x^{N-1} = \prod_{d|N-1} \Phi_d(x)$
 $\downarrow$
 $x^{N-1} \equiv \dots$
 x^{d-1}

Def Chiamo generatore (mod N) un elemento $g \in \mathbb{Z}/N\mathbb{Z}$ di ordine $\phi(N)$

FATTO Esiste un generatore mod p^n per ogni p dispari primo e $n \geq 1$.

• Se g genera mod p , allora g o $g+p$ generano mod p^2 .

Dim. Supponiamo che g generi modulo p ,
ma non modulo p^2 .

• $p-1 \mid \text{ord}_{p^2}(g)$ perché $\text{ord}_p(g) = p-1$

• $\text{ord}_{p^2}(g) \mid \phi(p^2) = p(p-1)$

$\rightarrow \text{ord}_{p^2}(g) = (p-1)$ oppure $p(p-1)$

Controlla se $g \not\equiv 1 \pmod{p^2}$ oppure no:

$$(g+p)^{p-1} \equiv g^{p-1} + \binom{p-1}{1} g^{p-2} \cdot p + \binom{p-1}{2} g^{p-3} p^2 + \dots \pmod{p^2}$$

$$\equiv 1 + \cancel{(p-1)g^{p-2}p} \pmod{p^2}$$

può fare 0 mod p^2 ? No.

$\rightarrow \text{ord}_{p^2}(g+p) = p(p-1)$
e quindi è un generatore!

• Prova g generatore mod p^2
 $\rightarrow g \equiv 1 + kp \pmod{p^3}$

Se $(k, p) = 1$
se $g^{p-1} = 1 + kp^2$,
 $g^{p-1} \equiv 1 \pmod{p^2}$

$p-1 \mid \text{ord}_{p^3}(g) \mid \phi(p^3) = p^2(p-1)$

$\downarrow$
 $\cancel{p-1}, p(p-1), p^2(p-1)$

$\uparrow$ perché è gen mod p^2

$\leftarrow$ Vogliamo dimostrare che è w_i

per dir. che non è w_i valgo $(g^{p-1})^{p-1} \not\equiv 1 \pmod{p^3}$

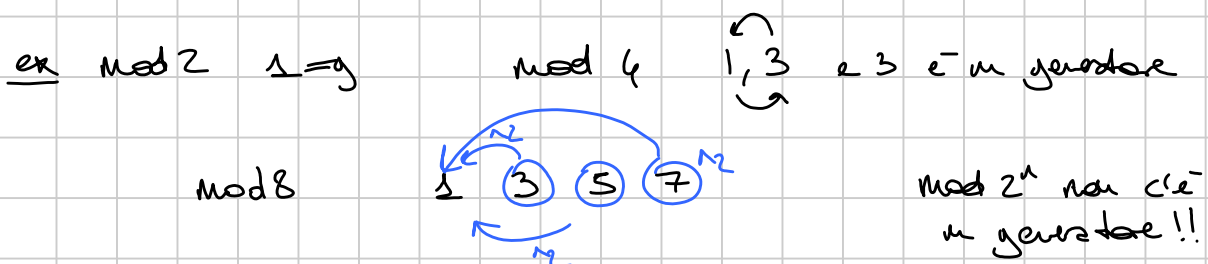
$$g^{p(p-1)} = (g^{p-1})^p = (1+kp)^p \equiv 1 + \binom{p}{1}kp + \binom{p}{2}k^2p^2 + \dots \pmod{p^3}$$

$$\equiv 1 + \boxed{kp^2} \not\equiv 0 \pmod{p^3}$$

perché se $k \neq 0$, allora $g^p \equiv 1 \pmod{p^2}$
e quindi non potrebbe generare $\pmod{p^3}$

• Ora se g genera $\pmod{p^3}$ allora $\pmod{p^4}$
 $g^p \equiv 1+kp \pmod{p^4}$ $(g^p)^{p^2} \equiv 1 \pmod{p^4}$
 e così via (formalizzare)
 per ind. 0

Oss Se g è un gen. $\pmod{p^2}$ è un gen. $\pmod{p^n}$ per ogni $n \geq 2$



Fatto c'è un gen. $\pmod{N}$ se solo se
 $N = 2, 4, p^n$ o $2p^n$ con p dispari e $n \geq 1$.

PROBLEMA n intero positivo, $p > n+1$ primo. Dimostrare che
 $p \mid 1^n + 2^n + 3^n + \dots + (p-1)^n$

Prendo g generatore modulo p .

$$\sum_{k=1}^{p-1} k^n = \sum_{k=0}^{p-2} (g^k)^n = 1 + g^n + g^{2n} + \dots + g^{(p-2)n} \pmod{p}$$

$$\equiv \frac{1 - g^{(p-1)n}}{1 - g^n} \equiv 0 \pmod{p}$$

$\neq 0$ per kp

PROBLEMA a, b interi coprimi

Ogni divisore ^{dispari} di $a^{2^n} + b^{2^n}$ è della forma $2^{u+1} \cdot m + 1$

Prendo p un primo dispari che divide $a^{2^n} + b^{2^n}$

n, m

OSSERVAZIONE SULLE POTENZE k -ESIME MODULO p

$g^a = g^b$? Dato a e b sono interi e g è una radice n -esima dell'unità
 $\Leftrightarrow a \equiv b \pmod{N}$

Potenze n -esime dell'1 sono quali? Quelli $a=0, \dots, N-1$

posso scrivere come $a \equiv 3k \pmod{N}$?

Se $(3, N) = 1$, $b \equiv \frac{1}{3} a \pmod{N}$

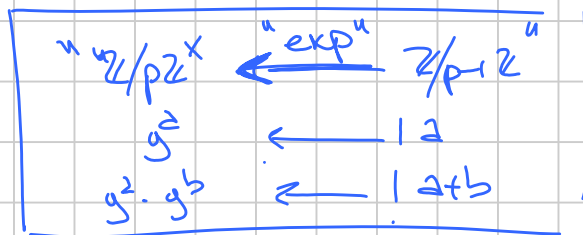
Se $(3, N) \neq 1$, sono tante parole
i multipli di 3 modulo N

$\{g^3, g^6, \dots\}$

E gli elementi di $(\mathbb{Z}/p\mathbb{Z})^\times$ si comportano come le radici $(p-1)$ dell'unità

$$g^a = g^b \Leftrightarrow a \equiv b \pmod{p-1}$$

le potenze k -esime $\Leftrightarrow$ i multipli di k
 in $(\mathbb{Z}/p\mathbb{Z})^\times$ modulo $p-1$



$$a^{2^n} + b^{2^n} \equiv 0 \pmod{p} \iff (a/b)^{2^n} \equiv -1 \pmod{p}$$

$$\text{ord}_p(a/b) \mid 2^{n+1} \text{ ma non } \mid 2^n$$

$$\implies \text{ord}_p(a/b) = 2^{n+1} \mid \phi(p) = p-1$$

$$\rightarrow p = 2^{n+1} \cdot m + 1$$

$$(2^{n+1}m_1 + 1)(2^{n+1}m_2 + 1) = 2^{n+1}(m_1 + m_2 + 2^{n+1}m_1m_2) + 1$$

PROBLEMA [BMO '14] Trovare tutte le 4-uple (a, b, c, d) di interi te

$$\frac{a^3 + 2b^3}{c^3 + 2d^3} = 2014 = 2 \cdot 19 \cdot 53$$

$$(a^3 + 2b^3) = 2014(c^3 + 2d^3)$$

• 1. $a/b \pmod{19}$ sono $6 = \frac{p-1}{3}$

Sono gli elementi di ordine che divide $6 = 18/3$

$$\sum_{d|6} \phi(d) = 6$$

• ~~$\begin{matrix} 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 8 & 7 & 4 & 7 \\ 1 & 8 & 7 & 4 & -18 & 12 \end{matrix}$~~

$$a^3 + 2b^3 \equiv 0 \pmod{19}$$

$$0 \mid 19/6$$

oppure

$$(a/b)^3 \equiv -2 \pmod{19}$$

$$(-2)^6 = 2^4 \cdot 2^2 = -3 \cdot 4 = -12 \not\equiv 1$$

$$\implies -2 \text{ non } \in \text{cubo}$$

→ se k non è coprimo con $p-1$

$$\frac{p-1}{\gcd(k, p-1)} = \frac{\phi(p)}{\gcd(k, \phi(p))} = 1$$

multiplo di $p-1$
se $a = g^k$

elementi

$$\neq 1$$

$$\text{ord}_p(a) \nmid \frac{p-1}{\gcd(k, p-1)}$$

$$\implies \mid (k, p-1)$$

$$19 \mid b \text{ e } 19 \mid d$$

$$a = 19a_1, b = 19b_1$$

$$19^2 a_1^3 + 2 \cdot 19^2 b_1^3 = 2 \cdot 53 (c^3 + 2d^3)$$

$$2 \cdot 53 (c^3 + 2d^3) \equiv 0 \pmod{19}$$

$$c \equiv d \equiv 0 \pmod{19}$$

$$c = 19c_1, d = 19d_1$$

$$19^2 a_1^3 + 2 \cdot 19^2 b_1^3 = 2 \cdot 53 \cdot 19^2 (c_1^3 + 2d_1^3)$$

Non ci sono soluzioni / INFINITA

LIFTING THE EXPONENT (LTE)

p primo. $v_p(n)$ è l'esponente di p nella fattorizzazione di n ,
 è quell'intero $N \in \mathbb{N}$ t.c. $p^N | n$ ma $p^{N+1} \nmid n$ ($p^N || n$)
 divide esattamente

Se scrivo n in base p ,

$v_p(n)$ è il numero di 0 con cui finisce n .

$$v_p(ab) = v_p(a) + v_p(b)$$

$$v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$$

Se $v_p(a) \neq v_p(b)$, allora ho $\ominus$

Lemma (LTE)

a, b interi distinti, p primo dispari che non divide a o b ,
 ma t.c. $p | a-b$. n intero positivo.

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

• Se n è dispari, vale ~~anche~~ $v_p(a^n + b^n) = v_p(a+b) + v_p(n)$ (e anche t.c. hp con il +)

• Se $p=2$:

• Se $4 | a-b$ allora vale LTE come sopra

• Se $2 || a-b$, allora $v_2(a^n - b^n) = v_2(a-b) + v_2(n) + v_2(n) - 1$

Dim. Procedendo per induzione mi basta fare il caso $n=q$ primo

$|q=p|$ oppure $|q \neq p|$

Ⓘ $(n,p)=1$

$$a^n - b^n = [(a-b) + b]^n - b^n$$

$$= \cancel{b^n} + \binom{n}{1} b^{n-1} (a-b) + \binom{n}{2} b^{n-2} (a-b)^2 + \dots$$

$$\underbrace{v_p(n) + v_p(b^{n-1}) + v_p(a-b)}_{\text{per I}} \quad \underbrace{v_p(\binom{n}{2}) + v_p(b^{n-2}) + 2v_p(a-b)}_{\text{per hp}}$$

$$v_p \geq 3v_p(a-b)$$

posso ignorare questo termine perché $v_p(\dots) > v_p(a-b)$

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

Ⓙ $n=q=p$

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

$$= \cancel{b^p} + p b^{p-1} (a-b) + \binom{p}{2} b^{p-2} (a-b)^2 + \binom{p}{3} b^{p-3} (a-b)^3 + \dots$$

$$\underbrace{v_p(p) + v_p(b^{p-1}) + v_p(a-b)}_{\substack{1 \\ \text{per I}}}$$

$$v_p \geq 3v_p(a-b) + \dots$$

$$v_p(\binom{p}{2}) + v_p(b^{p-2}) + 2v_p(a-b)$$

N

1 perché p è dispari

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

$$> 2v_p(a-b)$$

$$\Rightarrow v_p(2^p - b^p) = v_p(2 - b) + 1$$

0

$$(1, p) = 1$$

$$n = p$$

$$n = N \cdot p^m$$

come
con p

$$v_p(2^N - b^N) = v_p(2 - b)$$

"INDUZIONE"!

$$v_p(2^{Np} - b^{Np}) = v_p(2^N - b^N) + 1$$

$$v_p(2^{Np^2} - b^{Np^2}) = v_p(2^{Np} - b^{Np}) + 1$$

→ Se g generatore mod p^k , allora g generatore mod p^k $\forall k \geq 2$.

$$p \mid g^{p-1} - 1$$

$$\Rightarrow v_p(g^{p-1} - 1) = 1$$

$$\begin{aligned} \text{LTE} \rightarrow v_p(g^{p-1} - 1, p^k) &= v_p(g^{p-1} - 1) + v_p(p^k) \\ &= 1 + k = 1 + k \end{aligned}$$

$$\begin{aligned} p^{k+1} &\nmid (g^{p-1} - 1) \\ p^k &\nmid (g^{p-1} - 1) \end{aligned}$$

$$\text{ord}_{p^{k+1}}(g^{p-1}) = p^k$$

$$\rightarrow \text{ord}_{p^{k+1}}(g) = (p-1)p^k$$

$\Rightarrow g$ generatore modulo p^k

PROBLEMA Determinare il più grande intero k per cui

$$p = 2017$$

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

Ci sta dicendo di calcolare $v_p(\quad)$

$$v_p \left[(2016^{2017^{2018}} + 1) + (2018^{2017^{2016}} - 1) + 2017^{2016^{2018}} \right]$$

$$\text{LTE: } v_p(2016^{2017^{2018}} + 1) = v_p(2017) + v_p(2017^{2018}) = 2019$$

$$\text{LTE: } v_p(2018^{2017^{2016}} - 1) = v_p(2017) + v_p(2017^{2016}) = 2017$$

proprietà di v_p .

perché sono tutti diversi

$$\begin{aligned} &\ominus \min\{2016^{2018}, 2017, 2019\} \\ &\ominus = 2017 \end{aligned}$$

PROBLEMA Dimostrare che $\forall n$ intero positivo $\exists m$ (intero positivo) t.c.
 $7^n \mid 5^m + 3^m - 1$

$$v_7(5^m + 3^m - 1)$$

$$m=1 \rightarrow m=1 \checkmark$$

$$5+3-1=7$$

• Se LTE centrata qualcosa allora m deve essere una potenza di 7

$$5^m - 3^m - 1 + 4^m - 4^m$$

$$6^m - 2^m \cdot 3^m$$

$$\text{ord}_7(2) = 3$$

LTE
 mi serve
 m dispari
 (e $p=7$)

$$(5^m + 2^m) + (3^m + 4^m) - (1 + 2^m + 4^m)$$

$$v_p(5+2) + v_p(m)$$

$$v_p(3+4) + v_p(m)$$

$$v_p\left(\frac{8^m-1}{2^m-1}\right) = v_p(8^m-1) - v_p(2^m-1)$$

$$= v_p(7) + v_p(m) - 0$$

$$3 \nmid m \Rightarrow 0$$

$$\geq v_p(m) + 1$$

Scego $m = 7^{n-1}$ per ottenere la tesi per n.

LEMA (GUADAGNO DI PUNTO)

a, b interi positivi coprimi e $n > 1$ (non $a=b=1$)

Esiste un primo p che divide $a^n - b^n$ e che non divide $a-b$ tranne se $(n=2 \text{ e } a+b=2^k)$

Dim. • Ci basta dimostrare il contrario per un primo (per induzione)

• Supponiamo che il lemma sia falso:

Se $p \mid a^n - b^n$, allora $p \mid a-b$. APPLICHO LTE

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

$$\text{se } p=n, \text{ allora } v_p(a^n - b^n) = v_p(a-b) + 1$$

$$\text{se } p \neq n, \text{ allora } v_p(a^n - b^n) = v_p(a-b) + v_p(n)$$

Se $p=2$ e $p \mid a-b$

Se vale tutti i punti allora $\frac{a^n - b^n}{a-b} = n$ (*)

• Se $p=2 \neq n$, allora $v_2(a^n - b^n) = v_2(a-b) + v_2(n)$
 $p \nmid a-b$

$$\frac{a^n - b^n}{a-b} \neq n$$

$$2^{v_2(a+b)} \mid a+b$$

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

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

$$2^{v_2(a+b)} \mid a+b$$

$$2^{v_2(a+b)} \mid a+b$$

$$\sum 2^{\frac{1}{2}(a+b)} \frac{n-1}{2} + (?)$$

$$2^{\frac{1}{2}(a+b)+(n-2)} + 2^{\frac{1}{2}(a+b)+(n-4)} + \dots$$

$$2^{\frac{1}{2}(a+b)} (2^{n-2} + 2^{n-4} + \dots)$$

per induzione

$$2^{3-2} = 2 > 1$$

$n=2$

per (a,b) a $n=2$ ho $\frac{a^n - b^n}{a-b} = 2^{\frac{1}{2}(a+b)}$

$$\frac{a^2 - b^2}{a-b} = a+b$$

$n=4$

$$\frac{a^4 - b^4}{a-b} = (a+b)(a^2 + b^2) = 4 \cdot 2^{\frac{1}{2}(a+b)-1}$$

potenza di 2
 $\Rightarrow = 2$

PROBLEMA Trovare tutte le terne di interi positivi a, b, c di
 $a^7 + b^7 = 7^c$

Per il lemma GCD $a^7 + b^7$ ha un ^{fattore} primo che $a+b$ non aveva

$$(a+b) \left(\frac{a^7 + b^7}{a+b} \right) = 7^c$$

$$\parallel \quad \parallel$$

$$7^\alpha \quad 7^\beta$$

$$7 \mid a \Rightarrow 7 \mid b$$

Cerco una soluzione
con $(a,b)=1$

$$7 \mid a+b \text{ perché } a+b > 1$$

$$\alpha + \beta = \frac{1}{7}(a^7 + b^7) = \frac{1}{7}(a+b) + 1 = \alpha + 1$$

$$\Rightarrow \beta = 1$$

$$\frac{a^7 + b^7}{a+b} = 7$$

$$a^7 + b^7 = 7a + 7b$$

$$(a^7 \geq 7a) \Leftrightarrow a^6 \geq 7$$

$$\Leftrightarrow a \geq \sqrt[6]{7}$$

$$\Leftrightarrow a \geq 2$$

$$b=1$$

$$a^7 + 1 > 7a + 7$$

$a^7 \geq 7a + 6$ vero per induzione!

