RIPASSO; PRIMI ESERCIZI SUI GRUPPI

Note Title 11/9/2017

CONGRUENZE ESPONENZIALI

Modulo primo (o potenza di primo DISPARI)

$x^a \equiv 1 \mod p$

Quante soluzioni? Stiamo lavorando in $(\mathbb{Z}/p\mathbb{Z})^\times$ $(a, \varphi(p))$

FATTO $(\mathbb{Z}/p\mathbb{Z})^\times$ è CICLICO, ovvero

$$\left((\mathbb{Z}/p\mathbb{Z})^\times, \cdot \right) \simeq \left(\mathbb{Z}/(p-1)\mathbb{Z}, + \right)$$

Esempio $\left((\mathbb{Z}/5\mathbb{Z})^\times, \cdot \right)$ $\{1, 2, 3, 4\}$

$2^0 \equiv 1\ (5) \qquad 2^1 \equiv 2\ (5) \qquad 2^2 \equiv 4\ (5) \qquad 2^3 \equiv 3\ (5)$

$4 \cdot 3 = 2^2 \cdot 2^3 \equiv 2^{2+3}$

Gli esponenti "genuinamente diversi" sono
0, 1, 2, 3

FATTO $\Longleftrightarrow$ "esiste un generatore modulo p",

ovvero posso scegliere $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ t.c.

ogni $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ si scrive come g^i per qualche intero i. Questo i è ben definito in $\mathbb{Z}/(p-1)\mathbb{Z}$.

$$\underbrace{\mathrm{ord}_p(g)}_{\mathrm{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(g)} = p-1$$

L'equazione $x^a \equiv 1 \mod p$ è allora equivalente a

$$(g^i)^a \equiv 1 \mod p$$

$$\iff g^{ia} \equiv 1 \mod p$$

$$\iff \mathrm{ord}_p(g) \mid ia$$

$$\iff (p-1) \mid i \cdot a$$

φ(modulo)

$$\iff a i \equiv 0 \mod (p-1)$$

$$\iff \frac{a}{(a,p-1)} \cdot (a,p-1) \cdot i \equiv 0 \quad (p-1)$$

$$\iff \frac{a}{(a,p-1)} i \equiv 0 \mod \left(\frac{p-1}{(p-1,a)}\right)$$

coprimi

$$\iff i \equiv 0 \mod \left(\frac{p-1}{(p-1,a)}\right)$$

Il numero di soluzioni di questa congruenza che rispettino $\boxed{1 \le i \le p-1}$ e'

$$\frac{p-1}{(p-1)/(p-1,a)} = (a, p-1)$$

i miei x iniziali si scrivono come g^i, in modo unico se impongo $1 \le i \le p-1$

ESEMPIO $\quad x^3 \equiv 1 \mod 7$

$$\# \text{ soluzioni} = (3, 7-1) = 3$$

$g = 3 \qquad ord_7(3) = 6 : \quad 3^2 \equiv 2 \not\equiv 1 \ (7)$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad 3^3 \equiv -1 \not\equiv 1 \ (7)$

$$3^{3a} \equiv 1 \ (7) \iff 3a \equiv 0 \ (6)$$

$$\iff a \text{ pari}$$

Soluzioni : $\quad x = 3^a$, a pari, $0 \le a \le 5$

$$x \equiv 1 \ (7), \quad x \equiv 2 \ (7), \quad x \equiv 4 \ (7)$$

ESEMPIO 2 $\quad x^a \equiv 1 \mod 9 \quad$ (a param)

- $(x, 9) = 1$, altrimenti NO SOLUZIONI
- Ci sono $(a, \varphi(9)) = (a, 6)^{=d}$ soluzioni

- 4 casi: $d = 1, 2, 3, 6$

$d=1 \downarrow$ $x \equiv 1\ (9)$ ed è l'unica

$d=2 \downarrow$ $x \equiv \pm 1\ (9)$

$d=6 \rightarrow$ $(x, 9) = 1$

Caso $d = 3$: le 3 soluzioni sono

$\rightarrow$ i quadrati $(1, 4, 7)$

(se $x \equiv k^2$, $x^3 \equiv k^6 \equiv 1\ (9)$)

$\rightarrow$ i congrui a 1 modulo 3

(se $x^3 \equiv 1\ (9)$, allora $x^3 \equiv 1\ (3)$

$\Rightarrow x \equiv 1\ (3)$, e ci sono

esattamente 3 classi di resto

modulo 9 che sono $\equiv 1\ (3)$)

Radici quadrate: commenti

$$x^2 \equiv 77 \mod 103$$

Criterio di Eulero Sia $p \neq 2$ un primo.

Allora $a \in (\mathbb{Z}/_p\mathbb{Z})^\times$ è un quadrato modulo $p \iff a^{\frac{p-1}{2}} \equiv 1 \mod p$

DIM. $\boxed{\Rightarrow}$ Se $a \equiv b^2 \mod p$, allora

$$a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \underset{FLT}{\equiv} 1 \quad (p)$$

$\boxed{\Leftarrow}$ Consideriamo il polinomio

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

L'eqz. $q(x) \equiv 0 \mod p$ ha al più $\deg q = \frac{p-1}{2}$ soluzioni

Le conosciamo: sono i quadrati!

Tutti gli altri numeri modulo p, quindi, non sono soluzioni, ovvero: a non quadrato

$$\Rightarrow \quad a^{\frac{p-1}{2}} - 1 \not\equiv 0 \quad (p)$$ □

Oss $y = x^{\frac{p-1}{2}} \in \{1, -1\}$. Infatti

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

$\Rightarrow \quad y = \pm 1$

TRUCCO Supponiamo $p \equiv 3 \mod 4$.

Supponiamo anche x sia quadrato mod p.

Sia $y = x^{\frac{p+1}{4}}$. Allora

$$y^2 \equiv x^{\frac{p+1}{2}} \equiv x^{\frac{p-1}{2}+1}$$

$$\equiv \begin{cases} x, & \text{se } x^{\frac{p-1}{2}} \equiv 1\ (p) \\ -x, & \text{se } x^{\frac{p-1}{2}} \equiv -1\ (p) \end{cases}$$

Siccome x e' un quadrato $\equiv x$

ESEMPIO $x^2 \equiv 7 \mod 19$

Siccome $19 \equiv 3 \mod 4$, se esiste una rad. quadr. di 7 essa e' data da

$$7^{\frac{19+1}{4}} \equiv 7^5 \equiv 7^2 \cdot 7^2 \cdot 7$$

$$\equiv 11 \cdot 11 \cdot 7$$

$$\equiv 11 \mod 19$$

Per sapere se 7 sia o meno un quadrato basta

Calcolare $11^2 \equiv (-8)^2 \equiv 64 \equiv 7 \mod 19$

Una proprietà della ϕ di Eulero

$$m \mid n \implies \phi(m) \mid \phi(n)$$

Per il teorema di fattorizzazione unica possiamo scrivere $m = p_1^{e_1} \cdots p_k^{e_k}$ con i p_i primi distinti e gli esponenti $e_i \geq 1$

La condizione $m \mid n$ implica che la fattorizzazione in primi di n è della forma

$$n = p_1^{f_1} \cdots p_k^{f_k} q_1^{h_1} \cdots q_r^{h_r}$$

con
- $f_i \geq e_i$ per $i = 1, \dots, k$
- q_j primi distinti fra loro e dai p_i
- $r \geq 0$
- $h_i \geq 1$

Calcoliamo $\phi(m) = (p_1 - 1) p_1^{e_1 - 1} \cdots (p_k - 1) p_k^{e_k - 1}$

e $\quad \phi(n) = (p_1 - 1) p_1^{f_1 - 1} \cdots (p_k - 1) p_k^{f_k - 1} \times$

$$\times (q_1 - 1) q_1^{h_1 - 1} \cdots (q_r - 1) q_r^{h_r - 1}$$

Allora $\quad \dfrac{\phi(n)}{\phi(m)} = p_1^{f_1 - e_1} \cdots p_k^{f_k - e_k} (q_1 - 1) q_1^{h_1 - 1} \cdots (q_r - 1) q_r^{h_r - 1}$

è intero perché ogni f_i è

$\geq$ del corrispondente e_i

$\Longrightarrow \phi(m) \mid \phi(n)$

Idea pericolosa. Scrivo $n = md$ e calcolo

$$\phi(n) = \phi(m)\,\phi(d)$$

Questo non funziona, perché la moltiplicatività della ϕ vale solo se $(d, m) = 1$

BOTANICA: GRUPPI DI ORDINE PICCOLO

Sia G un gruppo

* $|G| = 1$ $\qquad G = \{id\}$ $\qquad id \cdot id = id$

* $|G| = 2$ $\qquad G = \{id, a\}$

	id	a
id	id	a
a	a	id

$G = (\mathbb{Z}/2\mathbb{Z}, +)$ $\qquad id = 0$ $\qquad a = 1$

$G = (\{\pm 1\}, \cdot)$ $\qquad id = 1$ $\qquad a = -1$

$G = (\{$rotazioni di $0°, 180°\}$, composizione$)$

* $|G| = 3$ $\qquad (|G| = $ primo$)$

$G = \{id, a, b\}$ $\qquad a \cdot a = \begin{cases} id \\ a \\ b \end{cases}$

Ma $a \cdot a = a \Rightarrow a = id$, NO

$a \cdot a = id \Rightarrow ord(a) = 2$, ma

l'ordine di ogni elemento deve

dividere $|G| = 3$ (Lagrange)

Per esclusione, $a \circ a = b$

: esistenza dell'inverso di a, oppure $a \circ b = a \circ a \circ a = id$

	id	a	b
id	id	a	b
a	a	b	id
b	b	id	a

INVERSI A SX E DX

Supponiamo che $a \circ b = id$ e $c \circ a = id$

$$c \circ (a \circ b) = c \circ a \circ b = (c \circ a) \circ b = id \circ b = b$$

$$\begin{aligned} &\| \\ &c \circ id = c \end{aligned} \Rightarrow \boxed{b = c}$$

Ovvero: inverso SX e DX coincidono! (in OGNI gruppo)

$$G = (\mathbb{Z}/_3\mathbb{Z}, +)$$

$$G = \left(\left\{ \begin{array}{l} \text{rotazioni di } 120°, \\ 240°,\ 0° \text{ nel piano} \end{array} \right\}, \text{ composizione} \right)$$

$$G = \left(\left\{ \begin{array}{l} \text{radici } 3^e \\ \text{dell'unità} \end{array} \right\}, \cdot \right)$$

E se $|G| =$ primo?

Sia $a \in G$, $a \neq id$. Allora G contiene il sottogruppo CICLICO generato da a, chiamiamolo H. Da una parte $|H| \mid |G| = p$, e $|H| \geq 2 \Rightarrow |H| = p \Rightarrow G = H$; dall'altra, $H \simeq \mathbb{Z}/p\mathbb{Z}$

(Isomorfo: $G \simeq H$ se esiste $\varphi : G \longrightarrow H$ bigezione tale che $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$)

prodotto in G — prodotto in H

$$H = \{ id, a, a^2, \dots, a^{p-1} \}$$

$\wr\!\!\downarrow$ "prendere l'esponente"

$$\mathbb{Z}/p\mathbb{Z} = \{ 0, 1, 2, \dots, p-1 \}$$

* $|G| = 4$. Se G contiene un elemento di ordine 4 è ciclico $\Rightarrow G \simeq \mathbb{Z}/4\mathbb{Z}$.

Altrimenti ogni elemento $\neq id$ ha ordine

2 (l'ordine $\mid 4$, è $= 1$ solo per id,

e non è 4 per ipotesi)

FATTO Sia G un gruppo in cui $g^2 = id$ per ogni $g \in G$. Allora G è abeliano.

DIM $(ab)^2 = id \Rightarrow abab = id$

$a^{-1} = a \quad b^{-1} = b$

$$ababb^{-1} = id \cdot b^{-1}$$
$$\Downarrow$$
$$aba = b$$
$$\Downarrow$$
$$a \cdot b \cdot a \cdot a^{-1} = b \cdot a^{-1}$$
$$\Downarrow$$
$$\boxed{a \cdot b = b \cdot a}$$

Questo vale per ogni a, b, quindi G è abeliano

$|G| = 4 \qquad G = \{id, a, b, c\}$

$a \cdot b = \cancel{id}$, $\cancel{a}$, $\cancel{b}$, c

	id	a	b	ab
id	id	a	b	ab
a	a	id	ab	b
b	b	ab	id	a
ab	ab	b	a	id

$$G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$(0, 0)$

$a = (0, 1)$

$b = (1, 0)$

$c = (1, 1)$

$$G = \left\{ \begin{array}{l} id, \ \text{riflessione } \longleftrightarrow \\ \text{riflessione } \updownarrow, \ \text{riflessione} \end{array} \right\}$$