I19L5

martedì 5 marzo 2019 10:30

G. PARMEGGIANI 5/3/2019

ALGEBRA E MATEMATICA DISCRETA (parte di Algebra)

Corso di Laurea: Informatica

QUANTI SONO GLI ELEMENTI INVERTIBILI IN $\mathbb{Z}_n$?

Tanti quanti sono i numeri a con

$$\begin{cases} 0 \leq a < n \\ MCD(a,n)=1 \end{cases}$$

Abbiamo finito l'ultima lezione dicendo che

se $n = 10$,

0

$\boxed{1}$

2

$\boxed{3}$

4

5

6

$\boxed{7}$

8

$\boxed{9}$

COPRIMI CON 10, E QUINDI INVERTIBILI MODULO 10

per cui gli invertibili in $\mathbb{Z}_n$ sono 4. In generale,

La FUNZIONE DI EULERO φ "conta" gli invertibili in $\mathbb{Z}_n$:

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$$

è definita da: $\varphi(n) =$ il numero dei naturali k tali che $\begin{cases} 0 \leq k < n \\ MCD(k,n)=1 \end{cases}$

Se p è un numero primo positivo allora $\varphi(p) = p-1$

In generale se $n \in \mathbb{N}$ e

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

è una fattorizzazione di n, dove $p_1, p_2, \dots, p_k$ sono primi distinti e $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$ con $\alpha_i > 0 \ \forall i = 1, \dots, k$

allora $$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

ESEMPIO $\varphi(5) = 5-1 = 4$ $\quad \left(\varphi(5) = 5\left(1-\frac{1}{5}\right) = 5\left(\frac{5-1}{5}\right) = \cancel{5}\cdot\frac{4}{\cancel{5}} = 4 \right)$

$\varphi(10) = \dots$ $\Rightarrow \varphi(10) = 10\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) =$

$10 = 2\cdot 5$ $\quad = \cancel{10}^{\,5}\cdot\frac{1}{\cancel{2}}\cdot\frac{4}{\cancel{5}} = 4$

$\varphi(20) = \dots$ $\Rightarrow \varphi(20) = 20\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) =$

$20 = 2^2\cdot 5$ $\quad = \cancel{20}^{\,\cancel{10}\,2}\cdot\frac{1}{\cancel{2}}\cdot\frac{4}{\cancel{5}} = 8$

$$\varphi(2^4\cdot 3^2\cdot 7^3) = 2^4\cdot 3^2\cdot 7^3\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right) = \dots$$

QUINDI IN NUMERO DEGLI ELEMENTI INVERTIBILI IN $\mathbb{Z}_n$ È $\varphi(n)$.

PER CASA: ESERCIZIO 1 (file: I19 casa T2.pdf)

SISTEMI DI CONGRUENZE

Un sistema di congruenze è

$$\begin{cases} a_1 x \equiv c_1 \mod m_1 \\ a_2 x \equiv c_2 \mod m_2 \\ \vdots \\ a_k x \equiv c_k \mod m_k \end{cases}$$

dove $a_i, c_i \in \mathbb{Z}$, $i = 1, \dots, k$

$m_i \in \mathbb{N}$, $m_i > 0$, $i = 1, \dots, k$

"Risolvere" il sistema significa

- dire se ha oppure no soluzioni
- nel caso le abbia, trovarle tutte

Un $x_0 \in \mathbb{Z}$ è UNA SOLUZIONE del sistema se è CONTEMPORANEAMENTE SOLUZIONE DI OGNI CONGRUENZA del sistema

NB1 : se una congruenza del sistema non ha soluzioni, il sistema non ha soluzioni

NB2 : Anche se tutte le congruenze del sistema hanno soluzioni, non è detto che il sistema abbia soluzioni

Ad Esempio: $\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 0 \bmod 6 \end{cases}$ non ha soluzioni (anche se entrambe le congruenze hanno soluzioni)

Il seguente teorema dà una condizione SUFFICIENTE affinché PARTICOLARI sistemi di congruenze abbiano soluzioni

più precisamente sistemi in cui $a_i = 1 \ \forall i = 1, \dots, k$
ossia sistemi in cui tutte le congruenze sono già risolte

TEOREMA CINESE DEI RESTI

Dati $n_1, n_2, \dots, n_k \in \mathbb{N}$, $n_i > 0$ $\quad i = 1, \dots, k$
A DUE A DUE COPRIMI (ossia tali che $MCD(n_i, n_j) = 1 \ \forall i \neq j$)

$\forall b_1, b_2, \dots, b_k \in \mathbb{Z}$ si ha che
$\exists$ INFINITE soluzioni intere del sistema di congruenze

$$\begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \\ \vdots \\ x \equiv b_k \bmod n_k \end{cases}$$

Esse stanno tutte nella stessa classe di congruenza modulo

$$n = n_1 \cdot n_2 \cdot \dots \cdot n_k$$

NB3 La condizione che gli n_i sono a due a due coprimi non è una condizione necessaria affinché un sistema di congruenze abbia soluzioni

ESEMPIO 1 $\quad n_1 = n_2 = 7 \quad \begin{cases} 5x \equiv 3 \bmod 7 \\ 3x \equiv 6 \bmod 7 \end{cases}$

Le soluzioni: tutti gli interi in $[2]_7$

ESEMPIO 2 $\quad n_1 = 2,\ n_2 = 4 \quad \begin{cases} x \equiv 0 \bmod 2 \\ x \equiv 2 \bmod 4 \end{cases}$

ha soluzione: tutti gli interi in $[2]_4$

Giustifichiamo con $k=2$ (due congruenze):

$\begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \end{cases}$ CON L'IPOTESI $MCD(n_1, n_2) = 1$. chiamo $\begin{cases} Ⓐ \text{ la } 1^a \text{ congruenza} \\ Ⓑ \text{ la } 2^a \text{ "} \end{cases}$

1° MODO (METODO DI NEWTON)

I) Chiamo $x_1 = b_1$ (è una particolare soluzione di Ⓐ)

II) Cerco $t_2 \in \mathbb{Z}$ tale che $x_1 + t_2 n_1 = x_2$ sia soluzione di Ⓑ:

che chiamo

$$b_1 + t_2 n_1 \equiv b_2 \bmod n_2$$
$$\Rightarrow t_2 n_1 \equiv (b_2 - b_1) \bmod n_2$$

(sto facendo i conti in $\mathbb{Z}_{n_2}$:

$[b_1 + t_2 n_1]_{n_2} = [b_2]_{n_2}$

$\quad ||$

$[b_1]_{n_2} + [t_2 n_1]_{n_2}$

$\Rightarrow [t_2 n_1]_{n_2} = [b_2]_{n_2} - [b_1]_{n_2}$

$\quad = [b_2 - b_1]_{n_2}$)

III) x_2 E' UNA SOLUZIONE DEL SISTEMA

IV) Per il teorema cinese dei resti, l'insieme di tutte le soluzioni del sistema è:

$$[x_2]_n = \{x_2 + kn \mid k \in \mathbb{Z}\} \text{ dove } n = n_1 \cdot n_2$$

ESEMPIO $\quad \begin{cases} x \equiv 4 \bmod 6 \\ x \equiv 3 \bmod 5 \end{cases}$ $\quad$ ($6 \to n_1$, $5 \to n_2$) $\quad MCD(n_1, n_2) = MCD(6,5) = 1$

Posso allora applicare il teorema cinese dei resti: il sistema ha infinite soluzioni intere, tutte in un'unica classe di congruenza modulo $n = n_1 \cdot n_2 = 6 \cdot 5 = 30$

I) chiamo $x_1 = 4$

II) Cerco $t_2 \in \mathbb{Z}$ tale che $x_1 + t_2 n_1 = x_2$ sia soluzione

che chiamo

di $x \equiv 3 \bmod 5$, ossia cerco $t_2 \in \mathbb{Z}$ tale che

$$4 + t_2 \cdot 6 \equiv 3 \bmod 5$$

$$6t_2 \equiv 3-4 \bmod 5$$

$$6t_2 \equiv -1 \bmod 5$$

$[6]_5 = [1]_5$ $\qquad$ $[-1]_5 = [4]_5$

$$t_2 \equiv 4 \bmod 5$$

$\boxed{III}$ Prendo ad esempio $t_2 = 4$, per cui

$$x_2 = x_1 + t_2 m_1 = 4 + 4 \cdot 6 = 4 + 24 = 28$$

$\boxed{IV}$ $x_2 = 28$ è una soluzione del sistema, e per il teorema cinese dei resti le soluzioni del sistema sono tutti e soli gli elementi dell'insieme

$$[x_2]_m = [28]_{30} = \{28 + 30k \mid k \in \mathbb{Z}\}$$

PER CASA: PUNTO 1) DELL'ESERCIZIO 2 (file I19casaT2.pdf)

---

se $K = 3$ (3 CONGRUENZE)

$$\begin{cases} x \equiv b_1 \bmod m_1 & \leftarrow \text{(A)} \\ x \equiv b_2 \bmod m_2 & \leftarrow \text{(B)} \\ x \equiv b_3 \bmod m_3 & \leftarrow \text{(C)} \end{cases}$$

CON L'IPOTESI:

$$\boxed{\begin{array}{l} MCD(m_1, m_2) = 1 \\ MCD(m_1, m_3) = 1 \\ MCD(m_2, m_3) = 1 \end{array}}$$

Trovata una soluzione x_3, tutte le soluzioni sono gli elementi dell'insieme

$$[x_3]_m = \{x_3 + mk \mid k \in \mathbb{Z}\}$$

dove $n = n_1 \cdot n_2 \cdot n_3$

PER TROVARE x_3 :

$\boxed{I}$ Chiamo $x_1 = b_1$, è una soluzione di (A)

$\boxed{II}$ cerco $t_2 \in \mathbb{Z}$ tale che $x_1 + t_2 \cdot n_1 = x_2$ sia

che chiamo

soluzione di (B)

$\boxed{III}$ allora x_2 è soluzione sia di (A) che di (B)

$\boxed{IV}$ cerco $t_3 \in \mathbb{Z}$ tale che $x_2 + t_3 \cdot (n_1 \cdot n_2) = x_3$ sia

che chiamo

soluzione di (C)

$\boxed{V}$ x_3 È UNA SOLUZIONE DEL SISTEMA

$\boxed{VI}$ Per il teorema cinese dei resti, l'insieme delle soluzioni del sistema è:

$$[x_3]_n = \{x_3 + nk \mid k \in \mathbb{Z}\} \text{ dove } n = n_1 \cdot n_2 \cdot n_3$$

ESEMPIO

$$\begin{cases} x \equiv \underset{b_1}{10} \mod \underset{n_1}{11} & \leftarrow (A) \\ x \equiv \underset{b_2}{5} \mod \underset{n_2}{6} & \leftarrow (B) \\ x \equiv \underset{b_3}{5} \mod \underset{n_3}{7} & \leftarrow (C) \end{cases}$$

MCD $(11,6)=1$
MCD $(11,7)=1$ $\Rightarrow$ $\exists\ \infty$ soluzioni, tutte nella stessa classe di congruenza modulo
MCD $(6,7)=1$

$$n = n_1 \cdot n_2 \cdot n_3 = 11 \cdot 6 \cdot 7 = 66 \cdot 7 = 462$$

$\boxed{I}$ $x_1 = 10$

$\boxed{II}$ cerco $t_2 \in \mathbb{Z}$ tale che $x_1 + t_2 n_1 = x_2$ sia

soluzione di (B) : $x \equiv 5 \mod 6$

allora $t_2 \in \mathbb{Z}$ è tale che $10 + t_2 \cdot 11 \equiv 5 \mod 6$

$$11 t_2 \equiv 5 - 10 \mod 6$$

$$11 t_2 \equiv -5 \mod 6$$

$[11]_6 = [5]_6$ $\qquad$ $[-5]_6 \equiv [1]_6$

$$5 t_2 \equiv 1 \mod 6$$

$MCD(5,6) = 1 \underset{\text{Bezout}}{\Rightarrow}$ $1 = 6 - 5 = 6 + 5 \cdot \underbrace{\boxed{(-1)}}_{t_2}$

siccome sto facendo i conti modulo 6,

e $[-1]_6 = [5]_6$ ottengo $t_2 = 5$

quindi $x_2 = x_1 + t_2 n_1 = 10 + 5 \cdot 11 = 10 + 55 = 65$

$\boxed{III}$ Cerco $t_3 \in \mathbb{Z}$ tale che

$x_3 = x_2 + t_3 \cdot n_1 \cdot n_2$ ha soluzione di (C) :

$$65 + t_3 \cdot 11 \cdot 6 \equiv 5 \mod 7$$

facendo i conti in $\mathbb{Z}_7$

$$66t_3 \equiv 5-65 \mod 7$$

$$66t_3 \equiv -60 \mod 7$$

$[66]_7 = [66-63]_7 = [3]_7$

$[-60]_7 = [-60+63]_7 = [3]_7$

$$3t_3 \equiv 3 \mod 7$$

$$\Downarrow$$

prendo $t_3 = 1$ e ottengo

$$x_3 = x_2 + t_3 \cdot n_1 \cdot n_2 = 65 + 1 \cdot 11 \cdot 6 = 65 + 66 = 131$$

$\boxed{IV}$ $x_3 = 131$ è una soluzione del sistema (infatti: $131 \equiv 10 \mod 11$, $131 \equiv 5 \mod 6$, $131 \equiv 5 \mod 7$)

$\boxed{V}$ l'insieme di tutte le soluzioni del sistema è

$$\{131 + 462k \mid k \in \mathbb{Z}\}$$

PER CASA: PUNTO 2) DELL'ESERCIZIO 2
(file: I19 casa T2.pdf)

In generale: se $k \geq 4$ e

$$\begin{cases} x \equiv b_1 \bmod n_1 & (1) \\ x \equiv b_2 \bmod n_2 & (2) \\ \vdots \\ x \equiv b_k \bmod n_k & (k) \end{cases}$$

con $MCD(n_i, n_j) = 1 \ \forall i \neq j$

itero il procedimento:

- $x_1 = b_1$ è una soluzione di (1)
- impongo che $x_1 + n_1 t_2 = x_2$ sia soluzione di (2) (cerco $t_2 \in \mathbb{Z}$ tale che, ...) ALLORA x_2 È SOLUZIONE SIA DI (1) CHE DI (2)
- impongo che $x_2 + n_1 \cdot n_2 t_3 = x_3$ sia soluzione di (3) (cerco $t_3 \in \mathbb{Z}$ tale che ...) ALLORA x_3 È SOLUZIONE SIA DI (1), CHE DI (2), CHE DI (3)
- impongo che $x_3 + n_1 \cdot n_2 \cdot n_3 t_4 = x_4$ sia soluzione di (4) (cerco $t_4 \in \mathbb{Z}$ tale che ...) ALLORA x_4 È SOLUZIONE DI (1), DI (2), DI (3) E DI (4)

⋮

trovo x_k che è una soluzione di tutte e k le congruenze.

Per il teorema cinese dei resti, l'insieme delle soluzioni del sistema è l'insieme dei numeri interi nella classe di congruenza

$$[x_k]_n = \{x_k + nt \mid t \in \mathbb{Z}\} \text{ dove } n = n_1 \cdot n_2 \cdot n_3 \cdot \ldots \cdot n_k$$