C. PARMEGGIANI 11/3/2019

ALGEBRA E MATEMATICA DISCRETA (parte di Algebra)

Corso di Laurea: Informatica

SVOLGIMENTO DEGLI ESERCIZI PER CASA 2 (1^a PARTE)

$\boxed{1}$ Si calcoli il numero degli elementi invertibili di $\mathbb{Z}_n$ per i seguenti n:

1) $n=3$
2) $n=6$
3) $n=9$
4) $n=12$
5) $n=84$
6) $n=7^2\cdot 2^5$

Il numero degli elementi invertibili di $\mathbb{Z}_n$ è $\varphi(n)$, e

1) se $n=3$ è $\varphi(n)=\varphi(3)=3-1=2$;

2) se $n=6=2\cdot 3$ è $\varphi(n)=\varphi(6)=6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=\cancel{6}^{\,2}\cdot\frac{1}{\cancel{2}}\cdot\frac{\cancel{2}}{\cancel{3}}=2$

3) se $n=9=3^2$ è $\varphi(n)=\varphi(9)=9\left(1-\frac{1}{3}\right)=\cancel{9}^{\,3}\cdot\frac{2}{\cancel{3}}=6$

4) se $n=12=2^2\cdot 3$ è $\varphi(n)=\varphi(12)=12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=$

$=\cancel{12}^{\,4}\cdot\frac{1}{\cancel{2}}\cdot\frac{\cancel{2}}{\cancel{3}}=4$

5) se $n=84=2^2\cdot 3\cdot 7$ è $\varphi(n)=\varphi(84)=84\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)=$

$$\begin{array}{r|l} 84 & 2 \\ 42 & 2 \\ 21 & 3 \\ 7 & 7 \end{array}$$

$=\cancel{84}^{\,12}\cdot\frac{1}{\cancel{2}}\cdot\frac{\cancel{2}}{\cancel{3}}\cdot\frac{\cancel{6}^{\,2}}{\cancel{7}}=12\cdot 2=24$

6) se $n=7^2\cdot 2^5$ è $\varphi(n)=\varphi(7^2\cdot 2^5)=7^2\cdot 2^5\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{7}\right)=$

$=7^{\cancel{2}}\cdot 2^5\cdot\frac{1}{\cancel{2}}\cdot\frac{\cancel{6}^{\,3}}{\cancel{7}}=7\cdot 2^5\cdot 3$

2 ① Si risolva il sistema $\begin{cases} x \equiv 2 \bmod 6 \\ x \equiv 10 \bmod 25 \end{cases}$ ($b_1 = 2$, $n_1 = 6$, $b_2 = 10$, $n_2 = 25$)

Poiché $MCD(n_1, n_2) = MCD(6, 25) = 1$, per il teorema cinese dei resti il sistema ha infinite soluzioni intere, tutte nella stessa classe di congruenza modulo $n = n_1 \cdot n_2 = 6 \cdot 25 = 150$

Cerchiamo una particolare soluzione x_0.

1° modo

$x_1 = 2$

$x_2 = x_1 + t_2 n_1$ cerco $t_2 \in \mathbb{Z}$ t.c.

$x_1 + t_2 n_1 \equiv 10 \bmod 25$

$2 + t_2 \cdot 6 \equiv 10 \bmod 25$

$6 t_2 \equiv 8 \bmod 25$ ($a = 6$, $b = 8$, $n = 25$)

$MCD(a, n) = 1 \Rightarrow \exists \alpha, \beta \in \mathbb{Z} \mid \alpha a + \beta n = 1 \Big\} \Rightarrow t_2 = \alpha q$

$b = qd \underset{\substack{\uparrow \\ d=1}}{=} q \Rightarrow q = 6$

$25 = 6 \cdot 4 + 1 \Rightarrow 1 = 25 + 6 \cdot (-4)$

($n = 25$, $a = 6$, $q_1 = 4$, $r_1 = 1$; $d = 1$, $n = 25$, $a = 6$, $\alpha = -4$)

$\Rightarrow t_2 = \alpha \cdot q = (-4) \cdot 8 = -32 \bmod n_2 = 25$

$[-32]_{25} = [-32 + 25]_{25} = [-7]_{25} = [18]_{25}$

Prendo $t_2 = 18$

e ottengo $x_2 = x_1 + t_2 \cdot n_1 = 2 + 18 \cdot 6 = 2 + 108 = 110$

x_2 è la x_0 che cercavo: le soluzioni del sistema sono tutti gli interi nella classe di congruenza

$$[x_2]_n = [110]_{150} = \{110 + 150k \mid k \in \mathbb{Z}\}$$

$\boxed{2° \text{ modo}}$

$$\begin{cases} x \equiv 2 \mod 6 \\ x \equiv 10 \mod 25 \end{cases}$$

b_1, n_1, n_2, b_2

$MCD(n_1, n_2) = 1 \Rightarrow \exists \alpha_1, \alpha_2 \in \mathbb{Z} \mid \quad \alpha_1 n_1 + \alpha_2 n_2 = 1$

e $\quad z = b_2 \alpha_1 n_1 + b_1 \alpha_2 n_2$ è una soluzione del sistema

$n_1 = 6$
$n_2 = 25$ $\Rightarrow$ $25 = 6 \cdot 4 + 1 \Rightarrow 1 = 25 \cdot 1 + 6 \cdot (-4)$

n_2, n_1, q_1, r_1 $\qquad$ n_2, α_2, n_1, α_1

$$\begin{aligned} z &= 10 \cdot (-4) \cdot 6 + 2 \cdot 1 \cdot 25 = \\ &= (-40) \cdot 6 + 50 = \\ &= -240 + 50 = \\ &= -190 \end{aligned}$$

L'insieme delle soluzioni del sistema è l'insieme degli interi nella classe di congruenza

$$[z]_n = [-190]_{150} = [-190 + 150 \cdot 2]_{150} = [110]_{150} = \{110 + 150k \mid k \in \mathbb{Z}\}$$

$\boxed{2}$ 2

$$\begin{cases} x \equiv 2 \mod 4 \\ x \equiv 6 \mod 7 \\ x \equiv 7 \mod 9 \end{cases}$$

b_1, n_1, n_2, b_2, n_3, b_3

Poiché $MCD(n_1, n_2) = MCD(4,7) = 1$, $MCD(n_1, n_3) = MCD(4,9) = 1$, $MCD(n_2, n_3) = MCD(7,9) = 1$ $\Rightarrow$ per il teorema cinese dei resti il sistema ha infinite soluzioni intere, tutte nella stessa classe di congruenza modulo $n = n_1 \cdot n_2 \cdot n_3 = 4 \cdot 7 \cdot 9 = 28 \cdot 9 = 252$

Cerco una soluzione x_0 del sistema

$x_1 = 2$

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

$$x_1 + t_2 n_1 \equiv 6 \mod 7$$
$$2 + t_2 \cdot 4 \equiv 6 \mod 7$$
$$4t_2 \equiv 6-2 \mod 7$$
$$4t_2 \equiv 4 \mod 7$$

Prendo $t_2 = 1$

$$x_2 = x_1 + t_2 n_1 = 2 + 1 \cdot 4 = 2 + 4 = 6$$

$x_3 = x_2 + t_3 n_1 n_2$ cerco $t_3 \in \mathbb{Z}$ tale che

$$x_2 + t_3 \cdot n_1 n_2 \equiv 7 \mod 9$$
$$6 + t_3 \cdot 4 \cdot 7 \equiv 7 \mod 9$$
$$28 t_3 \equiv 7 - 6 \mod 9$$
$$28 t_3 \equiv 1 \mod 9$$

$[28]_9 = [28-27]_9 = [1]_9$

$$t_3 \equiv 1 \mod 9$$

Prendo $t_3 = 1$

$$x_3 = x_2 + t_3 \cdot n_1 n_2 = 6 + 1 \cdot 4 \cdot 7 = 6 + 28 = 34$$

x_3 è la soluzione x_0 che cercavo. Dunque le soluzioni del sistema sono tutti i numeri interi dell'insieme

$$[x_3]_n = [34]_{252} = \{34 + 252k \mid k \in \mathbb{Z}\}$$