I19casaS1c
martedì 5 marzo 2019 09:30

S. PARTEGGIANI 5/3/2019

# ALGEBRA E MATEMATICA DISCRETA (parte di Algebra)

Corso di Laurea: Informatica

## SVOLGIMENTO DEGLI ESERCIZI PER CASA 1 (3ª PARTE)

**7** Si risolvano le seguenti congruenze (oppure per ciascuna di esse si dica se ha oppure no soluzioni, e, nel caso le abbia, se ci sono infinite)

1) $2x \equiv 3 \mod 5$ ($a$, $b$, $n$)

I Calcolo $d = MCD(a,n) = MCD(2,5) = 1$ ($a=2$, $n=5$)

II Siccome $d = 1 \mid 3 = b$, la congruenza ha infinite soluzioni intere, tutte in una unica ($d=1$) classe di congruenza modulo $n=5$.

III Cerco una soluzione $x_0$ di $2x \equiv 3 \mod 5$ ($a$, $b$, $n$)

$d = MCD(a,n) \Rightarrow \exists \alpha, \beta \in \mathbb{Z} \mid d = \alpha a + \beta n$
$d \mid b \Rightarrow \exists q \in \mathbb{Z} \mid b = dq$
$\Rightarrow b = a \cdot (\alpha q) + n(\beta q)$, $x_0 = \alpha q$

$a=2$, $n=5$, $d=1$ $\Rightarrow$ Euclide: $5 = 2 \cdot 2 + 1$ ($n$, $a$, $q_1$, $r_1 = d$)

$\Rightarrow 1 = 5 \cdot 1 + 2 \cdot (-2)$ ($d$, $n$, $\beta$, $a$, $\alpha$) $\Rightarrow$

$d = 1 \Rightarrow q = b = 3$

$\Rightarrow$ moltiplico $1 = 5 + 2 \cdot (-2)$ per $q = 3$

ottengo $3 = 5 \cdot 3 + 2 \cdot (-2) \cdot 3$ ($b$, $n$, $a$)

$x_0 \ (= \alpha \cdot q) = -6$

IV La congruenza ha come soluzioni tutti e soli i numeri interi

nelle classi di congruenza

$$[x_0]_5 = [-6]_5 = [4]_5 = \{4+5k \mid k \in \mathbb{Z}\}$$

scelgo un rappresentante positivo della classe $[-6]_5$:
prendo $c \in [-6]_5$ con $0 \le c < 5$, ossia

$$c = -6 + 5\cdot 2 = -6 + 10 = 4$$

---

2) $6x \equiv 9 \mod 15$

$a = 6$, $b = 9$, $n = 15$

I Calcolo $d = MCD(a,n) = MCD(6,15) = 3$

II $d = 3 \mid 9 = b \Rightarrow$ La congruenza ha infinite soluzioni intere, ripartite in $d = 3$ classi di congruenza modulo $n = 15$

III Cerco una soluzione $x_0$ della congruenza

$$\left.\begin{array}{l} \exists \alpha, \beta \in \mathbb{Z} \mid d = \alpha a + \beta n \\ \exists q \in \mathbb{Z} \mid b = dq \end{array}\right\} \Rightarrow b = a(\alpha q) + n(\beta q)$$

$x_0 = \alpha q$

cerco $\alpha$ e $\beta$: $\left.\begin{array}{l} a = 6 \\ n = 15 \end{array}\right\} \Rightarrow$

$$15 = 6\cdot 2 + 3$$
$$n \quad a \quad q_1 \quad z_1 = d$$

$$\Rightarrow \quad 3 = 15\cdot 1 + 6\cdot(-2)$$
$$d \quad n \quad \beta \quad a \quad \alpha$$

cerco $q$: $\left.\begin{array}{l} d = 3 \\ b = 9 \end{array}\right\} \Rightarrow q = \frac{b}{d} = \frac{9}{3} = 3$

$$\Rightarrow x_0 = \alpha \cdot q = (-2)\cdot 3 = -6$$

IV Scelgo un rappresentante positivo della classe di congruenza $[x_0]_{15}$:

$$[x_0]_{15} = [-6]_{15} = [-6+15]_{15} = [9]_{15}$$

Prendo $x_0 = 9$

$$x_1 = x_0 + 1\cdot\frac{n}{d} = 9 + 1\cdot\frac{15}{3} = 9+5 = 14$$

$$x_2 = x_0 + 2\cdot\frac{n}{d} = 9 + 2\cdot\frac{15}{3} = 9 + 2\cdot 5 = 9+10 = 19$$

N.B. $[x_2]_{15} = [19]_{15} = [19-15]_{15} = [4]_{15}$

le 3 classi di congruenza modulo 15 in cui si ripartiscono le soluzioni sono: $[4]_{15}$, $[9]_{15}$ e $[14]_{15}$

(Le soluzioni della congruenza sono:
$\{4+15k \mid k\in\mathbb{Z}\} \cup \{9+15k \mid k\in\mathbb{Z}\} \cup \{14+15k \mid k\in\mathbb{Z}\}$)

---

3) $7x \equiv 3 \mod 14$ ($a=7$, $b=3$, $n=14$)

I Calcolo $d = MCD(a,n) = MCD(7,14) = 7$

II Poiché $d = 7 \nmid 3 = b$, la congruenza NON HA SOLUZIONI.

---

4) $4x \equiv 8 \mod 12$ ($a=4$, $b=8$, $n=12$)

I Calcolo $d = MCD(a,n) = MCD(4,12) = 4$

II $d = 4 \mid 8 = b \Rightarrow$ la congruenza ha infinite soluzioni intere, ripartite in $d=4$ classi di congruenza modulo $n=12$

III Cerco una soluzione $x_0$ della congruenza

$\left.\begin{array}{l}\exists \alpha,\beta\in\mathbb{Z} \mid d = \alpha a + \beta n \\ \exists q\in\mathbb{Z} \mid b = qd\end{array}\right\} \Rightarrow b = a(\alpha q) + n(\beta q)$ ($\alpha q = x_0$)

$\left.\begin{array}{l}a=4\\ n=12\end{array}\right\} \Rightarrow 4 = 12\cdot 0 + 4$ ($d$, $n$, $\beta$, $a$) $\Rightarrow \boxed{\alpha = 1}$

$\left.\begin{array}{l}b=8\\ d=4\end{array}\right\} \Rightarrow q = \frac{b}{d} = \frac{8}{4} = 2$

$\Rightarrow x_0 = \alpha\cdot q = 1\cdot 2 = 2$

IV $x_0 = 2$

$x_1 = x_0 + 1\cdot\frac{n}{d} = 2 + 1\cdot\frac{12}{4} = 2+3 = 5$

$x_2 = x_0 + 2\cdot\frac{n}{d} = 2 + 2\cdot\frac{12}{4} = 2+2\cdot 3 = 2+6 = 8$

$x_3 = x_0 + 3\cdot\frac{n}{d} = 2 + 3\cdot\frac{12}{4} = 2+3\cdot 3 = 2+9 = 11$ ($d-1$)

Le 4 classi di congruenza modulo 12 in cui si ripartiscono le soluzioni sono: $[2]_{12}$, $[5]_{12}$, $[8]_{12}$, $[11]_{12}$

(le soluzioni delle congruenze sono: $\{2+12k \mid k\in\mathbb{Z}\} \cup \{5+12k \mid k\in\mathbb{Z}\} \cup \{8+12k \mid k\in\mathbb{Z}\} \cup \{11+12k \mid k\in\mathbb{Z}\}$)

---

5) $4x \equiv 2 \bmod 12$ ($a=4$, $b=2$, $n=12$)

I Calcolo $d = MCD(a,n) = MCD(4,12) = 4$

II Poiché $d = 4 \nmid 2 = b$, LA CONGRUENZA NON HA SOLUZIONI.

---

6) $4x \equiv 2 \bmod 11$ ($a=4$, $b=2$, $n=11$)

I Calcolo $d = MCD(a,n) = MCD(4,11) = 1$

II Poiché $d = 1 \mid 2 = b$, la congruenza ha infinite soluzioni intere, tutte in una unica (perché $d=1$) classe di congruenza modulo $n=11$

III Cerco la mia soluzione della congruenza:

$\exists \alpha,\beta\in\mathbb{Z} \mid d = \alpha a + \beta n \} \Rightarrow b = a(\alpha q) + n(\beta q)$
$\exists q\in\mathbb{Z} \mid b = dq$ ($x_0$)

$a=4$, $n=11$ $\Rightarrow$

$11 = 4\cdot 2 + 3$ ($n = a\cdot q_1 + r_1$) $\Rightarrow$ $3 = 11 - 4\cdot 2$

$4 = 3\cdot 1 + 1$ ($a = r_1\cdot q_2 + r_2 = d$) $\Rightarrow$ $1 = 4 - 3 = 4 - (11 - 4\cdot 2) = 4 - 11 + 4\cdot 2 = 4\cdot 3 + 11\cdot(-1)$

$\Rightarrow$ $1 = 4\cdot 3 + 11\cdot(-1)$ $\Rightarrow$ $d = 3$ ($d = a\cdot\alpha + n\cdot\beta$)

$$\left.\begin{matrix} b=2 \\ d=1 \end{matrix}\right\} \Rightarrow q = \frac{b}{d} = \frac{2}{1} = 2$$

$$\Rightarrow x_0 = \alpha q = 3 \cdot 2 = 6$$

IV le soluzioni delle congruenze sono tutti gli multipli delle classi

$$[6]_{11} = \{ 6 + 11k \mid k \in \mathbb{Z} \}.$$

---

8 Inverso, se esiste

1) L'inverso di 7 modulo 10

I $MCD(7,10) = 1 \Rightarrow \exists\, [7]_{10}^{-1}$.

II Calcolo $x_0$ soluzione di: $7x \equiv 1 \bmod 10$ (a, b, n)

$\exists \alpha, \beta \in \mathbb{Z} \mid 1 = \alpha a + \beta n$ ($1 = d = b$, $\alpha = x_0$, $\beta n$ multiplo di $n$)

$x_0 = \alpha q = \alpha$ ($d = b \Rightarrow q = 1$)

$a = 7,\ n = 10 \Rightarrow 10 = 7 \cdot 1 + 3 \Rightarrow 3 = 10 - 7$ ($n$, $a$, $q_1$, $r_1$)

$7 = 3 \cdot 2 + 1$ ($a$, $r_1$, $q_2$, $d$)

$\Rightarrow 1 = 7 - 3 \cdot 2 = 7 - (10-7) \cdot 2 =$

$= 7 - 10 \cdot 2 + 7 \cdot 2 =$

$= 7 \cdot 3 - 10 \cdot 2$

$\Rightarrow 1 = 7 \cdot 3 + 10 \cdot (-2) \Rightarrow x_0 = 3$ ($a$, $\alpha$, $c_n$)

III $[7]_{10}^{-1} = [3]_{10}$

---

2) L'inverso di 4 modulo 10

NON ESISTE perché $MCD(4,10) = 2 \neq 1$.

---

3) L'inverso di 6 modulo 15

NON ESISTE perché $MCD(6,15) = 3 \neq 1$.

4) L'inverso di 8 modulo 15

I) $MCD(8,15) = 1 \Rightarrow \exists\ [8]_{15}^{-1}$

II) Caso x0 soluzione di $8x \equiv 1 \bmod 15$ (a = 8, b = 1, n = 15)

$\exists \alpha, \beta \in \mathbb{Z} \mid 1 = \alpha a + \beta n$ (d = b = 1, $x_0 = \alpha$)

$a = 8,\ n = 15 \Rightarrow$

$15 = 8 \cdot 1 + 7 \Rightarrow 7 = 15 - 8$ ($n = a \cdot q_1 + r_1$)

$8 = 7 \cdot 1 + 1$ ($a = r_1 \cdot q_2 + r_2 = d$)

$\Rightarrow 1 = 8 - 7 = 8 - (15 - 8) = 8 - 15 + 8 = 8 \cdot 2 - 15$

$\Rightarrow 1 = 8 \cdot 2 + 15 \cdot (-1) \Rightarrow x_0 = 2$ ($a \cdot \alpha + n \cdot \beta$)

III) $[8]_{15}^{-1} = [2]_{15}$