ALGEBRA E MATEMATICA DISCRETA

Corso di Laurea: Informatica

SVOLGIMENTO DEGLI ESERCIZI PER CASA 1 (3ª PARTE)

9 Si risolvano le seguenti congruenze (ossia per ciascuna di esse si dica se ha oppure no soluzioni, e, nel caso le abbia, le si trovino tutte)

1) $\underset{a}{2}x \equiv \underset{b}{3} \bmod \underset{n}{5}$

$\boxed{\text{I}}$ Calcolo $d = MCD(a,n) \underset{\substack{a=2\\ n=5}}{=} MCD(2,5) = 1$

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

$\boxed{\text{III}}$ Cerco una soluzione x_0 di $\underset{a}{2}x \equiv \underset{b}{3} \bmod \underset{n}{5}$

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

$$\left.\begin{array}{l} a=2 \\ n=5 \\ d=1 \end{array}\right\} \underset{\text{Euclide}}{\Rightarrow} \underset{n}{5} = \underset{a}{2}\cdot \underset{q_1}{2} + \underset{r_1 = d}{1} \Rightarrow \boxed{\underset{d}{1} = \underset{n}{5}\cdot \underset{\beta}{1} + \underset{a}{2}\cdot \underset{\alpha}{(-2)}} \Rightarrow$$

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

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

ottengo $\underset{b}{3} = \underset{n}{5}\cdot 3 + \underset{a}{2}\cdot \boxed{(-2)\cdot 3} \rightarrow x_0 \ (= \alpha\cdot q) = -6$

$\boxed{\text{IV}}$ La congruenza ha come soluzioni tutti e soli i numeri interi nelle classe 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 $0 \le c < 5$, per cui

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

---

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

a b n

$a=6$
$n=15$

$\boxed{\text{I}}$ Calcolo $d = MCD(a,n) = MCD(6,15) = 3$

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

$\boxed{\text{III}}$ Cerco una soluzione x_0 della congruenza

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

cerco α e β:

$$\left.\begin{array}{l}a=6\\ n=15\end{array}\right\} \Rightarrow \underset{n}{15} = \underset{a}{6}\cdot \underset{q_1}{2} + \underset{r_1=d}{3}$$

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

cerco q:

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

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

$\boxed{\text{IV}}$ 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 b n

$\boxed{I}$ Calcolo $d = MCD(a,m) = MCD(7,14) = 7$

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

---

4) $4x \equiv 8 \mod 12$

a b n

$a = 4$
$m = 12$

$\boxed{I}$ Calcolo $d = MCD(a,n) = MCD(4,12) = 4$

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

$\boxed{III}$ Cerco una soluzione x_0 della congruenza

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

$$\left.\begin{array}{l}a=4\\ m=12\end{array}\right\} \Rightarrow \quad \underset{d}{4} = \underset{m}{12}\cdot\underset{\beta}{0} + \underset{a}{4}$$

$\boxed{\alpha = 1}$

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

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

$\boxed{IV}$ $x_0 = 2$

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

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

d-1

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

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

(Le soluzioni della congruenza 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) $\underset{a}{4}x \equiv \underset{b}{2} \bmod \underset{n}{12}$

$\boxed{I}$ Calcolo $d = MCD(a,n) = MCD(4,12) = 4$ ($a=4$, $n=12$)

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

---

6) $\underset{a}{4}x \equiv \underset{b}{2} \bmod \underset{n}{11}$

$\boxed{I}$ Calcolo $d = MCD(a,n) = MCD(4,11) = 1$ ($a=4$, $n=11$)

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

$\boxed{III}$ Cerco x_0 una soluzione della congruenza:

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

$$\left.\begin{array}{l}a=4\\ n=11\end{array}\right\} \Rightarrow \underset{n}{11} = \underset{a}{4}\cdot \underset{q_1}{2} + \underset{r_1}{3} \Rightarrow \boxed{3 = 11 - 4\cdot 2}$$

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

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

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

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

$\boxed{\text{IV}}$ le soluzioni della congruenza sono tutti gli interi della classe

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

$\boxed{8}$ Si calcoli, se esiste

1) L'inverso di 7 modulo 10

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

$\boxed{\text{II}}$ Cerco x_0 soluzione di: $\underset{a}{7}x\equiv \underset{b}{1} \bmod \underset{n}{10}$

$$\exists \alpha,\beta\in\mathbb{Z} \mid \underset{d=b}{1}=\underset{x_0}{\boxed{\alpha}}a+\underbrace{\beta n}_{\text{multiplo di } n}$$

$$\boxed{x_0=\alpha q=\alpha} \quad d=b \Rightarrow q=1$$

$$\left.\begin{array}{l} a=7 \\ n=10 \end{array}\right\} \Rightarrow \underset{n}{10}=\underset{a}{7}\cdot \underset{q_1}{1}+\underset{r_1}{3} \Rightarrow \boxed{3=10-7}$$

$$\underset{a}{7}=\underset{r_1}{3}\cdot \underset{q_2}{} \quad \underset{d}{1}$$

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

$$\Rightarrow \underset{a}{1=7}\cdot \underset{\alpha}{3}+\underset{n}{10}\cdot(-2) \Rightarrow x_0=3$$

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

---

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

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

$\boxed{\text{II}}$ Cerco x_0 soluzione di $\underset{a}{8}x \equiv \underset{b}{1} \bmod \underset{m}{15}$

$$\exists\, \alpha,\beta \in \mathbb{Z} \mid \underset{d=b}{1} = \underset{x_0}{\alpha} a + \beta m$$

$$\left.\begin{array}{l} a=8 \\ m=15 \end{array}\right\} \Rightarrow \quad \underset{m}{15} = \underset{a}{8} \cdot \underset{q_1}{1} + \underset{r_1}{7} \quad \Rightarrow \boxed{7 = 15-8}$$

$$\underset{a}{8} = \underset{r_1}{7} \cdot \underset{q_2}{1} + \underset{r_2=d}{1} \quad \Rightarrow \quad 1 = 8-7 = 8-(15-8) = 8-15+8 = 8\cdot 2-15$$

$$\Rightarrow \quad 1 = \underset{a}{8} \cdot \underset{\alpha}{2} + \underset{m}{15} \cdot (-1) \Rightarrow x_0 = 2$$

$\boxed{\text{III}}$ $[8]_{15}^{-1} = [2]_{15}$