Crittografia ed Aritmetica Modulare
LABORATORIO della Appendice al IV incontro
– con Soluzioni –

PLS - CAM

Padova, 7 novembre 2014

ATTIVITÀ 1.1. *Quali sono gli elementi invertibili in $\mathbb{Z}_m \times \mathbb{Z}_n$?*

- *Verificare che $(a+m\mathbb{Z}, b+n\mathbb{Z})$ è invertibile in $\mathbb{Z}_m \times \mathbb{Z}_n$ se e solo se sia $a+m\mathbb{Z}$ è invertibile in $\mathbb{Z}_m$ che $b+n\mathbb{Z}$ è invertibile in $\mathbb{Z}_n$. In tal caso l'inverso di $(a+m\mathbb{Z}, b+n\mathbb{Z})$ è ....*
- *Si dica quali tra $(\overline{2}, \overline{3})$, $(\overline{2}, \overline{2}) \in \mathbb{Z}_3 \times \mathbb{Z}_4$ sono invertibili, determinandone, quanto esistono, gli inversi.*

Svolgimento. i) $(a+m\mathbb{Z}, b+n\mathbb{Z})$ è invertibile in $\mathbb{Z}_m \times \mathbb{Z}_n$ se e solo se esiste $(a'+m\mathbb{Z}, b'+n\mathbb{Z}) \in \mathbb{Z}_m \times \mathbb{Z}_n$ tale che $(a+m\mathbb{Z}, b+n\mathbb{Z}) \cdot (a'+m\mathbb{Z}, b'+n\mathbb{Z}) = (1+m\mathbb{Z}, 1+n\mathbb{Z})$, cioè $(aa'+m\mathbb{Z}, bb'+n\mathbb{Z}) = (1+m\mathbb{Z}, 1+n\mathbb{Z})$. E ciò accade se e solo se $aa'+m\mathbb{Z} = 1+m\mathbb{Z}$ e $bb'+n\mathbb{Z} = 1+n\mathbb{Z}$, cioè se e solo se $a+m\mathbb{Z}$ è invertibile in $\mathbb{Z}_m$ e $b+n\mathbb{Z}$ è invertibile in $\mathbb{Z}_n$. Ciò dimostra anche che l'inverso di $(a+m\mathbb{Z}, b+n\mathbb{Z})$ è $(a'+m\mathbb{Z}, b'+n\mathbb{Z})$, ove $a'+m\mathbb{Z}$ è l'inverso di $a+m\mathbb{Z}$ e $b'+n\mathbb{Z}$ è l'inverso di $b+n\mathbb{Z}$.

ii) In base a quanto osservato in i), $(\overline{2}, \overline{3})$ è invertibile in $\mathbb{Z}_3 \times \mathbb{Z}_4$ con inverso $(\overline{2}, \overline{3})$, poiché $\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$ in $\mathbb{Z}_3$ e $\overline{3} \cdot \overline{3} = \overline{9} = \overline{1}$ in $\mathbb{Z}_4$. Invece $(\overline{2}, \overline{2})$ non è invertibile in $\mathbb{Z}_3 \times \mathbb{Z}_4$, poiché $\overline{2} \in \mathbb{Z}_4$ non è invertibile, essendo $(2,4) = 2 \neq 1$. ∎

ATTIVITÀ 1.2. *Si verifichi che se $a+mn\mathbb{Z} = b+mn\mathbb{Z}$ allora anche*

$$(a+m\mathbb{Z}, a+n\mathbb{Z}) = (b+m\mathbb{Z}, b+n\mathbb{Z}).$$

Svolgimento. Osserviamo che $a+mn\mathbb{Z} = b+mn\mathbb{Z}$ se e solo se $mn|b-a$. Ma allora a fortiori $m|b-a$ e $n|b-a$, dunque $a+m\mathbb{Z} = b+m\mathbb{Z}$ e $a+n\mathbb{Z} = b+n\mathbb{Z}$. ∎

ATTIVITÀ 1.4. *Assodato che* $12 = 3 \cdot 4 = 2 \cdot 6$*:*

- *si studi il comportamento di* $f_{3,4} : \mathbb{Z}_{12} \to \mathbb{Z}_3 \times \mathbb{Z}_4$*, elencandone le immagini* $f_{3,4}(\overline{a})$*, al variare di* $\overline{a} \in \mathbb{Z}_{12}$*;*
- *analogamente si consideri il caso* $f_{2,6} : \mathbb{Z}_{12} \to \mathbb{Z}_2 \times \mathbb{Z}_6$*.*
- *Cosa si può osservare, confrontando i due casi precedenti?*

Svolgimento. i) Consideriamo dapprima $f_{3,4} : \mathbb{Z}_{12} \to \mathbb{Z}_3 \times \mathbb{Z}_4$:

$$\begin{array}{ccc} f_{3,4}(\overline{0}) = (\overline{0},\overline{0}), & f_{3,4}(\overline{1}) = (\overline{1},\overline{1}), & f_{3,4}(\overline{2}) = (\overline{2},\overline{2}) \\ f_{3,4}(\overline{3}) = (\overline{0},\overline{3}), & f_{3,4}(\overline{4}) = (\overline{1},\overline{0}), & f_{3,4}(\overline{5}) = (\overline{2},\overline{1}) \\ f_{3,4}(\overline{6}) = (\overline{0},\overline{2}), & f_{3,4}(\overline{7}) = (\overline{1},\overline{3}), & f_{3,4}(\overline{8}) = (\overline{2},\overline{0}) \\ f_{3,4}(\overline{9}) = (\overline{0},\overline{1}), & f_{3,4}(\overline{10}) = (\overline{1},\overline{2}), & f_{3,4}(\overline{11}) = (\overline{2},\overline{3}). \end{array}$$

ii) Consideriamo ora $f_{2,6} : \mathbb{Z}_{12} \to \mathbb{Z}_2 \times \mathbb{Z}_6$:

$$\begin{array}{ccc} f_{2,6}(\overline{0}) = (\overline{0},\overline{0}), & f_{2,6}(\overline{1}) = (\overline{1},\overline{1}), & f_{2,6}(\overline{2}) = (\overline{0},\overline{2}) \\ f_{2,6}(\overline{3}) = (\overline{1},\overline{3}), & f_{2,6}(\overline{4}) = (\overline{0},\overline{4}), & f_{2,6}(\overline{5}) = (\overline{1},\overline{5}) \\ f_{2,6}(\overline{6}) = (\overline{0},\overline{0}), & f_{2,6}(\overline{7}) = (\overline{1},\overline{1}), & f_{2,6}(\overline{8}) = (\overline{0},\overline{2}) \\ f_{2,6}(\overline{9}) = (\overline{1},\overline{3}), & f_{2,6}(\overline{10}) = (\overline{0},\overline{4}), & f_{2,6}(\overline{11}) = (\overline{1},\overline{5}). \end{array}$$

iii) Osserviamo che mentre $f_{3,4}$ ha dodici distinte immagini, quindi è biiettiva, al contrario $f_{2,6}$ ha solo sei immagini distinte, quindi non è né iniettiva né suriettiva. ∎

HOMEWORK 1.7. *Assegnati* m*,* n *interi positivi e* $a, b \in \mathbb{Z}$*, consideriamo il sistema*

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \qquad (*)$$

Una soluzione di questo sistema è costituita da un medesimo intero $x \in \mathbb{Z}$ *che realizzi simultaneamente entrambe le congruenze.*

Utilizzando il Teorema 1.5 *si verifichi che:*

- *Se* m *e* n *sono coprimi, allora per ogni scelta di interi* a *e* b *il corrispondente sistema* (*) *ammette sempre almeno una soluzione.*
- *Se* m *e* n *sono coprimi e se* $x_0 \in \mathbb{Z}$ *è una soluzione di* (*)*, allora le altre soluzioni di* (*) *sono esattamente . . .*
- *Supponiamo ora che* $(m, n) = d > 1$*. Allora esiste sempre almeno una scelta di interi* a *e* b *per cui il corrispondente sistema* (*) *non ammette soluzioni (perché?). Sapreste come fare a scegliere questi* a *e* b *"patologici"?*

Svolgimento. i) Se m ed n sono coprimi, allora il Teorema 1.5 ci assicura che l'applicazione $f_{m,n}$ è biiettiva. In particolare è suriettiva. Quindi, assegnati ad arbitrio interi a e b, esiste un intero x tale che

$$f_{m,n}(x + mn\mathbb{Z}) = (x + m\mathbb{Z}, x + n\mathbb{Z}) = (a + m\mathbb{Z}, b + n\mathbb{Z}),$$

dunque $x \equiv a \mod m$ e $x \equiv b \mod n$.

ii) Seguendo l'argomento precedente, se x_0 è una soluzione di (*), la iniettività di $f_{m,n}$ sulle classi resto modulo mn garantisce che tutte e sole le altre soluzioni di (*) sono costituite dagli elementi della classe $x_0 + mn\mathbb{Z}$.

iii) Se $(m, n) = d > 1$ allora, in forza del Teorema 1.5, l'applicazione $f_{m,n}$ non è biiettiva, dunque non è suriettiva (dato che sia dominio che codominio hanno lo stesso numero mn di elementi). Ed allora esistono interi a_0 e b_0 tali che $f_{m,n}(x + mn\mathbb{Z}) = (x + m\mathbb{Z}, x + n\mathbb{Z}) \neq (a_0 + m\mathbb{Z}, b_0 + n\mathbb{Z})$ per ogni $x \in \mathbb{Z}$. Equivalentemente, il sistema di congruenze

$$\begin{cases} x \equiv a_0 \mod m \\ x \equiv b_0 \mod n \end{cases}$$

non ha soluzioni. Come determinare una tale coppia di interi a_0, b_0? Se supponiamo al contrario che una soluzione intera x esista, allora esistono interi α e β tali che $x = a_0 + \alpha m$ e $x = b_0 + \beta n$, da cui $a_0 - b_0 = -\alpha m + \beta n$, e dunque $a_0 - b_0 \in d\mathbb{Z}$ per l'HOMEWORK 2.7 del III incontro. Ricordando che $d \neq 1$, è dunque sufficiente scegliere una qualunque coppia di interi a_0 e b_0 tali che $a_0 - b_0 \notin d\mathbb{Z}$ (ad esempio $a_0 = b_0 + 1$) per assicurarsi che non vi sia alcuna soluzione x del sistema. ∎