Crittografia ed Aritmetica Modulare
LABORATORIO della Appendice al IV incontro

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.*

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?*

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"?*