Crittografia ed Aritmetica Modulare
LABORATORIO del IV incontro

PLS - CAM

Padova, 7 novembre 2014

ATTIVITÀ 1.1. *Dimostrare che se* $\overline{a_1} = \overline{a_2}$ *e se* $\overline{b_1} = \overline{b_2}$*, allora* $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ *e* $\overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2}$.

ATTIVITÀ 1.2. *In* $\mathbb{Z}_{12}$ *si calcolino le potenze successive delle classi* $\overline{4}$*,* $\overline{5}$*,* $\overline{6}$*. Si confrontino quindi i risultati ottenuti.*

Esempio 1.3. *Costruiamo ora le tabelle di addizione e di moltiplicazione per* $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$*,* $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ *e* $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$*:*

$\mathbb{Z}_2$

$+$	$\mid$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\mid$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\mid$	$\overline{1}$	$\overline{0}$

$\cdot$	$\mid$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\mid$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\mid$	$\overline{0}$	$\overline{1}$

$\mathbb{Z}_3$

$+$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\mid$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\mid$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\mid$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\mid$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}_4$

$+$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\mid$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\mid$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\mid$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\mid$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\mid$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\mid$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Notiamo subito che:

- queste tabelle sono simmetriche, in virtù del fatto che anche le nuove operazioni $+$ e $\cdot$ sono commutative;
- su ciascuna riga/colonna delle tabelle additive $+$ compare una diversa permutazione di tutti gli elementi (ottenuta "shiftando" la precedente);
- il comportamento delle righe/colonne della tabella moltiplicativa $\cdot$ di $\mathbb{Z}_4$ differisce da quello di $\mathbb{Z}_2$ e di $\mathbb{Z}_3$: in che cosa?

ATTIVITÀ 1.4. *Si scrivano le tabelle $+$ e $\cdot$ per $\mathbb{Z}_5$ e per $\mathbb{Z}_6$.*
- *In quali righe (o colonne) delle tabelle additive appare $\overline{0}$?*
- *In quali righe (o colonne) delle tabelle moltiplicative appare $\overline{1}$?*
- *Per quale $n = 2, 3, 4, 5, 6$, nelle distinte tabelle moltiplicative, appare $\overline{1}$ in ogni riga non corrispondente a $\overline{0}$?*

Dunque ogni elemento di $\mathbb{Z}_n$ ha un opposto, mentre non sempre è vero che ogni elemento non nullo di $\mathbb{Z}_n$ abbia un inverso. **Le classi $\overline{a}$ che risultano invertibili in $\mathbb{Z}_n$ sono esattamente quelle per cui a e n sono tra loro coprimi**, in forza del seguente

Teorema 1.5. *Sia $\overline{a} \in \mathbb{Z}_n$. Allora $\overline{a}$ ammette una classe inversa $\overline{a}^{-1}$ in $\mathbb{Z}_n$ se e solo se a è coprimo con n. In tal caso se $1 = \alpha a + \beta n$, con $\alpha, \beta \in \mathbb{Z}$, allora $\overline{a}^{-1} = \overline{\alpha}$.*

dal quale segue subito il

Corollario 1.6. *Se n è primo, allora tutte le classi diverse da $\overline{0}$ in $\mathbb{Z}_n$ ammettono una classe inversa. Viceversa, se n non è primo, allora in $\mathbb{Z}_n$ vi è sempre qualche classe diversa da $\overline{0}$ che non ammette classe inversa.*

HOMEWORK 1.7. *Si scriva una dimostrazione del corollario precedente.*

ATTIVITÀ 1.8. *Quali sono le classi invertibili in $\mathbb{Z}_{12}$? Si determini la classe inversa di ciascuna di esse.*

ATTIVITÀ 1.9. *Utilizzando l'algoritmo di Euclide esteso si verifichi che $\overline{364}$ è invertibile in $\mathbb{Z}_{865}$, e se ne calcoli la classe inversa.*

HOMEWORK 1.10. *Si utilizzi il programma sviluppato nell'*HOMEWORK 2.6 *del terzo incontro per scrivere il codice di un algoritmo che, assegnati $a, n \in \mathbb{Z}$, con $n \geq 2$, dica se $\overline{a}$ è invertibile in $\mathbb{Z}_n$ e, in caso affermativo, ne calcoli la classe inversa.*

HOMEWORK 1.11. *Esiste la PROVA DELL'11? Come funziona?*

Esercizio 2.1. *Verifichiamo che:*

- *qualunque sia $n \geq 2$ intero, risulta $\varphi(n) < n$;*
- $\varphi(1) = \ldots$?
- *se p è* **primo**, *allora $\varphi(p) = p - 1$;*
- *se p è* **primo** *e $k \geq 1$ è intero, allora*

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

- *Calcoliamo $\varphi(2)$, $\varphi(3)$, $\varphi(4)$, $\varphi(5)$, $\varphi(6)$, $\varphi(7)$, $\ldots \varphi(12), \ldots$*

Esercizio 2.2. *Assodato che $12 = 3 \cdot 4 = 2 \cdot 6$, è vero che $\varphi(12) = \varphi(3) \cdot \varphi(4) = \varphi(2) \cdot \varphi(6)$?*

ATTIVITÀ 3.2. *Si calcoli la funzione di Eulero sui primi 25 numeri interi positivi.*

HOMEWORK 3.3. *Si scriva il codice per un algoritmo che, utilizzando la fattorizzazione nel prodotto di primi, calcoli $\varphi(n)$ per ogni intero positivo n.*