Crittografia ed Aritmetica Modulare
LABORATORIO del IV incontro
– con Soluzioni –

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* $\overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2}$*.*

Svolgimento. Siano dunque $a_1 \equiv a_2 \mod n$ e $b_1 \equiv b_2 \mod n$. Ciò significa che esistono $h, k \in \mathbb{Z}$ tali che $a_1 = a_2 + nh$ e $b_1 = b_2 + nk$. Allora:

$$a_1 + b_1 = a_2 + nh + b_2 + nk = a_2 + b_2 + n(h + k)$$

e dunque $a_1 + b_1 \equiv a_2 + b_2 \mod n$; analogamente

$$a_1 \cdot b_1 = (a_2 + nh) \cdot (b_2 + nk) = a_2 \cdot b_2 + n(hb_2 + ka_2 + nhk)$$

e dunque $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \mod n$. Ciò dimostra quanto voluto. ∎

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.*

Svolgimento. $\overline{4}$, $\overline{4}^2 = \overline{16} = \overline{4}$, $\overline{4}^i = \overline{4}$, ... ogni potenza è sempre eguale a $\overline{4}$. Poi: $\overline{5}$, $\overline{5}^2 = \overline{25} = \overline{1}$, $\overline{5}^3 = \overline{5}$, $\overline{5}^4 = \overline{1}$, ... le potenze dispari restituiscono $\overline{5}$ e le pari $\overline{1}$. Infine: $\overline{6}$, $\overline{6}^2 = \overline{36} = \overline{0}$, $\overline{6}^3 = \overline{0}$, ... $\overline{6}^i = \overline{0}$, ... tutte le potenze con esponente maggiore di 1 sono eguali a $\overline{0}$. ∎

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* $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$*:*

$\mathbb{Z}_2$

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

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

$\mathbb{Z}_3$

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

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

$\mathbb{Z}_4$

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

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

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 $\overline{0}$?*

Svolgimento.

$\mathbb{Z}_5$

$+$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$-$	$-$	$-$	$-$	$-$	$-$	
$\overline{0}$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\mid$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\mid$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\mid$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\mid$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$-$	$-$	$-$	$-$	$-$	$-$	
$\overline{0}$	$\mid$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\mid$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\mid$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\mid$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}_6$

$+$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\mid$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\mid$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\mid$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\mid$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\mid$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\mid$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\mid$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\mid$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\mid$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\mid$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\mid$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Notiamo che in tutte le **tabelle additive** compare in ogni riga/colonna la classe $\overline{0}$, a dimostrazione del fatto che tutti gli elementi hanno opposto.

Non è così invece per le **tabelle moltiplicative**:

– nel caso di $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_5$ in ogni riga/colonna corrispondente ad un elemento diverso dalla classe $\overline{0}$ compare la classe $\overline{1}$, a dimostrazione del fatto che ogni elemento diverso da $\overline{0}$ ha un inverso. Ad esempio in $\mathbb{Z}_5$ troviamo le coppie di classi inverse $(\overline{1},\overline{1})$, $(\overline{2},\overline{3})$ e $(\overline{4},\overline{4})$;

– nel caso invece di $\mathbb{Z}_4$ e $\mathbb{Z}_6$ vediamo che poche sono le righe/colonne in cui compare $\overline{1}$: in $\mathbb{Z}_4$ risultano invertibili solo le classi $\overline{1}$ e $\overline{3}$, ed analogamente in $\mathbb{Z}_6$ solo le classi $\overline{1}$ e $\overline{5}$;

– notiamo inoltre che le righe/colonne delle tabelle moltiplicative in cui compare $\overline{1}$ sono esattamente quelle in cui possiamo ritrovare, senza ripetizioni, tutti gli elementi della classe resto corrispondente: in altre parole, le moltiplicazioni per un elemento invertibile (e solo queste) ne costituiscono una permutazione. ∎

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. Questo infatti non accade per $\mathbb{Z}_4$ e $\mathbb{Z}_6$. In tutti questi esempi possiamo osservare che **le classi $\overline{a}$ che risultano invertibili in $\mathbb{Z}_n$ sono esattamente quelle per cui a e n sono tra loro coprimi**. E questo è esattamente ciò che afferma il 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.*

Svolgimento. Se n è primo, allora ogni classe $\overline{a} \in \mathbb{Z}_n$ non nulla ha rappresentante a che è coprimo con n, dunque $\overline{a}$ è invertibile per il Teorema 1.5. Viceversa, se n non è primo, allora esiste un intero a con $0 < a < n$ tale che $a|n$: ciò fornisce una classe non nulla $\overline{a} \in \mathbb{Z}_n$ che non è invertibile, ancora in virtù del Teorema 1.5. ∎

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

Svolgimento. In forza del Teorema 1.5, le classi invertibili in $\mathbb{Z}_{12}$ sono tutte e sole quelle della forma $\overline{a}$ con $0 < a < 12$ e $(a, n) = 1$. Si trovano dunque le classi $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$. Notiamo che ciascuna di queste è inversa a sè stessa, poiché $1 \cdot 1 = 1$, $5 \cdot 5 = 25 \equiv 1$, $7 \cdot 7 = 49 \equiv 1$ ed infine $11 \equiv -1$ cosicché $11 \cdot 11 \equiv (-1) \cdot (-1) = 1$. ∎

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.*

Svolgimento.

	1	0	865	
-2	0	1	364	$865 = 364 \cdot 2 + 137$
-2	1	-2	137	$364 = 137 \cdot 2 + 90$
-1	-2	5	90	$137 = 90 \cdot 1 + 47$
-1	3	-7	47	$90 = 47 \cdot 1 + 43$
-1	-5	12	43	$47 = 41 \cdot 1 + 4$
-10	8	-19	4	$43 = 4 \cdot 10 + 3$
-1	-85	202	3	$4 = 3 \cdot 1 + 1$
	93	-221	1	
			0	

Otteniamo dunque che $1 = (420, 72) = 93 \cdot 865 - 221 \cdot 364$, che fornisce (cfr. Teorema 1.5)

$$\overline{364}^{-1} = \overline{-221} = \overline{-221 + 865} = \overline{644}.$$

∎

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.*

Svolgimento. È delegato ai docenti esperti di programmazione. ∎

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

Svolgimento. Prendendo spunto dalla spiegazione sulla prova del nove, assegnato un intero non negativo m con scrittura in cifre $x_i x_{i-1} \dots x_1 x_0$ in base 10, si ha che

$$m = x_0 + x_1 \cdot 10 + x_2 \cdot 10^2 + \dots x_i \cdot 10^i.$$

Ora $10 \equiv -1 \mod 11$, ed allora $10^2 \equiv (-1)^2 \equiv 1 \mod 11$, mentre $10^3 \equiv (-1)^3 \equiv -1 \mod 11$ e così via. Dunque gli addendi di qui sopra con indice j pari sono congrui a x_j modulo 11, mentre quelli con indice j dispari sono congrui a $-x_j$ modulo 11. Se ne deduce che

$$m \equiv x_0 - x_1 + x_2 - \dots + (-1)^i x_i \mod 11$$

cioè $\overline{m} = \overline{x_0 - x_1 + x_2 - \dots + (-1)^i x_i}$ in $\mathbb{Z}_{11}$.

In altre parole, la prova dell'11 si esegue ancora riducendo i numeri alla somma algebrica delle loro cifre, tenendo però conto che vi è un segno $\pm$ da attribuire a ciascuna di esse che varia in funzione della loro posizione nella scrittura decimale. ∎

Esercizio 2.1. *Verifichiamo che:*

- *qualunque sia $n \geq 2$ intero, risulta $\varphi(n) < n$;*
- $\varphi(1) = \dots$?
- *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 $\varphi(2)$, $\varphi(3)$, $\varphi(4)$, $\varphi(5)$, $\varphi(6)$, $\varphi(7)$, $\dots \varphi(12), \dots$*

Svolgimento. i) Infatti le classi in $\mathbb{Z}_n$ sono n, e la classe $\overline{0}$ non è mai invertibile.

ii) $\mathbb{Z}_1 = \{\overline{0}\}$ dunque $\varphi(1) = 0$.

iii) Infatti se p è primo, allora in $\mathbb{Z}_p$ ogni classe non nulla è invertibile, grazie al Corollario 1.6.

iv) Infatti gli interi a con $0 < a \leq p^k$ che non sono coprimi con p^k sono esattamente quelli divisibili per p, ed allora sono $p, 2p, 3p, \dots p^{k-1}p = p^k$, dunque sono in tutto p^{k-1}. Ma allora le classi invertibili sono in tutto $p^k - p^{k-1}$.

v) Se n è un primo o una sua potenza, allora per calcolare $\varphi(n)$ possiamo utilizzare i punti precedenti; altrimenti dobbiamo contare le classi con rappresentanti canonici coprimi con n. Otteniamo: $\varphi(2) = 1$, $\varphi(3) = 3 - 1 = 2$, $\varphi(4) = \varphi(2^2) = 2^2 - 2 = 2$, $\varphi(5) = 5 - 1 = 4$, $\varphi(6) = 2$, $\varphi(7) = 7 - 1 = 6$, $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$, $\varphi(9) = \varphi(3^2) = 3^2 - 3 = 6$, $\varphi(10) = 4$, $\varphi(11) = 11 - 1 = 10$, $\varphi(12) = 4$, ... ∎

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

Svolgimento. Dall'esercizio precedente abbiamo che $\varphi(12) = 4$, $\varphi(3) \cdot \varphi(4) = 2 \cdot 2 = 4$ e $\varphi(2) \cdot \varphi(6) = 1 \cdot 2 = 2$. Quindi è vera la prima eguaglianza, ma non la seconda. ∎

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

Svolgimento. Nell'Esercizio 2.1 abbiamo calcolato $\varphi(1), \ldots, \varphi(12)$. Ora proseguiamo sino al calcolo di $\varphi(25)$ utilizzando la formula del Teorema 3.1:

$$\varphi(13) = 13 - 1 = 12, \qquad \varphi(14) = \varphi(2 \cdot 7) = 1 \cdot 6 = 6,$$
$$\varphi(15) = \varphi(3 \cdot 5) = 2 \cdot 4 = 8, \qquad \varphi(16) = \varphi(2^4) = 2^3(2 - 1) = 8,$$
$$\varphi(17) = 17 - 1 = 16, \qquad \varphi(18) = \varphi(2 \cdot 3^2) = (2 - 1)3(3 - 1) = 6,$$
$$\varphi(19) = 19 - 1 - 18, \qquad \varphi(20) = \varphi(2^2 \cdot 5) = 2(2 - 1)(5 - 1) = 8,$$
$$\varphi(21) = \varphi(3 \cdot 7) = (3 - 1)(7 - 1) = 12, \qquad \varphi(22) = \varphi(2 \cdot 11) = (2 - 1)(11 - 1) = 10,$$
$$\varphi(23) = 23 - 1 = 22, \qquad \varphi(24) = \varphi(2^3 \cdot 3) = 2^2(2 - 1)(3 - 1) = 8,$$
$$\varphi(25) = \varphi(5^2) = 5(5 - 1) = 20.$$

∎

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*.*

Svolgimento. È delegato ai docenti esperti di programmazione. ∎