Crittografia ed Aritmetica Modulare
– IV incontro –

PLS - CAM

Padova, 7 novembre 2014

1 Aritmetica modulare

Sia n un intero positivo fissato. Denotiamo con

$$\mathbb{Z}_n = \{\overline{0},\ \overline{1},\ \overline{2},\ \ldots, \overline{n-1}\}$$

l'insieme delle classi resto modulo n.

Proviamo a definire delle operazioni di addizione e moltiplicazione in $\mathbb{Z}_n$ attraverso le usuali analoghe operazioni sui rappresentanti interi, cioè ponendo, per $\overline{a}, \overline{b} \in \mathbb{Z}_n$,

$$\overline{a} + \overline{b} := \overline{a+b} \qquad \text{e} \qquad \overline{a} \cdot \overline{b} := \overline{a \cdot b}. \tag{*}$$

Così, ad esempio, in $\mathbb{Z}_{12}$ otteniamo le eguaglianze

$$\overline{6} + \overline{9} = \overline{15} = \overline{3} \qquad \text{e} \qquad \overline{4} \cdot \overline{7} = \overline{28} = \overline{4}.$$

Come si vede, non sempre è possibile limitarsi ai rappresentanti canonici, poiché il risultato della somma o del prodotto (eventualmete iterati) tra numeri interi $0 \leq a, b < n$ non sempre è compreso nel medesimo intervallo. Ad esempio in $\mathbb{Z}_{12}$

$$\begin{aligned}\overline{4}^3 = \overline{4} \cdot \overline{4} \cdot \overline{4} = \overline{16} \cdot \overline{4} = \overline{4} \cdot \overline{4} = \overline{16} = \overline{4} \\ = \overline{16 \cdot 4} = \overline{64} = \overline{4}.\end{aligned}$$

Da quest'ultimo conto si comprende bene che non è affatto scontato che le cose debbano sempre funzionare bene (così come è *fortunosamente* avvenuto

in quest'esempio), perché il risultato dell'operazione potrebbe dipendere dal particolare intero che si è scelto quale rappresentante della classe. In altre parole per assicurarsi che le nuove operazioni (*) in $\mathbb{Z}_n$ siano correttamente definite, occorre controllare che il risultato delle somma $\overline{a}+\overline{b}$ e del prodotto $\overline{a}\cdot\overline{b}$ tra le classi $\overline{a}$ e $\overline{b}$ non dipenda dalla scelta dei rappresentanti a e b di queste ultime. Verifichiamolo:

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

$\mathbb{Z}_2$

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

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

$\mathbb{Z}_3$

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

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

$\mathbb{Z}_4$

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

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

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.

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 $\overline{a}^{-1} = \overline{\alpha}$.*

Dimostrazione. Se a è coprimo con n, cioè $(n, a) = 1$, allora applicando l'algoritmo di Euclide esteso determiniamo interi α e β tali che $1 = \alpha a + \beta n$. Dunque $\alpha a - 1 = -\beta n$, cioè $n | \alpha a - 1$. Ciò significa che $\alpha a \equiv 1 \mod n$, cioè che $\overline{\alpha} \cdot \overline{a} = \overline{\alpha a} = \overline{1}$. Ciò dimostra che $\overline{\alpha}$ è la classe inversa di $\overline{a}$.

Viceversa, supponiamo che $\overline{a}$ ammetta una classe inversa $\overline{b}$. Allora $\overline{1} = \overline{a} \cdot \overline{b} = \overline{ab}$, e dunque $ab \equiv 1 \mod n$. Ciò significa che $n | ab - 1$, dunque esiste un intero γ tale che $ab - 1 = n\gamma$. Si ha allora che $1 = ab - n\gamma$. Dunque se $d = (n, a)$, poiché d divide sia a che n, dalla eguaglianza precedente ricaviamo che $d | 1$. Dunque $d = 1$, cioè n ed a sono coprimi. ∎

Dal teorema precedente segue subito il seguente

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.*

Una applicazione famosa: LA PROVA DEL NOVE. *Dati due interi* $a, b \in \mathbb{Z}$*, se* $a = b$ *allora anche* $a \equiv b \mod 9$*, mentre il viceversa è generalmente falso. Tuttavia se* $a \neq b$ *vi è una certa probabilità (non nulla) che* $a \not\equiv b \mod 9$*. Inoltre nella* ATTIVITÀ 1.1 *si è verificato che le operazioni algebriche rispettano le congruenze. E questo è il motivo per cui si introduce in modo efficace la prova del nove.*

Svolgimento. Verifichiamo infatti che la usuale riduzione - degli operandi e del risultato di una operazione - che si attua nella prova del nove altro non è che la riduzione mod 9, quella cioè che associa ad un intero m la sua classe $\overline{m} \in \mathbb{Z}_9$. Assegnato un intero non negativo m, sia dunque $x_i x_{i-1} \dots x_1 x_0$ la sua scrittura in cifre in base 10. Allora

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

e dunque, essendo $10 \equiv 1 \mod 9$ e quindi anche $10^j \equiv 1^j \equiv 1 \mod 9$ per ogni $j = 1, \dots, i$, se ne deduce che

$$m \equiv x_0 + x_1 + x_2 + \dots x_i \mod 9$$

cioè che $\overline{m} = \overline{x_0 + x_1 + x_2 + \dots x_i}$. ∎

Se è vero che $10 \equiv 1 \mod 9$, è altrettanto vero che $10 \equiv -1 \mod 11$. Questo suggerisce il seguente

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

2 La funzione φ di Eulero

Vogliamo contare, per ogni intero positivo n, il numero $\sharp$ delle classi invertibili in $\mathbb{Z}_n$. Poiché sappiamo, in virtù del Teorema 1.5, che $\overline{a} \in \mathbb{Z}_n$ è invertibile se e solo se $(a, n) = 1$, ciò equivale a definire l'applicazione:

$$\varphi : \{n \in \mathbb{Z} \mid n > 0\} \to \mathbb{N}, \qquad n \mapsto \varphi(n) = \sharp\{\overline{a} \in \mathbb{Z}_n \mid (a, n) = 1\}.$$

Tale φ è detta FUNZIONE DI EULERO.

Vediamo subito alcune prime importanti proprietà di φ.

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*

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

(infatti se $0 \leq a < p^k$, allora $(a, p^k) \neq 1$ se e solo se $p|a$ ...).

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

Dato che si riesce facilmente a calcolare $\varphi(p^k)$ per p primo e $k \geq 1$ intero, e che ogni intero $n \geq 2$ si lascia fattorizzare nel prodotto di potenze intere di primi, sembra lecito sperare che si possa trovare una formula esplicita per $\varphi(n)$, qualunque sia $n \geq 2$. Naturalmente ciò che serve è una regolarità dell'azione di φ sui prodotti.

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

Dunque abbiamo appena dimostrato che in generale è falso che $\varphi(m{\cdot}n) = \varphi(m) \cdot \varphi(n)$. Tuttavia, abbiamo nello stesso tempo verificato che in almeno un caso ciò è vero, precisamente $\varphi(3) \cdot \varphi(4) = \varphi(3 \cdot 4)$, con $(3, 4) = 1$.

Teorema 2.3. *La funzione di Eulero è relativamente moltiplicativa, cioè per ogni coppia m, n di interi maggiori o eguali a 2*

$$\textit{se } (m, n) = 1 \textit{ allora } \varphi(mn) = \varphi(m)\varphi(n).$$

Alla dimostrazione di questo teorema è dedicata l'Appendice al IV incontro.

3 Calcolo esplicito di φ

Consideriamo ora un arbitrario intero $n \geq 2$. Sia $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ la sua fattorizzazione in prodotto di primi. Allora $n = p_1^{e_1} \cdot (p_2^{e_2} \cdots p_t^{e_t})$ fornisce una scrittura di n come prodotto di due fattori coprimi, perciò dal Teorema 2.3 otteniamo subito che $\varphi(n) = \varphi(p_1^{e_1})\,\varphi(p_2^{e_2} \cdots p_t^{e_t})$. A sua volta $p_2^{e_2} \cdots p_t^{e_t} = p_2^{e_2} \cdot (p_3^{e_3} \cdots p_t^{e_t})$ è un prodotto di fattori coprimi, e dunque $\varphi(n) = \varphi(p_1^{e_1})\,\varphi(p_2^{e_2})\,\varphi(p_3^{e_3} \cdots p_t^{e_t})$. Così, iterando il procedimento, otteniamo che

$$\varphi(n) = \varphi(p_1^{e_1})\,\varphi(p_2^{e_2}) \cdots \varphi(p_t^{e_t}).$$

Inoltre nell' Esempio 2.1 si è visto che se p è primo allora

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

Ciò dimostra il seguente

Teorema 3.1. *Se $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, con p_i primi a due a due distinti, allora*

$$\varphi(n) = p_1^{e_1-1}(p_1-1)\ p_2^{e_2-1}(p_2-1)\ \cdots\ p_t^{e_t-1}(p_t-1).$$

Facciamo ora un po' di pratica con la funzione di Eulero.

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.*

Come sappiamo, la determinazione di fattori primi "molto grandi" di un intero n è estremamente onerosa dal punto di vista computazionale.

Osservazione 3.4. *Supponiamo che p e q siano interi primi distinti e che n sia il loro prodotto. Allora:*

- *se conosciamo p e q, allora è evidente che sia $n = pq$ che $\varphi(n) = (p-1)(q-1)$ sono subito noti;*

- *viceversa, da* $\varphi(n) = \varphi(pq) = (p-1)(q-1) = pq - (p+q) + 1$ *ricaviamo subito* $p + q = n - \varphi(n) + 1$. *Perciò* p *e* q *sono le due soluzioni dell'equazione di secondo grado* $X^2 - (n - \varphi(n) + 1)X + n = 0$. *Dunque se conosciamo* n *e* $\varphi(n)$, *allora* p *e* q *sono subito noti.*

In definitiva, dal punto di vista del "costo computazionale", **assegnato** n**, conoscere** $\varphi(n)$ **è equivalente a conoscere i fattori primi** p **e** q **di** n.

Perciò a partire da n $(= pq)$, **la complessità algoritmica del calcolo di** $\varphi(n)$ è equivalente a quella della determinazione dei fattori primi p e q di n. Come vedremo, tale complessità **costituisce la base della sicurezza del metodo crittografico a chiave pubblica RSA**.