Crittografia ed Aritmetica Modulare
– Appendice al IV incontro –

PLS - CAM

Padova, 7 novembre 2014

1 Prodotto diretto di classi resto e Teorema Cinese del Resto

In questa Appendice ci proponiamo di dimostrare il Teorema 2.3 del IV incontro, che afferma che la funzione di Eulero è *relativamente moltiplicativa*, cioè che $\varphi(mn) = \varphi(m)\,\varphi(n)$ ogniqualvolta m ed n sono interi ≥ 2 tra loro *coprimi*.

Nel seguito, assumeremo sempre che m e n siano fissati numeri interi ≥ 2. Iniziamo con l'introdurre una naturale generalizzazione delle classi resto modulo n.

Consideriamo il prodotto cartesiano

$$\mathbb{Z}_m \times \mathbb{Z}_n = \{(\overline{a}, \overline{b}) \mid \overline{a} \in \mathbb{Z}_m,\ \overline{b} \in \mathbb{Z}_n\};$$

ad esempio

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2})\},$$

dove dobbiamo stare ben attenti ad intendere le prime entrate come classi modulo 2, e le seconde entrate come classi modulo 3.

Per evidenziare che gli elementi di $\mathbb{Z}_m \times \mathbb{Z}_n$ sono coppie ordinate di classi resto modulo interi, rispettivamente, m e n che sono generalmente distinti, preferiremo talvolta scrivere $(a + m\mathbb{Z}, b + n\mathbb{Z})$ in luogo di $(\overline{a}, \overline{b})$.

Così come abbiamo già fatto per $\mathbb{Z}_n$, possiamo naturalmente introdurre nuove operazioni di addizione e moltiplicazione in $\mathbb{Z}_m \times \mathbb{Z}_n$, semplicemente agendo sulle singole componenti. Poniamo cioè

$$(a_1 + m\mathbb{Z}, b_1 + n\mathbb{Z}) + (a_2 + m\mathbb{Z}, b_2 + n\mathbb{Z}) := (a_1 + a_2 + m\mathbb{Z}, b_1 + b_2 + n\mathbb{Z}),$$

$$(a_1 + m\mathbb{Z}, b_1 + n\mathbb{Z}) \cdot (a_2 + m\mathbb{Z}, b_2 + n\mathbb{Z}) := (a_1 a_2 + m\mathbb{Z}, b_1 b_2 + n\mathbb{Z}).$$

È dunque immediato verificare che $(0 + m\mathbb{Z}, 0 + n\mathbb{Z})$ è l'elemento neutro per l'addizione, così come $(1 + m\mathbb{Z}, 1 + n\mathbb{Z})$ è l'elemento neutro per la moltiplicazione.

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.*

Vogliamo ora trovare una relazione tra $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \times \mathbb{Z}_n$. Procedendo in modo naturale, ci chiediamo se è possibile associare ad ogni classe $a + mn\mathbb{Z} \in \mathbb{Z}_{mn}$ la coppia di classi $(a + m\mathbb{Z}, a + n\mathbb{Z}) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Ci chiediamo cioè se la posizione

$$f_{m,n} : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \qquad a + mn\mathbb{Z} \mapsto (a + m\mathbb{Z}, a + n\mathbb{Z})$$

definisca una applicazione. Dobbiamo per questo preoccuparci di controllare che il "risultato" $(a + m\mathbb{Z}, a + n\mathbb{Z}) \in \mathbb{Z}_m \times \mathbb{Z}_n$ non dipenda di fatto dalla scelta del rappresentante a della classe $a + mn\mathbb{Z} \in \mathbb{Z}_{mn}$, bensì solo dalla classe stessa.

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

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

Abbiamo dunque verificato che l'applicazione $f_{m,n}$ è ben definita. Calcoliamone ora un caso concreto, ad esempio $f_{2,3} : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$:

$$\begin{aligned} f_{2,3}(\overline{0}) &= (\overline{0}, \overline{0}), \\ f_{2,3}(\overline{1}) &= (\overline{1}, \overline{1}), \\ f_{2,3}(\overline{2}) &= (\overline{0}, \overline{2}), \\ f_{2,3}(\overline{3}) &= (\overline{1}, \overline{0}), \\ f_{2,3}(\overline{4}) &= (\overline{0}, \overline{1}), \\ f_{2,3}(\overline{5}) &= (\overline{1}, \overline{2}). \end{aligned}$$

Possiamo osservare che $f_{2,3}$ è biiettiva, ed inoltre essa si comporta in modo coerente con le operazioni di addizione e di moltiplicazione rispettivamente in $\mathbb{Z}_6$ e in $\mathbb{Z}_2 \times \mathbb{Z}_3$. Ad esempio:

$$f_{2,3}(\overline{1}) + f_{2,3}(\overline{3}) = (\overline{0}, \overline{1}) = f_{2,3}(\overline{4}),$$

ed anche

$$f_{2,3}(\overline{2}) \cdot f_{2,3}(\overline{4}) = (\overline{0}, \overline{2}) = f_{2,3}(\overline{2}) = f_{2,3}(\overline{8}).$$

Questa coerenza di $f_{m,n}$ con le operazioni introdotte, rispettivamente, nel suo dominio e codominio è un fatto del tutto generale. Infatti assegnati ad arbitrio interi positivi m ed n, qualunque siano $a, b \in \mathbb{Z}$ abbiamo

$$\begin{aligned} f_{m,n}(\overline{a}) + f_{m,n}(\overline{b}) &= (a + m\mathbb{Z}, a + n\mathbb{Z}) + (b + m\mathbb{Z}, b + n\mathbb{Z}) = \\ &= (a + b + m\mathbb{Z}, a + b + n\mathbb{Z}) = f_{m,n}(\overline{a + b}) = f_{m,n}(\overline{a} + \overline{b}) \end{aligned}$$

ed analogamente

$$\begin{aligned} f_{m,n}(\overline{a}) \cdot f_{m,n}(\overline{b}) &= (a + m\mathbb{Z}, a + n\mathbb{Z}) \cdot (b + m\mathbb{Z}, b + n\mathbb{Z}) = \\ &= (ab + m\mathbb{Z}, ab + n\mathbb{Z}) = f_{m,n}(\overline{ab}) = f_{m,n}(\overline{a} \cdot \overline{b}). \end{aligned}$$

Ciò dimostra la seguente

Proposizione 1.3. *L'applicazione $f_{m,n}$ rispetta le operazioni di addizione e di moltiplicazione, cioè $f_{m,n}(\overline{a} + \overline{b}) = f_{m,n}(\overline{a}) + f_{m,n}(\overline{b})$ e $f_{m,n}(\overline{a} \cdot \overline{b}) = f_{m,n}(\overline{a}) \cdot f_{m,n}(\overline{b})$.*

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?*

Dunque non sempre $f_{m,n}$ è suriettiva e/o iniettiva. Osserviamo comunque che, essendo il dominio $\mathbb{Z}_{mn}$ ed il codominio $\mathbb{Z}_m \times \mathbb{Z}_n$ entrambi insiemi finiti con il medesimo numero mn di elementi, l'applicazione $f_{m,n}$ è iniettiva se e solo se $f_{m,n}$ è suriettiva se e solo se $f_{m,n}$ è biiettiva.

Teorema 1.5 (TEOREMA CINESE DEL RESTO)**.** *L'applicazione* $f_{m,n}$ *è biiettiva se e solo se* m *e* n *sono coprimi.*

Dimostrazione. Supponiamo dapprima che $(m, n) = 1$, e proviamo che $f_{m,n}$ è iniettiva. Se $\overline{a}, \overline{b} \in \mathbb{Z}_{mn}$ sono tali che $f_{m,n}(\overline{a}) = f_{m,n}(\overline{b})$, allora

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

cioè

$$a + m\mathbb{Z} = b + m\mathbb{Z} \quad \text{e} \quad a + n\mathbb{Z} = b + n\mathbb{Z}.$$

Ciò significa che $a \equiv b \mod m$ e $a \equiv b \mod n$, cioè che $a - b$ è un intero diviso sia da m che da n. Poiché stiamo assumendo che m e n siano coprimi, ne deduciamo che $a - b$ è diviso anche dal loro prodotto mn, cioè $a \equiv b \mod mn$. Ma allora $\overline{a} = \overline{b}$ in $\mathbb{Z}_{mn}$, ed abbiamo concluso.

Viceversa, assumiamo ora che $d = (m, n) > 1$. Osserviamo che allora mn è un intero divisibile per d^2 e posto $a = mn/d \in \mathbb{Z}$, risulta sia $0 < a < mn$ che $m|a$ e $n|a$. Dunque

$$\overline{a} \neq \overline{0} \text{ in } \mathbb{Z}_{mn} \text{ e } f_{m,n}(\overline{a}) = (a + m\mathbb{Z}, a + n\mathbb{Z}) = (\overline{0}, \overline{0}) = f_{m,n}(\overline{0}).$$

Ciò prova che in tal caso $f_{m,n}$ non è iniettiva. ∎

Dunque se m e n sono coprimi, allora $f_{m,n}$ fornisce una biiezione tra $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \times \mathbb{Z}_n$, che conserva il prodotto in virtù della Proposizione 1.3. Inoltre $f_{m,n}(\overline{1}) = (\overline{1}, \overline{1})$. Ne deduciamo che $f_{m,n}$ induce una biiezione tra gli invertibili di $\mathbb{Z}_{mn}$ e gli invertibili di $\mathbb{Z}_m \times \mathbb{Z}_n$.

Abbiamo inoltre verificato, nella Attività 1.1, che gli elementi invertibili di $\mathbb{Z}_m \times \mathbb{Z}_n$ sono costituiti esattamente dalle coppie $(\overline{a}, \overline{b})$, ove $\overline{a}$ e $\overline{b}$ sono classi invertibili, rispettivamente, in $\mathbb{Z}_m$ ed in $\mathbb{Z}_n$.

Possiamo concludere pertanto che le classi invertibili di $\mathbb{Z}_{mn}$ sono tante quante le possibili coppie distinte $(\overline{a}, \overline{b})$, con $\overline{a}$ invertibile in $\mathbb{Z}_m$ e $\overline{b}$ invertibile in $\mathbb{Z}_n$.

Ciò dimostra il seguente importante

Corollario 1.6. *Se m e n sono coprimi, allora $\varphi(mn) = \varphi(m)\,\varphi(n)$.*

Concludiamo questa sezione con una applicazione del Teorema 1.5 ai sistemi di congruenze.

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"?*