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

PLS - CAM

Padova, 31 ottobre 2014

Esercizio 1.3. *Oggi, martedì 3 aprile, alle ore 21, devo prendere un treno per la Transilvania che mi porterà a destinazione in 57 ore. In che giorno ed a che ora arriverò?*

Svolgimento. Se sommo le 57 ore del viaggio alle ore 21 della partenza, ottengo 78 ore. Eseguendo la divisione intera per 24 ottengo:

$$78 = 24 \cdot 3 + 6$$

il che significa che arriverò 3 giorni dopo, cioè venerdì 6 aprile, alle ore 6. ∎

Esercizio 1.5. *Si verifichino le seguenti proprietà:*

- *se* $a|b$ *e* $b|c$*, allora* $a|c$*;*
- *se* $a|b$ *e* $b|a$*, allora ...*
- *se* $a|b$ *e* $a|c$*, allora* $a|\beta b + \gamma c$*, qualunque siano* $\beta, \gamma \in \mathbb{Z}$*;*
- $1|a$ *e* $a|0$*, per qualunque* $a \in \mathbb{Z}$*.*

Svolgimento. i) Se $a|b$, allora $b = ak_1$ per qualche $k_1 \in \mathbb{Z}$; similmente, se $b|c$ allora $c = bk_2$ per qualche $k_2 \in \mathbb{Z}$. Si ottiene quindi che $c = ak_1k_2$, cioè che $a|c$.

ii) Da $b = ak_1$ e $a = bk_2$, segue $a = ak_1k_2$, quindi $k_1k_2 = 1$: pertanto $k_1 = k_2 = 1$ oppure $k_1 = k_2 = -1$, dunque $a = b$ oppure $a = -b$.

iii) Se $b = ak_1$ e $c = ak_2$ allora, per ogni $\beta, \gamma \in \mathbb{Z}$, si ha che

$$\beta b + \gamma c = \beta a k_1 + \gamma a k_2 = a(\beta k_1 + \gamma k_2).$$

iv) Qualunque sia $a \in \mathbb{Z}$, si ha sempre $a = 1a$ e $0 = a0$. ∎

ATTIVITÀ 2.1. *Dopo aver fattorizzato entrambi i numeri, si calcoli*

$$d = (24750, 3900).$$

Svolgimento. $24750 = 2 \cdot 3^2 \cdot 5^3 \cdot 11$ e $3900 = 2^2 \cdot 3 \cdot 5^2 \cdot 13$, da cui si deriva che $d = (24750, 3900) = 2 \cdot 3 \cdot 5^2 = 150$. ∎

ATTIVITÀ 2.5. *Si determinino $d, \alpha, \beta \in \mathbb{Z}$ tali che*

$$d = (24750, 3900) = \alpha \cdot 24750 + \beta \cdot 3900.$$

Svolgimento. Utilizzando l'Algoritmo di Euclide esteso calcoliamo il massimo comune divisore tra 420 e 72, ed esprimiamolo come loro combinazione intera.

	1	0	24750	
-6	0	1	3900	$24750 = 3900 \cdot 6 + 1350$
-2	1	-6	1350	$3900 = 1350 \cdot 2 + 1200$
-1	-2	13	1200	$1350 = 1200 \cdot 1 + 150$
	3	-19	150	$1200 = 150 \cdot 8 + 0$
			0	

Otteniamo dunque che $(24750, 3900) = 150 = 3 \cdot 24750 - 19 \cdot 3900$. ∎

HOMEWORK 2.6. *Si scriva il codice (ad esempio in PARI/Gp) per un algoritmo che, assegnati interi positivi a e b, calcoli il loro massimo comune divisore $d = (a, b)$, e determini $\alpha, \beta \in \mathbb{Z}$ tali che $d = \alpha\, a + \beta\, b$.*

Svolgimento. È delegato ai docenti esperti di programmazione. ∎

HOMEWORK 2.7. *Si verifichi che gli interi che si ottengono come combinazione intera di preassegnati interi positivi a, b sono esattamente i multipli del loro massimo comune divisore $d = (a, b)$, cioè:*

$$\{z \in \mathbb{Z} \mid z = \alpha\, a + \beta\, b,\ \alpha, \beta \in \mathbb{Z}\} = d\mathbb{Z}.$$

Svolgimento. Nel terzo punto dell'Esercizio 1.5 si è verificato che ogni intero della forma $z = \alpha\, a + \beta\, b$, con $\alpha, \beta \in \mathbb{Z}$, è diviso da ogni comune divisore di a e b, quindi in particolare da $d = (a, b)$. Questo dimostra l'inclusione

$$\{z \in \mathbb{Z} \mid z = \alpha\, a + \beta\, b,\ \alpha, \beta \in \mathbb{Z}\} \subseteq d\mathbb{Z}.$$

Proviamo ora l'inclusione opposta. Sia $z \in d\mathbb{Z}$, cosicché $z = dk$ per qualche $k \in \mathbb{Z}$. In forza della formula di Bézout esistono interi α_0 e β_0 tali che $d = (a, b) = \alpha_0 a + \beta_0 b$, ed allora $z = dk = \alpha_0 ka + \beta_0 kb$, e si conclude scegliendo $\alpha = \alpha_0 k$ e $\beta = \beta_0 k$. ∎

ATTIVITÀ 3.4. *Si dimostri la* Proposizione 3.3. *Si assuma cioè che dividendo a e b per n si ottengano resti r_1 e r_2 rispettivamente, e si dimostri che allora $n|a-b$ se e solo se $r_1 = r_2$.*

Svolgimento. Sia dunque

$$a = nq_1 + r_1, \text{ con } 0 \leq r_1 < n, \quad \text{ed anche} \quad b = nq_2 + r_2, \text{ con } 0 \leq r_2 < n.$$

Se $r_1 = r_2$, allora $a - b = n(q_1 - q_2)$, dunque $n|a-b$. Viceversa, se $n|a-b$ allora, per il terzo punto dell'Esercizio 1.5, otteniamo che n divide anche

$$(a-b) - n(q_1 - q_2) = (a - nq_1) - (b - nq_2) = r_1 - r_2.$$

Poiché $0 \leq r_1 < n$ e $0 \leq r_2 < n$, si ha subito che $0 \leq |r_1 - r_2| < n$, e ciò unitamente al fatto che $n|r_1 - r_2$ implica che $r_1 - r_2 = 0$. ∎