Crittografia ed Aritmetica Modulare
LABORATORIO del III incontro

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?*

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* $a \in \mathbb{Z}$*.*

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

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

ATTIVITÀ 2.5. *Si determinino (per mezzo dell'Algoritmo di Euclide esteso)* $d, \alpha, \beta \in \mathbb{Z}$ *tali che*

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

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* $d = \alpha\, a + \beta\, b$*.*

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:*

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

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* $r_1 = r_2$*.*