Corso di Laurea in Matematica.
Algebra. a.a. 2023-24. Canale 1. Proff. Piazza e Viaggi
Compito a casa del 21/10/2023

Rivedere:

- Proprietà elementari del MCD di due interi
- Algoritmo di Euclide
- Identità di Bezout

Esercizio 1. Determinare il MCD ed un'identità di Bezout per $a = 14322$ e $b = 6153$.

Rivedere:

- L'anello $\mathbb{Z}_n$
- Equazioni diofantee di primo grado: $ax + by = c$, $a, b, c \in \mathbb{Z}$
- Elementi invertibili in $\mathbb{Z}_n$ e loro determinazione tramite Bezout
- l'equazioni congruenziale $aX \equiv b(n)$. Risolubilità e determinazione di tutte le soluzioni mod n.

Esercizio 2. Trovare tutte le soluzioni mod 33 dell'equazione congruenziale

$$121X \equiv 22(33)\,.$$

Esercizio 3.
1. Verificare che i numeri 897 e 4403 sono coprimi.
2. Determinare una soluzione $(\tilde{x}, \tilde{y}) \in \mathbb{Z} \times \mathbb{Z}$ dell'equazione diofantea

$$897x + 4403y = 1 \tag{1}$$

3. Verificare che se $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ è una soluzione dell'equazione omogonea associata, $897x + 4403y = 0$, allora $(\tilde{x} + x_0, \tilde{y} + y_0)$ è una soluzione di (1).
Viceversa, verificare che se $(x', y') \in \mathbb{Z} \times \mathbb{Z}$ è soluzione di (1) allora esiste (x_0, y_0) tale che $(x', y') = (\tilde{x}, \tilde{y}) + (x_0, y_0)$.
Suggerimento: $(x', y') = (\tilde{x}, \tilde{y}) + ((x', y') - (\tilde{x}, \tilde{y}))$. [1].
4. Determinare tutte le soluzioni di (1).
Suggerimento: per risolvere l'equazione omogenea il Lemma di Euclide può risultare utile.

Esercizio 4. Verificare che $[8]$ è invertibile in $\mathbb{Z}_{385}$. Determinare tale inverso ed utilizzarlo per risolvere l'equazione congruenziale

$$8x \equiv 3 \,(\mathrm{mod}\, 385).$$

Esercizio 5. Determinare $\mathcal{U}(\mathbb{Z}_{24})$.
Quali di questi hanno quadrato uguale all'unità ?

[1] In conclusione, le soluzioni di (1) si ottengono sommando ad una soluzione particolare di (1) tutte le soluzioni dell'equazione omogenea associata.
Questo è ovviamente un risultato generale, valido per una qualsiasi equazione diofantea $ax+by = c$