Corso di Laurea in Matematica.
Algebra 1. a.a. 2018-19. Proff. P. Papi e P. Piazza
Esercitazione <u>in classe</u> del 3/10/2018

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

Esercizio 1. Determinare il MCD ed un'identità di Bezout per $a = -123$ e $b = -39$.

Esercizio 2. Determinare il MCD ed un'identità di Bezout per $a = 14322$ e $b = 6153$.

- L'anello $\mathbb{Z}_n$
- 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 3. Trovare tutte le soluzioni mod 33 dell'equazione congruenziale

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

- Sistemi cinesi di equazioni congruenziali
- Teorema cinese del resto
- metodo di sostituzione

Esercizio 4. Trovare l'unica soluzione mod $385 = 5 \cdot 7 \cdot 11$ del sistema cinese

$$\begin{cases} X \equiv 3(5) \\ X \equiv 4(7) \\ X \equiv 4(11) \end{cases}.$$

Soluzione.
Rivediamo la soluzione, dato che è stata spiegata molto rapidamente alla fine della lezione.
La prima equazione ha soluzione generica $x = 3 + 5t_1$.
Sostituiamo questa soluzione generica nella seconda equazione; deve essere $3+5t_1 \equiv 4(7)$; aggiungiamo ad ambo i membri 4 ed otteniamo $7 + 5t_1 = 8(7)$ che possiamo riscrivere come $5t_1 = 1(7)$. Ma 5 e 7 sono comprimi (è qui che utilizziamo l'ipotesi) e quindi 5 ammette un inverso moltiplicativo mod (7) e questo inverso è 3. Ne segue che $t_1 = 3(7)$ e cioè $t_1 = 3 + 7t_2$. Quindi

$$x = 3 + 5(3 + 7t_2) = 18 + 5 \cdot 7t_2$$

Sostituiamo questa espressione nella terza equazione e otteniamo:
$18+5\cdot 7t_2 \equiv 4(11)$ che riscriviamo come $22+35t_2 \equiv 8(11)$ e cioè come $35t_2 \equiv 8(11)$. Ora, per ipotesi, 35 è coprimo con 11 e quindi 35 ammette un inverso mod 11. Per trovarlo osserviamo che, ovviamente, $35 \equiv 2(11)$ e che un inverso moltiplicativo di 2 mod 11 è 6. Riassumendo: $35t_2 \equiv 8(11)$ è uguale a $2t_2 \equiv 8(11)$ che moltiplicata per 6 dà $t_2 \equiv 48(11)$ che è la stessa cosa di $t_2 \equiv 4(11)$. Quindi $t_2 = 4 + 11t_3$.
Ora sostituiamo questa espressione in $x = 18 + 5 \cdot 7t_2$ e otteniamo

$$x = 18 + 5 \cdot 7t_2 = 18 + 5 \cdot 7(4 + 11t_3) = 158 + 5 \cdot 7 \cdot 11t_3\,.$$

Ne deduciamo che l'unica soluzione del sistema mod $5 \cdot 7 \cdot 11 = 385$ è 158.