*Università degli Studi di Roma "Tor Vergata"*

*CdL in Ingegneria Informatica*

corso di "Algebra e Logica" (prof. Fabio Gavarini)

# Tutorato su EQUAZIONI CONGRUENZIALI e MODULARI, ARITMETICA MODULARE

..... * .....

**1** — *(a)* Calcolare $MCD(267, 112)$ ed una identità di Bézout per esso.

*(b)* Calcolare (se esiste) una soluzione dell'equazione diofantea $267\,x + 112\,y = 14$ .

*(c)* Calcolare tutte le soluzioni in $\mathbb{Z}_{267}$ dell'equazione modulare $\overline{112}\,\overline{x} = \overline{14}$ .

*(d)* Calcolare, se esiste, l'inverso $\overline{112}^{-1} \in \mathbb{Z}_{267}$ della classe $\overline{112} \in \mathbb{Z}_{267}$ .

**2** — Calcolare tutte le soluzioni della equazione congruenziale $259\,x \equiv 16 \pmod{11}$ .

**3** — *(a)* Determinare se esista la classe $\overline{6}^{-1}$ inversa di $\overline{6}$ in $\mathbb{Z}_{30}$ e in $\mathbb{Z}_{31}$ . In ciascun caso, se la risposta è positiva si calcoli esplicitamente la classe inversa $\overline{6}^{-1}$ .

*(b)* Risolvere l'equazione modulare $\overline{96}\,\overline{x} = \overline{21}$ nell'anello $\mathbb{Z}_{30}$ .

*(c)* Risolvere l'equazione modulare $\overline{37}\,\overline{x} = \overline{29}$ nell'anello $\mathbb{Z}_{31}$ .

**4** — *(a)* Calcolare — se esiste — la classe $\overline{z}^{-1} \in \mathbb{Z}_{100}$ inversa della classe $\overline{z} \in \mathbb{Z}_{100}$ per i casi $z := 65$ e $z := -137$ .

*(b)* Risolvere l'equazione $\overline{237} \cdot \overline{x} = \overline{181}$ in $\mathbb{Z}_{100}$ .

*(c)* Risolvere l'equazione congruenziale $363 \cdot x \equiv 219 \pmod{100}$ in $\mathbb{Z}$ .

**5** — Calcolare, se esiste, l'inverso $\overline{z}^{-1}$ di ciascuno dei seguenti elementi nel rispettivo anello unitario: $\overline{z} := \overline{91} \in \mathbb{Z}_{100}$ , $\overline{z} := \overline{37} \in \mathbb{Z}_{42}$ , $\overline{z} := \overline{28} \in \mathbb{Z}_{42}$ , $\overline{z} := \overline{21} \in \mathbb{Z}_{55}$ .

**6** — Per ciascuno dei due valori $n = 17$ e $n = 18$ si consideri il rispettivo anello $\mathbb{Z}_n$ delle classi resto dei numeri interi modulo $n$ .

*(a)* Calcolare i due gruppi degli elementi invertibili

$$U(\mathbb{Z}_{17}) := \left\{ \overline{z} \in \mathbb{Z}_{17} \,\middle|\, \exists\, \overline{z}^{-1} \in \mathbb{Z}_{17} : \overline{z} \cdot \overline{z}^{-1} = \overline{1} \right\}$$
$$U(\mathbb{Z}_{18}) := \left\{ \overline{z} \in \mathbb{Z}_{18} \,\middle|\, \exists\, \overline{z}^{-1} \in \mathbb{Z}_{18} : \overline{z} \cdot \overline{z}^{-1} = \overline{1} \right\}$$

*(b)* Risolvere, se possibile, ciascuna delle tre equazioni seguenti:

$\overline{40} \cdot \overline{x} = -\overline{4}$ in $\mathbb{Z}_{17}$ , $\overline{40} \cdot \overline{x} = -\overline{13}$ in $\mathbb{Z}_{18}$ , $\overline{25} \cdot \overline{x} = \overline{6}$ in $\mathbb{Z}_{18}$ .

*(c)* Determinare — se esiste — la classe $\overline{40}^{\,-1} \in \mathbb{Z}_{17}$ inversa della classe $\overline{40} \in \mathbb{Z}_{17}$, la classe $\overline{40}^{\,-1} \in \mathbb{Z}_{18}$ inversa di $\overline{40} \in \mathbb{Z}_{18}$ e la classe $\overline{35}^{\,-1} \in \mathbb{Z}_{18}$ inversa di $\overline{35} \in \mathbb{Z}_{18}$.

*Soluzioni:* *(a)* $U(\mathbb{Z}_{17}) = \left\{ \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{15}, \overline{16} \right\}$, $U(\mathbb{Z}_{18}) = \left\{ \overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17} \right\}$

*(b)* $\overline{x} = \overline{5} \in \mathbb{Z}_{17}$, $\nexists\, \overline{x} \in \mathbb{Z}_{18}$, $\overline{x} = \overline{6} \in \mathbb{Z}_{18}$.

*(c)* $\overline{40}^{\,-1} = \overline{6}^{\,-1} = \overline{3} \in \mathbb{Z}_{17}$, $\nexists\, \overline{40}^{\,-1} \in \mathbb{Z}_{18}$,
$\overline{35}^{\,-1} = \overline{17}^{\,-1} = \overline{-1}^{\,-1} = -\overline{1}^{\,-1} = -\overline{1} = \overline{17} = \overline{35} \in \mathbb{Z}_{18}$.

**7** — *(a)* Calcolare i due gruppi degli elementi invertibili

$$U(\mathbb{Z}_{23}) := \left\{ \overline{z} \in \mathbb{Z}_{23} \,\middle|\, \exists\, \overline{z}^{\,-1} \in \mathbb{Z}_{23} : \overline{z} \cdot \overline{z}^{\,-1} = \overline{1} \right\}$$
$$U(\mathbb{Z}_{10}) := \left\{ \overline{z} \in \mathbb{Z}_{10} \,\middle|\, \exists\, \overline{z}^{\,-1} \in \mathbb{Z}_{10} : \overline{z} \cdot \overline{z}^{\,-1} = \overline{1} \right\}$$

*(b)* Risolvere, se possibile, ciascuna delle tre equazioni seguenti:

$\overline{6} \cdot \overline{x} = \overline{28}$ in $\mathbb{Z}_{10}$, $\quad \overline{6} \cdot \overline{x} = \overline{13}$ in $\mathbb{Z}_{10}$, $\quad \overline{45} \cdot \overline{x} = \overline{6}$ in $\mathbb{Z}_{23}$.

*(c)* Determinare — se esiste — la classe $\overline{6}^{\,-1} \in \mathbb{Z}_{23}$ inversa della classe $\overline{6} \in \mathbb{Z}_{23}$, la classe $\overline{6}^{\,-1} \in \mathbb{Z}_{10}$ inversa di $\overline{6} \in \mathbb{Z}_{10}$ e la classe $\overline{7}^{\,-1} \in \mathbb{Z}_{10}$ inversa di $\overline{7} \in \mathbb{Z}_{10}$.

**8** — Per ciascuno dei due valori $n = 14$ e $n = 13$ si consideri il rispettivo anello $\mathbb{Z}_n$ delle classi resto dei numeri interi modulo $n$.

*(a)* Calcolare i due gruppi degli elementi invertibili

$$U(\mathbb{Z}_{14}) := \left\{ \overline{z} \in \mathbb{Z}_{14} \,\middle|\, \exists\, \overline{z}^{\,-1} \in \mathbb{Z}_{14} : \overline{z} \cdot \overline{z}^{\,-1} = \overline{1} \right\}$$
$$U(\mathbb{Z}_{13}) := \left\{ \overline{z} \in \mathbb{Z}_{13} \,\middle|\, \exists\, \overline{z}^{\,-1} \in \mathbb{Z}_{13} : \overline{z} \cdot \overline{z}^{\,-1} = \overline{1} \right\}$$

*(b)* Risolvere, se possibile, ciascuna delle tre equazioni seguenti:

$\overline{21} \cdot \overline{x} = -\overline{35}$ in $\mathbb{Z}_{14}$, $\quad \overline{13} \cdot \overline{x} = \overline{20}$ in $\mathbb{Z}_{14}$, $\quad \overline{21} \cdot \overline{x} = -\overline{35}$ in $\mathbb{Z}_{13}$.

*(c)* Determinare — se esiste — la classe $\overline{21}^{\,-1} \in \mathbb{Z}_{14}$ inversa della classe $\overline{21} \in \mathbb{Z}_{14}$, la classe $\overline{21}^{\,-1} \in \mathbb{Z}_{13}$ inversa di $\overline{21} \in \mathbb{Z}_{13}$ e la classe $\overline{5}^{\,-1} \in \mathbb{Z}_{14}$ inversa di $\overline{5} \in \mathbb{Z}_{14}$.

*Soluzioni:* *(a)* $U(\mathbb{Z}_{14}) = \left\{ \overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13} \right\}$, $U(\mathbb{Z}_{13}) = \left\{ \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{11}, \overline{12} \right\}$

*(b)* $\overline{x} \in \left\{ \overline{1} + \overline{2} \cdot \overline{k} \;\middle|\; \overline{k} \in \mathbb{Z}_{14} \right\} = \left\{ \overline{1}, \overline{3}, \overline{5}, \ldots, \overline{11}, \overline{13} \right\} \subseteq \mathbb{Z}_{14}$,
$\overline{x} = \overline{8} \in \mathbb{Z}_{14}$, $\quad \overline{x} = \overline{7} \in \mathbb{Z}_{13}$.

*(c)* $\nexists\, \overline{21}^{\,-1} \in \mathbb{Z}_{14}$, $\quad \overline{21}^{\,-1} = \overline{8}^{\,-1} = \overline{5} \in \mathbb{Z}_{13}$, $\quad \overline{5}^{\,-1} = \overline{3} \in \mathbb{Z}_{14}$.

**9** — Scrivendo i numeri naturali in base $b :=$ CINQUE, determinare se il numero $N := (42103241)_b$ sia divisibile per $(4)_b$ oppure per $(11)_b$.

**10** — Scrivendo i numeri naturali in base $b :=$ NOVE, determinare se $N := (560382741)_b$ sia divisibile per $(84)_b$, oppure per $(11)_b$, oppure per $(3)_b$.

**11** — Siano $b := 10$, $b' := 5$, $b'' := 8$. Per ciascuna delle domande seguenti, si giustifichi adeguatamente la risposta:

*(a)* $(81034)_b$ è divisibile per $(3)_b$ ?

*(b)* $(27506)_b$ è divisibile per $(9)_b$ ?

*(c)* $(3180452)_b$ è divisibile per $(11)_b$ ?

*(d)* $(4301224)_{b'}$ è divisibile per $(6)_{b''}$ ?

**12** — Calcolare il resto $r$ nella divisione di $907^{64972}$ per $21$.

**13** — Calcolare il resto nella divisione per 20 dei tre numeri

$$a := 457^{35062867} \quad , \qquad b := 2384^{16} \quad , \qquad c := 645^{5607290843}$$

**14** — Calcolare il resto nella divisione per 11 dei due numeri

$$A := 1111111^{44444444} \quad , \qquad B := 999999999^{333333333}$$

**15** — Determinare, se esiste, un numero intero $z \in \mathbb{Z}$ tale che

$$31 \leq z \leq 50 \qquad \text{e} \qquad z \equiv N \mod 20$$

dove $N$ è il numero intero $N := 837^{65084}$. Se invece un tale $z$ non esiste, si spieghi perché.