ESERCIZI DI

ARITMETICA MODULARE

N.B.: il simbolo ⛑ *contrassegna gli esercizi (relativamente) più complessi.*

— ∗ —

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

2 — Sia $n \in \mathbb{Z}$ un intero che diviso per 7 ha resto 5 e sia $m \in \mathbb{Z}$ un intero che diviso per 7 ha resto 3. Dividendo $n + m$ per 7, che resto si trova? Dividendo $n \cdot m$ per 7, che resto si trova? *(giustificare adeguatamente le risposte)*

Suggerimento: *Le ipotesi dicono che* $[n]_7 = [5]_7 \in \mathbb{Z}_7$ *e* $[m]_7 = [3]_7 \in \mathbb{Z}_7$ *; quindi...*

3 — *(a)* Determinare se esistano le classi inverse $\overline{9}^{\,-1}$, $\overline{5}^{\,-1}$, $\overline{7}^{\,-1}$, $\left(\overline{9}\cdot\overline{7}\right)^{-1}$ e $\left(\overline{5}\cdot\overline{7}\right)^{-1}$ nell'anello $\mathbb{Z}_{20}$ degli interi modulo 20 . In caso negativo, si spieghi perché tale classe inversa non esista; in caso affermativo, si calcoli esplicitamente la suddetta classe inversa.

(b) Calcolare tutte le soluzioni dell'equazione modulare $\overline{647}\,\overline{x} = \overline{-516}$ in $\mathbb{Z}_{20}$.

(c) Calcolare tutte le soluzioni dell'equazione congruenziale $436\,x \equiv 92 \pmod{20}$ in $\mathbb{Z}$.

4 — Per ogni $n \in \mathbb{N}_+$ e per ogni $a \in \mathbb{Z}$, sia $f_{\overline{a}} : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ la funzione definita da $\overline{z} \mapsto f_{\overline{a}}(\overline{z}) := \overline{a} \cdot \overline{z}$ per ogni $\overline{z} \in \mathbb{Z}_n$.

(a) Dimostrare che $f_{\overline{a}}$ è iniettiva se e soltanto se è suriettiva.

(b) Verificare che la funzione $f_{\overline{a}}$ è $\mathbb{Z}_n$–lineare, cioè

$$f_{\overline{a}}(\overline{c}_1\,\overline{x}_1 + \overline{c}_2\,\overline{x}_2) = \overline{c}_1\, f_{\overline{a}}(\overline{x}_1) + \overline{c}_2\, f_{\overline{a}}(\overline{x}_2) \qquad \forall\ \overline{c}_1, \overline{c}_2 \in \mathbb{Z}_n\ , \quad \forall\ \overline{x}_1, \overline{x}_2 \in \mathbb{Z}_n\ .$$

(c) Posto $Ker(f_{\overline{a}}) := \left\{ \overline{z} \in \mathbb{Z}_n \,\middle|\, f_{\overline{a}}(\overline{z}) = \overline{0} \right\}$, dimostrare che

$$f_{\overline{a}} \text{ è iniettiva } \iff Ker(f_{\overline{a}}) = \left\{\overline{0}\right\}$$

(d) Posto $U(\mathbb{Z}_n) := \left\{ \overline{z} \in \mathbb{Z}_n \,\middle|\, \overline{z} \text{ è invertibile} \right\} = \left\{ \overline{z} \in \mathbb{Z}_n \,\middle|\, \exists\, \overline{\zeta} : \overline{z}\,\overline{\zeta} = \overline{1} \right\}$, dimostrare che $f_{\overline{a}}$ è suriettiva $\iff \overline{a} \in U(\mathbb{Z}_n)$.

(e) Dimostrare che $f_{\overline{a}}$ è iniettiva $\iff \overline{a} \in U(\mathbb{Z}_n)$.

Suggerimento: *Per la parte (e), l'implicazione "*$\Leftarrow$*" segue direttamente dalle definizione; l'implicazione inversa "*$\Rightarrow$*" invece richiede l'uso dei risultati in (a) e in (d) qui sopra.*

5 — Verificare che in $\mathbb{Z}_{21}$ si ha $\quad \overline{5}^{\,159} = -\overline{1}$, $\quad \overline{3}^{\,41} = \overline{12}$, $\quad \overline{15}^{\,159} = -\overline{6}$.

6 — Calcolare le ultime due cifre decimali di $7^{\,6503219}$.

7 — Calcolare il resto nella divisione per 20 dei tre numeri

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

8 — *Senza calcolare* esplicitamente il prodotto, verificare che

$$2468 \cdot 13579 \equiv -3 \pmod{25}$$

Suggerimento: Il problema è equivalente a verificare che sia $\overline{2468} \cdot \overline{13579} = -\overline{3}$ *in* $\mathbb{Z}_{25}$.

9 — *Senza calcolare* esplicitamente il prodotto che li definisce, determinare il resto della divisione per 10 e per 5 dei seguenti tre numeri:

$$a := 12345678 \cdot 90123 \ , \quad b := 9085679 \cdot 120001 \ , \quad c := 4876515329871674 \cdot 765976$$

Suggerimento: Si passi alle classi di congruenza modulo 10 (nel primo caso) e modulo 5 (nel secondo caso), e poi si facciano i calcoli in $\mathbb{Z}_{10}$ *e in* $\mathbb{Z}_5$ *rispettivamente.*

10 — Sia $N := \big(c_k c_{k-1} \cdots c_1 c_0\big)_b$ un numero naturale rappresentato in base $b :=$ DIECI .

(a) Dimostrare che $N \equiv c_k + c_{k-1} + \cdots + c_1 + c_0 \pmod{9}$.

(b) Dimostrare che $N \equiv c_0 - c_1 + \cdots + (-1)^{k-1} c_{k-1} + (-1)^k c_k \pmod{11}$.

(c) Usare il risultato in *(a)* per dimostrare che $54321 \cdot 98765 \neq 5363013565$.

(d) Usare il risultato in *(b)* per determinare se 121314151617 sia divisibile per 11.

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

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

Suggerimento: Si può sfruttare l'esercizio **10** *qui sopra.*

12 — Determinare il resto delle divisioni per 3, 9, 4 e 11 del numero $N := 3548917$.

Suggerimento: Nel caso della divisione per 9 e per 11 si può sfruttare l'esercizio **8**.

13 — Dato $b \in \mathbb{N}_+ \setminus \{1\}$, sia $N := \big(c_k c_{k-1} \cdots c_1 c_0\big)_b \in \mathbb{N}$ un numero naturale rappresentato in base b.

(a) Dimostrare che $N \equiv c_k + c_{k-1} + \cdots + c_1 + c_0 \pmod{(b-1)}$.

(b) Dimostrare che $N \equiv c_0 - c_1 + \cdots + (-1)^{k-1} c_{k-1} + (-1)^k c_k \pmod{(b+1)}$.

(c) Per ogni $d \in \mathbb{Z}$ che sia divisore di b, si ha $d \,\big|\, N \iff d \,\big|\, c_0$ (in parole, "N è divisibile per d se e soltanto se l'ultima cifra di N è divisibile per d").

(d) Per ogni $d \in \mathbb{Z}$ tale che $d \,\big|\, b$ ma $d^2 \nmid b$, si ha (per ogni $s \in \mathbb{N}_+$)

$$d^s \,\big|\, N \iff d^s \,\big|\, \big(c_{s-1} \cdots c_1 c_0\big)_b$$

(in parole, "N è divisibile per d se e soltanto se [il numero formato dal]le ultime s cifre di N è divisibile per d").

Suggerimento: *Le parti (a) e (b) sono la diretta generalizzazione delle analoghe parti dell'esercizio* **10** *qui sopra.*

14 — Calcolare tutte le soluzioni dell'equazione congruenziale

$$580397^{\,6250395}\, x \equiv -4251093768 \pmod{20}$$

Suggerimento: *L'equazione congruenziale assegnata corrisponde all'equazione modulare* $\overline{580397}^{\,6250395}\, \overline{x} = -\overline{4251093768}$ *in* $\mathbb{Z}_{20}$, *quindi si risolva quest'ultima e dalle sua soluzione si deduca la soluzione del problema iniziale.*

15 — Determinare tutti i numeri $x \in \mathbb{Z}$ che soddisfino *simultaneamente* le tre condizioni seguenti:

$$317\, x \equiv 287 \pmod{14} \quad (\text{in } \mathbb{Z}), \qquad -\overline{71}\, \overline{x} = \overline{414} \quad (\text{in } \mathbb{Z}_{11}), \qquad 101 \le x \le 200$$

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

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

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

17 — *(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 $z := -435$ e $z := 63$.

(b) Risolvere l'equazione $\overline{-563} \cdot \overline{x} = \overline{-908}$ in $\mathbb{Z}_{100}$.

(c) Risolvere l'equazione congruenziale $437 \cdot x \equiv 192 \pmod{100}$ in $\mathbb{Z}$.

18 — Determinare tutti i valori di $x \in \mathbb{Z}$ che siano soluzioni *simultaneamente* delle due equazioni modulari seguenti:

$$\circledast : \begin{cases} [39]_7 \cdot [x]_7 = -[15]_7 & \text{in } \mathbb{Z}_7 \\ [-13]_{11} \cdot [x]_{11} = [56]_{11} & \text{in } \mathbb{Z}_{11} \end{cases}$$

19 — *(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:

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

(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 $\overline{7} \in \mathbb{Z}_{10}$.

20 — Risolvere le seguenti equazioni modulari di secondo grado a coefficienti in $\mathbb{Z}_{11}$:

$$x^2 - \overline{8}\,x + \overline{4} = \overline{0} \quad , \qquad x^2 - \overline{3}\,x + \overline{5} = \overline{0} \quad , \qquad x^2 + \overline{3}\,x + \overline{6} = \overline{0}$$

Suggerimento: *Si provi ad applicare la consueta (!) formula risolutiva delle equazioni di secondo grado, discutendo se abbia effettivamente senso utilizzarla...*