SOLUZIONI: TEORIA DEI NUMERI

La numerazione è la stessa del file degli esercizi.

Sono svolti i **primi due esercizi di ogni blocco** — così ogni tipologia ha il suo modello — e **tutti quelli di livello ■■■■**. Degli algoritmi (Euclide, Bézout, teorema cinese) sono scritte **tutte le righe**: sono quelle che si devono imparare a mettere sul foglio, non il risultato.

1. Divisibilità e divisione euclidea

Esercizio 1.

$\to 3 \mid 12$

$\to$ Cerco un intero k con $12 = 3 \cdot k$. ($a \mid b$ vuol dire che b è a per qualcosa)

$\to k = 4$ funziona, quindi vero.

Esercizio 2.

$\to 12 \mid 3$

$\to$ Cerco un intero k con $3 = 12 \cdot k$.

$\to$ Non esiste: 3 : 12 non è intero. Quindi falso.

Esercizio 21.

$\to 47 = 5 \cdot q + r$

$\to$ Divido e tengo il resto **positivo**: $47 = 5 \cdot 9 + 2$. (la condizione $0 \leq r < d$ è quella che rende q e r unici)

$\to$ **q = 9, r = 2**

Esercizio 22.

$\to 100 = 7 \cdot q + r$

$\to$ Divido e tengo il resto **positivo**: $100 = 7 \cdot 14 + 2$.

$\to$ **q = 14, r = 2**

---

2. MCD e algoritmo di Euclide

Esercizio 41.

→ MCD$(12, 18)$

→ Applico l'algoritmo di Euclide: divido, tengo il resto, ripeto. (il MCD non cambia sostituendo il numero grande col resto)

→

$$\begin{aligned} 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

→ L'ultimo resto non nullo è **6**. (sono bastate 2 divisioni)

Esercizio 42.

→ MCD$(24, 36)$

→ Applico l'algoritmo di Euclide: divido, tengo il resto, ripeto.

→

$$\begin{aligned} 36 &= 1 \cdot 24 + 12 \\ 24 &= 2 \cdot 12 + 0 \end{aligned}$$

→ L'ultimo resto non nullo è **12**.

Esercizio 81.

→ MCD$(1071, 462)$

→ Applico l'algoritmo di Euclide: divido, tengo il resto, ripeto.

→

$$\begin{aligned} 1071 &= 2 \cdot 462 + 147 \\ 462 &= 3 \cdot 147 + 21 \\ 147 &= 7 \cdot 21 + 0 \end{aligned}$$

→ L'ultimo resto non nullo è **21**.

Esercizio 82.

→ MCD$(2322, 654)$

→ Applico l'algoritmo di Euclide: divido, tengo il resto, ripeto.

→

$$\begin{aligned} 2322 &= 3 \cdot 654 + 360 \\ 654 &= 1 \cdot 360 + 294 \\ 360 &= 1 \cdot 294 + 66 \\ 294 &= 4 \cdot 66 + 30 \\ 66 &= 2 \cdot 30 + 6 \\ 30 &= 5 \cdot 6 + 0 \end{aligned}$$

→ L'ultimo resto non nullo è **6**.

---

3. Identità di Bézout

Esercizio 101.

→ Trova x, y con $7x + 5y = \text{MCD}(7, 5)$

→ Prima Euclide, tenendo tutte le righe: (i coefficienti si trovano risalendo l'algoritmo)

→

$$\begin{aligned} 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

→ Poi risalgo: isolo il resto in ogni riga e sostituisco, senza mai moltiplicare 7 e 5 fra loro. (se si fanno i conti si perde di vista chi è a e chi è b)

→ $\mathbf{7} \cdot (\mathbf{-2}) + \mathbf{5} \cdot (\mathbf{3}) = \mathbf{1}$

→ Controllo: $-14 + 15 = 1$.

Esercizio 102.

→ Trova x, y con $11x + 4y = \text{MCD}(11, 4)$

→ Prima Euclide, tenendo tutte le righe:

→

$$\begin{aligned} 11 &= 2 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

→ Poi risalgo: isolo il resto in ogni riga e sostituisco, senza mai moltiplicare 11 e 4 fra loro.

→ $\mathbf{11} \cdot (\mathbf{-1}) + \mathbf{4} \cdot (\mathbf{3}) = \mathbf{1}$

→ Controllo: $-11 + 12 = 1$.

Esercizio 131.

→ Trova x, y con $1071x + 462y = \text{MCD}(1071, 462)$

→ Prima Euclide, tenendo tutte le righe:

→

$$\begin{aligned} 1071 &= 2 \cdot 462 + 147 \\ 462 &= 3 \cdot 147 + 21 \\ 147 &= 7 \cdot 21 + 0 \end{aligned}$$

→ Poi risalgo: isolo il resto in ogni riga e sostituisco, senza mai moltiplicare 1071 e 462 fra loro.

→ $\mathbf{1071 \cdot (-3) + 462 \cdot (7) = 21}$

→ Controllo: $-3213 + 3234 = 21$.

Esercizio 132.

→ Trova x, y con $240x + 46y = \text{MCD}(240, 46)$

→ Prima Euclide, tenendo tutte le righe:

→

$$\begin{aligned} 240 &= 5 \cdot 46 + 10 \\ 46 &= 4 \cdot 10 + 6 \\ 10 &= 1 \cdot 6 + 4 \\ 6 &= 1 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 0 \end{aligned}$$

→ Poi risalgo: isolo il resto in ogni riga e sostituisco, senza mai moltiplicare 240 e 46 fra loro.

→ $\mathbf{240 \cdot (-9) + 46 \cdot (47) = 2}$

→ Controllo: $-2160 + 2162 = 2$.

---

4. Equazioni diofantee lineari

Esercizio 146.

→ $6x + 15y = 9$

→ $\text{MCD}(6, 15) = 3$ e $3 \mid 9$: le soluzioni ci sono.

→ Con Bézout trovo una soluzione particolare: $x_0 = -6$, $y_0 = 3$. (si risolve $ax + by = \text{MCD}$ e si moltiplica tutto per c/MCD)

→ Tutte le soluzioni: $\mathbf{x = -6 + 5t,\ y = 3 - 2t}$, con t intero. (una soluzione non è LA soluzione: sono infinite)

→ Controllo con $t = 0$: $6 \cdot -6 + 15 \cdot 3 = 9$.

Esercizio 147.

$\rightarrow 3x + 5y = 7$

$\rightarrow \text{MCD}(3,5) = 1$ e $1 \mid 7$: le soluzioni ci sono.

$\rightarrow$ Con Bézout trovo una soluzione particolare: $x_0 = 14$, $y_0 = -7$.

$\rightarrow$ Tutte le soluzioni: $\mathbf{x = 14 + 5t,\ y = -7 - 3t}$, con t intero.

$\rightarrow$ Controllo con $t = 0$: $3 \cdot 14 + 5 \cdot -7 = 7$.

Esercizio 166.

$\rightarrow 105x + 42y = 21$

$\rightarrow \text{MCD}(105,42) = 21$ e $21 \mid 21$: le soluzioni ci sono.

$\rightarrow$ Con Bézout trovo una soluzione particolare: $x_0 = 1$, $y_0 = -2$.

$\rightarrow$ Tutte le soluzioni: $\mathbf{x = 1 + 2t,\ y = -2 - 5t}$, con t intero.

$\rightarrow$ Controllo con $t = 0$: $105 \cdot 1 + 42 \cdot -2 = 21$.

Esercizio 167.

$\rightarrow 91x + 65y = 13$

$\rightarrow \text{MCD}(91,65) = 13$ e $13 \mid 13$: le soluzioni ci sono.

$\rightarrow$ Con Bézout trovo una soluzione particolare: $x_0 = -2$, $y_0 = 3$.

$\rightarrow$ Tutte le soluzioni: $\mathbf{x = -2 + 5t,\ y = 3 - 7t}$, con t intero.

$\rightarrow$ Controllo con $t = 0$: $91 \cdot -2 + 65 \cdot 3 = 13$.

Esercizio 168.

$\rightarrow 144x + 90y = 18$

$\rightarrow \text{MCD}(144,90) = 18$ e $18 \mid 18$: le soluzioni ci sono.

$\rightarrow$ Con Bézout trovo una soluzione particolare: $x_0 = 2$, $y_0 = -3$.

$\rightarrow$ Tutte le soluzioni: $\mathbf{x = 2 + 5t,\ y = -3 - 8t}$, con t intero.

$\rightarrow$ Controllo con $t = 0$: $144 \cdot 2 + 90 \cdot -3 = 18$.

Esercizio 169.

$\rightarrow 221x + 187y = 34$

$\rightarrow \text{MCD}(221, 187) = 17$ e $17 \mid 34$: le soluzioni ci sono.

$\rightarrow$ Con Bézout trovo una soluzione particolare: $x_0 = -10$, $y_0 = 12$.

$\rightarrow$ Tutte le soluzioni: $\mathbf{x = -10 + 11t,\ y = 12 - 13t}$, con t intero.

$\rightarrow$ Controllo con $t = 0$: $221 \cdot -10 + 187 \cdot 12 = 34$.

Esercizio 170.

$\rightarrow 1071x + 462y = 63$

$\rightarrow \text{MCD}(1071, 462) = 21$ e $21 \mid 63$: le soluzioni ci sono.

$\rightarrow$ Con Bézout trovo una soluzione particolare: $x_0 = -9$, $y_0 = 21$.

$\rightarrow$ Tutte le soluzioni: $\mathbf{x = -9 + 22t,\ y = 21 - 51t}$, con t intero.

$\rightarrow$ Controllo con $t = 0$: $1071 \cdot -9 + 462 \cdot 21 = 63$.

Esercizio 171.

$\rightarrow 323x + 187y = 51$

$\rightarrow \text{MCD}(323, 187) = 17$ e $17 \mid 51$: le soluzioni ci sono.

$\rightarrow$ Con Bézout trovo una soluzione particolare: $x_0 = -12$, $y_0 = 21$.

$\rightarrow$ Tutte le soluzioni: $\mathbf{x = -12 + 11t,\ y = 21 - 19t}$, con t intero.

$\rightarrow$ Controllo con $t = 0$: $323 \cdot -12 + 187 \cdot 21 = 51$.

Esercizio 172.

$\rightarrow 154x + 88y = 22$

$\rightarrow \text{MCD}(154, 88) = 22$ e $22 \mid 22$: le soluzioni ci sono.

$\rightarrow$ Con Bézout trovo una soluzione particolare: $x_0 = -1$, $y_0 = 2$.

$\rightarrow$ Tutte le soluzioni: $\mathbf{x = -1 + 4t,\ y = 2 - 7t}$, con t intero.

$\rightarrow$ Controllo con $t = 0$: $154 \cdot -1 + 88 \cdot 2 = 22$.

Esercizio 173.

$\to 176x + 132y = 44$

$\to \text{MCD}(176, 132) = 44$ e $44 \mid 44$: le soluzioni ci sono.

$\to$ Con Bézout trovo una soluzione particolare: $x_0 = 1$, $y_0 = -1$.

$\to$ Tutte le soluzioni: $\mathbf{x = 1 + 3t,\ y = -1 - 4t}$, con t intero.

$\to$ Controllo con $t = 0$: $176 \cdot 1 + 132 \cdot -1 = 44$.

Esercizio 174.

$\to 255x + 165y = 30$

$\to \text{MCD}(255, 165) = 15$ e $15 \mid 30$: le soluzioni ci sono.

$\to$ Con Bézout trovo una soluzione particolare: $x_0 = 4$, $y_0 = -6$.

$\to$ Tutte le soluzioni: $\mathbf{x = 4 + 11t,\ y = -6 - 17t}$, con t intero.

$\to$ Controllo con $t = 0$: $255 \cdot 4 + 165 \cdot -6 = 30$.

Esercizio 175.

$\to 391x + 253y = 23$

$\to \text{MCD}(391, 253) = 23$ e $23 \mid 23$: le soluzioni ci sono.

$\to$ Con Bézout trovo una soluzione particolare: $x_0 = 2$, $y_0 = -3$.

$\to$ Tutte le soluzioni: $\mathbf{x = 2 + 11t,\ y = -3 - 17t}$, con t intero.

$\to$ Controllo con $t = 0$: $391 \cdot 2 + 253 \cdot -3 = 23$.

---

5. Primi e fattorizzazione

Esercizio 176.

$\to$ 2 è primo?

$\to$ Provo i divisori fino a $\sqrt{2} \approx 1$. (se $n = ab$ con $a \leq b$, allora $a \leq \sqrt{n}$)

$\to$ Nessuno divide 2: è primo.

Esercizio 177.

$\to$ 9 è primo?

→ Cerco un divisore fino a $\sqrt{9} \approx 3$.

→ $9 = 3 \cdot 3$: non è primo.

Esercizio 211.

→ Scomponi 360 in fattori primi

→ Divido per i primi, uno alla volta, finché resta 1. (il teorema fondamentale garantisce che la scomposizione è unica)

→ $360 = \mathbf{2^3 \cdot 3^2 \cdot 5}$

Esercizio 212.

→ Scomponi 720 in fattori primi

→ Divido per i primi, uno alla volta, finché resta 1.

→ $720 = \mathbf{2^4 \cdot 3^2 \cdot 5}$

---

6. Numero e somma dei divisori

Esercizio 226.

→ $d(12)$

→ Fattorizzo: $12 = 2^2 \cdot 3$. (senza fattorizzare non si può usare nessuna formula)

→ $d(12) = (2+1) \cdot (1+1) = \mathbf{6}$ (ogni divisore si costruisce scegliendo un esponente da 0 ad a_i)

Esercizio 227.

→ $d(18)$

→ Fattorizzo: $18 = 2 \cdot 3^2$.

→ $d(18) = (1+1) \cdot (2+1) = \mathbf{6}$

Esercizio 261.

→ $d(360)$ e $\sigma(360)$

→ Fattorizzo: $360 = 2^3 \cdot 3^2 \cdot 5$.

$\rightarrow d(360) = (3+1)\cdot(2+1)\cdot(1+1) = \mathbf{24}$

$\rightarrow \sigma(360) = (1+2+4+8)\cdot(1+3+9)\cdot(1+5) = \mathbf{1170}$ (si sommano le potenze di ogni primo, poi si moltiplica)

Esercizio 262.

$\rightarrow d(400)$ e $\sigma(400)$

$\rightarrow$ Fattorizzo: $400 = 2^4 \cdot 5^2$.

$\rightarrow d(400) = (4+1)\cdot(2+1) = \mathbf{15}$

$\rightarrow \sigma(400) = (1+2+4+8+16)\cdot(1+5+25) = \mathbf{961}$

$\rightarrow$ Nota: $d(400)$ è dispari, e infatti $400 = 20^2$ è un quadrato perfetto. (i divisori si accoppiano, tranne la radice)

---

7. Congruenze: calcoli modulari

Esercizio 286.

$\rightarrow 17 \cdot 23 \pmod 5$

$\rightarrow$ Riduco i fattori: $17 \equiv 2$ e $23 \equiv 3 \pmod 5$. (il prodotto si comporta bene con le congruenze: si può ridurre prima)

$\rightarrow 2 \cdot 3 = 6 \equiv \mathbf{1} \pmod 5$

$\rightarrow$ Controllo: $17 \cdot 23 = 391$, e $391 = 5 \cdot 78 + 1$.

Esercizio 287.

$\rightarrow 13 \cdot 29 \pmod 7$

$\rightarrow$ Riduco i fattori: $13 \equiv 6$ e $29 \equiv 1 \pmod 7$.

$\rightarrow 6 \cdot 1 = 6 \equiv \mathbf{6} \pmod 7$

$\rightarrow$ Controllo: $13 \cdot 29 = 377$, e $377 = 7 \cdot 53 + 6$.

Esercizio 296.

$\rightarrow$ Per quale valore di k il numero $2^3 \cdot 3^k$ ha esattamente 12 divisori?

$\rightarrow$ Scrivo $d(n)$ in funzione di k: gli esponenti sono 3 e k, quindi $d = (3+1)(k+1) = 4(k+1)$. (la formula vale con qualunque esponente, anche incognito)

$\rightarrow$ Deve fare 12: $4(k+1) = 12$, cioè $k+1 = 3$.

→ $\mathbf{k = 2}$

→ Controllo: 72 ha davvero 12 divisori.

Esercizio 297.

→ Per quale valore di k il numero $2^2 \cdot 3^k$ ha esattamente 15 divisori?

→ Scrivo $d(n)$ in funzione di k: gli esponenti sono 2 e k, quindi $d = (2+1)(k+1) = 3(k+1)$.

→ Deve fare 15: $3(k+1) = 15$, cioè $k+1 = 5$.

→ $\mathbf{k = 4}$

→ Controllo: 324 ha davvero 15 divisori.

Esercizio 306.

→ $7^{100} \pmod{10}$

→ Calcolo le prime potenze modulo 10: $7^1 \equiv 7$, $7^2 \equiv 9$, $7^3 \equiv 3$, $7^4 \equiv 1$. (le potenze modulo m si ripetono: trovato il ciclo, l'esponente si riduce)

→ Il ciclo è lungo 4.

→ $100 = 4 \cdot 25 + 0$, quindi $7^{100} \equiv \mathbf{1} \pmod{10}$.

Esercizio 307.

→ $3^{50} \pmod{10}$

→ Calcolo le prime potenze modulo 10: $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 7$, $3^4 \equiv 1$.

→ Il ciclo è lungo 4.

→ $50 = 4 \cdot 12 + 2$, quindi $3^{50} \equiv \mathbf{9} \pmod{10}$.

Esercizio 326.

→ $2^{200} \pmod{13}$

→ Calcolo le prime potenze modulo 13: $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 3 \ldots$.

→ Il ciclo è lungo 12.

→ $200 = 12 \cdot 16 + 8$, quindi $2^{200} \equiv \mathbf{9} \pmod{13}$.

Esercizio 327.

→ $3^{100} \pmod{17}$

→ Calcolo le prime potenze modulo 17: $3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 10, 3^4 \equiv 13 \ldots$.

→ Il ciclo è lungo 16.

→ $100 = 16 \cdot 6 + 4$, quindi $3^{100} \equiv \mathbf{13} \pmod{17}$.

---

8. Criteri di divisibilità

Esercizio 336.

→ 4725 è divisibile per 9?

→ Criterio del 9: sommo le cifre: $4 + 7 + 2 + 5 = 18$. ($10 \equiv 1$, quindi ogni potenza di 10 vale 1)

→ 18 è divisibile per 9, quindi 4725 pure: sì.

Esercizio 337.

→ 12345 è divisibile per 3?

→ Criterio del 3: sommo le cifre: $1 + 2 + 3 + 4 + 5 = 15$. ($10 \equiv 1$, quindi ogni potenza di 10 vale 1)

→ 15 è divisibile per 3, quindi 12345 pure: sì.

---

9. Inverso modulare ed equazioni congruenziali

Esercizio 361.

→ L'inverso di 7 modulo 26

→ $\text{MCD}(7, 26) = 1$: l'inverso esiste. (viene da Bézout: da $ax + my = 1$, modulo m resta $ax \equiv 1$)

→ Con Euclide esteso trovo $7 \cdot -11 + 26 \cdot 3 = 1$.

→ Quindi l'inverso è **15**.

→ Controllo: $7 \cdot 15 = 105 = 26 \cdot 4 + 1$.

Esercizio 362.

→ L'inverso di 3 modulo 10

→ $\text{MCD}(3, 10) = 1$: l'inverso esiste.

→ Con Euclide esteso trovo $3 \cdot -3 + 10 \cdot 1 = 1$.

→ Quindi l'inverso è **7**.

→ Controllo: $3 \cdot 7 = 21 = 10 \cdot 2 + 1$.

Esercizio 376.

→ $7x \equiv 3 \pmod{26}$

→ $\text{MCD}(7, 26) = 1$. (il MCD dice subito quante soluzioni aspettarsi)

→ Il MCD è 1: moltiplico per l'inverso di 7, che è 15.

→ $x \equiv 15 \cdot 3 = 45 \equiv \mathbf{19} \pmod{26}$

→ Controllo: $7 \cdot 19 = 133 \equiv 3 \pmod{26}$.

Esercizio 377.

→ $3x \equiv 4 \pmod{10}$

→ $\text{MCD}(3, 10) = 1$.

→ Il MCD è 1: moltiplico per l'inverso di 3, che è 7.

→ $x \equiv 7 \cdot 4 = 28 \equiv \mathbf{8} \pmod{10}$

→ Controllo: $3 \cdot 8 = 24 \equiv 4 \pmod{10}$.

Esercizio 386.

→ $35x \equiv 14 \pmod{91}$

→ $\text{MCD}(35, 91) = 7$.

→ $7 \mid 14$: divido tutto per 7, **modulo compreso**, e resta $5x \equiv 2 \pmod{13}$. (dividere solo i due membri e lasciare il modulo è l'errore tipico)

→ La congruenza ridotta ha una sola classe: $\mathbf{x \equiv 3 \pmod{13}}$. Modulo 91 sono 7 classi, che si ottengono aggiungendo 13 ogni volta.

→ Controllo: $35 \cdot 3 = 105 \equiv 14 \pmod{91}$.

Esercizio 387.

→ $24x \equiv 18 \pmod{30}$

$\rightarrow$ MCD$(24, 30) = 6$.

$\rightarrow$ $6 \mid 18$: divido tutto per 6, **modulo compreso**, e resta $4x \equiv 3 \pmod 5$.

$\rightarrow$ La congruenza ridotta ha una sola classe: $\mathbf{x \equiv 2 \pmod 5}$. Modulo 30 sono 6 classi, che si ottengono aggiungendo 5 ogni volta.

$\rightarrow$ Controllo: $24 \cdot 2 = 48 \equiv 18 \pmod{30}$.

Esercizio 388.

$\rightarrow$ $45x \equiv 15 \pmod{60}$

$\rightarrow$ MCD$(45, 60) = 15$.

$\rightarrow$ $15 \mid 15$: divido tutto per 15, **modulo compreso**, e resta $3x \equiv 1 \pmod 4$.

$\rightarrow$ La congruenza ridotta ha una sola classe: $\mathbf{x \equiv 3 \pmod 4}$. Modulo 60 sono 15 classi, che si ottengono aggiungendo 4 ogni volta.

$\rightarrow$ Controllo: $45 \cdot 3 = 135 \equiv 15 \pmod{60}$.

Esercizio 389.

$\rightarrow$ $33x \equiv 22 \pmod{55}$

$\rightarrow$ MCD$(33, 55) = 11$.

$\rightarrow$ $11 \mid 22$: divido tutto per 11, **modulo compreso**, e resta $3x \equiv 2 \pmod 5$.

$\rightarrow$ La congruenza ridotta ha una sola classe: $\mathbf{x \equiv 4 \pmod 5}$. Modulo 55 sono 11 classi, che si ottengono aggiungendo 5 ogni volta.

$\rightarrow$ Controllo: $33 \cdot 4 = 132 \equiv 22 \pmod{55}$.

Esercizio 390.

$\rightarrow$ $18x \equiv 12 \pmod{42}$

$\rightarrow$ MCD$(18, 42) = 6$.

$\rightarrow$ $6 \mid 12$: divido tutto per 6, **modulo compreso**, e resta $3x \equiv 2 \pmod 7$.

$\rightarrow$ La congruenza ridotta ha una sola classe: $\mathbf{x \equiv 3 \pmod 7}$. Modulo 42 sono 6 classi, che si ottengono aggiungendo 7 ogni volta.

$\rightarrow$ Controllo: $18 \cdot 3 = 54 \equiv 12 \pmod{42}$.

Esercizio 391.

$\rightarrow 28x \equiv 21 \pmod{49}$

$\rightarrow \text{MCD}(28, 49) = 7.$

$\rightarrow 7 \mid 21$: divido tutto per 7, **modulo compreso**, e resta $4x \equiv 3 \pmod{7}$.

$\rightarrow$ La congruenza ridotta ha una sola classe: $\mathbf{x \equiv 6 \pmod{7}}$. Modulo 49 sono 7 classi, che si ottengono aggiungendo 7 ogni volta.

$\rightarrow$ Controllo: $28 \cdot 6 = 168 \equiv 21 \pmod{49}$.

Esercizio 392.

$\rightarrow 26x \equiv 13 \pmod{39}$

$\rightarrow \text{MCD}(26, 39) = 13.$

$\rightarrow 13 \mid 13$: divido tutto per 13, **modulo compreso**, e resta $2x \equiv 1 \pmod{3}$.

$\rightarrow$ La congruenza ridotta ha una sola classe: $\mathbf{x \equiv 2 \pmod{3}}$. Modulo 39 sono 13 classi, che si ottengono aggiungendo 3 ogni volta.

$\rightarrow$ Controllo: $26 \cdot 2 = 52 \equiv 13 \pmod{39}$.

Esercizio 393.

$\rightarrow 40x \equiv 24 \pmod{56}$

$\rightarrow \text{MCD}(40, 56) = 8.$

$\rightarrow 8 \mid 24$: divido tutto per 8, **modulo compreso**, e resta $5x \equiv 3 \pmod{7}$.

$\rightarrow$ La congruenza ridotta ha una sola classe: $\mathbf{x \equiv 2 \pmod{7}}$. Modulo 56 sono 8 classi, che si ottengono aggiungendo 7 ogni volta.

$\rightarrow$ Controllo: $40 \cdot 2 = 80 \equiv 24 \pmod{56}$.

Esercizio 394.

$\rightarrow 15x \equiv 25 \pmod{35}$

$\rightarrow \text{MCD}(15, 35) = 5.$

$\rightarrow 5 \mid 25$: divido tutto per 5, **modulo compreso**, e resta $3x \equiv 5 \pmod{7}$.

$\rightarrow$ La congruenza ridotta ha una sola classe: $\mathbf{x \equiv 4 \pmod{7}}$. Modulo 35 sono 5 classi, che si ottengono aggiungendo 7 ogni volta.

$\rightarrow$ Controllo: $15 \cdot 4 = 60 \equiv 25 \pmod{35}$.

Esercizio 395.

$\to 22x \equiv 33 \pmod{55}$

$\to \text{MCD}(22, 55) = 11$.

$\to 11 \mid 33$: divido tutto per 11, **modulo compreso**, e resta $2x \equiv 3 \pmod{5}$.

$\to$ La congruenza ridotta ha una sola classe: $\mathbf{x \equiv 4 \pmod{5}}$. Modulo 55 sono 11 classi, che si ottengono aggiungendo 5 ogni volta.

$\to$ Controllo: $22 \cdot 4 = 88 \equiv 33 \pmod{55}$.

10. Piccolo Fermat e teorema di Eulero

Esercizio 396.

$\to 2^{100} \pmod{13}$

$\to 13$ è primo e non divide 2: per il piccolo teorema di Fermat $2^{12} \equiv 1 \pmod{13}$. (l'esponente si riduce modulo $p - 1$)

$\to 100 = 12 \cdot 8 + 4$, quindi $2^{100} \equiv 2^4$.

$\to$ **3**

Esercizio 397.

$\to 3^{200} \pmod{7}$

$\to 7$ è primo e non divide 3: per il piccolo teorema di Fermat $3^6 \equiv 1 \pmod{7}$.

$\to 200 = 6 \cdot 33 + 2$, quindi $3^{200} \equiv 3^2$.

$\to$ **2**

Esercizio 416.

$\to 3^{40} \pmod{100}$

$\to 100$ non è primo: calcolo $\varphi(100)$ dalla fattorizzazione $100 = 2^2 \cdot 5^2$, e viene 40. (Eulero generalizza Fermat: l'esponente si riduce modulo $\varphi(m)$)

$\to \text{MCD}(3, 100) = 1$, quindi $3^{40} \equiv 1 \pmod{100}$.

$\to 40 = 40 \cdot 1 + 0$, quindi il risultato è **1**.

Esercizio 417.

$\to 7^{100} \pmod{100}$

$\to 100$ non è primo: calcolo $\varphi(100)$ dalla fattorizzazione $100 = 2^2 \cdot 5^2$, e viene 40.

$\to \text{MCD}(7, 100) = 1$, quindi $7^{40} \equiv 1 \pmod{100}$.

$\to 100 = 40 \cdot 2 + 20$, quindi il risultato è **1**.

Esercizio 426.

$\to 13^{24} \pmod{35}$

$\to 35$ non è primo: calcolo $\varphi(35)$ dalla fattorizzazione $35 = 5 \cdot 7$, e viene 24.

$\to \text{MCD}(13, 35) = 1$, quindi $13^{24} \equiv 1 \pmod{35}$.

$\to 24 = 24 \cdot 1 + 0$, quindi il risultato è **1**.

Esercizio 427.

$\to 11^{40} \pmod{63}$

$\to 63$ non è primo: calcolo $\varphi(63)$ dalla fattorizzazione $63 = 3^2 \cdot 7$, e viene 36.

$\to \text{MCD}(11, 63) = 1$, quindi $11^{36} \equiv 1 \pmod{63}$.

$\to 40 = 36 \cdot 1 + 4$, quindi il risultato è **25**.

Esercizio 428.

$\to 17^{20} \pmod{32}$

$\to 32$ non è primo: calcolo $\varphi(32)$ dalla fattorizzazione $32 = 2^5$, e viene 16.

$\to \text{MCD}(17, 32) = 1$, quindi $17^{16} \equiv 1 \pmod{32}$.

$\to 20 = 16 \cdot 1 + 4$, quindi il risultato è **1**.

Esercizio 429.

$\to 19^{30} \pmod{44}$

$\to 44$ non è primo: calcolo $\varphi(44)$ dalla fattorizzazione $44 = 2^2 \cdot 11$, e viene 20.

$\rightarrow$ MCD$(19, 44) = 1$, quindi $19^{20} \equiv 1 \pmod{44}$.

$\rightarrow$ $30 = 20 \cdot 1 + 10$, quindi il risultato è **1**.

Esercizio 430.

$\rightarrow$ $23^{12} \pmod{55}$

$\rightarrow$ 55 non è primo: calcolo $\varphi(55)$ dalla fattorizzazione $55 = 5 \cdot 11$, e viene 40.

$\rightarrow$ MCD$(23, 55) = 1$, quindi $23^{40} \equiv 1 \pmod{55}$.

$\rightarrow$ $12 = 40 \cdot 0 + 12$, quindi il risultato è **1**.

Esercizio 431.

$\rightarrow$ $29^{20} \pmod{39}$

$\rightarrow$ 39 non è primo: calcolo $\varphi(39)$ dalla fattorizzazione $39 = 3 \cdot 13$, e viene 24.

$\rightarrow$ MCD$(29, 39) = 1$, quindi $29^{24} \equiv 1 \pmod{39}$.

$\rightarrow$ $20 = 24 \cdot 0 + 20$, quindi il risultato è **22**.

Esercizio 432.

$\rightarrow$ $31^{24} \pmod{49}$

$\rightarrow$ 49 non è primo: calcolo $\varphi(49)$ dalla fattorizzazione $49 = 7^2$, e viene 42.

$\rightarrow$ MCD$(31, 49) = 1$, quindi $31^{42} \equiv 1 \pmod{49}$.

$\rightarrow$ $24 = 42 \cdot 0 + 24$, quindi il risultato è **1**.

Esercizio 433.

$\rightarrow$ $37^{10} \pmod{51}$

$\rightarrow$ 51 non è primo: calcolo $\varphi(51)$ dalla fattorizzazione $51 = 3 \cdot 17$, e viene 32.

$\rightarrow$ MCD$(37, 51) = 1$, quindi $37^{32} \equiv 1 \pmod{51}$.

$\rightarrow$ $10 = 32 \cdot 0 + 10$, quindi il risultato è **25**.

Esercizio 434.

$\to 41^{16} \pmod{57}$

$\to$ 57 non è primo: calcolo $\varphi(57)$ dalla fattorizzazione $57 = 3 \cdot 19$, e viene 36.

$\to \text{MCD}(41, 57) = 1$, quindi $41^{36} \equiv 1 \pmod{57}$.

$\to 16 = 36 \cdot 0 + 16$, quindi il risultato è **55**.

Esercizio 435.

$\to 43^{20} \pmod{65}$

$\to$ 65 non è primo: calcolo $\varphi(65)$ dalla fattorizzazione $65 = 5 \cdot 13$, e viene 48.

$\to \text{MCD}(43, 65) = 1$, quindi $43^{48} \equiv 1 \pmod{65}$.

$\to 20 = 48 \cdot 0 + 20$, quindi il risultato è **16**.

---

11. Teorema cinese del resto

Esercizio 436.

$\to x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$

$\to$ I moduli sono a due a due coprimi: il teorema cinese dice che c'è una sola soluzione modulo 15.
(senza moduli coprimi il teorema non si applica, e la soluzione può non esistere)

$\to$ Unisco le prime 2 congruenze: $x \equiv 8 \pmod{15}$. (si scrive $x = r + mt$ e si sostituisce nella congruenza dopo)

$\to \mathbf{x \equiv 8 \pmod{15}}$

$\to$ Controllo: $8 = 3 \cdot 2 + 2$, $8 = 5 \cdot 1 + 3$.

Esercizio 437.

$\to x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$

$\to$ I moduli sono a due a due coprimi: il teorema cinese dice che c'è una sola soluzione modulo 6.

$\to$ Unisco le prime 2 congruenze: $x \equiv 5 \pmod{6}$.

$\to \mathbf{x \equiv 5 \pmod{6}}$

$\to$ Controllo: $5 = 2 \cdot 2 + 1$, $5 = 3 \cdot 1 + 2$.

Esercizio 451.

$\to x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$

→ I moduli sono a due a due coprimi: il teorema cinese dice che c'è una sola soluzione modulo 105.

→ Unisco le prime 2 congruenze: $x \equiv 8 \pmod{15}$.

→ Unisco le prime 3 congruenze: $x \equiv 23 \pmod{105}$.

→ $\mathbf{x \equiv 23 \pmod{105}}$

→ Controllo: $23 = 3 \cdot 7 + 2, 23 = 5 \cdot 4 + 3, 23 = 7 \cdot 3 + 2$.

Esercizio 452.

→ $x \equiv 1 \pmod{3}, x \equiv 2 \pmod{5}, x \equiv 3 \pmod{7}$

→ I moduli sono a due a due coprimi: il teorema cinese dice che c'è una sola soluzione modulo 105.

→ Unisco le prime 2 congruenze: $x \equiv 7 \pmod{15}$.

→ Unisco le prime 3 congruenze: $x \equiv 52 \pmod{105}$.

→ $\mathbf{x \equiv 52 \pmod{105}}$

→ Controllo: $52 = 3 \cdot 17 + 1, 52 = 5 \cdot 10 + 2, 52 = 7 \cdot 7 + 3$.

Esercizio 453.

→ $x \equiv 2 \pmod{4}, x \equiv 3 \pmod{5}, x \equiv 1 \pmod{7}$

→ I moduli sono a due a due coprimi: il teorema cinese dice che c'è una sola soluzione modulo 140.

→ Unisco le prime 2 congruenze: $x \equiv 18 \pmod{20}$.

→ Unisco le prime 3 congruenze: $x \equiv 78 \pmod{140}$.

→ $\mathbf{x \equiv 78 \pmod{140}}$

→ Controllo: $78 = 4 \cdot 19 + 2, 78 = 5 \cdot 15 + 3, 78 = 7 \cdot 11 + 1$.

Esercizio 454.

→ $x \equiv 1 \pmod{2}, x \equiv 2 \pmod{3}, x \equiv 4 \pmod{5}$

→ I moduli sono a due a due coprimi: il teorema cinese dice che c'è una sola soluzione modulo 30.

→ Unisco le prime 2 congruenze: $x \equiv 5 \pmod{6}$.

→ Unisco le prime 3 congruenze: $x \equiv 29 \pmod{30}$.

→ $\mathbf{x \equiv 29 \pmod{30}}$

→ Controllo: $29 = 2 \cdot 14 + 1, 29 = 3 \cdot 9 + 2, 29 = 5 \cdot 5 + 4$.

Esercizio 455.

$\rightarrow x \equiv 3 \pmod 5, x \equiv 4 \pmod 7, x \equiv 2 \pmod 9$

$\rightarrow$ I moduli sono a due a due coprimi: il teorema cinese dice che c'è una sola soluzione modulo 315.

$\rightarrow$ Unisco le prime 2 congruenze: $x \equiv 18 \pmod{35}$.

$\rightarrow$ Unisco le prime 3 congruenze: $x \equiv 263 \pmod{315}$.

$\rightarrow \mathbf{x \equiv 263 \pmod{315}}$

$\rightarrow$ Controllo: $263 = 5 \cdot 52 + 3, 263 = 7 \cdot 37 + 4, 263 = 9 \cdot 29 + 2$.

Esercizio 456.

$\rightarrow x \equiv 1 \pmod 4, x \equiv 3 \pmod 7, x \equiv 5 \pmod{11}$

$\rightarrow$ I moduli sono a due a due coprimi: il teorema cinese dice che c'è una sola soluzione modulo 308.

$\rightarrow$ Unisco le prime 2 congruenze: $x \equiv 17 \pmod{28}$.

$\rightarrow$ Unisco le prime 3 congruenze: $x \equiv 269 \pmod{308}$.

$\rightarrow \mathbf{x \equiv 269 \pmod{308}}$

$\rightarrow$ Controllo: $269 = 4 \cdot 67 + 1, 269 = 7 \cdot 38 + 3, 269 = 11 \cdot 24 + 5$.

Esercizio 457.

$\rightarrow x \equiv 2 \pmod 3, x \equiv 1 \pmod 8, x \equiv 4 \pmod{11}$

$\rightarrow$ I moduli sono a due a due coprimi: il teorema cinese dice che c'è una sola soluzione modulo 264.

$\rightarrow$ Unisco le prime 2 congruenze: $x \equiv 17 \pmod{24}$.

$\rightarrow$ Unisco le prime 3 congruenze: $x \equiv 257 \pmod{264}$.

$\rightarrow \mathbf{x \equiv 257 \pmod{264}}$

$\rightarrow$ Controllo: $257 = 3 \cdot 85 + 2, 257 = 8 \cdot 32 + 1, 257 = 11 \cdot 23 + 4$.

Esercizio 458.

$\rightarrow x \equiv 5 \pmod 7, x \equiv 2 \pmod 9, x \equiv 3 \pmod{13}$

$\rightarrow$ I moduli sono a due a due coprimi: il teorema cinese dice che c'è una sola soluzione modulo 819.

$\rightarrow$ Unisco le prime 2 congruenze: $x \equiv 47 \pmod{63}$.

→ Unisco le prime 3 congruenze: $x \equiv 614 \pmod{819}$.

→ $\mathbf{x \equiv 614 \pmod{819}}$

→ Controllo: $614 = 7 \cdot 87 + 5$, $614 = 9 \cdot 68 + 2$, $614 = 13 \cdot 47 + 3$.

Esercizio 459.

→ $x \equiv 1 \pmod{5}$, $x \equiv 2 \pmod{7}$, $x \equiv 3 \pmod{11}$

→ I moduli sono a due a due coprimi: il teorema cinese dice che c'è una sola soluzione modulo 385.

→ Unisco le prime 2 congruenze: $x \equiv 16 \pmod{35}$.

→ Unisco le prime 3 congruenze: $x \equiv 366 \pmod{385}$.

→ $\mathbf{x \equiv 366 \pmod{385}}$

→ Controllo: $366 = 5 \cdot 73 + 1$, $366 = 7 \cdot 52 + 2$, $366 = 11 \cdot 33 + 3$.

Esercizio 460.

→ $x \equiv 4 \pmod{9}$, $x \equiv 3 \pmod{10}$, $x \equiv 7 \pmod{13}$

→ I moduli sono a due a due coprimi: il teorema cinese dice che c'è una sola soluzione modulo 1170.

→ Unisco le prime 2 congruenze: $x \equiv 13 \pmod{90}$.

→ Unisco le prime 3 congruenze: $x \equiv 553 \pmod{1170}$.

→ $\mathbf{x \equiv 553 \pmod{1170}}$

→ Controllo: $553 = 9 \cdot 61 + 4$, $553 = 10 \cdot 55 + 3$, $553 = 13 \cdot 42 + 7$.

---

12. Da gara: vero o falso, errori, dimostrazioni

Esercizio 461.

→ $3 \mid 12$

→ vero (dove è falso basta un controesempio)

Esercizio 462.

→ $12 \mid 3$

→ falso

Esercizio 481.

→ $12 \mid 3$ perché $12 : 3 = 4$

→ Dov'è l'errore: la barra si legge «divide»: la cosa piccola sta a sinistra, ed è $3 \mid 12$. (quasi sempre è un'ipotesi del teorema che non è stata controllata)

→ La risposta giusta: $3 \mid 12$.

Esercizio 482.

→ da $6 \equiv 2 \pmod 4$ segue $3 \equiv 1 \pmod 4$

→ Dov'è l'errore: si semplifica solo per numeri coprimi col modulo, e $\text{MCD}(2,4) = 2$.

→ La risposta giusta: **si divide anche il modulo:** $3 \equiv 1 \pmod 2$.

Esercizio 491.

→ Dimostra che $n^2 + 1$ non è mai divisibile per 3.

→ Un quadrato è $\equiv 0$ o $1 \pmod 3$, quindi $n^2 + 1$ è $\equiv 1$ o 2: mai 0. (le tre mosse: guarda i resti, cerca il ciclo, fattorizza)

Esercizio 492.

→ Dimostra che il prodotto di due interi consecutivi è sempre pari.

→ Uno dei due è pari, quindi il prodotto ha il fattore 2.

Esercizio 493.

→ Dimostra che $d(n)$ è dispari se e solo se n è un quadrato perfetto.

→ I divisori si accoppiano (a con n/a) e coincidono solo quando $a = \sqrt{n}$.

Esercizio 494.

→ Dimostra che se p è primo e $p > 3$, allora $p^2 - 1$ è divisibile per 24.

→ $p^2 - 1 = (p-1)(p+1)$: fra due pari consecutivi uno è multiplo di 4, e uno dei tre numeri $p-1, p, p+1$ è multiplo di 3 — ma non p.

Esercizio 495.

→ Dimostra che la somma di tre interi consecutivi è divisibile per 3.

→ $n + (n+1) + (n+2) = 3(n+1)$.

Esercizio 496.

→ Dimostra che un numero e la somma delle sue cifre danno lo stesso resto modulo 9.

→ $10 \equiv 1 \pmod 9$, quindi ogni potenza di 10 è $\equiv 1$.

Esercizio 497.

→ Dimostra che se $\text{MCD}(a, b) = 1$ e $a \mid bc$, allora $a \mid c$.

→ Per Bézout $ax + by = 1$; moltiplicando per c si ha $acx + bcy = c$, e a divide entrambi gli addendi.

Esercizio 498.

→ Dimostra che esistono infiniti numeri primi.

→ Se fossero finiti, $p_1 p_2 \cdots p_k + 1$ non sarebbe divisibile per nessuno di loro: o è primo, o ha un fattore primo nuovo.

Esercizio 499.

→ Dimostra che $2^n - 1$ non è mai un quadrato perfetto per $n > 1$.

→ $2^n - 1 \equiv 3 \pmod 4$ per $n \geq 2$, mentre un quadrato è $\equiv 0$ o $1 \pmod 4$.

Esercizio 500.

→ Dimostra che se n è dispari, allora $n^2 \equiv 1 \pmod 8$.

→ $n = 2k + 1$ dà $n^2 = 4k(k+1) + 1$, e $k(k+1)$ è pari.