8. – Soluzione degli esercizi su: ***equazioni di primo grado in $\mathbb{Z}_n$***.

Esercizio 8.1

Sia $\mathbb{Z}_{652}$ l'anello delle classi di resto modulo 652. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{652}$ a cui z appartiene. Si trovino tutte le (eventuali) soluzioni in $\mathbb{Z}_{652}$ della seguente equazione:

$$[632]x = [388]\,.$$

Soluzione – Sia $x_0 \in \mathbb{Z}$ tale che $[x_0]$ è soluzione dell'equazione proposta; allora

$$[632] \cdot [x_0] = [388] \qquad \text{ossia} \qquad [632 \cdot x_0] = [388]$$

e dunque deve esistere $y_0 \in \mathbb{Z}$ tale che

$$632\, x_0 - 388 = 652\, y_0\,.$$

Siamo quindi ricondotti a considerare l'equazione diofantina

(*) $$632\, x - 652\, y = 388$$

della quale ci interessano soltano i valori della x, anzi le loro classi di resto modulo 652 (per questo motivo sarebbe equivalente considerare l'equazione diofantina

$$632\, x + 652\, y = 388$$

che nella x ha esattamente le stesse soluzioni).

Calcoliamo il MCD fra 632 e 652 mediante l'algoritmo di Euclide:

$652 = 632 \cdot 1 + 20$;
$632 = 20 \cdot 31 + 12$;
$20 = 12 \cdot 1 + 8$;
$12 = 8 \cdot 1 + 4$;
$8 = 4 \cdot 2 + 0$.

Il massimo comun divisore fra 632 e 652 è dunque 4; poiché si tratta di un divisore di 388, la (*) ha soluzione (e l'equazione proposta ha esattamente 4 soluzioni).

Cerchiamo adesso una soluzione per l'equazione

$$632\, x - 652\, y = 388\,.$$

Dai calcoli fatti per trovare il massimo comun divisore, abbiamo che

$$4 = 12 - 8 = 12 - (20 - 12) = 2 \cdot 12 - 20 = 2 \cdot (632 - 20 \cdot 31) - 20 =$$
$$= 2 \cdot 632 - 63 \cdot 20 = 2 \cdot 632 - 63 \cdot (652 - 632) = 632 \cdot 65 - 652 \cdot 63$$

e dunque

$$388 = 632 \cdot 6\,305 - 652 \cdot 6\,111\,.$$

Pertanto una soluzione dell'equazione $632\, x - 652\, y = 388$ è $(6\,305, 6\,111)$. La generica soluzione è

$$x := 6\,305 + \tfrac{652}{4} h, \quad y := 6\,111 + \tfrac{632}{4} h \qquad \text{(al variare di } h \text{ in } \mathbb{Z})$$

ossia

$$x := 6\,305 + 163h, \qquad y := 6\,111 + 158h \qquad \text{(al variare di } h \text{ in } \mathbb{Z}).$$

A noi interessano soltanto i valori della x, anzi fra questi ne vogliamo 4 che diano luogo a classi di resto distinte modulo 652. Basta prendere quattro valori interi consecutivi per h, ma per "fare bella figura" di solito si scelgono in modo che i valori risultanti per la x appartengano all'intervallo $[0, 651]$. Per $h := -38, -37, -36, -35$ si ottiene

$$x_1 = 111, \quad x_2 = 274, \quad x_3 = 437, \quad x_4 = 600\,.$$

Esercizio 8.2

Sia $\mathbb{Z}_{159}$ l'anello delle classi di resto modulo 159. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{159}$ a cui z appartiene. Si stabilisca, motivando la risposta, se $[31]$ ha inverso in $\mathbb{Z}_{159}$ e nel caso che la risposta sia affermativa si determini esplicitamente tale inverso.

Soluzione – Sappiamo che $[z]$ è invertibile in $\mathbb{Z}_{159}$ se e soltanto se

$$\text{MCD}(z, 159) = 1\,.$$

Calcoliamo allora il massimo comun divisore fra 31 e 159.

$159 = 31 \cdot 5 + 4$;
$31 = 4 \cdot 7 + 3$;
$4 = 3 \cdot 1 + 1$;
$3 = 1 \cdot 3$.

Dunque $\text{MCD}(31, 159) = 1$ e pertanto $[31]$ è invertibile in $\mathbb{Z}_{159}$.

Per trovarne l'inverso, cerchiamo in primo luogo un $x \in \mathbb{Z}$ tale che

$$31 \cdot x \equiv 1 \pmod{159}$$

ossia tale che

$$31x - 1 = 159y \quad \text{con } y \in \mathbb{Z}\,.$$

Si tratta di risolvere l'equazione diofantina

$$31x - 159y = 1$$

oppure (poiché a noi interessa soltanto trovare un valore per la x) l'equazione diofantina

$$31x + 159y = 1\,.$$

Per far ciò è sufficiente ricavare l'identità di Bezout partendo dai calcoli effettuati per trovare il massimo comun divisore fra 31 e 159. Si ha dunque

$$1 = 4 - 3 = 4 - (31 - 4 \cdot 7) = 4 \cdot 8 - 31 = (159 - 31 \cdot 5) \cdot 8 - 31 = 159 \cdot 8 - 41 \cdot 31\,.$$

Una soluzione dell'equazione diofantina

$$31x + 159y = 1$$

è dunque

$$x = -41, \qquad y = 8\,.$$

L'inverso di $[31]$ in $\mathbb{Z}_{159}$ è $[-41]$ (oppure, se si preferisce, $[118]$).

Esercizio 8.3

Sia $\mathbb{Z}_{24\,141}$ l'anello delle classi di resto modulo $24\,141$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{24\,141}$ a cui z appartiene. Si trovino tutte le (eventuali) soluzioni in $\mathbb{Z}_{24\,141}$ della seguente equazione:

$$[3\,420]x = [1\,047]\,.$$

Soluzione – Sia $x_0 \in \mathbb{Z}$ tale che $[x_0]$ è soluzione dell'equazione proposta; allora

$$[3\,420] \cdot [x_0] = [1\,047] \qquad \text{ossia} \qquad [3\,420 \cdot x_0] = [1\,047]$$

e dunque deve esistere $y_0 \in \mathbb{Z}$ tale che $\quad 3\,420\,x_0 - 1\,047 = 24\,141\,y_0\,.$

Siamo quindi ricondotti a considerare l'equazione diofantina

(*) $$3\,420\,x - 24\,141\,y = 1\,047$$

della quale ci interessano soltano i valori della x, anzi le loro classi di resto modulo $24\,141$ (per questo motivo sarebbe equivalente considerare l'equazione diofantina

$$3\,420\,x + 24\,141\,y = 1\,047$$

che nella x ha esattamente le stesse soluzioni).

Calcoliamo con l'algoritmo di Euclide il MCD fra $24\,141$ e $3\,420$.

$24\,141 = 3\,420 \cdot 7 + 201\,;$ $\qquad 3\,420 = 201 \cdot 17 + 3\,;$ $\qquad 201 = 3 \cdot 67\,.$

Il massimo comun divisore fra $24\,141$ e $3\,420$ è dunque 3; poiché si tratta di un divisore di $1\,047$, la (*) ha soluzione.

Cerchiamo adesso una soluzione per l'equazione

$$3\,420\,x - 24\,141\,y = 1\,047\,.$$

Dai calcoli fatti per trovare il massimo comun divisore, abbiamo che

$$3 = 3\,420 - 17 \cdot 201 = 3\,420 - 17 \cdot (24\,141 - 7 \cdot 3\,420) = 120 \cdot 3\,420 - 17 \cdot 24\,141$$

e dunque

$$1\,047 = 349 \cdot 3 = 41\,880 \cdot 3\,420 - 5\,933 \cdot 24\,141\,.$$

Pertanto una soluzione dell'equazione $\quad 3\,420\,x - 24\,141\,y = 1\,047 \quad$ è $\quad (41\,880, 5\,933)$. La generica soluzione è

$$x := 41\,880 + \tfrac{24\,141}{3}h, \qquad y := 5\,933 + \tfrac{3\,420}{3}h \quad \text{(al variare di } h \text{ in } \mathbb{Z})$$

ossia

$$x := 41\,880 + 8\,047h, \qquad y := 5\,933 + 1\,140h \quad \text{(al variare di } h \text{ in } \mathbb{Z}).$$

A noi interessano soltanto i valori della x, anzi fra questi ne vogliamo 3 che diano luogo a classi di resto distinte modulo $24\,141$. Basta prendere tre valori interi consecutivi per h, ma per "fare bella figura" di solito si scelgono in modo che i valori risultanti per la x appartengano all'intervallo $[0, 24\,140]$. Per $h := -5, -4, -3$ si ottiene

$$x_{-5} = 1\,645, \quad x_{-4} = 9\,692, \quad x_{-3} = 17\,739\,.$$

Esercizio 8.4

Sia $\mathbb{Z}_{652}$ l'anello delle classi di resto modulo 652. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{652}$ a cui z appartiene. Si dica quante sono le (eventuali) soluzioni in $\mathbb{Z}_{652}$ dell'equazione

$$[100]x = [0]$$

e le si trovino tutte.

Soluzione – È immediato che $[0]$ è una soluzione dell'equazione data. Essa è l'unica soluzione se e soltanto se $[100]$ non è divisore dello zero in $\mathbb{Z}_{652}$.

Se $a \neq 0$, sappiamo che $[a]$ è divisore dello zero in $\mathbb{Z}_n$ se e soltanto se il massimo comun divisore fra a e n è diverso da 1. Poiché

$652 = 100 \cdot 6 + 52$;
$100 = 52 \cdot 1 + 48$;
$52 = 48 \cdot 1 + 4$;
$48 = 4 \cdot 12 + 0$

il massimo comun divisore fra 652 e 100 è 4, dunque $[100]$ è un divisore dello zero in $\mathbb{Z}_{652}$.

Poiché $652 = 4 \cdot 163$, le soluzioni dell'equazione

$$[100]x = [0]$$

sono tutti e soli gli elementi di $\mathbb{Z}_{652}$ della forma $[h \cdot 163]$ con $h \in \mathbb{Z}$; ma poiché $4 \cdot 163 = 652$, valori di h che differiscono per multipli di 4 danno luogo allo stesso elemento di $\mathbb{Z}_{652}$. Dunque le soluzioni cercate sono 4, e si ottengono (ad esempio) per $h := 0, 1, 2, 3$. Esse sono

$$x_1 := [0]; \quad x_2 := [163]; \quad x_3 := [326]; \quad x_4 := [489].$$

Esercizio 8.5

Sia $\mathbb{Z}_{6\,499}$ l'anello delle classi di resto modulo $6\,499$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{6\,499}$ a cui z appartiene. Per ciascuno dei seguenti elementi di $\mathbb{Z}_{6\,499}$ si determini, qualora esista, un elemento $[a] \in \mathbb{Z}_{6\,499}$ diverso da $[0]$ che moltiplicato per lui dia come risultato $[0]$:

$$[469], \quad [485], \quad [523], \quad [19\,497].$$

Soluzione – Esiste un elemento $[a] \in \mathbb{Z}_{6\,499}$ diverso da $[0]$ tale che $[a][b] = [0]$ se e soltanto se $\mathrm{MCD}(6\,499, b) \neq 1$.

Calcoliamo $\mathrm{MCD}(6\,499, 469)$:

$6\,499 = 469 \cdot 13 + 402$; $\qquad 469 = 402 \cdot 1 + 67$;. $\qquad 402 = 67 \cdot 6$.

Dunque $\mathrm{MCD}(6\,499, 469) = 67$; poiché $6\,499 = 67 \cdot 97$, si ha

$$[469] \cdot [97] = [7 \cdot 67 \cdot 97] = [7 \cdot 6\,499] = [0].$$

Calcoliamo $\mathrm{MCD}(6\,499, 485)$:

$$6\,499 = 485 \cdot 13 + 194; \qquad 485 = 194 \cdot 2 + 97; \qquad 194 = 97 \cdot 2.$$

Dunque $\text{MCD}(6\,499,\,485) = 97$; poiché $6\,499 = 97 \cdot 67$, si ha

$$[485] \cdot [67] = [5 \cdot 97 \cdot 67] = [5 \cdot 6\,499] = [0]\,.$$

Calcoliamo $\text{MCD}(6\,499,\,523)$:

$$6\,499 = 523 \cdot 12 + 223\,;\quad 523 = 223 \cdot 2 + 77\,;\quad 223 = 77 \cdot 2 + 69\,;\quad 77 = 69 \cdot 1 + 8\,;$$

$$69 = 8 \cdot 8 + 5\,;\quad 8 = 5 \cdot 1 + 3\,;\quad 5 = 3 \cdot 1 + 2\,;\quad 3 = 2 \cdot 1 + 1\,;\quad 2 = 2 \cdot 1\,.$$

Dunque $\text{MCD}(6\,499,\,523) = 1$; pertanto non esiste alcun $[a] \in \mathbb{Z}_{6\,499}$ diverso da $[0]$ tale che $[a][523] = [0]$.

Calcoliamo infine $\text{MCD}(6\,499,\,19\,497)$: $\quad 19\,497 = 6\,499 \cdot 3$

dunque $[19\,497] = [0]$ in $\mathbb{Z}_{6\,499}$ e quindi $[a] \cdot [19\,497] = [0]$ per ogni $[a] \in \mathbb{Z}_{6\,499}$.

Esercizio 8.6

Sia $\mathbb{Z}_{6319}$ l'anello delle classi di resto modulo $6\,319$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{6\,319}$ a cui z appartiene. Per ciascuno dei seguenti elementi di $\mathbb{Z}_{6\,319}$ si determini, qualora esista, un elemento $[a] \in \mathbb{Z}_{6\,319}$ diverso da $[0]$ che moltiplicato per lui dia come risultato $[0]$:

$$[445],\quad [497],\quad [717],\quad [18\,957].$$

Soluzione – Esiste un elemento $[a] \in \mathbb{Z}_{6\,319}$ diverso da $[0]$ tale che $[a][b] = [0]$ se e soltanto se $\text{MCD}(6\,319, b) \neq 1$.

Calcoliamo $\text{MCD}(6\,319,\,445)$: $\quad 6\,319 = 445 \cdot 14 + 89\,;\quad 445 = 89 \cdot 5\,.$

Dunque $\text{MCD}(6\,319,\,445) = 89$; poiché $6\,319 = 89 \cdot 71$, si ha

$$[445] \cdot [71] = [5 \cdot 89 \cdot 71] = [5 \cdot 6\,319] = [0]\,.$$

Calcoliamo $\text{MCD}(6\,319,\,497)$:

$$6\,319 = 497 \cdot 12 + 355\,;\quad 497 = 355 \cdot 1 + 142\,;\quad 355 = 142 \cdot 2 + 71\,;\quad 142 = 71 \cdot 2\,.$$

Dunque $\text{MCD}(6\,319,\,497) = 71$; poiché $6\,319 = 71 \cdot 89$, si ha

$$[497] \cdot [89] = [7 \cdot 71 \cdot 89] = [7 \cdot 6\,319] = [0]\,.$$

Calcoliamo $\text{MCD}(6\,319,\,717)$:

$$6\,319 = 717 \cdot 8 + 583\,;\quad 717 = 583 \cdot 1 + 134\,;\quad 583 = 134 \cdot 4 + 47\,;\quad 134 = 47 \cdot 2 + 40\,;$$

$$47 = 40 \cdot 1 + 7\,;\quad 40 = 7 \cdot 5 + 5\,;\quad 7 = 5 \cdot 1 + 2\,;\quad 5 = 2 \cdot 2 + 1\,;\quad 2 = 2 \cdot 1\,.$$

Dunque $\text{MCD}(6\,319,\,717) = 1$; pertanto non esiste alcun $[a] \in \mathbb{Z}_{6\,319}$ diverso da $[0]$ tale che $[a][717] = [0]$.

Calcoliamo infine $\text{MCD}(6\,319,\,18\,957)$: $\quad 18\,957 = 6\,319 \cdot 3$

dunque $[18\,957] = [0]$ in $\mathbb{Z}_{6\,319}$ e quindi $[a] \cdot [18\,957] = [0]$ per ogni $[a] \in \mathbb{Z}_{6\,319}$.

Esercizio 8.7

Sia $\mathbb{Z}_{47\,435}$ l'anello delle classi di resto modulo $47\,435$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{47\,435}$ a cui z appartiene. Si trovino tutte le soluzioni in $\mathbb{Z}_{47\,435}$ della seguente equazione:

$$[6\,720]x = [55]\ .$$

Soluzione – Sia $x_0 \in \mathbb{Z}$ tale che $[x_0]$ è soluzione dell'equazione proposta; allora

$$[6\,720] \cdot [x_0] = [55] \qquad \text{ossia} \qquad [6\,720 \cdot x_0] = [55]$$

e dunque deve esistere $y_0 \in \mathbb{Z}$ tale che $\quad 6\,720\,x_0 - 55 = 47\,435\,y_0$.

Siamo quindi ricondotti a considerare l'equazione diofantina

(*) $$6\,720\,x - 47\,435\,y = 55$$

della quale ci interessano soltano i valori della x, anzi le loro classi di resto modulo $47\,435$ (per questo motivo sarebbe equivalente considerare l'equazione diofantina

$$6\,720\,x + 47\,435\,y = 55$$

che nella x ha esattamente le stesse soluzioni).

Calcoliamo con l'algoritmo di Euclide il MCD fra $47\,435$ e $6\,720$.

$47\,435 = 6\,720 \cdot 7 + 395$; $\qquad 6\,720 = 395 \cdot 17 + 5$; $\qquad 395 = 5 \cdot 79$.

Il massimo comun divisore fra $47\,435$ e $6\,720$ è dunque 5; poiché si tratta di un divisore di 55, la (*) ha soluzione.

Cerchiamo adesso una soluzione per l'equazione

$$6\,720\,x - 47\,435\,y = 55\,.$$

Dai calcoli fatti per trovare il massimo comun divisore, abbiamo che

$$5 = 6\,720 - 17 \cdot 395 = 6\,720 - 17 \cdot (47\,435 - 7 \cdot 6\,720) = 120 \cdot 6\,720 - 17 \cdot 47\,435$$

e dunque

$$55 = 11 \cdot 5 = 1\,320 \cdot 6\,720 - 187 \cdot 47\,435\,.$$

Pertanto una soluzione dell'equazione $6\,720\,x - 47\,435\,y = 55$ è $(1\,320, 187)$. La generica soluzione è

$$x := 1\,320 + \tfrac{47\,435}{5}h, \qquad y := 187 + \tfrac{6\,720}{5}h \quad \text{(al variare di } h \text{ in } \mathbb{Z})$$

ossia

$$x := 1\,320 + 9\,487h, \qquad y := 187 + 1\,344h \quad \text{(al variare di } h \text{ in } \mathbb{Z}).$$

A noi interessano soltanto i valori della x, anzi fra questi ne vogliamo 5 che diano luogo a classi di resto distinte modulo $47\,435$. Basta prendere cinque valori interi consecutivi per h, ma per "fare bella figura" di solito si scelgono in modo che i valori risultanti per la x appartengano all'intervallo $[0, 47\,434]$. Per $h := 0, 1, 2, 3, 4$ si ottiene

$$x_0 = 1\,320, \quad x_1 = 10\,807, \quad x_2 = 20\,294, \quad x_3 = 29\,781, \quad x_4 = 39\,268\,.$$

Esercizio 8.8

Sia $\mathbb{Z}_{13\,275}$ l'anello delle classi di resto modulo $13\,275$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{13\,275}$ a cui z appartiene. Si trovino tutte le soluzioni in $\mathbb{Z}_{13\,275}$ della seguente equazione:

$$[5\,690]x = [785]\,.$$

Soluzione – Sia $x_0 \in \mathbb{Z}$ tale che $[x_0]$ è soluzione dell'equazione proposta; allora

$$[5\,690] \cdot [x_0] = [785] \qquad \text{ossia} \qquad [5\,690 \cdot x_0] = [785]$$

e dunque deve esistere $y_0 \in \mathbb{Z}$ tale che

$$5\,690\,x_0 - 785 = 13\,275\,y_0\,.$$

Siamo quindi ricondotti a considerare l'equazione diofantina

(*) $$5\,690\,x - 13\,275\,y = 785$$

della quale ci interessano soltano i valori della x, anzi le loro classi di resto modulo $13\,275$ (per questo motivo sarebbe equivalente considerare l'equazione diofantina

$$5\,690\,x + 13\,275\,y = 785$$

che nella x ha esattamente le stesse soluzioni).

Calcoliamo con l'algoritmo di Euclide il MCD fra $13\,275$ e $5\,690$.

$13\,275 = 5\,690 \cdot 2 + 1\,895$; $\qquad 5\,690 = 1\,895 \cdot 3 + 5$; $\qquad 1\,895 = 5 \cdot 379$..

Il massimo comun divisore fra $13\,275$ e $5\,690$ è dunque 5; poiché si tratta di un divisore di 785, la (*) ha soluzione.

Cerchiamo adesso una soluzione per l'equazione

$$5\,690\,x - 13\,275\,y = 785\,.$$

Dai calcoli fatti per trovare il massimo comun divisore, abbiamo che

$$5 = 5\,690 - 3 \cdot 1\,895 = 5\,690 - 3 \cdot (13\,275 - 2 \cdot 5\,690) = 7 \cdot 5\,690 - 3 \cdot 13\,275$$

e dunque

$$785 = 5 \cdot 157 = 1\,099 \cdot 5\,690 - 471 \cdot 13\,275\,.$$

Pertanto una soluzione dell'equazione $5\,690\,x - 13\,275\,y = 785$ è $(1\,099, -471)$. La generica soluzione è

$$x := 1\,099 + \tfrac{13\,275}{5}h,\ \ y := -471 + \tfrac{5\,690}{5}h \quad \text{(al variare di } h \text{ in } \mathbb{Z})$$

ossia

$$x := 1\,099 + 2\,655h, \quad y := -471 + 1\,138h \quad \text{(al variare di } h \text{ in } \mathbb{Z}).$$

A noi interessano soltanto i valori della x, anzi fra questi ne vogliamo 5 che diano luogo a classi di resto distinte modulo $13\,275$. Basta prendere cinque valori interi consecutivi per h, ma per "fare bella figura" di solito si scelgono in modo che i valori risultanti per la x appartengano all'intervallo $[0, 13\,274]$. Per $h := 0, 1, 2, 3, 4$ si ottiene

$$x_0 = 1\,099, \quad x_1 = 3\,754, \quad x_2 = 6\,409, \quad x_3 = 9\,064, \quad x_4 = 11\,719\,.$$

Esercizio 8.9

Sia $\mathbb{Z}_{6\,161}$ l'anello delle classi di resto modulo $6\,161$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{6\,161}$ a cui z appartiene. Per ciascuno dei seguenti elementi di $\mathbb{Z}_{6\,161}$ si determini, qualora esista, un elemento $[a] \in \mathbb{Z}_{6\,161}$ diverso da $[0]$ che moltiplicato per lui dia come risultato $[0]$:

$$[427], \quad [505], \quad [523], \quad [18\,483].$$

Soluzione – Esiste un elemento $[a] \in \mathbb{Z}_{6\,161}$ diverso da $[0]$ tale che $[a][b] = [0]$ se e soltanto se $\text{MCD}(6\,161, b) \neq 1$.

Calcoliamo $\text{MCD}(6\,161, 427)$:

$6\,161 = 427 \cdot 14 + 183$; $\quad 427 = 183 \cdot 2 + 61$;. $\quad 183 = 61 \cdot 3$.

Dunque $\text{MCD}(6\,161, 427) = 61$; poiché $6\,161 = 61 \cdot 101$, si ha

$$[427] \cdot [101] = [7 \cdot 61 \cdot 101] = [7 \cdot 6\,161] = [0].$$

Calcoliamo $\text{MCD}(6\,161, 505)$:

$$6\,161 = 505 \cdot 12 + 101; \qquad 505 = 101 \cdot 5.$$

Dunque $\text{MCD}(6\,161, 505) = 101$; poiché $6\,161 = 101 \cdot 61$, si ha

$$[505] \cdot [61] = [5 \cdot 101 \cdot 61] = [5 \cdot 6\,161] = [0].$$

Calcoliamo $\text{MCD}(6\,161, 523)$:

$6\,161 = 523 \cdot 11 + 408$; $\quad 523 = 408 \cdot 1 + 115$; $\quad 408 = 115 \cdot 3 + 63$; $\quad 115 = 63 \cdot 1 + 52$;

$63 = 52 \cdot 1 + 11$; $52 = 11 \cdot 4 + 8$; $11 = 8 \cdot 1 + 3$; $8 = 3 \cdot 2 + 2$; $3 = 2 \cdot 1 + 1$; $2 = 2 \cdot 1$.

Dunque $\text{MCD}(6\,161, 523) = 1$; pertanto non esiste alcun $[a] \in \mathbb{Z}_{6\,161}$ diverso da $[0]$ tale che $[a][523] = [0]$.

Calcoliamo infine $\text{MCD}(6\,161, 18\,483)$: $\quad 18\,483 = 6\,161 \cdot 3$

dunque $[18\,483] = [0]$ in $\mathbb{Z}_{6\,161}$ e quindi $[a] \cdot [18\,483] = [0]$ per ogni $[a] \in \mathbb{Z}_{6\,161}$.

Esercizio 8.10

Sia $\mathbb{Z}_{126}$ l'anello delle classi di resto modulo 126. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{126}$ a cui z appartiene. Si stabilisca, motivando la risposta, se $[47]$ ha inverso in $\mathbb{Z}_{126}$ e nel caso che la risposta sia affermativa si determini esplicitamente tale inverso.

Soluzione – Sappiamo che $[z]$ è invertibile in $\mathbb{Z}_{126}$ se e soltanto se

$$\text{MCD}(z, 126) = 1.$$

Calcoliamo allora il massimo comun divisore fra 47 e 126.

$126 = 47 \cdot 2 + 32$; $\quad 47 = 32 \cdot 1 + 15$; $\quad 32 = 15 \cdot 2 + 2$;

$15 = 2 \cdot 7 + 1$; $\quad 2 = 2 \cdot 1$.

Dunque MCD$(47,\,126)=1$ e pertanto $[47]$ è invertibile in $\mathbb{Z}_{126}$.

Per trovarne l'inverso, cerchiamo in primo luogo un $x\in\mathbb{Z}$ tale che

$$47\cdot x\equiv 1 \pmod{126}$$

ossia tale che

$$47x-1=126y \quad \text{con } y\in\mathbb{Z}\,.$$

Si tratta di risolvere l'equazione diofantina

$$47x-126y=1$$

oppure (poiché a noi interessa soltanto trovare un valore per la x) l'equazione diofantina

$$47x+126y=1\,.$$

Per far ciò è sufficiente ricavare l'identità di Bezout partendo dai calcoli effettuati per trovare il massimo comun divisore fra 47 e 126. Si ha dunque

$$1=15-2\cdot 7=15-(32-15\cdot 2)\cdot 7=15\cdot 15-7\cdot 32=15\cdot(47-32)-7\cdot 32=$$
$$=15\cdot 47-22\cdot 32=15\cdot 47-22\cdot(126-47\cdot 2)=59\cdot 47-22\cdot 126\,.$$

Una soluzione dell'equazione diofantina $47x+126y=1$ è dunque $x=59$, $y=-22$.

L'inverso di $[47]$ in $\mathbb{Z}_{126}$ è $[59]$.

Esercizio 8.11

Sia $\mathbb{Z}_{30\,705}$ l'anello delle classi di resto modulo $30\,705$. Per ogni $z\in\mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{30\,705}$ a cui z appartiene. Si trovino tutte le (eventuali) soluzioni in $\mathbb{Z}_{30\,705}$ della seguente equazione:

$$[2\,772]x=[291]\,.$$

Soluzione – Sia $x_0\in\mathbb{Z}$ tale che $[x_0]$ è soluzione dell'equazione proposta; allora

$$[2\,772]\cdot[x_0]=[291] \qquad \text{ossia} \qquad [2\,772\cdot x_0]=[291]$$

e dunque deve esistere $y_0\in\mathbb{Z}$ tale che $\quad 2\,772\,x_0-291=30\,705\,y_0\,.$

Siamo quindi ricondotti a considerare l'equazione diofantina

(*) $$2\,772\,x-30\,705\,y=291$$

della quale ci interessano soltano i valori della x, anzi le loro classi di resto modulo $30\,705$ (per questo motivo sarebbe equivalente considerare l'equazione diofantina

$$2\,772\,x+30\,705\,y=291$$

che nella x ha esattamente le stesse soluzioni).

Calcoliamo con l'algoritmo di Euclide il MCD fra $30\,705$ e $2\,772$.

$30\,705=2\,772\cdot 11+213\,;\qquad 2\,772=213\cdot 13+3\,;\qquad 213=3\cdot 71\,.$

Il massimo comun divisore fra $30\,705$ e $2\,772$ è dunque 3; poiché si tratta di un divisore di 291, la (*) ha soluzione.

Cerchiamo adesso una soluzione per l'equazione

$$2\,772\,x - 30\,705\,y = 291\,.$$

Dai calcoli fatti per trovare il massimo comun divisore, abbiamo che

$$3 = 2\,772 - 13 \cdot 213 = 2\,772 - 13 \cdot (30\,705 - 11 \cdot 2\,772) = 144 \cdot 2\,772 - 13 \cdot 30\,705$$

e dunque

$$291 = 97 \cdot 3 = 13\,968 \cdot 2\,772 - 1\,261 \cdot 30\,705\,.$$

Pertanto una soluzione dell'equazione $2\,772\,x - 30\,705\,y = 291$ è $(13\,968, 1\,261)$. La generica soluzione è

$$x := 13\,968 + \tfrac{30\,705}{3}h, \qquad y := 1\,261 + \tfrac{2\,772}{3}h \quad \text{(al variare di } h \text{ in } \mathbb{Z})$$

ossia

$$x := 13\,968 + 10\,235h, \qquad y := 1\,261 + 924h \quad \text{(al variare di } h \text{ in } \mathbb{Z}).$$

A noi interessano soltanto i valori della x, anzi fra questi ne vogliamo 3 che diano luogo a classi di resto distinte modulo $30\,705$. Basta prendere tre valori interi consecutivi per h, ma per "fare bella figura" di solito si scelgono in modo che i valori risultanti per la x appartengano all'intervallo $[0, 30\,704]$. Per $h := -1, 0, 1$ si ottiene

$$x_{-1} = 3\,733, \quad x_0 = 13\,968, \quad x_1 = 24\,203\,.$$

Esercizio 8.12

Sia $\mathbb{Z}_{668}$ l'anello delle classi di resto modulo 668. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{668}$ a cui z appartiene. Si dica quante sono le (eventuali) soluzioni in $\mathbb{Z}_{668}$ dell' equazione

$$[100]x = [0]$$

e le si trovino tutte.

Soluzione – È immediato che $[0]$ è una soluzione dell'equazione data. Essa è l'unica soluzione se e soltanto se $[100]$ non è divisore dello zero in $\mathbb{Z}_{668}$.

Se $a \neq 0$, sappiamo che $[a]$ è divisore dello zero in $\mathbb{Z}_n$ se e soltanto se il massimo comun divisore fra a e n è diverso da 1. Poiché

$668 = 100 \cdot 6 + 68$;
$100 = 68 \cdot 1 + 32$;
$68 = 32 \cdot 2 + 4$;
$32 = 4 \cdot 8 + 0$

il massimo comun divisore fra 668 e 100 è 4, dunque $[100]$ è un divisore dello zero in $\mathbb{Z}_{668}$.

Poiché $668 = 4 \cdot 167$, le soluzioni dell'equazione

$$[100]x = [0]$$

sono tutti e soli gli elementi di $\mathbb{Z}_{668}$ della forma $[h \cdot 167]$ con $h \in \mathbb{Z}$; ma poiché $4 \cdot 167 = 668$, valori di h che differiscono per multipli di 4 danno luogo allo stesso elemento di $\mathbb{Z}_{668}$. Dunque le soluzioni cercate sono 4, e si ottengono (ad esempio) per $h := 0, 1, 2, 3$. Esse sono

$$x_1 := [0]; \quad x_2 := [167]; \quad x_3 := [334]; \quad x_4 := [501].$$

Esercizio 8.13

Sia $\mathbb{Z}_{668}$ l'anello delle classi di resto modulo 668. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{668}$ a cui z appartiene. Si trovino tutte le (eventuali) soluzioni in $\mathbb{Z}_{668}$ della seguente equazione:

$$[664]x = [356].$$

Soluzione – Sia $x_0 \in \mathbb{Z}$ tale che $[x_0]$ è soluzione dell'equazione proposta; allora

$$[664] \cdot [x_0] = [356] \qquad \text{ossia} \qquad [664 \cdot x_0] = [356]$$

e dunque deve esistere $y_0 \in \mathbb{Z}$ tale che

$$664\, x_0 - 356 = 668\, y_0.$$

Siamo quindi ricondotti a considerare l'equazione diofantina

(*) $$664\, x - 668\, y = 356$$

della quale ci interessano soltano i valori della x, anzi le loro classi di resto modulo 652 (per questo motivo sarebbe equivalente considerare l'equazione diofantina

$$664\, x + 668\, y = 356$$

che nella x ha esattamente le stesse soluzioni).

Calcoliamo il MCD fra 664 e 668 mediante l'algoritmo di Euclide:

$$668 = 664 \cdot 1 + 4; \qquad 664 = 4 \cdot 166 + 0.$$

Il massimo comun divisore fra 664 e 668 è dunque 4; poiché si tratta di un divisore di 356, la (*) ha soluzione (e l'equazione proposta ha esattamente 4 soluzioni).

Cerchiamo adesso una soluzione per l'equazione

$$664\, x - 668\, y = 356.$$

Dai calcoli fatti per trovare il massimo comun divisore, abbiamo che

$$4 = 668 - 664$$

e dunque

$$356 = 664 \cdot (-89) + 668 \cdot 89.$$

Pertanto una soluzione dell'equazione $664\, x - 668\, y = 356$ è $(-89, -89)$. La generica soluzione è

$$x := -89 + \tfrac{668}{4} h, \quad y := -89 + \tfrac{664}{4} h \qquad \text{(al variare di } h \text{ in } \mathbb{Z})$$

ossia

$$x := -89 + 167h, \qquad y := -89 + 166h \qquad \text{(al variare di } h \text{ in } \mathbb{Z}).$$

A noi interessano soltanto i valori della x, anzi fra questi ne vogliamo 4 che diano luogo a classi di resto distinte modulo 668. Basta prendere quattro valori interi consecutivi per h, ma per "fare bella figura" di solito si scelgono in modo che i valori risultanti per la x appartengano all'intervallo $[0, 667]$. Per $h := 1, 2, 3, 4$ si ottiene

$$x_1 = 78, \quad x_2 = 245, \quad x_3 = 412, \quad x_4 = 579\,.$$

Esercizio 8.14

Sia $\mathbb{Z}_{6059}$ l'anello delle classi di resto modulo $6\,059$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{6059}$ a cui z appartiene. Per ciascuno dei seguenti elementi di $\mathbb{Z}_{6059}$ si determini, qualora esista, un elemento $[a] \in \mathbb{Z}_{6059}$ diverso da $[0]$ che moltiplicato per lui dia come risultato $[0]$:

$$[415], \quad [723], \quad [949], \quad [18\,177].$$

Soluzione – Esiste un elemento $[a] \in \mathbb{Z}_{6059}$ diverso da $[0]$ tale che $[a][b] = [0]$ se e soltanto se $\mathrm{MCD}(6\,059, b) \neq 1$.

Calcoliamo $\mathrm{MCD}(6\,059, 415)$:

$$6\,059 = 415 \cdot 14 + 249\,; \qquad 415 = 249 \cdot 1 + 166\,; \qquad 249 = 166 \cdot 1 + 83\,; \qquad 166 = 83 \cdot 2\,.$$

Dunque $\mathrm{MCD}(6\,059, 415) = 83$; poiché $6\,059 = 83 \cdot 73$, in $\mathbb{Z}_{6059}$ si ha

$$[415] \cdot [73] = [5 \cdot 83 \cdot 73] = [5 \cdot 6\,059] = [0]\,.$$

Calcoliamo $\mathrm{MCD}(6\,059, 723)$:

$$6\,059 = 723 \cdot 8 + 275\,; \quad 723 = 275 \cdot 2 + 173\,; \quad 275 = 173 \cdot 1 + 102\,; \quad 173 = 102 \cdot 1 + 71\,;$$

$$102 = 71 \cdot 1 + 31\,; \qquad 71 = 31 \cdot 2 + 9\,; \qquad 31 = 9 \cdot 3 + 4\,; \qquad 9 = 4 \cdot 2 + 1\,; \qquad 4 = 1 \cdot 4\,.$$

Dunque $\mathrm{MCD}(6\,059, 723) = 1$; pertanto non esiste alcun $[a] \in \mathbb{Z}_{6059}$ diverso da $[0]$ tale che $[a][717] = [0]$.

Calcoliamo $\mathrm{MCD}(6\,059, 949)$:

$$6\,059 = 949 \cdot 6 + 365\,; \quad 949 = 365 \cdot 2 + 219\,; \quad 365 = 219 \cdot 1 + 146\,; \quad 21\,9 = 146 \cdot 1 + 73\,;$$

$$146 = 73 \cdot 2\,.$$

Dunque $\mathrm{MCD}(6\,059, 949) = 73$; poiché $6\,059 = 73 \cdot 83$, in $\mathbb{Z}_{6059}$ si ha

$$[949] \cdot [83] = [13 \cdot 73 \cdot 83] = [13 \cdot 6\,059] = [0]\,.$$

Calcoliamo infine $\mathrm{MCD}(6\,059, 18\,177)$: $\quad 18\,177 = 6\,059 \cdot 3$

dunque $[18\,177] = [0]$ in $\mathbb{Z}_{6059}$ e quindi $[a] \cdot [18\,177] = [0]$ per ogni $[a] \in \mathbb{Z}_{6059}$.

Esercizio 8.15

Sia $\mathbb{Z}_{6077}$ l'anello delle classi di resto modulo $6\,077$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{6077}$ a cui z appartiene. Per ciascuno dei seguenti elementi di $\mathbb{Z}_{6077}$ si determini, qualora esista, un elemento $[a] \in \mathbb{Z}_{6077}$ diverso da $[0]$ che moltiplicato per lui dia come risultato $[0]$:

$$[413], \quad [515], \quad [569], \quad [18\,231].$$

Soluzione – Esiste un elemento $[a] \in \mathbb{Z}_{6077}$ diverso da $[0]$ tale che $[a][b] = [0]$ se e soltanto se $\mathrm{MCD}(6\,077, b) \neq 1$. Calcoliamo $\mathrm{MCD}(6\,077, 413)$:

$6\,077 = 413 \cdot 14 + 295$;
$413 = 295 \cdot 1 + 118$;
$295 = 118 \cdot 2 + 59$;
$118 = 59 \cdot 2$.

Dunque $\mathrm{MCD}(6\,077, 413) = 59$; poiché $6\,077 = 59 \cdot 103$, si ha

$$[413] \cdot [103] = [7 \cdot 59 \cdot 103] = [7 \cdot 6\,077] = [0].$$

Calcoliamo $\mathrm{MCD}(6\,077, 515)$:

$$6\,077 = 515 \cdot 11 + 412; \qquad 515 = 412 \cdot 1 + 103; \qquad 412 = 103 \cdot 4.$$

Dunque $\mathrm{MCD}(6\,077, 515) = 103$; poiché $6\,077 = 103 \cdot 59$, si ha

$$[515] \cdot [59] = [5 \cdot 103 \cdot 59] = [5 \cdot 6\,077] = [0].$$

Calcoliamo $\mathrm{MCD}(6\,077, 569)$:

$$6\,077 = 569 \cdot 10 + 387; \quad 569 = 387 \cdot 1 + 182; \quad 387 = 182 \cdot 2 + 23; \quad 182 = 23 \cdot 7 + 21;$$
$$23 = 21 \cdot 1 + 2; \quad 21 = 2 \cdot 10 + 1; \quad 2 = 2 \cdot 1.$$

Dunque $\mathrm{MCD}(6\,077, 569) = 1$; pertanto non esiste alcun $[a] \in \mathbb{Z}_{6077}$ diverso da $[0]$ tale che $[a][569] = [0]$.

Calcoliamo infine $\mathrm{MCD}(6\,077, 18\,231)$: $\quad 18\,231 = 6\,077 \cdot 3$

dunque $[18\,231] = [0]$ in $\mathbb{Z}_{6077}$ e quindi $[a] \cdot [18\,231] = [0]$ per ogni $[a] \in \mathbb{Z}_{6077}$.

Esercizio 8.16

Sia $\mathbb{Z}_{52\,615}$ l'anello delle classi di resto modulo $52\,615$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{52\,615}$ a cui z appartiene. Si trovino tutte le soluzioni in $\mathbb{Z}_{52\,615}$ della seguente equazione:

$$[4\,750]x = [55]$$

Soluzione – Sia $x_0 \in \mathbb{Z}$ tale che $[x_0]$ è soluzione dell'equazione proposta; allora

$$[4\,750] \cdot [x_0] = [55] \qquad \text{ossia} \qquad [4\,750 \cdot x_0] = [55]$$

e dunque deve esistere $y_0 \in \mathbb{Z}$ tale che $\quad 4\,750\, x_0 - 55 = 52\,615\, y_0$.

Siamo quindi ricondotti a considerare l'equazione diofantina

(*) $$4\,750\,x - 52\,615\,y = 55$$

della quale ci interessano soltano i valori della x, anzi le loro classi di resto modulo $52\,615$ (per questo motivo sarebbe equivalente considerare l'equazione diofantina

$$4\,750\,x + 52\,615\,y = 55$$

che nella x ha esattamente le stesse soluzioni).

Calcoliamo con l'algoritmo di Euclide il MCD fra $52\,615$ e $4\,750$.

$52\,615 = 4\,750 \cdot 11 + 365$; $\quad 4\,750 = 365 \cdot 13 + 5$; $\quad 365 = 5 \cdot 73$.

Il massimo comun divisore fra $52\,615$ e $4\,750$ è dunque 5; poiché si tratta di un divisore di 55, la (*) ha soluzione.

Cerchiamo adesso una soluzione per l'equazione

$$4\,750\,x - 52\,615\,y = 55\,.$$

Dai calcoli fatti per trovare il massimo comun divisore, abbiamo che

$$5 = 4\,750 - 13 \cdot 365 = 4\,750 - 13 \cdot (52\,615 - 11 \cdot 4\,750) = 144 \cdot 4\,750 - 13 \cdot 52\,615$$

e dunque

$$55 = 11 \cdot 5 = 1\,584 \cdot 4\,750 - 143 \cdot 52\,615\,.$$

Pertanto una soluzione dell'equazione $4\,750\,x - 52\,615\,y = 55$ è $(1\,584, 143)$. La generica soluzione è

$$x := 1\,584 + \tfrac{52\,615}{5}h, y := 143 + \tfrac{4\,750}{5}h \quad \text{(al variare di } h \text{ in } \mathbb{Z})$$

ossia

$$x := 1\,584 + 10\,523h, \quad y := 143 + 950h \quad \text{(al variare di } h \text{ in } \mathbb{Z}).$$

A noi interessano soltanto i valori della x, anzi fra questi ne vogliamo 5 che diano luogo a classi di resto distinte modulo $52\,615$. Basta prendere cinque valori interi consecutivi per h, ma per "fare bella figura" di solito si scelgono in modo che i valori risultanti per la x appartengano all'intervallo $[0, 52\,614]$. Per $h := 0, 1, 2, 3, 4$ si ottiene

$$x_0 = 1\,584, \quad x_1 = 12\,107, \quad x_2 = 22\,630, \quad x_3 = 33\,153, \quad x_4 = 43\,676\,.$$

Esercizio 8.17

Sia $\mathbb{Z}_{167}$ l'anello delle classi di resto modulo 167. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{167}$ a cui z appartiene. Si stabilisca, motivando la risposta, se $[27]$ ha inverso in $\mathbb{Z}_{167}$ e nel caso che la risposta sia affermativa si determini esplicitamente tale inverso.

Soluzione – Sappiamo che $[z]$ è invertibile in $\mathbb{Z}_{167}$ se e soltanto se

$$\text{MCD}(z, 167) = 1\,.$$

Calcoliamo allora il massimo comun divisore fra 27 e 167.

$$167 = 27 \cdot 6 + 5\,; \quad 27 = 5 \cdot 5 + 2\,; \quad 5 = 2 \cdot 2 + 1\,; \quad 5 = 2 \cdot 2 + 1\,; \quad 2 = 2 \cdot 1\,.$$

Dunque MCD$(27, 167) = 1$ e pertanto $[27]$ è invertibile in $\mathbb{Z}_{167}$.

Per trovarne l'inverso, cerchiamo in primo luogo un $x \in \mathbb{Z}$ tale che

$$27 \cdot x \equiv 1 \pmod{167}$$

ossia tale che

$$27x - 1 = 167y \quad \text{con } y \in \mathbb{Z}\,.$$

Si tratta di risolvere l'equazione diofantina

$$27x - 167y = 1$$

oppure (poiché a noi interessa soltanto trovare un valore per la x) l'equazione diofantina

$$27x + 167y = 1\,.$$

Per far ciò è sufficiente ricavare l'identità di Bezout partendo dai calcoli effettuati per trovare il massimo comun divisore fra 27 e 167. Si ha dunque

$$1 = 5 - 2 \cdot 2 = 5 - (27 - 5 \cdot 5) \cdot 2 = 5 \cdot 11 - 27 \cdot 2 =$$
$$= (167 - 27 \cdot 6) \cdot 11 - 27 \cdot 2 = 167 \cdot 11 - 68 \cdot 27\,.$$

Una soluzione dell'equazione diofantina $27x + 167y = 1$ è dunque $x = -68$, $y = 11$.

L'inverso di $[27]$ in $\mathbb{Z}_{167}$ è $[-68]$ (oppure, se si preferisce, $[99]$).

Esercizio 8.18

Sia $\mathbb{Z}_{14\,763}$ l'anello delle classi di resto modulo $14\,763$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{14\,763}$ a cui z appartiene. Si trovino tutte le soluzioni in $\mathbb{Z}_{14\,763}$ della seguente equazione:

$$[6\,328]x = [777]\,.$$

Soluzione – Sia $x_0 \in \mathbb{Z}$ tale che $[x_0]$ è soluzione dell'equazione proposta; allora

$$[6\,328] \cdot [x_0] = [777] \qquad \text{ossia} \qquad [6\,328 \cdot x_0] = [777]$$

e dunque deve esistere $y_0 \in \mathbb{Z}$ tale che

$$6\,328\,x_0 - 777 = 14\,763\,y_0\,.$$

Siamo quindi ricondotti a considerare l'equazione diofantina

(*) $$6\,328\,x - 14\,763\,y = 777$$

della quale ci interessano soltano i valori della x, anzi le loro classi di resto modulo $14\,763$ (per questo motivo sarebbe equivalente considerare l'equazione diofantina

$$6\,328\,x + 14\,763\,y = 777$$

che nella x ha esattamente le stesse soluzioni).

Calcoliamo con l'algoritmo di Euclide il MCD fra $14\,763$ e $6\,328$.

$$14\,763 = 6\,328 \cdot 2 + 2\,107\,; \qquad 6\,328 = 2\,107 \cdot 3 + 7\,; \qquad 2\,107 = 7 \cdot 301\,.$$

Il massimo comun divisore fra $14\,763$ e $6\,328$ è dunque 7; poiché si tratta di un divisore di 777, la (*) ha soluzione.

Cerchiamo adesso una soluzione per l'equazione

$$6\,328\,x - 14\,763\,y = 777\,.$$

Dai calcoli fatti per trovare il massimo comun divisore, abbiamo che

$$7 = 6\,328 - 3 \cdot 2\,107 = 6\,328 - 3 \cdot (14\,763 - 2 \cdot 6\,328) = 7 \cdot 6\,328 - 3 \cdot 14\,763$$

e dunque

$$777 = 7 \cdot 111 = 777 \cdot 6\,328 - 333 \cdot 14\,763\,.$$

Pertanto una soluzione dell'equazione $6\,328\,x - 14\,763\,y = 777$ è $(777, -333)$. La generica soluzione è

$$x := 777 + \tfrac{14\,763}{7}h, \quad y := -333 + \tfrac{6\,328}{7}h \quad \text{(al variare di } h \text{ in } \mathbb{Z})$$

ossia

$$x := 777 + 2\,109h, \quad y := -333 + 904h \quad \text{(al variare di } h \text{ in } \mathbb{Z}).$$

A noi interessano soltanto i valori della x, anzi fra questi ne vogliamo 7 che diano luogo a classi di resto distinte modulo $14\,763$. Basta prendere sette valori interi consecutivi per h, ma per "fare bella figura" di solito si scelgono in modo che i valori risultanti per la x appartengano all'intervallo $[0, 14\,762]$. Per $h := 0, 1, 2, 3, 4, 5, 6$ si ottiene

$$x_0 = 777, \quad x_1 = 2\,886, \quad x_2 = 4\,995, \quad x_3 = 7\,104, \quad x_4 = 9\,213, \quad x_5 = 11\,322, \quad x_6 = 13\,431\,.$$

Esercizio 8.19

Sia $\mathbb{Z}_{345}$ l'anello delle classi di resto modulo 345. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{345}$ a cui z appartiene. Si stabilisca, motivando la risposta, se $[31]$ ha inverso in $\mathbb{Z}_{345}$ e nel caso che la risposta sia affermativa si determini esplicitamente tale inverso.

Soluzione – Sappiamo che $[z]$ è invertibile in $\mathbb{Z}_{345}$ se e soltanto se

$$\mathrm{MCD}(z, 345) = 1\,.$$

Calcoliamo allora il massimo comun divisore fra 31 e 345.

$$345 = 31 \cdot 11 + 4\,; \qquad 31 = 4 \cdot 7 + 3\,; \qquad 4 = 3 \cdot 1 + 1\,; \qquad 3 = 1 \cdot 3\,.$$

Dunque $\mathrm{MCD}(31, 345) = 1$ e pertanto $[31]$ è invertibile in $\mathbb{Z}_{345}$.

Per trovarne l'inverso, cerchiamo in primo luogo un $x \in \mathbb{Z}$ tale che

$$31 \cdot x \equiv 1 \pmod{345}$$

ossia tale che

$$31x - 1 = 345y \quad \text{con } y \in \mathbb{Z}\,.$$

Si tratta di risolvere l'equazione diofantina

$$31x - 345y = 1$$

oppure (poiché a noi interessa soltanto trovare un valore per la x) l'equazione diofantina

$$31x + 345y = 1\,.$$

Per far ciò è sufficiente ricavare l'identità di Bezout partendo dai calcoli effettuati per trovare il massimo comun divisore fra 31 e 345. Si ha dunque

$$1 = 4 - 3 = 4 - (31 - 4 \cdot 7) = 4 \cdot 8 - 31 = (345 - 31 \cdot 11) \cdot 8 - 31 =$$

$$= 345 \cdot 8 - 89 \cdot 31\,.$$

Una soluzione dell'equazione diofantina $31x + 345y = 1$ è dunque $x = -89$, $y = 8$.

L'inverso di $[31]$ in $\mathbb{Z}_{345}$ è $[-89]$ (oppure, se si preferisce, $[256]$).

Esercizio 8.20

Sia $\mathbb{Z}_{5671}$ l'anello delle classi di resto modulo $5\,671$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{5671}$ a cui z appartiene. Per ciascuno dei seguenti elementi di $\mathbb{Z}_{5671}$ si determini, qualora esista, un elemento $[a] \in \mathbb{Z}_{5671}$ diverso da $[0]$ che moltiplicato per lui dia come risultato $[0]$:

$$[371],\quad [535],\quad [619],\quad [17\,013].$$

Soluzione – Esiste un elemento $[a] \in \mathbb{Z}_{5671}$ diverso da $[0]$ tale che $[a][b] = [0]$ se e soltanto se $\mathrm{MCD}(5\,671, b) \neq 1$.

Calcoliamo $\mathrm{MCD}(5\,671, 371)$:

$$5\,671 = 371 \cdot 15 + 106\,; \qquad 371 = 106 \cdot 3 + 53\,; \qquad 106 = 53 \cdot 2\,.$$

Dunque $\mathrm{MCD}(5\,671, 371) = 53$; poiché $5\,671 = 53 \cdot 107$, si ha

$$[371] \cdot [107] = [7 \cdot 53 \cdot 101] = [7 \cdot 5\,671] = [0]\,.$$

Calcoliamo $\mathrm{MCD}(5\,671, 535)$:

$$5\,671 = 535 \cdot 12 + 101\,; \qquad 535 = 107 \cdot 5\,.$$

Dunque $\mathrm{MCD}(5\,671, 535) = 107$; poiché $5\,671 = 107 \cdot 53$, si ha

$$[535] \cdot [53] = [5 \cdot 107 \cdot 53] = [5 \cdot 5\,671] = [0]\,.$$

Calcoliamo $\mathrm{MCD}(5\,671, 619)$:

$$5\,671 = 619 \cdot 9 + 100\,; \quad 619 = 100 \cdot 6 + 19\,; \quad 100 = 19 \cdot 5 + 5\,;$$

$$19 = 5 \cdot 3 + 4\,; \qquad 5 = 4 \cdot 1 + 1\,; \qquad 4 = 4 \cdot 1\,.$$

Dunque $\mathrm{MCD}(5\,671, 619) = 1$; pertanto non esiste alcun $[a] \in \mathbb{Z}_{5671}$ diverso da $[0]$ tale che $[a][619] = [0]$.

Calcoliamo infine $\mathrm{MCD}(5\,671, 17\,013)$: $\quad 17\,013 = 5\,671 \cdot 3$

dunque $[17\,013] = [0]$ in $\mathbb{Z}_{5671}$ e quindi $[a] \cdot [17\,013] = [0]$ per ogni $[a] \in \mathbb{Z}_{5671}$.

Esercizio 8.21

Sia $\mathbb{Z}_{401\,475}$ l'anello delle classi di resto modulo $401\,475$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{401\,475}$ a cui z appartiene. Si stabilisca quante soluzioni ha in $\mathbb{Z}_{401\,475}$ l'equazione

$$[4\,510]\,x = [4\,435]$$

e si scrivano tutte esplicitamente.

Soluzione – Sia $x_0 \in \mathbb{Z}$ tale che $[x_0]$ è soluzione dell'equazione proposta; allora

$$[4\,510]\cdot[x_0] = [4\,435] \qquad \text{ossia} \qquad [4\,510\cdot x_0] = [4\,435]$$

e dunque deve esistere $y_0 \in \mathbb{Z}$ tale che

$$4\,510\,x_0 - 4\,435 = 401\,475\,y_0\,.$$

Siamo quindi ricondotti a considerare l'equazione diofantina

(*) $$4\,510\,x - 401\,475\,y = 4\,435$$

della quale ci interessano soltano i valori della x, anzi le loro classi di resto modulo $401\,475$ (per questo motivo sarebbe equivalente considerare l'equazione diofantina

$$4\,510\,x + 401\,475\,y = 4\,435$$

che nella x ha esattamente le stesse soluzioni).

Calcoliamo il MCD fra $4\,510$ e $401\,475$ mediante l'algoritmo di Euclide:

$401\,475 = 4\,510\cdot 89 + 85\,;\quad 4\,510 = 85\cdot 53 + 5\,;\quad 85 = 5\cdot 17 + 0\,.$

Il massimo comun divisore fra $4\,510$ e $401\,475$ è dunque 5; poiché si tratta di un divisore di $4\,435$, la (*) ha soluzione (e l'equazione proposta ha esattamente 5 soluzioni).

Cerchiamo adesso una soluzione per l'equazione

$$4\,510\,x - 401\,475\,y = 4\,435\,.$$

Dai calcoli fatti per trovare il massimo comun divisore, abbiamo che

$$5 = 4\,510 - 85\cdot 53 = 4\,510 - (401\,475 - 4\,510\cdot 89)\cdot 53 =$$

$$= 4\,510\cdot(89\cdot 53 + 1) - 401\,475\cdot 53 = 4\,510\cdot 4\,718 - 401\,475\cdot 53$$

e dunque

$$4\,435 = 4\,510\cdot 4\,184\,866 - 401\,475\cdot 47\,011\,.$$

Pertanto una soluzione dell'equazione $4\,510\,x - 401\,475\,y = 4\,435$ è $(4\,184\,866, 47\,011)$. La generica soluzione è

$$x := 4\,184\,866 + \tfrac{401\,475}{5}h,\ y := 47\,011 + \tfrac{4\,510}{5}h \quad \text{(al variare di } h \text{ in } \mathbb{Z})$$

ossia

$$x := 4\,184\,866 + 80\,295h,\ y := 47\,011 + 902h \quad \text{(al variare di } h \text{ in } \mathbb{Z}).$$

A noi interessano soltanto i valori della x, anzi fra questi ne vogliamo 5 che diano luogo a classi di resto distinte modulo $401\,475$. Basta prendere cinque valori interi consecutivi per h, ma per "fare bella figura" di solito si scelgono in modo che i valori risultanti per la x appartengano all'intervallo $[0, 401\,474]$. Per $h := -52, -51, -50, -49, -48$ si ottiene

$$x_1 = 9\,526,\quad x_2 = 89\,821,\quad x_3 = 170\,116,\quad x_4 = 250\,411,\quad x_5 = 330\,706\,.$$

Esercizio 8.22

Sia $\mathbb{Z}_{416\,745}$ l'anello delle classi di resto modulo $416\,745$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{416\,745}$ a cui z appartiene. Si stabilisca quante soluzioni ha in $\mathbb{Z}_{416\,745}$ l'equazione

$$[5\,020]\,x = [4\,985]$$

e si scrivano tutte esplicitamente.

Soluzione – Sia $x_0 \in \mathbb{Z}$ tale che $[x_0]$ è soluzione dell'equazione proposta; allora

$$[5\,020] \cdot [x_0] = [4\,985] \qquad \text{ossia} \qquad [5\,020 \cdot x_0] = [4\,985]$$

e dunque deve esistere $y_0 \in \mathbb{Z}$ tale che

$$5\,020\,x_0 - 4\,985 = 416\,745\,y_0\,.$$

Siamo quindi ricondotti a considerare l'equazione diofantina

(*) $$5\,020\,x - 416\,745\,y = 4\,985$$

della quale ci interessano soltano i valori della x, anzi le loro classi di resto modulo $416\,745$ (per questo motivo sarebbe equivalente considerare l'equazione diofantina

$$5\,020\,x + 416\,745\,y = 4\,985$$

che nella x ha esattamente le stesse soluzioni).

Calcoliamo il MCD fra $5\,020$ e $416\,745$ mediante l'algoritmo di Euclide:

$416\,745 = 5\,020 \cdot 83 + 85\,;\quad 5\,020 = 85 \cdot 59 + 5\,;\quad 85 = 5 \cdot 17 + 0\,.$

Il massimo comun divisore fra $5\,020$ e $416\,745$ è dunque 5; poiché si tratta di un divisore di $4\,985$, la (*) ha soluzione (e l'equazione proposta ha esattamente 5 soluzioni).

Cerchiamo adesso una soluzione per l'equazione

$$5\,020\,x - 416\,745\,y = 4\,985\,.$$

Dai calcoli fatti per trovare il massimo comun divisore, abbiamo che

$$5 = 5\,020 - 85 \cdot 59 = 5\,020 - (416\,745 - 5\,020 \cdot 83) \cdot 59 =$$

$$= 5\,020 \cdot (83 \cdot 59 + 1) - 416\,745 \cdot 59 = 5\,020 \cdot 4\,898 - 416\,745 \cdot 59$$

e dunque

$$4\,985 = 5\,020 \cdot 4\,883\,306 - 416\,745 \cdot 58\,823\,.$$

Pertanto una soluzione dell'equazione $5\,020\,x - 416\,745\,y = 4\,985$ è $(4\,883\,306, 58\,823)$. La generica soluzione è

$$x := 4\,883\,306 + \tfrac{416\,745}{5}h,\ y := 58\,823 + \tfrac{5\,020}{5}h \quad \text{(al variare di } h \text{ in } \mathbb{Z})$$

ossia

$$x := 4\,883\,306 + 83\,349h, \qquad y := 47\,011 + 1\,040h \quad \text{(al variare di } h \text{ in } \mathbb{Z}).$$

A noi interessano soltanto i valori della x, anzi fra questi ne vogliamo 5 che diano luogo a classi di resto distinte modulo $416\,745$. Basta prendere cinque valori interi consecutivi per h, ma per "fare bella figura" di solito si scelgono in modo che i valori risultanti per la x appartengano all'intervallo $[0, 416\,744]$. Per $h := -58, -57, -56, -55, -54$ si ottiene

$$x_1 = 49\,064, \quad x_2 = 132\,413, \quad x_3 = 215\,762, \quad x_4 = 299\,111, \quad x_5 = 382\,460\,.$$

Esercizio 8.23

Sia $\mathbb{Z}_{410\,095}$ l'anello delle classi di resto modulo $410\,095$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{410\,095}$ a cui z appartiene. Si stabilisca quante soluzioni ha in $\mathbb{Z}_{410\,095}$ l'equazione

$$[5\,190]\,x = [4\,985]$$

e si scrivano tutte esplicitamente.

Soluzione – Sia $x_0 \in \mathbb{Z}$ tale che $[x_0]$ è soluzione dell'equazione proposta; allora

$$[5\,190] \cdot [x_0] = [4\,985] \qquad \text{ossia} \qquad [5\,190 \cdot x_0] = [4\,985]$$

e dunque deve esistere $y_0 \in \mathbb{Z}$ tale che

$$5\,190\,x_0 - 4\,985 = 410\,095\,y_0\,.$$

Siamo quindi ricondotti a considerare l'equazione diofantina

(*) $$5\,190\,x - 410\,095\,y = 4\,985$$

della quale ci interessano soltano i valori della x, anzi le loro classi di resto modulo $410\,095$ (per questo motivo sarebbe equivalente considerare l'equazione diofantina

$$5\,190\,x + 410\,095\,y = 4\,985$$

che nella x ha esattamente le stesse soluzioni).

Calcoliamo il MCD fra $5\,190$ e $410\,095$ mediante l'algoritmo di Euclide:

$410\,095 = 5\,190 \cdot 79 + 85\,;\quad 5\,190 = 85 \cdot 61 + 5\,;\quad 85 = 5 \cdot 17 + 0\,.$

Il massimo comun divisore fra $5\,190$ e $410\,095$ è dunque 5; poiché si tratta di un divisore di $4\,985$, la (*) ha soluzione (e l'equazione proposta ha esattamente 5 soluzioni).

Cerchiamo adesso una soluzione per l'equazione

$$5\,190\,x - 410\,095\,y = 4\,985\,.$$

Dai calcoli fatti per trovare il massimo comun divisore, abbiamo che

$$5 = 5\,190 - 85 \cdot 61 = 5\,190 - (410\,095 - 5\,190 \cdot 79) \cdot 61 =$$

$$= 5\,190 \cdot (79 \cdot 61 + 1) - 401\,475 \cdot 61 = 5\,190 \cdot 4\,820 - 410\,095 \cdot 61$$

e dunque

$$4\,985 = 5\,190 \cdot 4\,805\,540 - 410\,095 \cdot 60\,817\,.$$

Pertanto una soluzione dell'equazione $5\,190\,x - 410\,095\,y = 4\,985$ è $(4\,805\,540, 60\,817)$. La generica soluzione è

$$x := 4\,805\,540 + \tfrac{410\,095}{5}h,\ y := 60\,817 + \tfrac{5\,190}{5}h \quad \text{(al variare di } h \text{ in } \mathbb{Z})$$

ossia

$$x := 4\,805\,540 + 82\,019h,\ \ y := 60\,817 + 1\,038h \quad \text{(al variare di } h \text{ in } \mathbb{Z}).$$

A noi interessano soltanto i valori della x, anzi fra questi ne vogliamo 5 che diano luogo a classi di resto distinte modulo $410\,095$. Basta prendere cinque valori interi consecutivi per h, ma per "fare bella figura" di solito si scelgono in modo che i valori risultanti per la x appartengano all'intervallo $[0, 410\,094]$. Per $h := -58, -57, -56, -55, -54$ si ottiene

$$x_1 = 48\,438,\quad x_2 = 130\,457,\quad x_3 = 212\,476,\quad x_4 = 294\,495,\quad x_5 = 376\,514\,.$$

Esercizio 8.24

Sia $\mathbb{Z}_{416\,185}$ l'anello delle classi di resto modulo $416\,185$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{416\,185}$ a cui z appartiene. Si stabilisca quante soluzioni ha in $\mathbb{Z}_{416\,185}$ l'equazione

$$[5\,700]\,x = [4\,435]$$

e si scrivano tutte esplicitamente.

Soluzione – Sia $x_0 \in \mathbb{Z}$ tale che $[x_0]$ è soluzione dell'equazione proposta; allora

$$[5\,700] \cdot [x_0] = [4\,435] \qquad \text{ossia} \qquad [5\,700 \cdot x_0] = [4\,435]$$

e dunque deve esistere $y_0 \in \mathbb{Z}$ tale che

$$5\,700\,x_0 - 4\,435 = 416\,185\,y_0\,.$$

Siamo quindi ricondotti a considerare l'equazione diofantina

(*) $$5\,700\,x - 416\,185\,y = 4\,435$$

della quale ci interessano soltano i valori della x, anzi le loro classi di resto modulo $416\,185$ (per questo motivo sarebbe equivalente considerare l'equazione diofantina

$$5\,700\,x + 416\,185\,y = 4\,435$$

che nella x ha esattamente le stesse soluzioni).

Calcoliamo il MCD fra $5\,700$ e $416\,185$ mediante l'algoritmo di Euclide:

$$416\,185 = 5\,700 \cdot 73 + 85\,; \quad 5\,700 = 85 \cdot 67 + 5\,; \quad 85 = 5 \cdot 17 + 0\,.$$

Il massimo comun divisore fra $5\,700$ e $416\,185$ è dunque 5; poiché si tratta di un divisore di $4\,435$, la (*) ha soluzione (e l'equazione proposta ha esattamente 5 soluzioni).

Cerchiamo adesso una soluzione per l'equazione

$$5\,700\,x - 416\,185\,y = 4\,435\,.$$

Dai calcoli fatti per trovare il massimo comun divisore, abbiamo che

$$5 = 5\,700 - 85 \cdot 67 = 5\,700 - (416\,185 - 5\,700 \cdot 73) \cdot 67 =$$

$$= 5\,700 \cdot (73 \cdot 67 + 1) - 416\,185 \cdot 67 = 5\,700 \cdot 4\,892 - 416\,185 \cdot 67$$

e dunque

$$4\,435 = 5\,700 \cdot 4\,339\,204 - 416\,185 \cdot 59\,429\,.$$

Pertanto una soluzione dell'equazione $5\,700\,x - 416\,185\,y = 4\,435$ è $(4\,339\,204, 59\,429)$. La generica soluzione è

$$x := 4\,339\,204 + \tfrac{416\,185}{5}h,\ y := 59\,429 + \tfrac{5\,700}{5}h \quad \text{(al variare di } h \text{ in } \mathbb{Z})$$

ossia

$$x := 4\,339\,204 + 83\,237h, \qquad y := 59\,429 + 1\,140h \quad \text{(al variare di } h \text{ in } \mathbb{Z}).$$

A noi interessano soltanto i valori della x, anzi fra questi ne vogliamo 5 che diano luogo a classi di resto distinte modulo $416\,185$. Basta prendere cinque valori interi consecutivi per h, ma per "fare bella figura" di solito si scelgono in modo che i valori risultanti per la x appartengano all'intervallo $[0, 416\,184]$. Per $h := -52, -51, -50, -49, -48$ si ottiene

$$x_1 = 10\,880, \quad x_2 = 94\,117, \quad x_3 = 177\,354, \quad x_4 = 260\,591, \quad x_5 = 343\,828\,.$$