Capitolo 8

L'anello degli interi $\mathbb{Z}$

In questo capitolo approfondiamo lo studio dell'anello $\mathbb{Z}$. In particolare ci concentreremo sull'algoritmo di divisione in $\mathbb{Z}$ e le sue applicazioni. Le proprietà di cui ci occuperemo riguardano la possibilità di dividere un elemento per un altro. Iniziamo introducendo alcune definizioni generali sugli anelli che riguardano appunto i fattori di un elemento.

§ 8.1 Elementi irriducibili ed elementi primi

Definizione 8.1. *Siano a, b elementi di A. Si dice che a* **divide** *b se esiste $c \in A$ tale che $b = ac$. In simboli "a divide b" si scrive a/b e "a non divide b" si scrive $a \not/ b$.*

Definizione 8.2. *Sia A un anello commutativo con identità. Un elemento $a \in A$, che non è invertibile e che non è 0_A, si dice*

- **riducibile** *in A se può essere scritto come un prodotto $a = bc$, $b, c \in A$, in cui nè b nè c sono invertibili;*
- **irriducibile** *se e non è riducibile, ossia se non si può decomporre in un prodotto tranne che nel prodotto di una unità per un elemento associato ad a;*
- **primo** *in A se ogni volta che divide un prodotto allora divide uno dei due fattori. In simboli: $a/bc \Longrightarrow a/b$ oppure a/c.*

NOTA BENE Si faccia attenzione al fatto che 0_A e gli elementi invertibili di A non sono mai, per definizione, nè riducibili, nè irriducibili, nè primi.

Esempio 8.3. In $\mathbb{Z}$ il numero 2 è un elemento irriducibile poiché non può essere scritto come prodotto, a meno di non usare i fattori 1, -1, 2 e -2 che sono rispettivamente unità di $\mathbb{Z}$ oppure associati a 2 in $\mathbb{Z}$. Il numero 2 è anche primo in $\mathbb{Z}$ perché un prodotto è pari soltanto quando almeno uno dei due fattori è pari (ossia 2 è primo perché $2/ab \Longrightarrow 2/a$ oppure $2/b$). Invece 0 e 1 e -1 non sono nè riducibili, nè irriducibili, nè primi.

Esempio 8.4. Si consideri in $\mathbb{Z}_6$ l'elemento [2]. [2] è primo in $\mathbb{Z}_6$: infatti, se [2] divide $[a] \cdot [b] = [a \cdot b]$, allora a è pari o altrimenti b è pari. Tuttavia, [2] non è irriducibile in $\mathbb{Z}_6$: è sufficiente osservare che $[2] = [2] \cdot [4]$, è né [2] né [4] sono invertibili in $\mathbb{Z}_6$ (si veda la tabella della moltiplicazione di $\mathbb{Z}_6$ nel Capitolo 9).

Osservazione 8.5. Nelle scuole elementari e medie spesso si dice che un numero è primo se non è decomponibile in un prodotto, confondendo quindi primo con irriducibile. Questa confusione non porta ad errori poiché l'insieme degli elementi irriducibili di $\mathbb{Z}$ coincide con l'insieme degli elementi primi di $\mathbb{Z}$ ossia, relativamente a $\mathbb{Z}$, queste due nozioni risultano essere equivalenti. Questa proprietà è parte del **Teorema fondamentale dell'aritmetica** ed è un fatto tutt'altro che ovvio o banale. Inoltre le due nozioni non sono per nulla equivalenti in generale.

Definizione 8.6. *Un dominio A si dice* **dominio fattoriale** *o* **dominio a fattorizzazione unica** *(in breve* **U.F.D.**, *dall'inglese Unique Factorization Domain) se ogni elemento $a \in A$ non nullo e non invertibile si decompone in modo unico (a meno dell'ordine e di fattori moltiplicativi invertibili) nel prodotto di elementi irriducibili.*

§ 8.2 La divisione euclidea

La **divisione con resto** oggetto di questo paragrafo è semplicemente il primo tipo di divisione che si impara alle elementari (prima dell'introduzione delle frazioni), ma è anche un importantissimo strumento di calcolo e di dimostrazione per le proprietà dell'anello $\mathbb{Z}$.

Teorema 8.7. *Per ogni coppia a, b di numeri interi, con $b \neq 0$, esistono e sono univocamente determinati i numeri interi q (quoziente) ed r (resto), tali che $a = bq + r$ con $0 \leq r < |b|$.*

Dimostrazione. Per prima cosa dimostriamo che degli interi q ed r siffatti esistono e poi proveremo che sono univocamente determinati. Osserviamo intanto che è sufficiente provare l'asserto nel caso $a \geq 0$ e $b > 0$. Se infatti $b < 0$ e si ha $a = (-b)q + r$ allora $a = b(-q) + r$; analogamente se $a < 0$, $b \geq 0$ e si ha $(-a) = bq + r$ allora $a = b(-q-1) + (b-r)$ con $0 \leq b - r < |b|$ (oppure $a = b(-q)$ se $r = 0$). Siano, allora, $a \geq 0$ e $b > 0$. Procediamo per induzione su a. Se $a = 0$, basta prendere $q = r = 0$. Supponiamo l'asserto vero per tutti gli interi $a' < a$ e proviamolo per a. Se $a < b$, è sufficiente prendere $q = 0$ ed $r = a$. Se $a \geq b$, l'asserto è vero per i numeri $(a-b)$ e b, ossia esistono q' e r' tali che $(a-b) = bq' + r'$ e $0 \leq r' < |b|$. Allora $q = q' + 1$ e $r = r'$ soddisfano le condizioni volute. Proviamo ora l'unicità di q ed r. Supponiamo che valgano le relazioni $a = bq + r$ e $a = bq' + r'$ con $0 \leq r \leq r' < |b|$. Sottraendo membro a membro si ottiene $b(q - q') = (r' - r)$ ossia $b/(r' - r)$. Essendo $|b| > r' - r \geq 0$, allora $r' - r = 0$ e quindi anche $q - q'$ deve essere nullo. □

Definizione 8.8. *Siano k un numero intero ≥ 2 detto* **base** *e C un insieme di k simboli detti* **cifre** *associati ai numeri compresi tra 0 e $k-1$. Si dice* **scrittura posizionale** *di numero intero positivo a una sequenza ordinata $c_s c_{s-1} \dots c_1 c_0$ tale che $c_i \in C$ ed $a = c_s k^s + c_{s-1} k^{s-1} + \cdots + c_1 k + c_0$.*

La scrittura posizionale di un numero negativo b si ottiene premettendo il segno $-$ alla scrittura posizionale di $a = -b$.

Corollario 8.9. *Fissata una base k e un insieme di cifre C, ogni numero intero positivo a possiede una e una sola scrittura posizionale e ogni seuquenza del tipo $c_s c_{s-1} \dots c_1 c_0$ con $c_i \in C$ è la scrittura posizionale di un numero intero.*

Dimostrazione. Per provare che una tale scrittura esiste (ed anche per calcolarla) procediamo per induzione su a. Se $0 \leq a \leq k-1$, allora $a = c_0$, con $c_0 \in C$. Sia allora $a \geq k$ e supponiamo l'asserto vero per tutti in numeri minori di a. Eseguiamo la divisione di a per k: $a = qk + r$, con $0 \leq r \leq k-1$. Per l'ipotesi induttiva, l'asserto è vero per il quoziente q. Se $q = c'_{s'} k^{s'} + c'_{s'-1} k^{s'-1} + \cdots + c'_1 k + c'_0$, la scrittura di a si ottiene ponendo $s = s' + 1$, $c_i = c'_{i-1}$ e $c_0 = r$. Per i numeri negativi si usa la scrittura posizionale dell'opposto preceduta dal segno $-$. $\square$

Esempio 8.10. Introduciamo le nuove cifre $*$ per il numero 10 e $\bullet$ per 11 oltre alle 10 cifre abituali. La notazione in base 12 del numero (che in base 10 si scrive) 419 è $2 * \bullet$ poiché $419 = 2 \cdot 12^2 + 10 \cdot 12 + 11$. Per calcolarla a partire da 419 si eseguono le divisioni: $419 = 34 \cdot 12 + 11$ con resto $11 = c_0 = \bullet$

$34 = 2 \cdot 12 + 10$ con resto $10 = c_1 = *$

$2 = 0 \cdot 12 + 2$ con resto $2 = c_2 = 2$.

Nel seguito di questo paragrafo e nel prossimo ci occuperemo dei divisori di un numero intero e supporremo sempre di lavorare con numeri positivi e con fattori positivi. Tutte le proprietà dimostrate, però, valgono per tutti i numeri interi, anche per i negativi, poiché ogni numero intero è associato ad un numero positivo, cioè differisce da un positivo per un fattore moltiplicativo invertibile 1 o -1.

Definizione 8.11. *Si dice* **massimo comun divisore** *di due interi a e b non entrambi nulli il numero intero positivo $k = MCD(a, b)$ tale che k/a, k/b e $\forall h \in \mathbb{Z}$ t.c. h/a e h/b si ha h/k.*

Il MCD quindi è il più grande divisore comune ad a e b, non solo rispetto alla relazione d'ordine totale $\leq$, ma anche rispetto alla divisibilità.

Esempio 8.12. Non ha senso definire il $MCD(0, 0)$ poiché l'insieme dei divisori di 0 coincide con $\mathbb{Z}$ e quindi non ha massimo. Invece, se $a \in \mathbb{Z}$, $a \neq 0$, allora $MCD(a, 0) = |a|$.

L'aver richiesto che il MCD sia un numero positivo fa sì che, se esiste (cosa non ovvia ma che proveremo essere vera), allora è unico. Per provare che il massimo comun divisore esiste useremo il seguente lemma.

Lemma 8.13. *Siano $a, b \in \mathbb{Z}$, $b \neq 0$ e sia r il resto della divisione di a per b. Allora $MCD(a, b)$ e $MCD(b, r)$ (se esistono) coincidono.*

Dimostrazione. Sia $a = bq + r$. Ogni divisore comune a b e r divide anche a; d'altra parte si ha anche $r = a - bq$ e quindi ogni divisore comune ad a e b divide anche r. $\square$

Teorema 8.14. (Identità di Bézout) *Siano a, b due interi non entrambi nulli. Allora esistono dei numeri interi opportuni (ma non unici!) x, y tali che*

$$MCD(a, b) = ax + by.$$

Grazie al Lemma 8.13 possiamo calcolare il massimo comun divisore $MCM(a, b)$ e i numeri interi x, y che compaiono nell'identità di Bézout, col metodo noto come **algoritmo euclideo** o algoritmo delle divisioni successive. Per calcolare il massimo comun divisore di due numeri a, b, con $b \neq 0$ si procede nel modo seguente:

$$MCD(a, b) = MCD(b, r_1) = MCD(r_1, r_2) = MCD(r_2, r_3) = \cdots = MCD(r_k, 0) = r_k$$

dove r_1 è il resto della divisione di a per b, r_2 è il resto della divisione di b per r_1 e r_{i+1} è il resto della divisione di r_{i-1} per r_i. Questo procedimento ha al più b passi (poiché $b > r_1 > r_2 > \cdots > r_k > 0$) e si ferma non appena si trova un resto nullo. Il $MCD(a, b)$ è l'ultimo resto non nullo trovato. Procedendo a ritroso da $r_k = r_{k-2} - r_{k-1}q_{k-1}$ ed utilizzando le relazione trovate ad ogni divisione $r_i = r_{i-1}q_{i-1} + r_{i-2}$, si ricava l'identità di Bézout.

Esempio 8.15. Vogliamo calcolare $MCD(a = 3522, b = 321)$:

- $3522 = \mathbf{321} \cdot 10 + \mathbf{312}$
- $321 = \mathbf{312} \cdot 1 + \mathbf{9}$
- $312 = \mathbf{9} \cdot 34 + \mathbf{6}$
- $9 = \mathbf{6} \cdot 1 + \mathbf{3}$
- $6 = \mathbf{3} \cdot 2 + \mathbf{0}$.

Pertanto $MCD(3522, 321) = 3$.

Esempio 8.16. Procedimento per calcolare $MCD(6852, 3997)$:

1) $6852 = 3997 \cdot 1 + 2855$

2) $3997 = 2855 \cdot 1 + 1142$

3) $2855 = 1142 \cdot 2 + 571$

4) $1142 = 571 \cdot 2 + 0$

Allora $MCD(6852, 3997) = 571$. Procedimento per calcolare l'identità di Bézout:

3) $571 = 2855 - 1142 \cdot 2$

2) $1142 = 3997 - 2855$ da cui, sostituendo nella precedente, $571 = 2855 - (3997 - 2855) \cdot 2$ ossia $571 = 2855 \cdot 3 + 3997 \cdot (-2)$

1) $2855 = 6852 - 3997$ da cui, sostituendo nella precedente, $571 = (6852 - 3997) \cdot 3 + 3997 \cdot (-2)$ ossia $571 = 6852 \cdot 3 + 3997 \cdot (-5)$.

Corollario 8.17. *Siano* $a, b, c \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. *Allora:*

$$\exists x, y \in \mathbb{Z} \text{ tali che } c = ax + by \iff MCD(a, b)/c.$$

Dimostrazione. Siano $d = MCD(a, b)$ e $d = ax' + by'$ l'identità di Bézout. Se $c = ax + by$, ogni divisore comune ad a e b divide anche c; in particolare d/c. Viceversa, se $c = dt$, allora $c = ax + by$, dove si ponga $x = x't$, $y = y't$. □

Le equazioni del tipo $ax + by = c$ con $a, b, c \in \mathbb{Z}$ nelle incognite x, y di cui si cercano suluzioni $(x = m, y = n)$ in $\mathbb{Z}^2$ si dicono **equazioni Diofanteee lineari in due incognite**. Osseriviamo infine che il minimo comune multiplo di due numeri si ottiene facilmente a partire dal loro massimo comun divisore come: $mcm(a, b) = \frac{ab}{MCD(a,b)}$ e quindi può essere, anch'esso, calcolato mediante l'algoritmo euclideo.

L'indovinello dei 4 galloni

John McLane è un poliziotto statunitense. Sta inseguendo un pazzo che lascia bombe in giro per New York. Di fianco ad una fontana trova una valigetta e due taniche da 3 e 5 galloni rispettivamente. Nella valigetta c'è una bomba controllata da una bilancia. Per disinnescare la bomba John deve appoggiare sopra la bilancia una tanica con esattamente 4 galloni d'acqua. Ha un minuto di tempo prima che la bomba esploda quindi per misurare i 4 galloni può usare solo le due taniche che ha a portata di mano. Come fa? (Indovinello tratto dal film "Die hard- Duri a morire") SOLUZIONE: dobbiamo cercare le soluzioni all'equazione diofantea

$$5x + 3y = 4. \tag{1}$$

Infatti, abbiamo a disposizione due contenitori della capacità di 3 e 5 galloni rispettivamente, con i quali dobbiamo ottenere (versando acqua in un contenitore o svuotandola da uno all'altro) esattamente 4 galloni. Cerchiamo soluzioni intere per x e y perché i contenitori non sono graduati: cercare di riempire uno dei due contenitori "a metàrq', rischieremmo di far esplodere la bomba a causa di un'imprecisione! Le uniche mosse che ci garantiscono precisione, sono quelle di riempire completamente un contenitore (+1) o svuotarlo completamente (-1). Posso travasare acqua da un recipiente all'altro, ma per essere "precisi", posso travasare completamente un contenitore pieno nell'altro. Questo non "influisce"sulle variabili dell'equazione. L'equazione (1) ha soluzione se e solo se $MCD(5,3)|4$ (Corollario 8.17). In effetti $MCD(5,3) = 1$, quindi l'equazione (1) ha soluzione! Per trovarla (con certezza!), calcoliamo $MCD(5,3)$ con l'algoritmo euclideo per poi esplicitare l'identit'a di Bézout:

1) $5 = 1 \cdot 3 + 2$

2) $3 = 1 \cdot 2 + 1$

3) $2 = 2 \cdot 1 + 0$

Da queste equazioni troviamo $x', y' \in \mathbb{Z}$ tali che $5x' + 3y' = 1$:

2) $1 = 3 - 2$

1) $2 = 5 - 3$ da cui, sostituendo nella precedente, $1 = 3 - (5 - 3)$ ossia $1 = 2 \cdot 3 - 5$.

Quindi $x' = -1$, $y' = 2$. Una soluzione (non è l'unica!!!!) dell'equazione (1) è $x = -4, y = 8$. In pratica: John McLane deve riempire alla fontana la tanica da 3 galloni per 8 volte. Ogni volta che lo riempie, la svuota in quello da 5. Di volta in volta, il recipiente da 5 galloni si riempirà fino all'orlo, e John dovrà svuotarlo per 4 volte. Alla fine di questo procedimento, nella tanica da 5 galloni ci saranno esattamente 4 galloni di acqua! Non è l'unica soluzione!!!!! John può anche riempire 3 volte il recipiente da 3, travasare man mano in quello da 5 e poi svuotare quello da 5 solo 1 volta: $3 \cdot 3 - 5 = 4$.

§ 8.3 Il teorema fondamentale dell'aritmetica

In questo paragrafo proveremo che ogni numero intero, non nullo e non invertibile, si fattorizza in modo essenzialmente unico (ossia a meno di permutazioni dei fattori e di cambiamenti di segno) nel prodotto di numeri primi. Ci sarà utile la seguente

Definizione 8.18. *Sia a un elemento di un anello A commutativo con identità. Due fattorizzazioni $a = b_1 \cdots b_k$ e $a = c_1 \cdots c_h$ sono* **essenzialmente la stessa fattorizzazione** *di a se $k = h$ e per ogni $i = 1, \ldots, k$ si ha $b_i = u_i c_{\sigma(i)}$, dove le u_i sono unità di A e σ è una opportuna permutazione degli indici. In altre parole due fattorizzazioni sono essenzialmente la stessa se differiscono solo per l'ordine dei fattori e per eventuali fattori moltiplicativi invertibili.*

Lemma 8.19. *Sia a un numero intero $\neq 0, 1, -1$. Allora a può essere scritto come prodotto di numeri interi irriducibili $a = a_1 \cdot \dots \cdot a_k$.*

Dimostrazione. Senza perdere in generalità, possiamo supporre $a \geq 2$ e considerare solo fattori ≥ 2. Procediamo per induzione su a. Se $a = 2$, allora a è irriducibile, $k = 1$, $a = a_1$ e non c'è nulla da provare. Supponiamo l'asserto vero per tutti gli interi n, $2 \leq n < a$ e proviamo che vale anche per a. Se a è irriducibile, come prima $k = 1$, $a = a_1$. Se invece a si può scrivere come prodotto $a = bc$, con b, c non invertibili, allora i fattori sono tali che $2 \leq b, c < a$ e quindi grazie all'ipotesi induttiva possiamo scrivere $b = b_1 \cdots b_i$, $c = c_1 \cdots c_j$ e quindi $k = i + j$, $a = b_1 \cdots b_i \cdot c_1 \cdots c_j$. □

Lemma 8.20. *Sia p un numero intero $\neq 0, 1, -1$. Allora :*

$$p \text{ è primo} \Longleftrightarrow p \text{ è irriducibile.}$$

Dimostrazione. "$\Longrightarrow$" Supponiamo che p sia primo. Se $p = mn$ con $m, n \in \mathbb{Z}$, allora p/mn e quindi, essendo primo, deve dividere almeno uno dei fattori. Se $m = pq$, allora $p = pqn$, da cui, per la cancellazione, $qn = 1$. Questa uguaglianza dice che n è una unità di $\mathbb{Z}$ e quindi che p non ha decomposizioni effettive in un prodotto, cioè è irriducibile. "$\Longleftarrow$" Sia p un numero irriducibile e siano a, b interi tali che p/ab e $p \not/ a$. Proviamo che allora p/b. Dalle ipotesi fatte segue che $MCD(a, p) = 1$; possiamo allora scrivere l'identità di Bézout $1 = xa + yp$ (Teorema 8.14). Moltiplicando i due membri per b e ricordando che p/ab ossia che esiste $c \in \mathbb{Z}$ tale che $pc = ab$, troviamo: $b = xab + pyb = p(xc + yb)$ e quindi p/b. □

Teorema 8.21. (Teorema fondamentale dell'aritmetica) *$\mathbb{Z}$ è un dominio a fattorizzazione unica ossia ogni numero intero $\neq 0, 1, -1$ si fattorizza in modo essenzialmente unico nel prodotto di numeri primi.*

Dimostrazione. I risultati precedenti mostrano che ogni numero intero a ($a \neq 0, 1, -1$) si fattorizza nel prodotto di irriducibili e che gli irriducibili in $\mathbb{Z}$ sono anche primi. Allora a si fattorizza nel prodotto di numeri primi. Rimane da provare che la fattorizzazione è essenzialmente unica. Supponiamo che tutti i fattori siano positivi (sostituendo eventualmente i negativi con i loro opposti). Sia $a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_h$, con fattori p_i e q_j tutti primi. Procediamo per induzione su k. Se $k = 1$, allora $a = p_1$ è irriducibile e quindi anche $h = 1$ e $p_1 = q_1$. Supponiamo che la scrittura sia unica per i prodotti di $k - 1$ fattori irriducibili e proviamolo per i prodotti di k fattori irriducibili. Poiché p_k è primo e divide $q_1 q_2 \cdots q_h$, allora p_k divide uno dei q_i: possiamo supporre di riordinare i q_i in modo che p_k/q_h. Ma anche q_h è irriducibile e quindi $p_k = q_h$. Allora si ha $a = p_1 p_2 \cdots p_{k-1} p_k = q_1 q_2 \cdots q_{h-1} p_k$. Mediante la cancellazione otteniamo $p_1 p_2 \cdots p_{k-1} = q_1 q_2 \cdots q_{h-1}$, che è un prodotto di $k - 1$ fattori irriducibili. Dall'ipotesi induttiva segue che $k - 1 = h - 1$ (ossia $k = h$) e che, a meno dell'ordine, le due fattorizzazioni coincidono, ossia $p_1 = q_1$,

..., $p_{k-1} = q_{k-1}$. Avendo già provato che $p_k = q_k$, abbiamo dimostrato per intero l'unicità della fattorizzazione di a. □

Un modo conveniente per scrivere la fattorizzazione di un intero a nel prodotto di fattori primi è quello di raccogliere mediante esponenti i fattori uguali, ottenendo scritture del tipo $a = p_1^{m_1} \cdots p_r^{m_r}$, dove i p_i sono primi distinti. L'esponente m_i si dice **molteplicità** di p_i in a.

Corollario 8.22. *In $\mathbb{Z}$ ci sono infiniti numeri primi.*

Dimostrazione. Supponiamo per assurdo che esistano solo un numero finito di primi $p_1, \ldots, p_r$. L'intero $n = (p_1 \cdots p_r) + 1$ non è divisibile esattamente per alcun p_i e quindi non è divisibile per alcun primo. Troviamo così un numero $\neq 0, 1, -1$ privo di fattori primi, in contrasto con quanto provato. □

Si noti che la precedente è una vera dimostrazione per assurdo e non, come si potrebbe pensare, un metodo per costruire un ulteriore numero primo a partire da r primi assegnati. Ad esempio il numero $n = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) + 1$ non è primo, ma si decompone nel prodotto di 59 e 509.

§ 8.4 Esercizi

8.1 Calcolare MCD di 18779 e 4183 usando l'algoritmo euclideo.

8.2 Scrivere l'identità di Bézout per i numeri 45 e 51.

8.3 Calcolare il MCD e l'identità di Bézout dei numeri $a = 148131$ e $b = 36951$.

8.4 Determinare la scrittura posizionale in base 7, 2 e 13 del numero (che nella abituale base 10 si scrive) 4581.

8.5 Scrivere nella abituale base 10 i numeri $(110101)_7$, $(110101)_2$, $(110101)_{13}$, dove l'indice indica la base usata.

8.6 Si consideri il numero $(201)_{16}$, scritto in base 16, e si riscriva lo stesso numero in base 5.

8.7 Consideriamo $k = 16$, e adottiamo la notazione $a = 10, b = 11, c = 12, d = 13, e = 14, f = 15$. Si consideri il numero $(f41c)_{16}$, scritto in base 16, e si riscriva lo stesso numero in base 8.

8.8 Consideriamo $k = 16$, e adottiamo la notazione $a = 10, b = 11, c = 12, d = 13, e = 14, f = 15$. Si consideri il numero $(f41c)_{16}$, scritto in base 16, e si riscriva lo stesso numero in base 8.

8.9 Si scriva il numero intero 8000 in base 16.

8.10 Trovare il MCD di 39758 e di 54573 ed esplicitare l'identità di Bézout.

8.11 Trovare il MCD di 8037 e di 13395 ed esplicitare l'identità di Bézout. Calcolare inoltre $mcm(8037, 13395)$.

8.12

1. Trovare il MCD di 3105 e 2277 ed esplicitare l'identità di Bézout.
2. Trovare tutti gli $x, y \in \mathbb{Z}$ che sono soluzione per l'equazione $3105x + 2277y = 2070$.
3. Trovare il mcm di 3105 e 2277.

8.13 Determinare un numero $a \in \mathbb{Z}$ tale che $\{16h + 18k \mid h, k \in \mathbb{Z}\} = a\mathbb{Z}$, dove $a\mathbb{Z} = \{at \mid t \in \mathbb{Z}\}$.

8.14 Trovare il MCD e il mcm di 138788 e 62329, e quindi determinare un numero $a \in \mathbb{Z}$ tale che $\{138788\,x + 62329\,y \mid x, y \in \mathbb{Z}\} = a\mathbb{Z}$, dove $a\mathbb{Z} = \{at \mid t \in \mathbb{Z}\}$.

8.15 I produttori della serie di film Die Hard vogliono girare un ultimo film della serie, in cui l'eroe John McLane muore a causa dell'indovinello delle taniche: gli vengono fornite una tanica di capacità n galloni e una di capacità m galloni, e deve ottenere esattamente 3 galloni, solo riempiendo completamente e svuotando completamente le taniche, altrimenti scoppierà una bomba.
Quali tra le seguenti coppie di interi n, m porta di sicuro alla morte John McLane?

1. $n = 972, m = 504$;
2. $n = 1705, m = 1001$;
3. $n = 899, m = 1247$.

8.16 Determinare il MCD di 6120, 720 e 880.

8.17 Sia p un numero primo. Provare che per ogni $a \in \mathbb{Z}$ si ha $MCD(a, p) = 1$ oppure $MCD(a, p) = p$.

8.18 Dire se le seguenti equazioni hanno soluzioni intere:

$$35\,x + 84\,y = 6 \qquad 49\,x + 168\,y = 14.$$