Rozdział 3

ARYTMETYKA MODULARNA

3.1. Algorytm dzielenia

Definicja 3.1.1. Liczbę $\lfloor x \rfloor$ nazywa się **częścią całkowitą** (cechą) liczby rzeczywistej x. Różnicę $x - \lfloor x \rfloor$ nazywa się **częścią ułamkową** (mantysą) liczby rzeczywistej x i oznacza $\{x\}$.

Uwaga 3.1.2. Z powyższej definicji oraz definicji funkcji podłoga wynika, że $\lfloor x \rfloor \in \mathbb{C}$ i $\{x\} \in \langle 0, 1)$.

Niech $n \in \mathbb{C}$ i $p \in \mathbb{N}$ będą dowolnymi liczbami. Wtedy iloraz q dzielenia liczby n przez p równy jest $\left\lfloor \frac{n}{p} \right\rfloor \in \mathbb{C}$, zaś resztę z tego dzielenia $r \in \{0, 1, 2, \ldots, p-1\}$ oznacza się n **mod** p. Wobec tego możemy zapisać

$$n = p \left\lfloor \frac{n}{p} \right\rfloor + n \ \mathbf{mod}\ p. \tag{3.1}$$

Z wzoru (3.1) wynika definicja "mod" jako działania dwuargumentowego

$$n \ \mathbf{mod}\ p = n - p \left\lfloor \frac{n}{p} \right\rfloor. \tag{3.2}$$

Uwaga 3.1.3. Zauważmy, że powyżej zakładano, że dzielnik p jest tylko liczbą dodatnią. Oczywiście powyższe rozważania można rozszerzyć na ujemne dzielniki, ale wówczas należy zmodyfikować albo definicję ilorazu, albo definicję reszty. W literaturze i implementacjach komputerowych funkcjonują dwie różne definicje. Na potrzeby tego skryptu ograniczymy nasze rozważania tylko do dodatnich dzielników.

Definicja 3.1.4. Największą liczbę całkowitą, która dzieli liczby całkowite n i m nazywa się największym wspólnym dzielnikiem i oznacza $\mathbf{NWD}(n, m)$, tzn.

$$\mathbf{NWD}(n, m) = \max\{k \in \mathbb{C} : k|m \ \wedge \ k|n\}.$$

Uwaga 3.1.5. Z definicji 3.1.4 wynika, że $1 \leqslant \mathbf{NWD}(m, n) \leqslant \min\{m, n\}$. Oczywiście jeśli $d\Big|a$, to $(-d)\Big|a$. Wynika stąd, że $\mathbf{NWD}(m, n) > 0$. Ponadto $\mathbf{NWD}(m, 0) = |m|$, dla dowolnej liczby całkowitej $m \neq 0$.

Uwaga 3.1.6. Zauważmy, że największy wspólny dzielnik liczb m i n jest liczbą całkowitą spełniającą warunki

1. $\mathbf{NWD}(n, m)\Big|m$ i $\mathbf{NWD}(n, m)\Big|n$,
2. jeśli $d\Big|m$ i $d\Big|n$, to $d \leqslant \mathbf{NWD}(n, m)$.

Ponadto wprost z definicji 3.1.4 wynika, że dla dowolnych liczb całkowitych n i m

$$\mathbf{NWD}(m, n) = \mathbf{NWD}(n, m), \tag{3.3}$$
$$\mathbf{NWD}(m, n) = \mathbf{NWD}(-m, n). \tag{3.4}$$

Stwierdzenie 3.1.7. *Dla dowolnych liczb całkowitych n i m*

$$\mathbf{NWD}(m,n) = \mathbf{NWD}(n, m \ \boldsymbol{mod}\ n). \tag{3.5}$$

Bazując na równości (3.5) możemy zbudować tzw. Algorytm Euklidesa wyznaczania największego wspólnego dzielnika, który przebiega w następujących krokach
Krok 1. Wczytaj liczby a i b.
Krok 2. Oblicz $r = a$ **mod** b.
Krok 3. $a := b$, $b := r$.
Krok 4. Jeśli $b = 0$, to $d = a$. W przeciwnym razie wróć do kroku 2.

Zasadę działania algorytmu Euklidesa można pokazać wykorzystując następujące **twierdzenie o dzieleniu z resztą.**

Twierdzenie 3.1.8. *Niech $p \in \mathbb{N}$. Dla każdej liczby całkowitej n istnieje dokładnie jedna para liczb całkowitych q i r spełniających warunki*

$$n = p \cdot q + r, \qquad 0 \leqslant r < p.$$

Twierdzenie 3.1.9. Tożsamość Bézouta

$$\bigwedge_{m,n\in\mathbb{C}} \bigvee_{s,t\in\mathbb{C}} \mathbf{NWD}(m,n) = ms + nt. \tag{3.6}$$

Rozszerzenie algorytmu Euklidesa

Krok 1. $a := a$, $a' := b$, $x := 1$, $x' := 0$, $y := 0$, $y' := 1$
Krok 2. DOPÓKI $a' \neq 0$ WYKONUJ

$$\begin{array}{ll} q := \lfloor \frac{a}{a'} \rfloor & \\ a := a', & a' := a - qa' \\ x := x', & x' := x - qx' \\ y := y', & y' := y - qy' \end{array}$$

Krok 3. $\mathbf{NWD}(a,b) := a$

Definicja 3.1.10. Jeśli $\mathbf{NWD}(n,m) = 1$, to liczby n i m nazywamy **względnie pierwszymi**.

Uwaga 3.1.11. Jeśli m i n są względnie pierwsze, to $\bigvee_{s,t\in\mathbb{C}} ms + nt = 1$.

3.2. Liniowe równanie diofantyczne

Równanie $ax+by = c$ z niewiadomymi x, y i danymi $a, b, c \in \mathbb{C}$ nazywa się **liniowym równaniem diofantycznym**. Aby wyznaczyć rozwiązanie tego równania w zbiorze liczb całkowitych najpierw zauważmy, że za pomocą rozszerzonego algorytmu Euklidesa dla danych a i b możemy wyznaczyć liczby $x_0, y_0 \in \mathbb{C}$ takie, że $ax_0+by_0 = \mathbf{NWD}(a,b)$. Wynika stąd, że liniowe równanie diofantyczne będzie miało rozwiązanie w zbiorze $\mathbb{C}$ wtedy i tylko wtedy, gdy $\mathbf{NWD}(a,b)\Big|c$. Załóżmy więc, że $\mathbf{NWD}(a,b)\Big|c$. Wtedy mnożąc równanie $ax_0+by_0 = \mathbf{NWD}(a,b)$ stronami przez $d = \dfrac{c}{\mathbf{NWD}(a,b)}$ otrzymujemy

$$adx_0 + bdy_0 = c.$$

Oznacza, to że para

$$s = \frac{c}{\mathbf{NWD}(a,b)}x_0, \quad t = \frac{c}{\mathbf{NWD}(a,b)}y_0$$

jest jednym z rozwiązań równania $ax + by = c$. Aby wyznaczyć wszystkie rozwiązania tego równania załóżmy, że $x \neq s$ i $y \neq t$ jest parą rozwiązań liniowego równania diofantycznego. Wtedy mamy

$$\begin{aligned} as + bt &= ax + by \\ a(s-x) &= b(y-t) \\ \frac{a}{\mathbf{NWD}(a,b)}(s-x) &= \frac{b}{\mathbf{NWD}(a,b)}(y-t) \end{aligned} \tag{3.7}$$

Ponieważ $\mathbf{NWD}\left(\frac{a}{\mathbf{NWD}(a,b)}, \frac{b}{\mathbf{NWD}(a,b)}\right) = 1$, to równanie (3.7) jest spełnione wtedy i tylko wtedy, gdy

$$\frac{a}{\mathbf{NWD}(a,b)}\Big|(y-t) \quad \wedge \quad \frac{b}{\mathbf{NWD}(a,b)}\Big|(s-x).$$

Zatem

$$\bigvee_{k\in\mathbb{C}} s - x = \frac{b}{\mathbf{NWD}(a,b)}k, \quad \bigvee_{k\in\mathbb{C}} y - t = \frac{a}{\mathbf{NWD}(a,b)}k.$$

Wobec tego zbiór rozwiązań liniowego równania diofantycznego $ax + by = c$ tworzą pary liczb postaci

$$\begin{aligned} x &= \frac{c}{\mathbf{NWD}(a,b)}x_0 - \frac{b}{\mathbf{NWD}(a,b)}k, \\ y &= \frac{c}{\mathbf{NWD}(a,b)}y_0 + \frac{a}{\mathbf{NWD}(a,b)}k; \quad k \in \mathbb{C} \end{aligned}$$

Uwaga 3.2.1. Zauważmy, że jeśli c nie jest podzielne przez $\mathbf{NWD}(a,b)$, to równanie diofantyczne nie ma rozwiązania.

3.3. Relacja kongruencji

Definicja 3.3.1. Dla danej liczby $p \in \mathbb{N}$ mówimy, że liczby całkowite m i n **są przystające modulo** p jeśli dają takie same reszty przy dzieleniu przez p. Relację przystawania modulo p nazywa się **relacją kongruencji** i oznacza $\equiv_p$. Liczbę m nazywa się **modułem kongruencji**

Uwaga 3.3.2. Bezpośrednio z definicji 3.3.1 mamy

$$m \equiv_p n \quad \Leftrightarrow \quad m \ \mathbf{mod}\ p = n \ \mathbf{mod}\ p.$$

Twierdzenie 3.3.3. *$m \equiv_p n$ wtedy i tylko wtedy, gdy $\bigvee_{k\in\mathbb{C}} m - n = kp$.*

Uwaga 3.3.4. Każde dwie liczby całkowite przystają do siebie modulo 1 dla tego też rozważa się tylko kongruencje o module większym od 1.

W dalszej części zakładamy, że wszystkie moduły są liczbami naturalnymi i większymi od 1.

Twierdzenie 3.3.5. *Dla ustalonego p relacja kongruencji $\equiv_p$ jest relacją równoważności w zbiorze liczb całkowitych.*

Zbiór ilorazowy relacji $\equiv_p$ oznaczamy $\mathbb{Z}_p$. Zazwyczaj reprezentantów klas abstrakcji utożsamiamy z tymi klasami i piszemy $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$.

Podstawowe własności kongruencji

Niech $a, b, c, d \in \mathbb{C}$ i $p \in \mathbb{N}$. Jeśli $a \equiv_p b$ i $c \equiv_p d$, to

- $a + c \equiv_p b + d,$ (3.8)
- $a - c \equiv_p b - d,$ (3.9)
- $ac \equiv_p bd,$ (3.10)
- $a^n \equiv_p b^n, \ n \in \mathbb{N}.$ (3.11)

Ponadto, jeśli $d \neq 0$, to

- $ad \equiv_{dp} bd \Leftrightarrow a \equiv_p b,$ (3.12)
- $a \equiv_{dp} b \Rightarrow a \equiv_p b.$ (3.13)

Stwierdzenie 3.3.6. *Jeśli liczby naturalne p i d są względnie pierwsze, to*

$$ad \equiv_p bd \Leftrightarrow a \equiv_p b \tag{3.14}$$

Stwierdzenie 3.3.7. *Jeśli liczby naturalne m i n są względnie pierwsze, to*

$$\big(a \equiv_m b \ \wedge \ a \equiv_n b\big) \Leftrightarrow a \equiv_{mn} b.$$

Uwaga 3.3.8. Z powyższych własności wynika, że kongruencje można dodawać, odejmować, mnożyć i potęgować stronami.

Natomiast **kongruencji nie można dzielić stronami**. Istotnie $48 \equiv_{10} 18$ (bo $48 - 18 = 3 \cdot 10$) oraz $12 \equiv_{10} 2$, (bo $12 - 2 = 10$), ale po podzieleniu tych kongruencji stronami dostajemy kongruencję $4 \equiv_{10} 9$, która nie jest prawdziwa, gdyż $4 - 9 = -5$ nie jest liczbą podzielną przez 10.

Natomiast kongruencję możemy podzielić stronami przez liczbę $d \neq 0$, jeśli

1) d jest liczbą względnie pierwszą z modułem kongruencji.
2) moduł dzieli się przez liczbę d i wówczas dzielimy przez d nie tylko kongruencję, ale i jej moduł.

Definicja 3.3.9. Liczbę m' nazywamy **odwrotną do liczby** $m \in \mathbb{C}$ **modulo** $p \in \mathbb{N}$, jeśli $m' \cdot m \equiv_p 1$.

Jeśli istnieje liczba odwrotna modulo p do liczby m, to liczbę m nazywamy **odwracalną modulo p**.

Uwaga 3.3.10. Liczba odwrotna modulo p nie zawsze istnieje i nie jest jednoznacznie wyznaczona.

Twierdzenie 3.3.11. *Liczba całkowita m jest odwracalna modulo p wtedy i tylko wtedy, gdy* $\mathbf{NWD}(m, p) = 1$.

Aby wyznaczyć liczbę odwrotną do liczby m modulo p należy znaleźć liczby s i t takie, że $ms + pt = 1$. Wtedy szukaną liczbą odwrotną do liczby m jest liczba s. Do wyznaczenia s i t możemy oczywiście wykorzystać rozszerzony algorytm Euklidesa.

Definicja 3.3.12. Kongruencję $a \cdot x \equiv_p b$ dla danych $a, b \in \mathbb{C}$ i dowolnego $p \in \mathbb{N}$, nazywamy **kongruencją liniową z niewiadomą** x.

Uwaga 3.3.13. Zauważmy, że jeśli istnieje rozwiązanie kongruencji liniowej $a \cdot x \equiv_p b$, to b jest podzielne przez $\mathbf{NWD}(a, p)$. Istotnie, niech x_0 będzie rozwiązaniem kongruencji $a \cdot x \equiv_p b$. Wtedy istnieje $k \in \mathbb{C}$ taka, że $ax_0 - b = kp$. Stąd $ax_0 - kp = b$. Ponieważ $\mathbf{NWD}(a, p)\Big|a$ i $\mathbf{NWD}(a, p)\Big|p$, to oczywiście $\mathbf{NWD}(a, p)\Big|(ax_0 - kp)$, co oznacza, że $\mathbf{NWD}(a, p)\Big|b$.

Stąd i z prawa kontrapozycji wynika, że jeśli b nie jest podzielne przez $\mathbf{NWD}(a, p)$, to kongruencja liniowa $a \cdot x \equiv_p b$ nie ma rozwiązania.

Ponadto, jeśli $\mathbf{NWD}(a, p) = d \neq 1$ i $d\Big|b$, to zbiór rozwiązań kongruencji $ax \equiv_p b$ jest taki sam jak zbiór rozwiązań kongruencji $\dfrac{a}{d}x \equiv_{\frac{p}{d}} \dfrac{b}{d}$.

Stwierdzenie 3.3.14. *Jeśli* $p \Big| a$*, to rozwiązaniem kongruencji* $a \cdot x \equiv_p 0$ *jest każda liczba całkowita* x*.*

Stwierdzenie 3.3.15. *Jeśli* $p \Big| a$ *i* $b \neq 0$ *nie jest podzielne przez* p*, to kongruencja* $a \cdot x \equiv_p b$ *nie ma rozwiązania.*

Stwierdzenie 3.3.16. *Jeśli* a *i* b *są podzielne przez* p*, to rozwiązaniem kongruencji* $a \cdot x \equiv_p b$ *jest dowolna liczba całkowita* x*.*

Stwierdzenie 3.3.17. *Jeśli* $\mathbf{NWD}(a,p) = 1$*, to kongruencja liniowa ma nieskończenie wiele rozwiązań danych wzorem* $x = sb + kp$*,* $k \in \mathbb{C}$*, gdzie* s *jest liczbą odwrotną do liczby* a *modulo* p*.*

3.4. Zadania

Zadanie 3.1. Udowodnić własność algebraiczną działania **mod** zwaną **prawem rozdzielności**

$$(cx) \ \mathbf{mod}\ (cy) = c(x \ \mathbf{mod}\ y)$$

Zadanie 3.2. Niech $x, y, m, n, a, b, c, d \in \mathbb{C}$ będą takimi liczbami, że $m = ax + by$ i $n = cx + dy$, gdzie $|ad - bc| \neq 1$. Udowodnić, że $\mathbf{NWD}(n,m) = \mathbf{NWD}(x,y)$.

Zadanie 3.3. Wykorzystując dowód nie wprost udowodnić, że

$$\mathbf{NWD}(m,n) = d \implies \mathbf{NWD}\left(\frac{m}{d}, \frac{n}{d}\right) = 1. \tag{3.15}$$

Zadanie 3.4. Udowodnić, że jeśli $a, b \in \mathbb{C}$ są względnie pierwsze, to

(a) $\mathbf{NWD}(5a + 3b, 8a + 5b) = 1$,

(b) $\mathbf{NWD}(5a + 4b, 4a + 3b) = 1$.

Zadanie 3.5. Korzystając z algorytmu Euklidesa znaleźć $\mathbf{NWD}(m,n)$ oraz liczby s i t takie, że $\mathbf{NWD}(m,n) = s \cdot m + t \cdot n$ dla podanych liczb m i n

(a) $m = 20$, $n = 14$; **(c)** $m = 72$, $n = 17$;

(b) $m = 30$, $n = 60$; **(d)** $m = 44$, $n = 11$.

Zadanie 3.6. Wyznaczyć liczby całkowite x, y spełniające równanie

(a) $8x + 3y = 4$, **(f)** $8x - 2y = 4$,

(b) $21x + 111y = 3$, **(g)** $4x + 26y = 42$,

(c) $7x - 11y = 41$, **(h)** $2x + 6y = 3$,

(d) $3x + 5y = 11$, **(i)** $9x + 3y = 39$,

(e) $10x + 37y = 2$, **(j)** $5x - 3y = 4$.

Zadanie 3.7. Do przewozu zboża są do dyspozycji worki 60-cio kilogramowe i 80-cio kilogramowe. Ile potrzeba poszczególnych worków do przewozu 440 kg zboża (zakładamy, że worki muszą być pełne)?

Zadanie 3.8. Ile biletów po 3 zł i po 5 zł można kupić za 149 zł, jeśli należy wydać wszystkie pieniądze?

Zadanie 3.9. Dla każdej z podanych liczb m znaleźć jedyną liczbę całkowitą n w zbiorze $\{0, 1, 2, 3\}$ taką, że $m \equiv_4 n$

(a) -17, **(b)** -7, **(c)** 7, **(d)** 17.

Zadanie 3.10. Wypisać elementy zbioru
$A_k = \{m \in \mathbb{C} \cap < -10, 10 >: m \equiv_3 k\}$ dla $k = 0, 1, 2, 3, 4, 5$.

Zadanie 3.11. Udowodnić, że jeżeli a, b, c są kolejnymi liczbami całkowitymi, to $a^2 + b^2 + c^2 \equiv_3 2$.

Zadanie 3.12. Wyznaczyć resztę z dzielenia liczby $1^{100} + 2^{100} + 3^{100} + 4^{100} + 5^{100} + 6^{100} + 7^{100} + 8^{100} + 9^{100}$ przez 5.

Zadanie 3.13. Udowodnić, że liczba $5^{36} - 1$ jest podzielna przez 13.

Zadanie 3.14. Udowodnić, że liczba $53^{53} - 33^{33}$ jest podzielna przez 10.

Zadanie 3.15. Udowodnić, że liczba $4^{2n+1} + 3^{n+2}$ jest podzielna przez 13.

Zadanie 3.16. Udowodnić, że liczba $7^{222} + 1$ jest podzielna przez 5.

Zadanie 3.17. Pokazać, że 6 jest ostatnią cyfrą liczby 6^n dla dowolnego $n \in \mathbb{N}$.

Zadanie 3.18. Pokazać, że dwie ostatnie cyfry liczby 76^n to 7 i 6, dla dowolnego $n \in \mathbb{N}$?

Zadanie 3.19. Jaka jest ostatnia cyfra liczby 7^{100}?

Zadanie 3.20. Wyznaczyć dwie ostatnie cyfry liczby 2^{999}.

Zadanie 3.21. Wyznaczyć dwie ostatnie cyfry liczby $76^{57} - 57^{76}$.

Zadanie 3.22. Wyznaczyć dwie ostatnie cyfry liczby $99^{99} - 51^{51}$.

Zadanie 3.23. Liczby odwrotne do liczby m modulo p różnią się o wielokrotność liczby p.

Zadanie 3.24. Znaleźć liczbę odwrotną do liczby m modulo p.

(a) $m = 22$, $p = 2$; **(c)** $m = 21$, $p = 8$;

(b) $m = 8$, $p = 21$; **(d)** $m = 50$, $p = 7$.

Zadanie 3.25. Rozwiązać kongruencje

(a) $5 \cdot x \equiv_{26} 1$, **(g)** $4 \cdot x \equiv_{26} 1$,

(b) $17 \cdot x \equiv_{26} 1$, **(h)** $8 \cdot x \equiv_{13} 4$,

(c) $8 \cdot x \equiv_{13} 4$, **(i)** $99 \cdot x \equiv_{13} 1$,

(d) $21 \cdot x \equiv_{36} 5$; **(j)** $4 \cdot x \equiv_7 6$;

(e) $3 \cdot x \equiv_{100} 59$; **(k)** $16 \cdot x \equiv_{24} 8$;

(f) $3 \cdot x \equiv_{13} 5$; **(l)** $12 \cdot x \equiv_2 8$.

3.5. Odpowiedzi i wskazówki do zadań

3.2 Niech $d = \mathbf{NWD}(m, n)$. Wtedy $d \big| m$ i $d \big| n$. Wobec tego dla dowolnych $x, y \in \mathbb{C}$ mamy $d \Big| (mx + ny)$. Zatem z uwagi 3.1.6 wynika, że $d \leqslant \mathbf{NWD}(mx + ny)$. Jeśli $d' = \mathbf{NWD}(m, mx + ny)$, $x, y \in \mathbb{C}$, to $d' \Big| m$ i $d' \Big| (mx + ny)$. W szczególności kładąc $x = 0$ i $y = 1$ mamy $d' \Big| n$. Wobec tego $d' \leqslant \mathbf{NWD}(n, m) = d$. Otrzymaliśmy więc $d \leqslant d' \leqslant d$, co oznacza, że $\mathbf{NWD}(n, m) = \mathbf{NWD}(m, mx + ny)$. Postępując podobnie pokażemy, że $\mathbf{NWD}(n, m) = \mathbf{NWD}(mx + ny, n)$.

3.3 Niech $d = \mathbf{NWD}(m,n)$ i $d' = \mathbf{NWD}\left(\frac{n}{d}, \frac{m}{d}\right)$. Wtedy

$$\bigvee_{k_1 \in \mathbb{C}} \frac{m}{d} = k_1 d' \ \wedge \bigvee_{k_2 \in \mathbb{C}} \frac{n}{d} = k_2 d'.$$

Wobec tego $m = k_1 d' d$ i $n = k_2 d' d$, czyli $d'd \Big| m$ i $d'd \Big| n$. Zatem $d'd \leqslant d$, na mocy uwagi 3.1.6. Stąd wynika, że $d' \leqslant 1$. Ale na mocy uwagi 3.1.5 mamy $d' \geqslant 1$. Wobec tego $d' = 1$.

3.5 (a) $\mathbf{NWD}(m,n) = 2$, $s = -2$, $t = 3$, (b) $\mathbf{NWD}(m,n) = 30$, $s = 1$, $t = 0$, (c) $\mathbf{NWD}(m,n) = 1$, $s = -4$, $t = 17$, (d) $\mathbf{NWD}(m,n) = 11$, $s = 0$, $t = 1$,

3.6 (a) $x = -4 + 3k$, $y = 12 - 8k$, $k \in \mathbb{C}$, (b) $x = 16 + 111k$, $y = -3 - 21k$,
(c) $-123 + 11k$, $y = -82 + 7k$, (d) $x = 22 + 5k$, $y = -11 - 3k$,
(e) $x = -22 + 37k$, $y = 6 - 10k$, (f) $x = 2k$, $y = -2 + 8k$,
(g) $x = -126 + 26k$, $y = 21 - 4k$, (h) $x, y \in \emptyset$,
(i) $x = 3k$, $y = 13 - 9k$, (j) $x = -4 + 3k$, $y = 8 - 5k$,

3.7 Albo potrzebujemy czterech worków 80-cio kg i dwa worki 60-cio kg, albo jeden worek 80-cio kg i sześć worków 60-cio kg.

3.8 Istnieje 10 różnych rozwiązań tego zadania. Za 149 zł można kupić:

biletów po 3 zł	48	43	38	33	28	23	18	13	8	3
biletów po 5 zł	1	4	7	10	13	16	19	22	25	28

3.9 (a) 3, (b) 1, (c) 3, (d) 1,

3.11 Skoro a, b, c są kolejnymi liczbami całkowitymi, to $a = b - 1$ i $c = b + 1$. Wobec tego

$$\begin{aligned} a^2 + b^2 + c^2 - 2 &= (b-1)^2 + b^2 + (b+1)^2 - 2 \\ &= b^2 - 2b + 1 + b^2 + b^2 + 2b + 1 - 2 = 3b^2, \end{aligned}$$

co oznacza, że $3 \Big| (a^2 + b^2 + c^2 - 2)$, gdyż $b \in \mathbb{C}$.

3.17 Pytanie o ostatnią cyfrę w liczbie n, to pytanie o to do jakiej liczby, liczba n jest kongruentna modulo 10. Zatem mamy udowodnić, że $6^n \equiv_{10} 6$. Wykorzystamy zasadę indukcji matematycznej.

I krok indukcyjny: Dla $n = 1$ mamy $6 \equiv_{10} 6$, co oczywiście jest prawdą.

II krok indukcyjny:

Założenie: $6^n \equiv_{10} 6$

Teza: $6^{n+1} \equiv_{10} 6$

Dowód: Mnożąc stronami kongruencje z założenia i I kroku indukcyjnego otrzymamy $6^{n+1} \equiv_{10} 6^2$. Oczywiście $6^2 \equiv_{10} 6$. Ponieważ kongruencja jest relacją przechodnią, to dostajemy tezę.

3.24 (a) nie istnieje, bo $\mathbf{NWD}(22, 2) = 2 \neq 1$, (b) 8, (c) 5, (d) 1

3.25 (a) $x = 21 + 26k$, $k \in \mathbb{C}$, (b) $x = 23 + 26k$, (c) $x = 20 + 13k$, (d) $x \in \emptyset$,
(e) $x = 53 + 100k$, (f) $x = 6 + 13k$, (g) $x \in \emptyset$, (h) $x = 7 + 13k$,
(i) $x = 5 + 13k$, (j) $x = 5 + 7k$, (k) $x = 2 + 3k$, (l) $x \in \emptyset$.