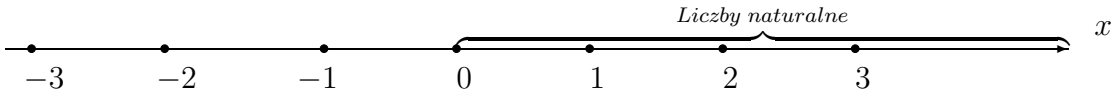
SZKOŁA PODSTAWOWA HELIANTUS
02-892 WARSZAWA
ul. BAŻANCIA 16



Oś liczbowa. Liczby całkowite

DZIELENIE Z RESZTĄ. KONGRUENCJA[1]

Tadeusz STYŠ

WARSZAWA 2020

[1]Rozdział 6. Matematyka dla Szkoły Podstawowej i Liceum Ogólnokształcącego.

Contents

Chapter 1

Dzielenie z resztą. Cechy podzielności. Kongruencja.

1.1 Wstęp

Ten rozdział jest opracowany dla rozszerzonego programu matematyki i dotyczy podzielności liczb naturalnych. Treść rozdziału, ćwiczenia, przykłady i zadania dostosowane są do poziomu uczniów klas starszych szkoły podstawowej.

Operacje dzielenia z resztą i cechy podzielności liczb naturalnych opisane są w sytemie dziesiętnym.

W tym rozdziale wprowadzone jest pojęcie liczb przystających i operacja dzielenia z resztą modulo n. Pojęcie kongruencji czyli przystawania liczb całkowitych a i b względem liczby naturalnej n wykracza poza podstawę programową, jednak jest istotnym tematem w programie rozszerzonym. Podobnie równanie liniowe Diofantosa i roszerzony algorytm Euklidesa wykraczają poza podstawę programową ale doskonale pasują do programu rozszerzonego w ramach kółka z matematyki dla klas starszych.

Ćwiczenia z zadaniami dostosowanymi do programu podstawowego i do programu rozszerzonego.

1.2 Cechy podzielności liczb naturalnych

Cechy podzielności liczb naturalnych wynikają z ogólnego zapisu liczb w systemie pozycyjnym. Przypominamy, że w systemie dziesiętnym, każdą liczbę

n-cyfrową piszemy w postaci

$$\begin{aligned} m &= \alpha_{n-1}\alpha_{n-2}\cdots\alpha_1\alpha_0 \\ &= \alpha_{n-1} * 10^{n-1} + \alpha_{n-2} * 10^{n-2} + \cdots + \alpha_1 * 10^1 + \alpha_0 * 10^0 \end{aligned}$$

gdzie

$$\alpha_{n-1}, \alpha_{n-2}, \cdots, \alpha_1, \alpha_0$$

są cyframi liczby m o wartościach $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$.
Teraz sformułujemy i podamy prosty dowód cechy podzielności liczby naturalnej przez 3

1.2.1 Cecha podzielności liczby naturalnej przez 3 lub przez 9

Liczba naturalna

$$m = \alpha_{n-1}\alpha_{n-2}\cdots\alpha_1\alpha_0$$

jest podzielna przez 3 wtedy i tylko wtedy, jeżeli jej suma cyfr

$$\alpha_{n-1} + \alpha_{n-2} + \cdots + \alpha_1 + \alpha_0$$

dzieli się przez 3. Ponadto, jeżeli suma cyfr liczby m dzieli się przez 9 to liczba m również jest podzielna przez 9.
Zanim podamy dowód tej cechy, rozpatrzmy kilka przykładów jej zastosowania.

Przykład 1.1 *Niech* $m = 24$. *Cyfry tej liczby dwucyfrowej, gdy* $n = 2$, *to* $\alpha_1 = 2$ *i* $\alpha_0 = 4$
Suma cyfr

$$\alpha_1 + \alpha_0 = 2 + 4 = 6$$

jest podzielna przez 3. *Zatem liczba* 24 *jest podzielna przez* 3. *Rzeczywiście*

$$24 : 3 = 8$$

Przykład 1.2 *Niech* $m = 381$. *Cyfry tej liczby trzycyfrowej, gdy* $n = 3$, *to* $\alpha_2 = 2 = 3$, $\alpha_1 = 8$ *i* $\alpha_0 = 1$
Suma cyfr

$$\alpha_2 + \alpha_1 + \alpha_0 = 3 + 8 + 1 = 12$$

jest podzielna przez 3, *bo* $12 : 3 = 4$. *Zatem liczba* 381 *jest podzielna przez* 3. *Rzeczywiście*

$$381 : 3 = 127$$

Przykład 1.3 *Niech* $m = 5673$. *Cyfry tej liczby czterocyfrowej* $n = 4$, *to* $\alpha_3 = 5$, $\alpha_2 = 6$, $\alpha_1 = 7$ *i* $\alpha_0 = 3$
Suma cyfr

$$\alpha_3 + \alpha_2 + \alpha_1 + \alpha_0 = 5 + 6 + 7 + 3 = 21$$

jest podzielna przez 3. *Zatem liczba* 5673 *jest podzielna przez* 3. *Rzeczywiście*

$$5673 : 3 = 1891$$

Przykład 1.4 *Niech* $m = 48537$. *Cytry tej liczby pięciocyfrowej, gdy* $n = 5$, *to* $\alpha_4 = 4,\ \alpha_3 = 8,\ \ \alpha_2 = 5,\ \ \alpha_3 = 7$ *i* $\alpha_0 = 7$
Suma cyfr

$$\alpha_3 + \alpha_2 + \alpha_1 + \alpha_0 = 4 + 8 + 5 + 3 + 7 = 27$$

jest podzielna przez 3 *i przez* 9. *Zatem liczba* 5673 *jest podzielna przez* 3 *i przez* 9. *Rzeczywiście*

$$48537 : 3 = 16177, \quad i \quad 48537 : 9 = 5393$$

Dowód w przypadku liczb dwucyfrowych. Liczby dwucyfrowe piszemy w postaci

$$\alpha_1\alpha_0 = \alpha_1 * 10 + \alpha_0$$

Proste przekształcenie wyrażenia algebraicznego

$$\begin{aligned} \alpha_1 * 10 + \alpha_0 &= \alpha_1 * 10 + \alpha_0 - (\alpha_1 + \alpha_0) + (\alpha_1 + \alpha_0) \\ &= \alpha_1(10 - 1) + (\alpha_1 + \alpha_0) \\ &= 9 * \alpha_1 + (\alpha_1 + \alpha_0) \end{aligned}$$

zawiera składnik $9 * \alpha_1$ z czynnikiem 9, zatem ten składnik jest podzielny przez 3 i przez 9.

Skąd wnioskujemy, że:

Jeżeli suma cyfr $\alpha_1 + \alpha_0$ *jest podzielny przez* 3 *lub* 9 *to liczba* m *jest podzielna przez* 3 *lub przez* 9.

Prawdą jest również zdanie odwrotne:

Jeżeli liczba m *jest podzielna przez* 3 *lub przez* 9 *to suma jej cyfr* $\alpha_1 + \alpha_0$ *też jest podzielna przez* 3 *lub przez* 9.

Te dwa zdania wyrażamy jednym zdaniem:

Liczba m *jest podzielna przez* 3 *lub przez* 9 *wtedy i tylko wtedy, jeżeli jej suma cyfr* $\alpha_1 + \alpha_0$ *jest podzielna przez* 3 *lub przez* 9.

Ta relacja w obie strony nazywa się warunkiem koniecznym i dostatecznym. W tym przykładzie jest to warunek konieczny i dostateczny podzielności liczby m przez 3 lub przez 9.

Powtórzmy dowód cechy podzielności liczby m przez 3 lub przez 9 dla liczb trzycyfrowych.

Dowód w przypadku liczb trzycyfrowych. Liczby trzycfrowe piszemy w

postaci

$$\alpha_2\alpha_1\alpha_0 = \alpha_2 * 100 + \alpha_1 * 10 + \alpha_0$$

Proste przekształcenie wyrażenia algebraicznego

$$\begin{aligned} \alpha_2 * 100 + \alpha_1 * 10 + \alpha_0 &= \alpha_2 * 100 + \alpha_1 * 10 + \alpha_0 \\ &\quad -(\alpha_2 + \alpha_1 + \alpha_0) + (\alpha_2 + \alpha_1 + \alpha_0) \\ &= \alpha_2 * (100 - 1) + \alpha_1(10 - 1) + (\alpha_2 + \alpha_1 + \alpha_0) \\ &= 99 * \alpha_2 + 9 * \alpha_1 + (\alpha_2 + \alpha_1 + \alpha_0) \end{aligned}$$

zawiera składnik $99 * \alpha_2 + \ 9 * \alpha_1$, który dzieli się przez 3 i przez 9. Zatem, jeżeli suma cyfr $\alpha_2 + \alpha_1 + \alpha_0$ jest podzielna przez 3 lub przez 9 to liczba m jest również podzielna przez 3 lub przez 9.

Skąd wnioskujemy, że:

Jeżeli suma cyfr $\alpha_2 + \alpha_1 + \alpha_0$ *jest podzielny przez* 3 *lub* 9 *to liczba* m *jest podzielna przez* 3 *lub przez* 9*.*

Prawdą jest również zdanie odwrotne:

Jeżeli liczba m *jest podzielna przez* 3 *lub przez* 9 *to suma jej cyfr* $\alpha_2 + \alpha_1 + \alpha_0$ *też jest podzielna przez* 3 *lub przez* 9*.*

Te dwa zdania wyrażamy jednym zdaniem:

Liczba m *jest podzielna przez* 3 *lub przez* 9 *wtedy i tylko wtedy, jeżeli jej suma cyfr* $\alpha_2 + \alpha_1 + \alpha_0$ *jest podzielna przez* 3 *lub przez* 9*.*

Ta relacja w obie strony nazywa się warunkiem koniecznym i dostatecznym podzielności liczby m przez 3 lub przez 9.

W przypadku ogólnym dla liczb *n-cyfrowych*, schemat dowodu cechy podzielności liczby m przez 3 lub przez 9 jest taki sam jak dla liczb dwucyfrowych i trzycyfrowych.

Zadanie 1.1 *Wiadomo, że liczba naturalna* m *jest podzielna przez* 3 *i ma dokładnie* 4 *dzielniki, których suma równa jest* 128*. Znajdź tą liczbę.*

1.2.2 Cecha podzielności liczby naturalnej przez 5

Bardzo łatwo rozpoznać liczbę m, która jest podzielna przez 5. Mianowicie, zachodzi następujące cecha podzielności:

Liczba naturalna m *jest podzielna przez* 5 *wtedy i tylko wtedy, jeżeli jej cyfry jedności są* 0 *lub* 5*.*

Przykład 1.5 *Łatwo sprawdzamy, że liczby*

$$30, 35, 40, 45, 150, 155, 2360, 2365, 9800, 9855, 9890, 9995$$

są podzielne przez 5

Dowód cechy podzielności liczby m przez 5.

Dla uproszczenia , rozpatrzymy liczbę trzycyfrową m, która ma cyfrę jedności 0 lub 5. Wtedy liczba m rozkłada się na iloczyn liczby 5 przez liczbę naturalą. Mianowicie, mamy

$$\begin{aligned} m &= \alpha_2 * 10^2 + \alpha_1 * 10 \\ &= 5 * (2 * \alpha_2 * 10 + 2 * \alpha_1) \end{aligned}$$

lub

$$\begin{aligned} m &= \alpha_2 * 10^2 + \alpha_1 * 10 + 5 \\ &= 5 * (2 * \alpha_2 * 10 + 2 * \alpha_1 + 1) \end{aligned}$$

W przypadku ogólnym liczb n-cyfrowych, które mają cyfrę jedności 0 lub 5 mamy również rozkład liczby m na iloczyn liczby 5 przez liczbę naturalną. Mianowicie

$$\begin{aligned} m &= \alpha_{n-1} * 10^{n-1} + \alpha_{n-2} * 10^{n-2} + \cdots + \alpha_1 * 10^1 \\ &= 5 * (2 * \alpha_{n-1} * 10^{n-2} + 2 * \alpha_{n-2} * 10^{n-3} + \cdots + 2 * \alpha_1) \end{aligned}$$

lub

$$m = 5 * (2 * \alpha_{n-1} * 10^{n-2} + 2 * \alpha_{n-2} * 10^{n-3} + \cdots + 2 * \alpha_2 + \alpha_1)$$

Zatem w przypadku ogólnym liczba m, która ma cyfrę jedności 0 lub 5 jest podzielna przez 5.

1.3 Dzielenie liczb przez 3 z resztą

Każda liczba naturalna m dzieli się przez 3 lub dzieli się przez 3 z resztą 1 lub z resztą 2.

Wtedy piszemy

$m = 3k$ $\quad gdy \quad liczba \quad m \quad jest \quad podzielna \quad przez \ 3$

$m = 3k + 1$ $\quad gdy \quad liczba \quad m \quad jest \quad podzielna \quad przez \ 3, \quad reszta \ 1$

$m = 3k + 2$ $\quad gdy \quad liczba \quad m \quad jest \quad podzielna \quad przez \ 3, \quad reszta \ 2$

Przykład 1.6 *Wykonaj dzielenie z resztą*

- $33 : 3 = 11 \quad reszta \quad 0$
- $34 : 3 = 11 \quad reszta \quad 1$
- $35 : 3 = 11 \quad reszta \quad 2$

lub piszemy dzielenie w postaci ułamków

- $\frac{33}{3} = 11 \quad reszta \quad 0$
- $\frac{34}{3} = 11 + \frac{1}{3} \quad reszta \quad 1$
- $\frac{35}{3} = 11 + \frac{2}{3} \quad reszta \quad 2$

Przykład 1.7 *Suma trzech kolejnych liczb podzielnych przez* 3 *równa jest* 36. *Jakie to liczby?*

Rozwiązanie.

Napiszmy trzy kolejne liczby podzielne przez 3

$$3k - 3,\ 3k,\ \ 3k + 3$$

Suma tych liczb

$$(3k - 3) + 3k + (3k + 3) = 9k = 36$$

Skąd obliczamy

$$9k = 36, \qquad k = 36 : 9 \qquad k = 4.$$

Odpowiedź:

$$3k - 3 = 3 * 4 - 3 = 9,$$

$$3k = 3 * 4 = 12,$$

$$3k + 3 = 3 * 4 + 1 = 15$$

Kolejnymi liczbami podzelnymi przez 3, których suma równa jest 36 są liczby

$$9, \qquad 12 \qquad 15$$

Sprawdzenie:

$$9 + 12 + 15 = 36$$

Zadanie 1.2 *Suma trzech kolejnych liczb podzielnych przez* 3 *równa jest* 72. *Jakie to liczby?*

Zadanie 1.3 *Suma trzech kolejnych liczb podzielnych przez* 3 *z resztą* 1 *jest równa* 75. *Jakie to liczby?*

Zadanie 1.4 *Suma trzech kolejnych liczb podzielnych przez* 3 *z resztą* 2 *jest równa* 105. *Jakie to liczby?*

1.4 Dzielenie liczb przez 5 z resztą

Każda liczba naturalna m dzieli się przez 5 lub dzieli się przez 5 z resztą 1 lub resztą 2 lub z resztą 3 lub z resztą 4.

Wtedy piszemy

$$m = 5k \quad gdy \quad liczba \quad m \quad jest \quad podzielna \quad przez \quad 5$$

$$m = 5k+1 \quad gdy \quad liczba \quad m \quad jest \quad podzielna \quad przez \quad 5, \quad reszta \quad 1$$

$$m = 5k+2 \quad gdy \quad liczba \quad m \quad jest \quad podzielna \quad przez \quad 5, \quad reszta \quad 2$$

$$m = 5k+3 \quad gdy \quad liczba \quad m \quad jest \quad podzielna \quad przez \quad 5, \quad reszta \quad 3$$

$$m = 5k+4 \quad gdy \quad liczba \quad m \quad jest \quad podzielna \quad przez \quad 5, \quad reszta \quad 4$$

Przykład 1.8 *Wykonaj dzielenie przez* 5 *z resztą*

- $35 : 5 = 7 \quad reszta \quad 0$
- $36 : 5 = 7 \quad reszta \quad 1$
- $37 : 5 = 7 \quad reszta \quad 2$
- $38 : 5 = 7 \quad reszta \quad 3$
- $39 : 5 = 7 \quad reszta \quad 4$

lub piszemy dzielenie w postaci ułamków

- $\frac{35}{5} = 7 \quad reszta \quad 0$
- $\frac{36}{5} = 7 + \frac{1}{5} \quad reszta \quad 1$
- $\frac{37}{5} = 7 + \frac{2}{5} \quad reszta \quad 2$
- $\frac{38}{5} = 7 + \frac{2}{5} \quad reszta \quad 3$
- $\frac{39}{5} = 7 + \frac{2}{5} \quad reszta \quad 4$

Przykład 1.9 *Suma trzech kolejnych liczb podzielnych przez* 5 *równa jest* 45. *Jakie to liczby?*

Napiszmy trzy kolejne liczby podzielne przez 3
Rozwiązanie.

$$5k-5,\ 5k,\ \ 5k+5$$

Suma tych liczb

$$(5k-5)+5k+(5k+5)=15k=45$$

Skąd obliczamy k

$$15k=45,\qquad k=45:15\qquad k=3.$$

Skąd obliczmy trzy kolejne liczby podzielne przez 5, których suma równa jest 45

$$5k-5=5*3-5=10,$$

$$5k=5*3=15,$$

$$5k+5=5*3+5=20$$

Kolejnymi liczbami podzelnymi przez 5, których suma równa jest 45 są liczby

$$10,\qquad 15\qquad 20$$

Sprawdzenie:

$$10+15+20=45$$

Zadanie 1.5 *Suma trzech kolejnych liczb podzielnych przez* 5 *z resztą* 1 *równa jest* 108. *Jakie to liczby?*

Rozwiązanie.
Napiszmy trzy kolejne liczby podzielne przez 5 z resztą 1

$$5k+1,\ 5k+6,\ \ 5k+11$$

Suma tych liczb

$$(5k+1)+(5k+6)+(5k+11)=15k+18=108$$

Skąd obliczamy k

$$15k=90,\qquad k=90:15\qquad k=6.$$

Skąd obliczmy trzy kolejne liczby podzielne przez 5, których suma równa jest 108

$$5k+1=5=5*6+1+31,$$

$$5k+6=5*6+6=36,$$

$$5k+11=5*6+11=41$$

Kolejnymi liczbami podzelnymi przez 5, których suma równa jest 45 są liczby

$$31, \quad 36 \quad 41$$

Sprawdzenie:

$$31 + 36 + 41 = 108$$

Zadanie 1.6 *Suma dwóch kolejnych liczb podzielnych przez* 5 *z resztą* 2 *jest równa* 79. *Jakie to liczby?*

Zadanie 1.7 *Suma trzech kolejnych liczb podzielnych przez* 5 *z resztą* 3 *jest równa* 129. *Jakie to liczby?*

1.4.1 Ogólna zasada podzielności liczb naturalnych z resztą

Każda liczba naturalna m dzieli się przez liczbę naturalną n z resztą r. W wyniku dzielenia otrzymujemy całość k i resztę r.[1]
Wtedy piszemy

$$m : n = k + r : n \quad lub \quad \frac{m}{n} = k + \frac{r}{n} \quad lub \quad m = k * n + r$$

gdzie reszta $r = 0, 1, 2, ..., n - 1$.
Z operacją dzielenia liczb z resztą łączymy funkcje całość z dzielenia liczby m przez liczbę n.

• Funkcje całość z dzielenia, piszemy $E[m : n]$ lub $[m : n]$.

Wartość funkcji całość z $E[m : n]$ jest równa największej liczbie całkowitej nie większej od $m : n$.

Zatem

$$E[m : n] \leq m : n \qquad lub \qquad [m : n] \leq m : n.$$

Na przykład niech $m = 37, \quad n = 5$.

Największa liczba całkowita z tego dzielenia, ale nie większa od

$$37 : 5 = 7\frac{2}{5}$$

jest równa 7, piszemy

$$E[37 : 5] = E[\frac{37}{5}] = 7 \qquad lub \qquad [37 : 5] = [\frac{37}{5}] = 7.$$

Przykład 1.10 *Oblicz całość i resztę z dzielenia liczb* $m = 36,\ 37,\ 38,\ 39\ 40,\ 41$ *przez* $n = 6$.
Podaj wzór ogólny dzielenia liczby m *przez* 6 *z resztą* r.

[1] Wartość funkcji całość z ułamka x, piszemy $E[x] \leq x$ lub $[x] \leq x$, równa jest największej liczbie całokowitej nie większej od x. Po angielsku Entire of x

Rozwiązanie:

$36 : 6 = 6$, *liczba* 36 *jest podzielna przez* 6, *z reszta* 0, *calosc* $k = 6,\ r = 0.$

$37 : 6 = 6$, *liczba* 37 *dzieli sie przez* 6, *z reszta* 1, *calosc* $k = 6,\ r = 1,$

$38 : 6 = 6$, *liczba* 38 *dzieli sie przez* 6, *z reszta* 2, *calosc* $k = 6,\ r = 2,$

$39 : 6 = 6$, *liczba* 37 *dzieli sie przez* 6, *z reszta* 3, *calosc* $k = 6,\ r = 3,$

$40 : 6 = 6$, *liczba* 40 *dzieli sie przez* 6, *z reszta* 4, *calosc* $k = 6,\ r = 4,$

$41 : 6 = 6$, *liczba* 31 *dzieli sie przez* 6, *z reszta* 5, *calosc* $k = 6,\ r = 5,$

Wzór ogólny dzielenia liczby naturalnej m przez 6

$$m = 6k + r, \quad z \ \ reszta \ \ r = 0, 1, 2, 3, 4, 5.$$

Zadanie 1.8 *Stosując wzór ogólny dzielenia liczby naturalnej m przez* 6 *wykaż, że każda liczba pierwsza* $p > 3$ *dzieli się przez* 6 *z resztą* 1 *lub z resztą* 5 *i wtedy można napisać liczbę p w postaci*

$$p = 6 * k + 1, \quad lub \ \ p = 6k - 1 \ \ dla \ \ pewnej \ liczby \ naturalnej \ k$$

Napisz liczbę pierwszą $p = 7901$ *w postaci* $p = 6k - 1$

1.5 Liczby przystające. Kongruencja

Liczby całkowite a i b nazywamy przystające względem liczby naturalnej n, jeżeli ich różnica $a - b$ jest podzielna przez n.
Na przykład

13 przystaje do 3 względem 2, bo $(13 - 3) : 2 = 5$, gdy $a = 13,\ b = 3,\ n = 2.$

47 przystaje do 35 względem 6, bo $(47 - 35) : 6 = 2,$

gdy $a = 47,\ b = 35,\ n = 6.$

Liczby przytające są również nazywane liczbami kogruentnymi. Kongruencja po polsku znaczy przystawanie.
Karol Gauss (1777-1835) wprowadził oznaczenia operacji modulo.

$$a \ \equiv \ b(mod\ n)$$

Powyższy zapis rozumiemy, że różnica $a - b$ jest podzielna przez n. To znaczy

$$a - b = k * n$$

dla pewnej liczby całkowitej k.

Przykład 1.11 *Pisząc*

$$27 \equiv 13(mod\ 7)$$

rozumiemy, że różnica $27 - 13$ *jest podzielna przez 7. W tym przykładzie*

$$(27 - 13) : 7 = 2.$$

To znaczy, że $27 - 13 = 2 * 7$ *dla* $k = 2$.

Przykład 1.12 *Które kongruencje są prawdziwe?*

$7 \equiv 3(mod\ 2)$, *prawdziwa bo* $(7 - 3) : 2 = 4 : 2 = 2$

$12 \equiv 5(mod\ 4)$, *nieprawdziwa bo* $(12 - 5) = 7$, 7 *niepodzielne przez* 4

Z operacją dzielenia z resztą łączymy operacje modulo $r \equiv m(mod\ n)$

• Mianowicie, resztę z dzielenia liczby m przez lliczbę n, piszemy

$$r = m(mod\ n).$$

Wynik operacji modulo jest równa różnicy

$$r = (m : n - E[m : n]) * n$$

lub

$$r = (m : n - [m : n]) * n.$$

Na przykład niech

$$m = 37, \quad n = 5.$$

Wtedy obliczamy wartość funkcji modulo, reszte z tego dzielenia

$$r = (37 : 5 - E[37 : 5]) * 5 = (7\frac{2}{5} - 7) * 5 = 2$$

lub

$$r = (37 : 5 - [37 : 5]) * 5 = (7\frac{2}{5} - 7) * 5 = 2.$$

1.5.1 Dzielenie modulo

Wynik dzielenia modulo liczby całkowitej a przez liczbę naturalą n równy jest reszcie z dzielenia liczby a przez liczbę n. Zatem, operacja modulo określona jest na zbiorze liczb całkowitych.

Na przykład

$$r = 25(mod\ 15) = 10 \quad bo \quad 25 : 15 = 1 + reszta \quad 10$$

$$r = 37(mod\ 12) = 1 \quad bo \quad 37 : 12 = 3 + reszta \quad 1$$

Dokładny wylnik

$$\frac{25}{15} = 1 + \frac{10}{15}$$
$$\frac{37}{12} = 3 + \frac{1}{12}$$

Wtedy piszemy

$$r = a(mod\ n), \quad 25(mod 15) = 10, \quad gdy \quad a = 25, \quad n = 15, \quad reszta \quad r = 10$$

$$r = a(mod\ n), \quad 37(mod 12) = 1, \quad gdy \quad a = 37, \quad n = 12, \quad reszta \quad r = 1$$

Przykład 1.13 *Oblicz* $47(mod\ 5)$

Obliczamy

$$47 : 5 = 9 + reszta \quad 2,$$

Odpowiedź:

$$47(mod\ 5) = 2$$

Przykład 1.14 *Oblicz* $123(mod\ 7)$

Obliczamy

$$123 : 7 = 17 + reszta \quad 4,$$

Odpowiedź:

$$123(mod\ 7) = 4$$

1.5.2 Własności operacji modulo

Relacja $\equiv$ kongruencji, to znaczy relacja przystawania liczb całkowitych ma podobne własności jak zwykła relacja równości $=$.
Własności kongruencji:

1. **Własność symetrii**

   $a \equiv b(mod\ n) \quad to \quad b \equiv a(mod\ n)$

   Przykład 1.15 *Rozpatrzmy kongruencje*

   $$15 \equiv 3(mod\ 4) \qquad i \qquad 3 \equiv 15(mod\ 4)$$

   $$a = 15, \quad b = 3$$

   Liczby $a = 15$ i $b = 3$ są przystające względem liczby naturalnej $n = 4$ w obu przypadkach, gdyż

   $$(15 - 3) : 4 = 3 \qquad i \qquad (3 - 15) : 4 = -3$$

2. **Operacja przechodnia**

   Jeżeli liczby a i b oraz liczby b i c są przystające względem liczby n, to znaczy prawdziwe są kongruencje

   $$a \equiv b((mod\ n) \quad i \quad b \equiv c(mod\ n)$$

   to liczby a i c też są przystające względem liczby n, to znaczy

   $$a \equiv c(mod\ n)$$

   Przykład 1.16 *Rozpatrzmy dwie kongruencje*

   $$20 \equiv 12(mod\ 4) \qquad i \qquad 12 \equiv 8(mod\ 4),$$

   $$a = 20, \quad b = 12, \quad c = 8, \quad n = 4.$$

   Liczby $a = 20$ i $c = 8$ też są przystające względem liczby 4, gdyż

   $$20 \equiv 8(mod\ 4)$$

   ponieważ różnica

   $$(20 - 8) : 4 = 3$$

3. **Dodawanie i mnożenie kongruencji**
   Jeżeli prawdziwe są kongruencje

   $$a \equiv b(mod\ n) \quad i \quad c \equiv d(mod\ n)$$

   to suma stron tych kongruencji

   $$a + c \equiv b + d(\text{mod } n)$$

   oraz iloczyn stron tych kongruencji

   $$a \cdot c \equiv b \cdot d(\text{mod } n)$$

   Przykład 1.17 *Rozpatrzmy dwie kongruencje*

   $$15 \equiv 3(mod\ 4) \qquad i \qquad 20 \equiv 5(mod\ 4)$$

   $$a = 15, \quad b = 3 \quad c = 20, \quad d = 4, \quad n = 4$$

   Liczby 15 i 3 są przystają względem liczby naturalnej $n = 4$, gdyż różnice

   $$(15 - 3) : 4 = 3 \qquad i \qquad (3 - 15) : 4 = -3$$

   są podzielne przez 4.

4. **Mnożenie kongruencji przez siebie. Potęga Kongruencji.** Mnożąc stronami kongruencję
$$a \equiv b(mod\ n)\}$$
przez siebie, otrzymamy
$$a^2 \equiv b^2(\text{mod } n), \quad a^3 \equiv b^3(mod\ n)\},\ \ldots, a^k \equiv b^k(mod\ n)\}$$
dla każdego naturalnego $k = 1, 2, 3, ...;$

Przykład 1.18 *Rozpatrzmy kongruencje*
$$9 \equiv 3(mod\ 2)$$
$$a = 9, \quad b = 3, \quad n = 2.$$
Mnożąc tą kongruencje stronami, otrzymamy
$$9^2 \equiv 3^2(mod\ 2), \quad 9^3 \equiv 3^3(mod\ 2), ..., 9^k \equiv 3^k(mod\ 2)$$
lub
$$81 \equiv 9(mod\ 2), \quad 729 \equiv 27(mod\ 2),\ \ldots, 9^k \equiv 3^k(mod\ 2)$$
Sprawdzamy:

$(81 - 9) : 2 = 36, \quad (729 - 27) : 2 = 702 : 2 = 351, ..., (9^k - 3^k) : 2 =) : 2$

Różnica $9^k - 3^k$ jest również podzielna przez 2. Ponieważ cyfry jedności liczb 9^k i 3^k są nieparzyste. Mianowicie cyfry jedności liczby 9^k to
$$1, 9, 1, 9, 1, 9, ...;$$
i cyfry jedności liczby 3^k to
$$9, 7, 1, 9, 7, 1, ...;$$
Różnica liczba nieparzystych jest liczbą parzystą.
Zatem liczba $9^k - 3^k$ jest podzielna przez 2 dla każdej liczby naturalnej $k = 1, 2, 3, ...;$
Skąd wynika, że liczby 9^k i 3^k są przystające modulo 2.

Przykład 1.19 *Liczba*
$$43^{125} - 33^{125}$$
jest podzielna przez 10.

Podnosząc stronami kongruencje
$$43 \equiv 33(mod\ 10)$$
do potęgi 125, otrzymamy kongruencje
$$43^{125} \equiv 33^{125}(mod\ 10)$$

Liczba 43 przystaje do liczby 33 modulo 10, gdyż

$$(43 - 33) : 10 = 1$$

Dlatego liczba 43^{125} przestaje do liczby 33^{125} modulo 10. Zatem różnica

$$43^{125} - 33^{125}$$

jest podzielna przez 10. Zastosowanie kongruencji do sprawdzania podzielności liczb wskażemy w następującym przykładzie

Przykład 1.20 *Stosując własność mnożenia stronami kongruencji, potęgowania stronami kongruencji, udowodnij, że liczba* $7^{246} + 1$ *jest podzielna przez* 10.

Rozwiązanie. Zauważmy, że liczba $7^2 + 1 = 50$ jest podzielna przez 10. To znaczy, że liczba 49 przystaje do liczby -1 modulo 10. Zatem mamy

$$49 \equiv -1(mod\ 10)$$

Podnosząc stronami tą kongruencje do potęgi 123, otrzymamy

$$49^{123} \equiv (-1)^{123}(mod\ 10), \qquad 7^{246} \equiv (-1)^{123}(mod\ 10)$$

Skąd, wynika kongruencja

$$7^{246} \equiv -1(mod\ 10)$$

która oznacza, że liczba $7^{246} + 1$ jest podzielna przez 10.

1.5.3 Rozwiązywanie kongruencji liniowych

Ogólna postać kongruencji liniowej

$$a * x \equiv b(mod\ n)$$

w której w spółczynniki $a,\ b$ są liczbami całkowitymi, natomiast n jest liczbą naturalną.
Rozwiązać kongruencję liniową znaczy wyznaczyć wszystkie liczby całkowite, które podstawione na x spełniają kongruencje, to znaczy znaleść wszystkie wartości całkowite x dla których liczba $a * x$ przystaje do liczby b modulo n.
W pierwszej kolejności powstaje pytanie, podobnie jak w przypadku innych równań, ile rozwiązań ma kongruencja liniowa? Z góry można spodziewać się że kongruencja liniowa może mieć

- jedno rozwiązanie, to znaczy istnieje tylko jedna liczba całkowita x_0 przystająca do liczby b modulo n taka, że

$$a * x_0 \equiv b(mod\ n)$$

- więcej niż jedno rozwiązanie, to znaczy istnieje skończona lub nawet nieskończona ilość liczb całkowitych $x_1, x_2, ..., x_k, ...$; które są przystające do liczby b modulo n. To znaczy

$$a * x_k \equiv b(mod\ n), \qquad k = 1, 2, 3, ...;$$

- kongruencja nie ma rozwiązań.

Istnienie rozwiązania kongruencji liniowej wynika z następującego warunku koniecznego i wystarczającego:

Warunek konieczny i wystarczający
Kongruencja liniowa

$$a * x \equiv b(mod\ n)$$

ma rozwiązanie wtedy i tylko wtedy, gdy największy wspólny dzielnik $NWD(a, n)$ liczb a i n jest dzielnikiem liczby b, to znaczy $NWD(a, b)|n$.
Po przeczytaniu powyższego wstępu o kongruencjach liniowych należy rozwiąwiązać kilka kongruencji, ażeby poznać sposoby ich rozwiązywania.

Przykład 1.21 *Rozwiąż kongruencje*

$$2 * x \equiv 3(mod\ 2)$$

Sprawdzamy warunek konieczny i wystarczający istnienia rozwiązania tej kongruencji.
Największy wspólny dzielnik

$$NWD(a, b) = NWD(2, 2) = 2$$

nie dzieli współczynnika

$$b = 3, \qquad 2 \nmid 3.$$

Zatem nie istnieje rozwiązanie tej kongruencji.

Przykład 1.22 *Rozwiąż kongruencje*

$$3 * x \equiv 6(mod\ 9)$$

Sprawdzamy warunek konieczny i wystarczający istnienia rozwiązania tej kongruencji.
Największy wspólny dzielnik

$$NWD(a, b) = NWD(3, 9) = 3$$

dzieli współczynnik

$$b = 6, \quad 3|6, \quad 6 : 3 = 2.$$

Zatem istnieje rozwiązanie tej kongruencji.
Z definicji kongruencji mamy równanie

$$3 * x - 6 = 9 * k,$$

dla wszystkich wartości calkowitych $k = 0, \pm 1, \pm 2, \pm 3, ...;$

Skąd obliczamy rozwiązanie

$$3 * x = 9 * k + 6, \quad x_k = 3 * k + 2, \quad dla \quad k = 0, \pm 1, \pm 2, \pm 3, ...;$$

Sprawdzenie:

Podstwiając rozwiązanie

$$x_k = 3 * k + 2, \quad dla \quad k = 0, \pm 1, \pm 2, \pm 3, ...;$$

do kongruencji

$$3 * x \equiv 6 (mod\ 9)$$

otrzymamy

$$3 * (3 * k + 2) \equiv 6 (mod\ 9),$$

Skąd wynika tożsamość

$$(9 * k + 6 - 6) : 9 = 9 * k, \quad 9 * k = 9 * k$$

dla każdej całkowitej wartości $k = 0, \pm 1, \pm 2, \pm 3, ...;$

1.6 Rozwiązanie równania liniowego Diofantosa

Ogólna postać równań liniowych Diofantosa

$$a * x + b * y = c \tag{1.1}$$

gdzie współczynniki $a,\ b,\ c$ są danymi liczbami całkowitymi, niewiadomych x i y również szukamy w liczbach całkowitych.

1.6.1 Rozszerzony algorytm Euklidesa.

Rozszerzony algorytm Euklidesa wyznaczania największego wspólnego dzielnika $NWD(a, b)$ prowadzi również do rozwiązania równania liniowego Diofantosa, jeżeli rozwiązanie tego równania istnieje.

Warunek istnienia rozwiązania równania liniowego Diofantosa.
Równanie liniowe Diofantosa o współczynnikach całkowitych $a,\ b,\ c$

$$a * x + b * y = c \tag{1.2}$$

ma rozwiązanie w liczbach całkowitych wtedy i tylko wtedy, gdy największy wspólny dzielnik $NWD(a, b)$ współczynników a i b jest również dzielnikiem współczynnika c.

Zauważamy, że jeżeli liczba d jest dzielnikiem liczb r_0 i r_1 to rownież jest

dzielnikiem ich sumy $r_0 + r_1$ i różnicy $r_0 - r_1$.
Wykonując dzielenie

$$\frac{r_0}{r_1} = k_0 + \frac{r_2}{r_1}$$

obliczamy resztę

$$r_2 = r_0 - k_0 * r_1.$$

Tutaj k_0 jest całością z dzielenia liczby naturalnej liczb r_0/r_1.
Teraz staje się jasne, że jeżeli liczba d jest wspólnym dzielnikiem liczb r_0 i r_1 to jest również dzielnikiem reszty r_2.

Kolejne reszty z dzielenia obliczamy według schematu tak długo aż kolejna obliczona reszta $r_m = 0$.

$$\begin{array}{cc|c} a = r_0, \;\; b = r_1 & & reszta \\ - - - - - - - & & - - - \\ \frac{r_0}{r_1} = k_0 + \frac{r_2}{r_1} & | & r_2 = r_0 - k_0 * r_1 \\ \frac{r_1}{r_2} = k_1 + \frac{r_3}{r_2} & | & r_3 = r_1 - k_1 * r_2 \\ \frac{r_2}{r_3} = k_2 + \frac{r_4}{r_3} & | & r_4 = r_2 - k_2 * r_3 \\ \cdots & \cdots & \cdots \\ \frac{r_{m-2}}{r_{m-3}} = k_{m-2} + \frac{r_m}{r_{m-1}} & | & r_m = r_{m-2} - k_{m-2} * r_{m-1} \\ \frac{r_{m-1}}{r_m} = k_{m-1} & | & r_{m+1} = 0 \end{array}$$

Ciąg reszt $r_0 > r_1 > r_2 \cdots > r_{m-1} > r_m$ jest malejący i kończy się na reszcie $r_m \neq 0$, gdyż następne reszty $r_{m+1} = 0,\ r_{m+2} = 0, ...;$ są równe zero.
Ostatnia reszta z dzielenia r_m różna od zera jest największym wspólnym dzielnikiem liczb naturalnych $a = r_0$ i $b = r_1$. Zauważmy, że największy wspólny dzielnik r_m liczb r_0 i r_1 jest również największym wspólnym dzielnikiem wszystkich poprzednich reszt $r_{m-1}, r_{m-2}, \cdots, r_2, r_1, r_0$

Rozszerzony algorytm Euklidesa dotyczy rozwiniętej formy reszt, która prowadzi do rozwiązania równania Diofantosa. Mianowicie, ostatnia reszta różna od zera

$$r_m = NWD(a, b)$$

jest największym wspólnym dzielnikiem liczb a i b.

Zauważmy, że reszty określone są wzorem rekurencyjnym z warunkami początkowymi

$$\begin{array}{rcll} r_0 & = & a, \quad r_1 = b, & warunki\ poczatkowe \\ r_m & = & r_{m-2} - k_{m-2} * r_{m-1}, & m = 2, 3, 4, ...; \end{array}$$

Podstawiają $r_0 = a, \;\; r_1 = b$

do reszty

$$r_2 = r_0 - k_0 * r_1$$

otrzymamy resztę

$$r_2 = a - k_0 * b.$$

Podobnie podstawiając $r_1 = b, \;\; r_2 = a - k_1 * b$

do reszty

$$r_3 = r_1 - k_2 * r_2$$

otrzymamy resztę

$$r_4 = (1 + k_1 * k_2)a - (k_0 + k_2 + k_0 * k_1 * k_2)b.$$

w postaci lewej strony równania Diofantosa o współczynnikach a i b.

Dalej podstawiając na r_2 i r_3 prawe strony powyższych równości, po uporządkowaniu współczynników przy a i b, otrzymamy resztę

$$r_5 = -(k_1 + k_3 + k_* k_2 * k_3)a + (1 + k_0 * k_1 + k_0 * k_3 + k) * k_1 * k_2 * k_3)b.$$

w postaci lewej strony równania Diofantosa o współczynnikach a i b.

Obliczanie następnych reszt $r_6, \;\; r_7, ...; r_m$ przez podstawianie wcześniej określonych reszt przez współczynniki a i b prowadzi do wyrażenia reszty w postaci

$$r_m = a * w_1(k_0, k_1, ..., k_m) + b * w_2(k_0, k_1, ..., k_m)$$

gdzie wielkości

$$w_1(k_0, k_1, k_2, ..., k_m)) \;\; i \;\; w_2(k_0, k_1, ..., k_m)$$

określone są przez dane współczynniki a i b równania Diofantosa.

Ponieważ największy wspólny dzielnik $NWD(a, b) = r_m$ to zachodzi równość

$$a * w_1(k_0, k_1, ..., k_m) + b * w_2(k_0, k_1, ..., k_m) = NWD(a, b)$$

Mnożąc obie strony powyższej równości przez stałą

$$K = \frac{c}{NWD(a, b)}.$$

otrzymamy równość Diofantosa

$$a * K * w_1(k_0, k_1, ..., k_m) + b * K * w_2(k_0, k_1, ..., k_m) = c$$

z której wynika szczególne rozwiązanie równania Diofantosa

$$x = K * w_1(k_0, k_1, ..., k_m), \quad y = K * w_2(k_0, k_1, ..., k_m)$$

Niżej podajemy tablicę wielkości w_1 i w_2 w przypadku $m = 2, 3, 4, 5$

m	$w_1(k_0, k_1, k_2, k_3)$	$w_2(k_0, k_1, k_2, k_3)$
2	1	$-k_0$
3	$-k_1$	$1 + k_1$
4	$1 + k_1 * k_2$	$-(k_0 + k2 + k + 0 * k_1 * k_2)$
5	$-(k_1 + k_3 + k_1 * k_2 * k_3)$	$1 + k_0 * k_1 + k_0 * k_3 + k_2 * k_3 + k_o * k_1 * k_2 * k_3$

Korzystają z systemów obliczeniowych takich jak *Mathematica* [2] obliczamy największy wspólny dzielnik jedną instrukcją

```
GCD[a,b]
```

Na przykład największy wspólny dzielnik liczb $a = 105$ i $b = 56$ obliczamy wykonując instrukcje w systemie *Mathematica*

```
GCD[105,56]
out          7
```

Podobnie można rozwiązać w systemie *Mathematica* jedną instukcją równanie liniowe Diofantosa

$$a * x + b * y = c$$

o współczynnikach całkowitych $a,\ b,\ c$.

```
ExtendedGCD[a,b]

out          { GCD[a,b],{x,y}}
```

Rozpatrzmy następujący przykład:

Przykład 1.23 *Rozwiąż równanie Diofantosa*

$$5 * x + 3 * y = 1$$

w systemie Mathematica

Rozwiązanie:

```
ExtendedGCD[5,3]

out                 {1,{-1,2}}
```

Sprawdzenie rozwiązania $x = -1,\ \ y = 2$

$$5 * (-1) + 3 * 2 = 1$$

[2] Mathematica for doing Mathematics, by Stephen Wolfram

1.6.2 Przykłady

Stosowanie rozszerzonego algorytmu Euklidesa do rozwiązywania liniowych równań Diofantosa jest znacznie prostrze od jego ogólnego opisu. Niżej podajemy kilka przykładów zastosowania rozszerzonego algorytmu Euklidesa.

Przykład 1.24 *Rozwiąż równanie Diofantosa*

$$2 * x + 3 * y = 4. \tag{1.3}$$

Rozwiązanie:
W tym przykładzie łatwo określamy największy wspólny dzielnik współczynników $a = 2,\ b = 3$ i $c = 4$ równania liniowego Diofantosa. Mianowicie

$$NWD(2, 3) = 1$$

Również łatwo sprawdzymy warunek konieczny i wystarczający istnienia rozwiązania tego równania, gdyż największy wspólny dzielnik $NWD(2, 3) = 1$ dzieli współczynnik $c = 4$. Zatem rozwiązanie równiania (1.3) istnieje.
Stosując rozszerzony algorytm Euklidesa zanajdziemy rozwiązanie równania liniowego (1.3).

Mianowicie, najpierw znajdź największy wspólny dzielnik liczb 2 i 3 według schematu

$a = r_0 = 2,\ \ b = r_1 = 3$	$reszta$
$\frac{3}{2} = 1 + \frac{1}{2}$	$r_2 = 3 - 1 * 2 = 1$
$\frac{2}{1} = 2$	$r_3 = 0$

Skąd piszemy największy wspólny dzielnik $N(2, 3) = r_2 = 1$ w postaci równości

$$3 - 2 * 1 = 1 \quad lub \quad 2 * (-1) + 3 * 1 = 1$$

Zauważamy, że tutaj

$$\begin{aligned} &m = 2, \\ &k_0 = 1, \qquad\qquad k_1 = 0, \\ &w_1(k_0, k_1) = -1, \quad w_2(k_0, k_1) = 1, \\ &K = 4 \end{aligned}$$

Mnożąc powyższą równość przez stałą $K = 4$, otrzymamy wyrażenie Diofantosa tego równania

$$2 * 4 * (-1) + 3 * 4 * 1 = 4$$

skąd wynika rozwiązanie szczególne

$$x = 4 * (-1) = -4 \quad i \quad y = 4 * 1 = 4$$

Sprawdzenie:

$$2 * x + 3 * y = 2 * (-4) + 3 * 4 = 4$$

Przykład 1.25 *Rozwiąż równanie Diofantosa*

$$16 * x + 7 * y = 11. \tag{1.4}$$

Rozwiązanie:
W tym przykładzie łatwo określamy największy wspólny dzielnik współczynników $a = 16,\ b = 7$ równania liniowego Diofantosa. Mianowicie

$$NWD(16, 7) = 1$$

Również łatwo sprawdzymy warunek konieczny i wystarczający istnienia rozwiązania tego równania, gdyż największy wspólny dzielnik $NWD(16, 7) = 1$ dzieli współczynnik $c = 11$. Zatem rozwiązanie równiania (1.4) istnieje.
Stosując rozszerzony algorytm Euklidesa zanajdziemy rozwiązanie równania liniowego (1.4).

Mianowicie, najpierw znajdź największy wspólny dzielnik liczb 16 i 7 według schematu

$$\begin{array}{ll} a = r_0 = 16, \ \ b = r_1 = 7 & | \ \ reszta \\ - - - - - - - - - - - & \quad - - - - - - - - - - \\ \frac{16}{7} = 2 + \frac{2}{7} & | \ \ r_2 = 16 - 7 * 2 = 2 \\ \frac{7}{2} = 3 + \frac{1}{7} & | \ \ r_3 = 7 - 3 * 2 = 1 \\ \frac{2}{1} = 2 & | \ \ r_4 = 0. \end{array}$$

Skąd piszemy największy wspólny dzielnik $N(16, 7) = r_3 = 1$ w postaci równości

$$r_3 = 7 - 3 * 2 = 1 \quad lub \quad r_3 = 7 * 1 - 3 * (16 - 7 * 2) = 1, \quad 16 * (-3) + 7 * 7 * 1 = 1$$

Zauważamy, że tutaj

$$\begin{array}{ll} m = 3, & \\ k_0 = 2, & k_1 = 3, \ \ k_2 = 2 \\ w_1(k_0, k_1, k_2) = -3, & w_2(k_0, k_1, k_2) = 7, \\ K = 11 & \end{array}$$

Mnożąc powyższą równość przez stałą $K = 11$, otrzymamy wyrażenie Diofatosa tego równania

$$16 * 11 * (-3) + 7 * 11 * 7 = 11$$

Skąd wynika rozwiązanie szczególne

$$x = 11 * (-3) = -33 \quad i \quad y = 11 * 7 = 77.$$

Sprawdzenie:

$$16 * x + 7 * y = 16 * (-33) + 7 * 77 = 11$$

Rozwiążmy następne równanie z większą ilością obliczanych reszt.

Przykład 1.26 *Rozwiąż równanie liniowe Diofantosa*

$$975 * x + 690 * y = 360 \tag{1.5}$$

Rozwiązanie:

Niżej znajdujemy największy wspólny dzielnik równania (1.5) stosując rozszerzony algorytm Euklidesa, żeby znaleść rozwiązania równania (1.5). To równanie ma rozwiązanie, gdyż spełnia warunek konieczny i wystarczający. Mianowicie, największy wspólny dzielnik $NWD(975, 690) = 15$ dzieli współczynnik $c = 360$

$a = r_0 = 975,\ b = r_1 = 690$	$reszta$
$anie$	
$\frac{975}{690} = 1 + \frac{285}{690}$	$r_2 = 975 - 1 * 690 = 285$
$\frac{690}{285} = 2 + \frac{120}{285}$	$r_3 = 690 - 2 * 285 = 120$
$\frac{285}{120} = 2 + \frac{45}{120}$	$r_4 = 285 - 2 * 120 = 45$
$\frac{120}{45} = 2 + \frac{30}{45}$	$r_5 = 120 - 2 * 45 = 30$
$\frac{45}{30} = 1 + \frac{15}{30}$	$r_6 = 45 - 1 * 30 = 15$

Ciąg reszt

$$975 > 690 > 285 > 120 > 45 > 30 > 15$$

jest malejący.
Ostatnia reszta z dzielenia $r_6 = 15$ różna od zera jest największym wspólnym dzielnikiem liczb naturalnych $a = r_0 = 975$ i $b = r_1 = 690$. Zauważmy, że największy wspólny dzielnik $r_6 = NWD(975, 690) = 15$ jest również największym wspólnym dzielnikiem wszystkich poprzednich reszt

$$r_2 = 285,\ r_3 = 120,\ r_4 = 45,\ r_5 = 30,\ r_6 = 15.$$

Dalej stosujemy roszerzenie algorytmu Euklidesa, żeby znaleść rozwiązanie równania (1.5). W tym celu zapiszemy resztę $r_6 = NWD(975, 690) = 15$ w postaci wyrażenia Diofantosa równania (1.5).

$$\begin{aligned} r_6 &= 45 - 1 * 30 \\ &= 45 - (120 - 2 * 45) \\ &= 45 - (120 - 2 * (285 - 2 * 120)) \\ &= 45 - (120 - 2 * (285 - 2 * (690 - 2 * 285))) \\ &= 45 - (120 - 2 * (285 - 2 * (690 - 2 * (975 - 1 * 690)))) \\ &= 975 * (17 * 24) + 690 * (-24 * 24) \end{aligned}$$

Wyrażenie Diofantosa równania (1.5) otrzymamy zbierając współczynników przy współczynnikach równania $a = 975$ i $b = 690$

$$975 * (408) + 690(-576) = 15$$

Mnożąc obie strony powyższej równości przez stałą

$$K = \frac{c}{NWD[a, b]} = \frac{360}{15} = 24$$

otrzymamy równość Diofantosa dla równania (1.5).
Skąd rozwiązanie szczególne równania (1.5)

$$x = w_1 = 408, \quad y = w_2 = -576.$$

Sprawdzenie:

$$975 * 408 - 690 * 576 = 360.$$

Przykład 1.27 *Rozwiąż równanie Diofatosa*

$$42 * x + 36 * y = 78 \tag{1.6}$$

Największy wspólny dzielnik $NWD(42, 78) = 6$ współczynników $a = 42$ i $c = 78$ dzieli współczynnik $b = 36$. Zatem rozwiązanie tego równania istnieje.

Stosując rozszerzony algorytm Euklidesa, obliczmy największy wspólny dzielnik liczb $a = 78$ i $b = 42$ i jednocześnie znajdziemy rozwiązanie równania (1.6). W liczbie $a = 78$ liczba $b = 42$ miejści się raz i zostaje reszta 36.

Dalej wykonujemy dzielenia według schematu

$$\begin{array}{rcl} a = 78, \;\; b = 42 & | & reszta \\ - - - - - - - - & & - - - \\ \dfrac{78}{42} = 1 + \dfrac{36}{78} & | & 36 = 78 - 42 \\ \dfrac{42}{36} = 1 + \dfrac{6}{36} & | & 6 = 42 - 36 \\ \dfrac{36}{6} = 6 & | & 0 \end{array}$$

Rozwiązanie równania (1.6) otrzymamy wyrażając ostatnią resztę 6 przez reszty poprzednie.

Mianowucie, piszemy

$$6 = 42 - 36$$

Mnożąc obie strony przez $\dfrac{78}{6} = 13$ otrzymamy wyrażenie Diofantosa

$$42 * 13 - 36 * 13 = 6 * 13 = 78$$

Skąd otrzymamy rozwiązanie szczególne równnia (1.6)

$$x = w_1 = 13, \;\; |; \; y = w_2 = -13.$$

Sprawdzenie:

Podstawiając do równaia (1.6) $x = 13, \;\; y = -13$, otrzymamy równość

$$42 * 13 - 36 * 13 = 78$$

1.7 Zadania

Zadanie 1.9 *Oblicz*

(i) $8 + 10(mod\ 4) =$

(ii) $2 + 5(mod\ 7) =$

(iii) $12(mod\ 7) + 13(mod\ 8) =$

Zadanie 1.10 *Dodaj, odejmij i pomnóż stronami kongruencje. Sprawdź wyniki tych operacji.*

$$18 \equiv 10(mod\ 4)$$

oraz

$$25 \equiv 17(mod\ 4)$$

Zadanie 1.11 *Znajdź największy wspólny dzielnik liczb* $a = 105$ *i* $b = 91$

Zadanie 1.12 *Znajdź największy wspólny dzielnik liczb* $a = 1995$ *i* $b = 1190$

Zadanie 1.13 *Rozwiąż równanie Diofantosa*

$$25 * x + 12 * y = 1$$

Zadanie 1.14 *Rozwiąż równanie Diofantosa*

$$5 * x - 3 * y = 9$$