0.1 Liczby przystające

Dzielenie liczb całkowitych z resztą łączy się z pojęciem liczb przystających i operacją modulo, to jest z kongruenją.
Kongruencja czyli przystawania liczb całkowitych a i b względem liczby naturalnej n wykracza poza podstawę programową. Jednak jest istotnym tematem w programie rozszerzonym matematyki. 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.

Karol Gauss (1777-1835 n.e.) wprowadził oznaczenia operacji modulo na liczbach całkowitych

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

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

$$(a-b) : n = k \qquad lub \qquad \frac{a-b}{n} = k, \qquad a - b = k * n$$

dla pewnej liczby całkowitej k.

Przykład 0.1 *Pisząc*

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

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

$$(27-13) : 7 = 14 : 2 = 2, \qquad lub \qquad \frac{27-13}{7} = 2, \qquad 27 - 13 = 2 * 7$$

gdzie $a = 27,\ b = 13,\ n = 7,\ k = 2.$

Resztę r z dzielenia liczby całkowitej a przez liczbę naturalną n obliczamy stosując operację modulo. Mianowicie piszmy

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

Na przykład dla $a = 7$ i $n = 3$ reszta $r = 1$, ponieważ

$$7 : 3 = 2 + \frac{1}{7}.$$

Wynik dzielenia $7 : 3$ to jest 2 całe i reszta 1.

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

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

Zauważmy, że liczby całkowite a i b są przystające względem liczby naturalnej n, wtedy i tylko wtedy, jeżeli podzielone przez n mają tą samą resztę r
Na przykład

7 przystaje do 3 względem 2, ponieważ różnica

$$(7-3) : 2 = 2$$

jest podzielna przez 2, reszta $r = 0$.
Również z dzielenia liczby 7 przez 2 i z dzielenia liczby 3 przez 2 mamy tą samą resztę $r = 1$.

$$7 : 2 = 3 + reszta\ 1 \ \ oraz \ \ 3 : 2 = 1 + reszta\ 1$$

0.2 Dzielenie modulo

Wynik dzielenia modulo liczby całkowitej a przez liczbę naturalą n równy jest reszcie z dzielenia liczby a przez liczbę n.
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 dzielenia

$$25 : 15 = \frac{25}{15} = 1 + \frac{10}{15}$$

$$37 : 12 = \frac{37}{12} = 3 + \frac{1}{12}$$

Przykład 0.2 *Oblicz* $47(mod\ 5)$

Obliczamy

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

Odpowiedź:

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

Przykład 0.3 *Oblicz* $123(mod\ 7)$

Obliczamy

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

Odpowiedź:

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

0.2.1 Własności operacji modulo

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

1. **Własnośc symetrii**

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

   Przykład 0.4 *Liczba* 15 *przystaje do liczby* 3 *modulo* 4 *i liczba* 3 *przystaje do liczby* 15 *modulo* 4, *piszemy*

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

2. **Operacja przechodnia**

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

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

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

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

   Własnośc przystawania liczb a, b względem n przechodzi na liczby a, c.

Przykład 0.5 *Rozpatrzmy dwie kongruencje*

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

Tutaj mamy

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

Zauważamy, że liczby $a = 20$ i $c = 8$ też są przystające względem liczby 4, gdyż różnica

$$20 - 8 = 12$$

jest podzielna przez 4.

3. **Dodawanie kongruencji.** Kongruencje możemy dodawać stronami.
To znaczy, jeżeli a przystaje do b modulo n i c przystaje do d modulo n
to

$$a + c \quad przystaqje\ do \quad b + d \quad modulo\ \ n.$$

Wtedy piszemy, jeżeli

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

to

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

Przykład 0.6 *Rozpatrzmy dwie kongruencje*

$$15 \equiv 3(mod\ 4) \qquad i \quad 37 \equiv 5(mod\ 4)$$

Tutaj mamy

$$a = 15, \quad b = 3 \quad c = 37, \quad d = 5, \quad n = 4.$$

Sumując stronami powyższe kongruencje otrzymamy kongruencje prawdziwą

$$15 + 37 \equiv\ 3 + 5(mod\ 4), \qquad 52 \equiv 8\ (mod\ 4),$$

ponieważ $(52 - 8) : 4 = 44 : 4 = 11$.

4. **Mnożenie kongruencji przez siebie.** Kongruencję możemy mnożyć stronami

$$a \equiv b(mod\ n), \quad a^2 \equiv b^2(\text{mod } n), \quad a^3 \equiv b^3(mod\ n), \quad ... \quad , a^k \equiv b^k(mod\ n),$$

dla każdego naturalnego $k = 1, 2, 3, ...$;
Jasne, że jeżeli a przystaje do b modulo n to $a - b$ jest podzielne przez n. Piszemy

$$a \equiv b(mod\ n), \quad to \quad (a - b)\ \ jest\ podzielne\ przez\ n.$$

Również a^2 przystaje do b^2 modulo n. Piszemy

$$a^2 \equiv b^2(mod\ n), \quad bo \quad (a^2 - b^2) = (a - b)(a + b)\ \ jest\ podzielne\ przez\ n$$

Przykład 0.7 *Rozpatrzmy kongruencje*

$$9 \equiv 3(mod\ 2)$$

Tutaj mamy

$$a = 9, \quad b = 3, \quad n = 2.$$

Mnożąc tą kongruencje stronami, otrzymamy

$$9 \equiv 3(mod\ 2), \quad 9^2 \equiv 3^2(\text{mod } 2), \quad 9^3 \equiv 3^3(mod\ 2), \quad \ldots \quad , 9^k \equiv 3^k(mod\ 2),$$

dla każdego naturalnego $k = 1, 2, 3, ...;$
Sprawdzamy, że powyższe kongruencje są prawdziwe. Mianowicie, 9 przystaje do 3 modulo 2, ponieważ $9 - 3 = 6$ jest podzielne przez 2. Piszemy

$$9 \equiv 3(mod\ 2), \quad bo \quad (9 - 3) : 2 = 6 : 2 = 3.$$

Podobnie, 9^2 przystaje do 3^2 modulo 2, ponieważ

$$9^2 - 3^2 = 81 - 9 = 72$$

jest podzielne przez 2. Piszemy

$$9^2 \equiv 3^2(mod\ 2), \quad bo \quad (9^2 - 3^2) : 2 = (81 - 9) : 2 = 72 : 2 = 36.$$

Sprawdzamy, że 9^3 przystaje do 3^3 modulo 2

$$(9^3 - 3^3) : 2 = (729 - 27) : 2 = 702 : 2 = 351.$$

Ogólnie różnica $9^k - 3^k$ jest również podzielna przez 2 dla każdego $k = 1, 2, 3, ...;$.
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 parzysta i podzielna przez 2 dla każdej liczby naturalnej $k = 1, 2, 3, ...;$
Skąd wynika, że 9^k przystaje do 3^k modulo 2 dla każdego $k = 1, 2, 3, ...;$

Przykład 0.8 *Stosując operację modulo sprawdź, że liczba*

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

jest podzielna przez 10.

Rozwiązanie. 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

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

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

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

jest podzielna przez 10.

Przykład 0.9 *Stosując własność mnożenia 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.

0.2.2 Równanie liniowe kongruencji

Ogólna postać równania liniowego kongruencji

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

W tym równaniu dane współczynniki a, b są liczbami całkowitymi, oraz n jest daną liczbą naturalną. Natomiast x jest niewiadomą, której wartości całkowitej szukamy.
Rozwiązać kongruencję liniową to znaczy znaleźć wszystkie wartości całkowite x dla których liczba $a * x$ przystaje do liczby b modulo n.
Zauważmy, że x spełnia równanie

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

wtedy i tylko wtedy, jeżeli różnica $a * x - b$ jest podzielna przez n.
Wtedy mamy następujące równości

$$(a * x - b) : n = k \quad lub \quad \frac{ax - b}{n} = k \quad lub \quad ax - b = k * n$$

dla pewnego całkowitego k.
W pierwszej kolejności powstaje pytanie, 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 taka, że

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

- więcej niż jedno rozwiązanie $x_1, x_2, ..., x_k, ...$; które spełniają rownanie

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

- kongruencja nie ma rozwiązań.

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

Warunek konieczny i wystarczający
Równanie liniowej kongruencji

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

ma rozwiązanie wtedy i tylko wtedy, gdy największy wspólny dzielnik $NWD(a, n)$ liczb a i n jest dzielnikiem liczby b, to znaczy $NWD(a, b)|n$.
Niżej podamy kilka przykładów rozwiązania kongruencji liniowych.

Przykład 0.10 *Rozwiąż równanie*

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

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

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

nie dzieli współczynnika

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

Zatem nie istnieje rozwiązanie tej kongruencji.

Przykład 0.11 *Rozwiąż równanie*

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

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 $k = 0, \pm1, \pm2, \pm3, ...;$

Skąd obliczamy rozwiązanie

$$3 * x = 9 * k + 6, \quad x_k = 3 * k + 2, \quad dla \quad k = 0, \pm1, \pm2, \pm3, ...;$$

Sprawdzenie:

Podstwiając rozwiązanie

$$x_k = 3 * k + 2, \quad dla \quad k = 0, \pm1, \pm2, \pm3, ...;$$

do kongruencji

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

otrzymamy

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

Skąd wynika, że

$$3 * x_k - 6 = (9 * k + 6 - 6) = 9k$$

jest podzielne przez 9 dla każdej całkowitej wartości $k = 0, \pm 1, \pm 2, \pm 3, ...;$
Zatem $x_k = 3 * k + 2$ spełnia równanie kongruencji

$$3 * x_k \equiv 6(mod\ 9), \quad k = 0, \pm 1, \pm 2, \pm 3, ...;$$

0.3 Równanie liniowe Diofantosa

Ogólna postać równania liniowego Diofantosa

$$a * x + b * y = c, \tag{1}$$

gdzie dane współczynniki $a,\ b,\ c$ są liczbami całkowitymi. Rozwiązania x, y szukamy również w liczbach całkowitych.

0.3.1 Warunek konieczny i dostateczny istnienia rozwiązania równania Diofantosa.

Równanie liniowe Diofantosa o współczynnikach całkowitych $a,\ b,\ c$

$$a * x + b * y = c \tag{2}$$

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

0.4 Rozwiązanie równania Diofantosa

Algorytm Euklidesa wyznaczania największego wspólnego dzielnika $NWD(a, b) = r_m$ prowadzi do rozwiązania równania Diofantosa. Przed podaniem ogólnego opisu rozszerzonego algorytmu Euklidesa i jego zastosowania do rozwiązania równania Diofantosa, niżej podamy kilka przykładów.

Przykład 0.12 *Rozwiąż równanie Diofantosa*

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

Rozwiązanie:
W tym przykładzie łatwo określamy największy wspólny dzielnik współczynników

$$a = 3,\ b = 2$$

równania liniowego Diofantosa

$$3 * x + 2 * y = 4.$$

Mianowicie

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

Również łatwo sprawdzamy warunek konieczny i wystarczający istnienia rozwiązania tego równania, gdyż największy wspólny dzielnik $NWD(3,2) = 1$ dzieli wyraz wolny $c = 4$. Zatem rozwiązanie istnieje.
Stosując rozszerzony algorytm Euklidesa znajdziemy rozwiązanie równania liniowego Diofantosa.

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

$$\begin{array}{l|l} a = r_0 = 3, \;\; b = r_1 = 2 & reszta \\ - - - - - - - - - - - - & - - - - - - - - - - \\ \dfrac{r_0}{r_1} = \dfrac{3}{2} = 1 + \dfrac{1}{2} & r_2 = r_0 - r_1 = \underbrace{3 - 1 * 2 = 1} \\ \dfrac{r_1}{r_2} = \dfrac{2}{1} = 2 & r_3 = 0 \end{array}$$

Największy wspólny dzielnik

$$N(3,2) = r_2 = 3 - 1 * 2 = 1$$

piszemy w postaci równości

$$r_0 - r_1 = 1 \quad lub \quad 3 - 2 * 1 = 1.$$

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

$$4 * r_0 - 4 * r_1 = 4 \quad lub \quad 3 * \underbrace{4} + 2 * \underbrace{(-4 * 1)} = 4.$$

Skąd wynika rozwiązanie szczególne

$$x = \underbrace{4}, \qquad y = \underbrace{-4}.$$

Sprawdzenie:

$$3 * x + 2 * y = 3 * 4 - 2 * 4 = 4.$$

Przykład 0.13 *Rozwiąż równanie Diofantosa*

$$16 * x + 7 * y = 11. \tag{4}$$

Rozwiązanie:
W tym przykładzie łatwo określamy największy wspólny dzielnik współczynników

$$a = 16, \quad b = 7$$

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 wyraz wolny $c = 11$. Zatem rozwiązanie równiania (4) istnieje.
Stosując rozszerzony algorytm Euklidesa zanajdziemy rozwiązanie równania liniowego (4).

Mianowicie, najpierw znajdziemy największy wspólny dzielnik współczynników $a = 16$ i $b = 7$ według niżej podanego schematu

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

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

$$r_1 - 3 * r_2 = 1, \qquad 7 - 3 * 2 = 1$$

lub

$$7 * 1 - 3 * \underbrace{(16 - 7 * 2)}_{r_2} = 1,$$

lub rownosc Diofantesa

$$\underbrace{16}_{a} * (-3) + \underbrace{7}_{b} * 7 * 1 = 1.$$

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

$$\underbrace{16}_{a} * \underbrace{11 * (-3)}_{x} + \underbrace{7}_{b} * \underbrace{11 * 7}_{y} = 11$$

Skąd wynika rozwiązanie szczególne

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

Sprawdzenie:

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

Przykład 0.14 *Rozwiąż równanie Diofatosa*

$$78 * x + 42 * y = 36 \tag{5}$$

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

Stosując rozszerzony algorytm Euklidesa, obliczmy największy wspólny dzielnik liczb $a = 78$ i $b = 42$ i jednocześnie znajdziemy rozwiązanie równania (5).
W liczbie $a = 78$ liczba $b = 42$ miejści się raz i zostaje reszta 36.
Dalej wykonujemy dzielenia według schematu

$$\begin{array}{ll} a = r_0 = 78, \;\; b = r_1 = 42 & | \quad reszta \\ - - - - - - - - & \quad - - - - - - - - - - - - - \\ \frac{r_0}{r_1} = \frac{78}{42} = 1 + \frac{36}{78} & | \quad r_2 = r_0 - r_1 = 78 - 42 = 36 \\ \frac{r_1}{r_2} = \frac{42}{36} = 1 + \frac{6}{36} & | \quad r_3 = r_1 - r_2 = 42 - 36 = 6 \\ \frac{36}{6} = 6 & | \quad r_4 = 0 \end{array}$$

Rozwiązanie równania (5) otrzymamy wyrażając ostatnią resztę $r_3 = 6$ przez poprzednią resztę $r_2 = 36$ i przez dane współczynniki $a = r_0 = 78,\ b = r_1 = 42$

Mianowucie, piszemy

$$r_3 = r_1 - r_2 = 6,$$

$$r_3 = r_1 - \underbrace{(r_0 - r_1)}_{r_2} = 2r_1 - r_0 = 6,$$

$$2 * \underbrace{42}_{r_1} - \underbrace{78}_{r_0} = 6$$

Mnożąc obie strony ostatniej równości przez stałą $K = \dfrac{36}{6} = 6$ otrzymamy wyrażenie Diofantosa

$$2 * 42 * 6 - 78 * 6 = 6 * 6, \quad lub \quad 42 * \underbrace{2 * 6}_{x} + 78 * \underbrace{(-6)}_{y} = 36.$$

Skąd otrzymamy rozwiązanie szczególne równnia (5)

$$x = 2 * 6 = 12, \qquad y = -6.$$

Sprawdzenie:

Podstawiając do równaia (5) $x = 12,\ \ y = -6$, otrzymamy równość

$$42 * 12 - 78 * 6 = 36.$$

Rozwiążmy następne równanie z większą ilością obliczanych reszt.

Przykład 0.15 *Rozwiąż równanie liniowe Diofantosa*

$$975 * x + 690 * y = 360 \tag{6}$$

Rozwiązanie:

To równanie ma rozwiązanie, gdyż spełnia warunek konieczny i wystarczający. Mianowicie, największy wspólny dzielnika $NWD(975, 690) = 15$ jest dzielnikiem wyrazu wolnego $c = 360$ ponieważ $360 : 15 = 20$. Zatem istnieje rozwiązanie tego równania.
Rozwiązanie równania (6) znajdziemy stosując algorytm Euklidesa wyznaczania największego wspólnego dzielnika współczynników $a = 975$ i $b = 690$ równania Diofantesa (6). Zatem obliczamy kolejne reszty według niżej podanego schematu

$a = r_0 = 975,\ b = r_1 = 690$	$reszta$
$\dfrac{r_0}{r_1} = \dfrac{975}{690} = 1 + \dfrac{285}{690}$	$r_2 = 975 - 1 * 690 = 285$
$\dfrac{r_1}{r_2} = \dfrac{690}{285} = 2 + \dfrac{120}{285}$	$r_3 = 690 - 2 * 285 = 120$
$\dfrac{r_2}{r_3} = \dfrac{285}{120} = 2 + \dfrac{45}{120}$	$r_4 = 285 - 2 * 120 = 45$
$\dfrac{r_3}{r_4} = \dfrac{120}{45} = 2 + \dfrac{30}{45}$	$r_5 = 120 - 2 * 45 = 30$
$\dfrac{r_4}{r_5} = \dfrac{45}{30} = 1 + \dfrac{15}{30}$	$r_6 = 45 - 1 * 30 = 15$
$\dfrac{r_5}{r_6} = \dfrac{30}{15} = 2$	$r_7 = 0$

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. W tym celu napiszemy resztę

$$r_6 = r_4 - r_5 = 15$$

w postaci która jest określona przez dane współczynniki $a = r_0 = 975$ i $b = r_1 = 690$. Mianowicie, mamy wzór rekurencyny, ponieważ każda reszta następna określona jest przez dwie reszty poprzednie

$$\begin{aligned}
r_2 &= r_0 - r_1,\\
r_3 &= r_1 - 2 * r_2 = r_1 - 2 * \underbrace{(r_0 - r_1)}_{r_2} = 3r_1 - 2r_0,\\
r_4 &= r_2 - 2 * r_3 = \underbrace{r_0 - r_1}_{r_2} - 2\,\underbrace{(3r_1 - 2r_0)}_{r_3} = 5r_0 - 7r_1,\\
r_5 &= r_3 - 2 * r_4 = \underbrace{3r_1 - 2r_0}_{r_3} - 2\,\underbrace{(5r_0 - 7r_1)}_{r_4} = 17r_1 - 12r_0,\\
r_6 &= r_4 - r_5 = \underbrace{5r_0 - 7r_1}_{r_4} - \underbrace{(17r_1 - 12r_0)}_{r_5} = 17r_0 - 24r_1.
\end{aligned}$$

Z ostatniego z powyższych wyrażeń mamy równość

$$17r_0 - 24r_1 = 15 \quad bo \quad 17 * \underbrace{975}_{r_0} - 24 * \underbrace{690}_{r_1} = 15.$$

Mnożąc obie strony powyższej równości przez stałą

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

otrzymamy równość Diofantosa

$$\begin{aligned}
&975 * 17 * 24 - 690 * 24 * 24 = 15 * 24,\\
&975 * \underbrace{408}_{x} + 690 * \underbrace{(-576)}_{y} = 360.
\end{aligned}$$

Skąd otrzymujemy rozwiązanie szczególne równania (6)

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

Sprawdzenie:

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

0.5 Rozszerzony algorytm Euklidesa

Niżej podamy ogólny opis rozszerzonego algorytmu Euklidesa. Najpierw 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 $r_0 - r_1$.
Mianowicie 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 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

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

Ciąg reszt

$$r_0 > r_1 > r_2 \cdots > r_{m-1} > r_m$$

jest malejący i kończy się na ostatniej reszcie $r_m \neq 0$. Następne reszty $r_{m+1} = 0,\ r_{m+2} = 0, ...;$ są równe zero.
Ostatnia reszta z dzielenia $r_m \neq 0$ różna od zera jest największym wspólnym dzielnikiem liczb całkowitych $a = r_0$ i $b = r_1$. Tutaj kończy się algorytm Euklidesa znajdowania największego wspólnego dzielnika danych dwóch liczb całkowitych.
Teraz zauważmy, że największy wspólny dzielnik $d = r_m$ 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

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

jest największym wspólnym dzielnikiem liczb $a = r_0$ i $b = r_1$.

Kolejne reszty podane w powyżeszej tabeli są określone wzorem rekurencyjnym z warunkami początkowymi

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

Podstawiają $r_0 = a,\ \ r_1 = b$ do reszty

$$r_2 = r_0 - k_0 * r_1$$

otrzymamy resztę

$$r_2 = a - k_0 * b$$

określoną przez dane liczby całkowite a i b.
Podobnie podstawiając $r_1 = b,\ \ r_2 = a - k_0 * b$ do reszty

$$r_3 = r_1 - k_1 * r_2$$

otrzymamy resztę

$$r_3 = b - k_1(a - k_0 * b) = a(-k_1) + b(1 + k_0 * k_1)$$

określoną przez dane liczby całkowite a i b.
Również podstawmy do reszty

$$r_4 = r_2 - k_2 * r_3$$

już określone reszty r_2 i r_4 przez dane a i b

$$r_2 = a - k_0 * b \qquad i \qquad r_3 = a(-k_1) + b(1 + k_0 * k_1).$$

Wtedy otrzymamy resztę

$$\begin{aligned} r_4 &= a - k_0 * b - k_2(-a * k_1 + b(1 + k + 0 * k_1)) \\ &= a(1 + k_1 * k_2) - b(k_0 + k_2 + k_0 * k_1 * k_2) \end{aligned}$$

określoną przez liczby całkwite a i b.

Dalej podstawmy do reszty

$$r_5 = r_3 - k_3 * r_4$$

już określone reszty r_3 i r_4 przez dane liczby całkowite a i b.
Po uporządkowaniu współczynników przy a i b, otrzymamy resztę

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

określoną przez dane liczby całkwite a i b.
Obliczanie następnych reszt $r_6,\ r_7, ...; r_m$ przez podstawianie wcześniej określonych reszt przez liczby całkowitete a i b prowadzi do wyrażenia reszty r_m 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 całkowite 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* [1] 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 0.16 *Rozwiąż równanie Diofantosa*

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

w systemie Mathematica

Rozwiązanie:

```
ExtendedGCD[5,3]

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

Sprawdzenie rozwiązania $NWD(5, 3) = 1, \quad x = -1,\ \ y = 2.$

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

[1] Mathematica for doing Mathematics, by Stephen Wolfram

0.6 Zadania

Zadanie 0.1 *Oblicz*

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

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

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

Zadanie 0.2 *Dodaj, odejmij i pomnóż stronami kongruencje:*

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

oraz

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

Sprawdź wyniki tych operacji.

Zadanie 0.3 *Znajdź największy wspólny dzielnik liczb* $a = 105$ *i* $b = 91$.

Zadanie 0.4 *Znajdź największy wspólny dzielnik liczb* $a = 1995$ *i* $b = 1190$.

Zadanie 0.5 *Rozwiąż równanie Diofantosa*

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

Zadanie 0.6 *Rozwiąż równanie Diofantosa*

$$9 * x - 6 * y = 12.$$