Wybrane pojęcia i twierdzenia z wykładu z teorii liczb

1. Podzielność

Przedmiotem badań teorii liczb są własności liczb całkowitych.

Zbiór liczb całkowitych oznaczać będziemy symbolem $\mathbb{Z}$.
Zbiór liczb naturalnych oznaczać będziemy symbolem $\mathbb{N}$.

Zasada minimum. Jeśli zbiór X jest niepustym podzbiorem zbioru liczb naturalnych, to w zbiorze X istnieje liczba najmniejsza.

Definicja. Liczba całkowita b jest podzielna przez liczbę całkowitą a $(a \neq 0)$, jeśli istnieje taka liczba całkowita k, że $b = k\,a$.

Piszemy wtedy $a \mid b$ i czytamy:
(i) a dzieli b,
(ii) a jest podzielnikiem b,
(iii) b jest podzielna przez a.
Jeśli liczba całkowita b nie jest podzielna przez liczbę całkowitą a, to piszemy $a \nmid b$.

Twierdzenie. Niech $a, b, c, m \in \mathbb{Z}$, przy czym $a, m \neq 0$.

(1) Jeśli $a \mid b$, to $a \mid b\,c$.

(2) Jeśli $a \mid b$ i $b \mid c$, to $a \mid c$, $(b \neq 0)$.

(3) Jeśli $a \mid b$ i $a \mid c$, to $a \mid (bx + cy)$ dla dowolnych $x, y \in \mathbb{Z}$.

(4) Jeśli $a \mid b$ i $b \mid a$, to $|a| = |b|$ $(b \neq 0)$.

(5) Jeśli $a \mid b$ i $a > 0$, $b > 0$, to $a \leq b$.

(6) $a \mid b$ wtedy i tylko wtedy gdy $m\,a \mid m\,b$.

Twierdzenie. Dla dowolnej liczby całkowitej b i dowolnej liczby całkowitej $a \neq 0$, istnieją liczby całkowite k i r, takie, że

$$b = k\,a + r, \quad 0 \leq r < |a|\,.$$

Jeśli $a \nmid b$, to zachodzi nierówność ostra.

Liczbę r nazywamy resztą z dzielenia liczby b przez liczbę a.

Definicja największego wspólnego dzielnika. Liczbę $a \in \mathbb{Z}\setminus\{0\}$ nazywamy wspólnym dzielnikiem liczb całkowitych b i c, jeśli $a \mid b$ i $a \mid c$. Jeśli przynajmniej jedna sposród liczb b i c jest różna od zera, to wśród wspólnych dzielników liczb b, c (których jest skończenie wiele) istnieje największy. Ten największy spośród wspólnych dzielników liczb b,c nazywamy największym wspólnym dzielnikiem liczb b i c.

Największy wspólny dzielnik liczb b i c oznaczamy symbolem (b, c) lub $\mathrm{Nwd}(b, c)$.

W podobny sposób definiujemy największy wspólny dzielnik liczb całkowitych $b_1, b_2, ...b_n$ z których przynajmniej jedna jest różna od zera. Dzielnik ten oznaczamy symbolem $(b_1, b_2, ...b_n)$.

Twierdzenie. Jeśli $g = (b, c)$ jest największym wspólnym dzielnikiem liczb całkowitych b i c, to istnieją liczby całkowite x_0, y_0 takie, że

$$g = b\,x_0 + c\,y_0.$$

Innymi słowy: największy wspólny dzielnik liczb całkowitych b i c jest kombinacją liniową tych liczb o współczynikach całkowitych.

Twierdzenie. Największy wspólny dzielnik liczb całkowitych b i c może być scharakteryzowany w następujący sposob:

(1) Jako najmniejsza liczba naturalna należąca do zbioru

$$A = \{bx + cy : x, y \in \mathbb{Z}\}.$$

(2) Jako wspólny naturalny dzielnik liczb b i c podzielny przez każdy inny wspólny dzielnik tych liczb.

Twierdzenie (Algorytm Euklidesa). Niech b i c będą dwiema liczbami całkowitymi, przy czym $c > 0$. Największy wspólny dzielnik liczb b i c może być obliczony przy pomocy serii równości:

$$\begin{array}{rcrcll}
b & = & k_1 \cdot c & + & r_1, & 0 < r_1 < c, \\
c & = & k_2 \cdot r_1 & + & r_2, & 0 < r_2 < r_1, \\
r_1 & = & k_3 \cdot r_2 & + & r_3, & 0 < r_3 < r_2, \\
r_2 & = & k_4 \cdot r_3 & + & r_4, & 0 < r_4 < r_3, \\
 & & & \vdots & & \vdots \\
r_{j-2} & = & k_j \cdot r_{j-1} & + & r_j, & 0 < r_j < r_{j-1}, \\
r_{j-1} & = & k_{j+1} \cdot r_j. & & &
\end{array}$$

Ostatnia **reszta** r_j **jest największym wspólnym** dzielnikiem liczb b i c.

Przykład. Niech $b = 3102$, $c = 1044$. Algorytm Euklidesa daje nam równości

$$\begin{array}{rcrcl}
3102 & = & 2 \cdot 1044 & + & 1014, \\
1044 & = & 1 \cdot 1014 & + & 30, \\
1014 & = & 33 \cdot 30 & + & 24, \\
30 & = & 1 \cdot 24 & + & 6, \\
24 & = & 4 \cdot 6. & &
\end{array}$$

Ostatnia reszta jest równa 6. Zatem $(3102, 1044) = 6$.

Z poprzednich równości otrzymujemy kolejno

$$\begin{aligned}
6 &= 30 - 1 \cdot 24 = 30 - (1014 - 33 \cdot 30) = 34 \cdot 30 - 1014 = \\
&= 34 \cdot (1044 - 1014) - 1014 = 34 \cdot 1044 - 35 \cdot 1014 = \\
&= 34 \cdot 1044 - 35 \cdot (3102 - 2 \cdot 1044) = (-35) \cdot 3102 + 104 \cdot 1044.
\end{aligned}$$

Stąd

$$(3102, 1044) = (-35) \cdot 3102 + 104 \cdot 1044.$$

Zatem największy wspólny dzielnik liczb 3102 i 1044 jest kombinacją liniową tych liczb o współczynnikach odpowiednio $x_0 = -35$ i $y_0 = 104$.

Definicja najmniejszej wspólnej wielokrotności. Niech $a_1, a_2, ..., a_n$ będą liczbami całkowitymi różnymi od zera. Powiemy, że liczba całkowita b jest wspólną wielokrotnością liczb $a_1, a_2, ..., a_n$, jeśli $a_i \mid b$ dla każdego $i \in \{1, 2, ..., n\}$. Najmniejsza ze wspólnych wielokrotności dodatnich liczb $a_1, a_2, ..., a_n$ nazywa się najmniejszą wspólną wielokrotnością tych liczb.

Najmniejszą wspólną wielokrotność liczb $a_1, a_2, ..., a_n$ oznaczamy symbolem $[a_1, a_2, ..., a_n]$ lub $\mathrm{Nww}(a_1, a_2, ..., a_n)$.

Twierdzenie. Każda wspólna wielokrotność liczb całkowitych różnych od zera $a_1, a_2, ..., a_n$ jest podzielna przez ich najmniejszą wspólną wielokrotność $[a_1, a_2, ..., a_n]$.

Twierdzenie. Iloczyn największego wspólnego dzielnika dwóch liczb naturalnych i ich najmniejszej wspólnej wielokrotności jest równy iloczynowi tych liczb. Czyli

$$(a, b) \cdot [a, b] = a \cdot b, \quad a, b \in \mathbb{N}.$$

Przykład. Obliczyć najmniejszą wspólną wielokrotność liczb 3102 i 1044.

Rozwiązanie

$(3102, 1044) = 6$. Zatem na mocy powyższego twierdzenia

$$[3102, 1044] = \frac{3102 \cdot 1044}{6} = 539748.$$

2. Równania nieoznaczone

Twierdzenie. Niech $a_1, a_2, ..., a_n, b$ będą liczbami całkowitymi z których przynajmniej jedna liczba a_i jest różna od zera ($i \in \{1, 2, ..., n\}$).

Na to by równanie postaci

$$a_1x_1 + a_2x_2 + ... + a_nx_n = b$$

miało rozwiązanie w liczbach całkowitych potrzeba i wystarcza, by największy wspólny dzielnik liczb $a_1, a_2, ..., a_n$ dzielił liczbę b.

Definicja liczb względnie pierwszych. Liczby całkowite a, b nazywamy liczbami względnie pierwszymi, jeśli $(a, b) = 1$.

Twierdzenie. Na to by równanie postaci

$$ax + by = c, \quad a, b, c \in \mathbb{Z}, \quad a^2 + b^2 > 0,$$

miało rozwiązanie w liczbach całkowitych potrzeba i wystarcza, by $(a, b) \mid c$.

Spostrzeżenie. Niech będzie dane równanie postaci

$$(*) \qquad ax + by = 1, \quad a, b \in \mathbb{Z}, \quad a^2 + b^2 > 0.$$

Jeśli liczby całkowite a, b są względnie pierwsze, to równanie $(*)$ posiada rozwiązanie w liczbach całkowitych.

Twierdzenie. Jeśli para liczb całkowitych (x_0, y_0) jest pewnym rozwiązaniem równania

$$ax + by = c, \quad a, b, c \in \mathbb{Z}, \quad a^2 + b^2 > 0,$$

to wszystkie rozwiązania tego równania w liczbach całkowitych otrzymujemy ze wzoru

$$x = x_0 + \frac{b}{(a, b)}\, t, \quad y = y_0 - \frac{a}{(a, b)}\, t, \quad t \in \mathbb{Z}.$$

Przykład. Równanie

$$(*) \qquad 435x + 2012y = 6$$

rozwiązać w liczbach całkowitych.

Rozwiązanie

Największy wspólny dzielnik liczb 435 i 2112 jest równy 3. Równanie$(*)$ ma rozwiązanie, gdyż $3 \mid 12$. Ponadto łatwo obliczyć, że

$$(**) \qquad 435 \cdot (-335) + 2112 \cdot 69 = (435, 2012) = 3.$$

Mnożąc obie strony równości $(**)$ przez 2 otrzymujemy

$$435 \cdot (-335 \cdot 2) + 2112 \cdot (69 \cdot 2) = 3 \cdot 2 = 6.$$

Czyli

$$435 \cdot (-670) + 2112 \cdot 138 = 6.$$

Znaleźliśmy zatem rozwiązanie szczególne równania $(*)$ $x_0 = -670$, $y_0 = 138$.

Zgodnie z powyższym twierdzeniem rozwiązanie, równania $(*)$ ma postać

$$x = -670 + 704\, t, \quad y = 138 + 145\, t, \quad t \in \mathbb{Z}.$$

3. Liczby pierwsze

Definicja liczb pierwszych. Jeśli poza dzielnikami trywialnymi liczba naturalna n, większa od jedności, nie posiada innych dzielników naturalnych, to nazywamy ją **l**iczbą pierwszą.

Dokładniej: liczba $n \in \mathbb{N} \setminus \{1\}$ jest liczbą pierwszą, jeśli jedynymi jej dzielnikami naturalnymi są liczba 1 oraz liczba n.

Twierdzenie. (Zasadnicze twierdzenie arytmetyki). Niech a, b, c będą dowolnymi liczbami naturalnymi. Jeśli $(a, b) = 1$ i $a \mid b \cdot c$, to $a \mid c$.

Twierdzenie. (Podstawowe twierdzenie arytmetyki) Każda liczba naturalna n większa od jedności daje się przedstawić jednoznacznie, z dokładnością do kolejności czynników, w postaci iloczynu liczb pierwszych. To znaczy, że gdy dane są dwa rozkłady

$$n = p_1 \cdot p_2 \cdot ... \cdot p_k, \quad \text{oraz} \quad n = q_1 \cdot q_2 \cdot ... \cdot q_l$$

tej samej liczby naturalnej n na czynniki pierwsze, to $k = l$ i można liczby p_j i q_s ($j \in \{1, 2, ..., k\}$, $s \in \{1, 2, ..., l\}$), tak uporządkować, by odpowiadające sobie czynniki były równe.

Twierdzenie. Każda liczba złożona n ma dzielnik pierwszy mniejszy lub równy $\sqrt{n}$.

Powyższe twierdzenie jest równoważne twierdzeniu

Twierdzenie. Jeśli liczba naturalna $n > 1$ nie jest podzielna przez żadną liczbę pierwszą mniejszą lub równą $\sqrt{n}$, to jest liczbą pierwszą.

Sito Eratostenesa (276-194). Weźmy pod uwagę ciąg liczb naturalnych

$$(*_1) \qquad 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, ...$$

Usuńmy z naszego ciągu $(*_1)$ wszystkie liczby większe od pierwszej liczby pierwszej $p_1 = 2$ i podzielne przez 2. Otrzymujemy ciąg

$$(*_2) \qquad 2, 3, 5, 7, 9, 11, 13, 15, 17, 19, ...$$

Pierwszą nieusuniętą liczbą większą od 2 jest liczba pierwsza $p_2 = 3$. Usuwamy teraz z naszego ciągu wszystkie liczby większe od 3 będące wielokrotnościami liczby 3. Otrzymujemy ciąg

$$(*_3) \qquad 2, 3, 5, 7, 11, 13, 17, 19, ...$$

Pierwszą nieusuniętą liczbą niepodzielną przez 2 i 3 jest liczba pierwsza $p_3 = 5$.
Postępowanie kontynuujemy i za n-tym razem otrzymujemy n-tą liczbę pierwszą p_n. Następnie usuwamy z naszego ciągu wszystkie liczby większe od p_n będące wielokrotnościami liczby p_n. Pierwszą nieusuniętą liczbą jest liczba pierwsza p_{n+1}.

Jeśli ciąg jest skończony postaci

$$(**) \qquad 2, 3, 4, 5..., N,$$

to postępowanie możemy zakończyć po otrzymaniu największej liczby pierwszej $p_k \leq \sqrt{N}$. Wszystkie liczby pozostałe w ciągu $(**)$ większe od liczby p_k są liczbami pierwszymi.

Przykład. Weźmy pod uwagę ciąg liczb naturalnych

$$(***) \qquad (2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, ..., 83, 84, 85)\,.$$

Wykreślmy z naszego ciągu wszystkie liczby parzyste większe od $p_1 = 2$. Otrzymujemy ciąg

$$(2, 3, 5, 7, 9, 11, 13, 15, 17, ..., 83, 85)\,.$$

Pierwszą nieskreśloną liczbą występującą po liczbie $p_1 = 2$, niepodzielną przez 2, jest liczba 3. Wykreślamy wszystkie wielokrotności liczby 3 większe od $p_2 = 3$. Otrzymujemy ciąg

$$(2, 3, 5, 7, 11, 13, 17, , ..., 83, 85)\,.$$

Pierwszą nieskreśloną liczbą występującą po liczbie $p_2 = 3$, niepodzielną przez 2 i 3, jest liczba 5. Skreślamy teraz wszystkie liczby będące wielokrotnościami liczby 5, większe od $p_3 = 5$. Otrzymujemy ciąg

$$(2, 3, 5, 7, 11, 13, 17, , ..., 83)\,.$$

Nasze postępowanie skończy dla $p_4 = 7$ (gdyż 7 jest największą liczbą pierwszą mniejszą od $\sqrt{85}$), po skreśleniu wszystkich wielokrotności 7 większych od 7. Liczby pozostałe w ciągu $(***)$ po skreśleniu wielokrotności liczb $2, 3, 5, 7$ (oprócz liczb $2, 3, 5, 7$) są pierwsze. W rezultacie otrzymujemy wszystkie liczby pierwsze zawarte w zbiorze $\{2, 3, 4, 5, 6, ..., 85\}$. Są to liczby:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83.$$

4. Funkcja Eulera

Wielki matematyk niemiecki Carl Freidrich Gauss (1777-1855) zdefiniował funkcję $\varphi : \mathbb{N} \to \mathbb{N}$ określoną następująco: $\varphi(n)$, gdzie $n \in \mathbb{N}$, jest ilością liczb naturalnych niewiększych od n i względnie pierwszych z n.

Obecnie tę funkcje nazywa się funkcją Eulera od nazwiska wybitnego matematyka szwajcarskiego Leonarda Eulera (1707-1783).

Definicję funkcji Eulera φ możemy zapisać również w postaci

$$\varphi(n) = card\,\{k \in \mathbb{N} : k \leq n \ \wedge \ (k, n) = 1\}\,, \quad n \in \mathbb{N},$$

gdzie symbol $cardA$ oznacza moc zbioru A ($A = \{k \in \mathbb{N} : k \leq n \quad (k, n) = 1\}$).

Przyklad.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6

Funkcja Eulera ma zastosowanie w kryptografii.

Twierdzenie. (Własności funkcji Eulera)

(1) Jeśli p jest liczbą pierwszą, to

$$\varphi(p) = p - 1.$$

(2) Jeśli $\alpha \in \mathbb{N}$ i p jest liczbą pierwszą, to

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1)$$

lub równoważnie

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

(3) Jeśli $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{N}$ i $n = p_1^{\alpha_1}\, p_2^{\alpha_2}\, ...\, p_k^{\alpha_k}$, gdzie $p_1, p_2, ..., p_k$ są różnymi liczbami pierwszymi, to

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right).$$

(4) Jeśli $n = p_1\, p_2\, ...\, p_k$, gdzie $p_1, p_2, ..., p_k$ są różnymi liczbami pierwszymi, to

$$\varphi(n) = (p_1 - 1)\,(p_2 - 1)\,...\,(p_k - 1).$$

(5) Jeśli $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{N}$ i $n = p_1^{\alpha_1}\, p_2^{\alpha_2}\, ...\, p_k^{\alpha_k}$, gdzie $p_1, p_2, ..., p_k$ są różnymi liczbami pierwszymi, to

$$\varphi(n) = \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2})\,...\varphi(p_k^{\alpha_k}).$$

(7) Jeśli $m, n \in \mathbb{N}$ i $(m, n) = 1$, to

$$\varphi(m\,n) = \varphi(m)\;\varphi(n).$$

(8) Jeśli $n_1,\ n_2,\ ...\,, n_k \in \mathbb{N}$ i jeśli $(n_i, n_j) = 1$ dla $i \neq j$ $(i, j \in \{1, 2, ...k\})$ (tzn. liczby $n_1,\ n_2,\ ...\,, n_k$ są parami względnie pierwsze), to

$$\varphi(n_1\, n_2\, ...\, n_k) = \varphi(n_1)\;\varphi(n_2)\;\;...\varphi(n_k).$$

5. Kongruencje

Definicja kongruencji. O dwóch liczbach całkowitych a i b mówimy, że przystają do siebie modulo m $(m \in \mathbb{N})$, jeśli $m \mid (a - b)$.

Jeśli liczby a i b przystają do siebie modulo m, to piszemy $a \equiv b\,(\mathrm{mod} m)$. Czyli

$$a \equiv b\,(\mathrm{mod} m) \Longleftrightarrow \underset{k\in\mathbb{Z}}{\exists}\; a - b = k\,m.$$

Relacja $\equiv$ nazywa się kongruencją w zbiorze liczb całkowitych.

Twierdzenie. Niech a, b, c, d będą dowolnymi liczbami całkowitymi. Niech m będzie dowolną liczbą naturalną. Wówczas

(1) $a \equiv a\,(\mathrm{mod} m)$ (zwrotność relacji $\equiv$).

(2) Jeśli $a \equiv b\,(\mathrm{mod} m)$, to $b \equiv a\,(\mathrm{mod} m)$ (symetria relacji $\equiv$).

(3) Jeśli $a \equiv b\,(\mathrm{mod} m)$ i $b \equiv c\,(\mathrm{mod} m)$, to $a \equiv c\,(\mathrm{mod} m)$ (przechodniość relacji $\equiv$).

(4) Jeśli $a \equiv b\,(\mathrm{mod} m)$, to $(a-b) \equiv 0\,(\mathrm{mod} m)$.

(5) Jeśli $a \equiv b\,(\mathrm{mod} m)$ i $c \equiv d\,(\mathrm{mod} m)$, to $a+c \equiv (b+d)\,(\mathrm{mod} m)$.

(6) Jeśli $a \equiv b\,(\mathrm{mod} m)$ i $c \equiv d\,(\mathrm{mod} m)$, to $a\,c \equiv (b\,d)\,(\mathrm{mod} m)$.

(7) Jeśli $a_i \equiv b_i\,(\mathrm{mod} m)$, $(a_i, b_i \in \mathbb{Z},\ i \in \{1,2,..,k\})$, to $\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i\,(\mathrm{mod} m)$.

(8) Jeśli $a \equiv b\,(\mathrm{mod} m)$, to $a^k \equiv b^k\,(\mathrm{mod} m)$, $(k \in \mathbb{N})$.

(9) Jeśli $a \equiv b\,(\mathrm{mod} m)$ i $d > 0$ i $d \mid m$, to $a \equiv b\,(\mathrm{mod} d)$.

(10) Jeśli $a \equiv b\,(\mathrm{mod} m)$ i $c > 0$, to $a\,c \equiv b\,c\,(\mathrm{mod} m\,c)$.

(11) Jeśli $c\,a \equiv c\,b\,(\mathrm{mod} m)$ i $(c,m) = 1$, to $a \equiv b\,(\mathrm{mod} m)$.

Twierdzenie. Niech f oznacza wielomian o współczynnikach całkowitych. Wówczas, jeśli $a \equiv b\,(\mathrm{mod} m)$, to $f(a) \equiv f(b)\,(\mathrm{mod} m)$.

Przykład. (Cecha podzielności przez 11). Liczba naturalna a dzieli się przez 11 wtedy i tylko wtedy, gdy różnica pomiędzy sumą jej cyfr znajdujących się na miejscach nieparzystych, a sumą jej cyfr znajdujących się na miejscach parzystych jest podzielna przez 11.

Rozwiązanie

Niech liczba a w rozwinięciu dziesiętnym ma postać $a = a_n (10)^n + a_{n-1} (10)^{n-1} + ... + a_1 10 + a_0$. Zauważmy dalej, że $10 \equiv -1\,(\mathrm{mod} 11)$. Wobec powyższego twierdzenia $f(10) \equiv f(-1)\,(\mathrm{mod} 11)$, gdzie f jest wielomianem postaci $a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$. Zatem

$$a = a_n (10)^n + a_{n-1} (10)^{n-1} + ... + a_1 10 + a_0 \equiv a_n (-1)^n + a_{n-1} (-1)^{n-1} + ... + a_1 (-1) + a_0\,(\mathrm{mod} 11).$$

Twierdzenie. (Chińskie twierdzenie o resztach). Niech $m_1, m_2, ..., m_n$ $(n > 1)$, będą liczbami naturalnymi parami względnie pierwszymi, tzn $(m_i, m_j) = 1$ dla $i \neq j$ $(i, j \in \{1,2,...,n\})$ i niech $r_1, r_2, ..., r_n$ będą dowolnymi liczbami całkowitymi. Wówczas istnieje wspólne rozwiązanie układu kongruencji

$$(*) \qquad \begin{aligned} x &\equiv r_1\,(\mathrm{mod} m_1), \\ x &\equiv r_2\,(\mathrm{mod} m_2), \\ &\vdots \\ x &\equiv r_n\,(\mathrm{mod} m_n). \end{aligned}$$

Rozwiązanie, to jest jedyne modulo $m = m_1\, m_2 \ldots m_n$.

Czyli, jeśli x_0 jest pewnym rozwiązaniem układu $(*)$, to liczba całkowita x jest rozwiązaniem układu $(*)$ wtedy i tylko wtedy gdy jest postaci $x = x_0 + k\,m$, gdzie $m = m_1\, m_2 \ldots m_n$, $k \in \mathbb{Z}$.

Rozwiązywanie kongruencji typu $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \equiv 0 \,(\mathrm{mod} m)$

Niech $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ będzie wielomianem o współczynnikach całkowitych i niech $m \in \mathbb{N}$. Każdą liczbę całkowitą taką, że $f(c) \equiv 0 \,(\mathrm{mod} m)$ nazywamy pierwiastkiem kongruencji $f(x) \equiv 0 \,(\mathrm{mod} m)$.

Spostrzeżenie 1. Niech c będzie pierwiastkiem kongruencji $f(x) \equiv 0 \,(\mathrm{mod} m)$. Jeśli $d \equiv c \,(\mathrm{mod} m)$, to d też jest pierwiastkiem tej kongruencji.

Spostrzeżenie 2. Wszystkie pierwiastki kongruencji $f(x) \equiv 0 \,(\mathrm{mod} m)$ możemy wyznaczyć sprawdzając jej prawdziwość dla liczb ze zbioru $\{0, 1, 2, ..., m-1\}$, czyli reszt modulo m.

Uwaga. Przyjęto nie rozróżniać pierwiastków kongruencji $f(x) \equiv 0 \,(\mathrm{mod} m)$, które przystają do siebie modulo m. Traktujemy takie pierwiastki jako jeden pierwiastek tej kongruencji. Mówiąc, że kongruencja $f(x) \equiv 0 \,(\mathrm{mod} m)$ posiada trzy pierwiastki mamy na myśli trzy różne klasy liczb całkowitych modulo m.

Przykład. Kongruencja $x^{100} - 1 \equiv 0 \,(\mathrm{mod} 5)$ ma cztery pierwiastki są nimi liczby $1, 2, 3, 4$. Natomiast wszystkie rozwiązania można opisać wzorem $x = k + 5t$, $k \in \{1, 2, 3, 4\}$.

Kongruencje typu $ax \equiv b \,(\mathrm{mod} m)$

Twierdzenie. Niech $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, $g = (a, m)$. Kongruencja postaci

$$ax \equiv b \,(\mathrm{mod} m)$$

ma rozwiązanie wtedy i tylko wtedy, gdy $g \mid b$. Jeśli warunek jest spełniony, to rozwiązania tworzą ciąg arytmetyczny o różnicy $\dfrac{m}{g}$, dając g rozwiązań modulo m.

Spostrzeżenie 3. Kongruencja postaci $ax \equiv b \,(\mathrm{mod} p)$, gdzie p jest liczbą pierwszą i $p \nmid a$, ma dokładnie jeden pierwiastek.

Przykład. Ile rozwiązań posiada kongruencja

$$(*) \qquad 15x \equiv 25 \,(\mathrm{mod} 35)?$$

Podać te rozwiązania.

Rozwiązanie

Kongruencja $(*)$ ma pięć rozwiązań, gdyż $g = (15, 35) = 5$ i $5 \mid 25$. Znajdziemy te rozwiązania. Z definicji kongruencji otrzymujemy

$$15x - 35y = 25, \quad x, y \in \mathbb{Z}.$$

Dzieląc obie strony równania przez 5, mamy

$$3x - 7y = 5.$$

Para liczb $x_0 = 4, y_0 = 1$ stanowi rozwiązanie szczególne naszego równania. Rozwiązanie modulo 5 ma postać $x = 4 + 5s$, $s \in \mathbb{Z}$.

Ponieważ $\frac{35}{5} = 7$, to rozwiązania modulo 35 tworzą ciąg arytmetyczny o pięciu wyrazach i o różnicy 7

$$\begin{array}{rcrcl} x & = & 4 & + & 35t \\ x & = & 11 & + & 35t \\ x & = & 18 & + & 35t \quad , \quad t \in \mathbb{Z}. \\ x & = & 25 & + & 35t \\ x & = & 32 & + & 35t \end{array}$$

Twierdzenie Lagrange'a. Niech $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ będzie wielomianem o współczynnikach całkowitych. Jeśli p jest liczba pierwszą i $p \nmid a_n$, to kongruencja $f(x) \equiv 0 \,(\mathrm{mod} p)$ ma co najwyżej n pierwiastków.

Twierdzenie Wilsona. Jeśli p jest liczba pierwszą, to $(p-1)! \equiv -1 \,(\mathrm{mod} p)$.

Twierdzenie Eulera. Dla każdej liczby całkowitej a względnie pierwszej z $m \in \mathbb{N}$

$$a^{\varphi(m)} \equiv 1 \,(\mathrm{mod} m).$$

Twierdzenia Fermata (małe) (a). Dla każdej liczby całkowitej a niepodzielnej przez liczbę pierwszą p zachodzi kongruencja

$$a^{p-1} \equiv 1 \,(\mathrm{mod} p).$$

Małe twierdzenie Fermata jest często formułowane w postaci

*Twierdzenia Fermata (małe) (b).*Dla każdej liczby całkowitej a i dowolnej liczby pierwszej p

$$a^p \equiv a \,(\mathrm{mod} p).$$