

TALENT - podzielność, kongruencje i równania diofantyczne

Najstarsza i najważniejsza część teorii liczb zajmuje się podzielnością.

- **Definicja 0.1** *Mówimy, że liczba całkowita a dzieli się przez liczbę całkowitą b , jeżeli istnieje taka liczba całkowita d , że $a = bd$.*

Piszemy wtedy $b|a$. Mówimy, że b i d są **dzielnikami** liczby a . Oczywiście każda liczba dzieli się przez 1 i przez siebie. Są to tzw. **dzielniki trywialne**. Relacja podzielności $|$ jest w zbiorze \mathbf{Z} zwrotna, słabo antysymetryczna i przechodnia. Ponadto jeżeli $b|a$ i $b|c$, to $b|(a+c)$ oraz jeżeli $b|a$ lub $b|c$, to $b|ac$. Łatwo się przekonać, że twierdzenia odwrotne nie zachodzą.

Niech a będzie liczbą całkowitą ujemną. Wówczas $-a$ jest liczbą naturalną i jeżeli liczba k jest jej dzielnikiem czyli $-a = k \cdot l$ dla pewnego $l \in \mathbb{N}$, to $a = (-k) \cdot l$, tzn liczba całkowita $(-k)$ jest dzielnikiem liczby a . Zatem przy badaniu podzielności liczb wystarczy się ograniczyć do badania podzielności liczb naturalnych.

- **Definicja 0.2** *Liczby naturalne większe od 1, które mają tylko trywialne dzielniki, nazywamy **liczbami pierwszymi**.*
- **Definicja 0.3** *Liczby naturalne większe od m, n nazywamy **względnie pierwszymi**, jeżeli ich jedynym wspólnym dzielnikiem jest 1.*
- **Definicja 0.4** *Liczbę $n > 0$ nazywamy **złożoną**, jeżeli dzieli się bez reszty przez jakąś liczbę od siebie mniejszą a większą od 1.*
- **Twierdzenie 0.1** (EUKLIDES¹). *Każda liczba naturalna większa od 1 jest pierwsza lub jest iloczynem liczb pierwszych.*

D o w ó d. Przeprowadzimy go w oparciu o porządkową zasadę indukcji:

Liczba 2 spełnia tezę, bo jest pierwsza. Przypuśćmy, że wszystkie liczby mniejsze od n (większe od 1) spełniają tezę. Jeśli n nie jest pierwsza, to możemy ją przedstawić jako iloczyn $n = kl$, gdzie $k, l > 1$, więc $k, l < n$. Jako mniejsze od n , dają się one rozłożyć na czynniki pierwsze, lub same są pierwsze. To daje rozkład n na czynniki pierwsze. ■

- **Twierdzenie 0.2** (EUKLIDES). *Istnieje nieskończenie wiele liczb pierwszych.*

D o w ó d. Istotnie, niech p_1, p_2, \dots, p_n będą liczbami pierwszymi. Sprawdzimy, że niezależnie od tego, jak zostały wybrane i ile ich jest, istnieje co najmniej jeszcze jedna liczba pierwsza. Rozważmy liczbę $a = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$. Zgodnie z Twierdzeniem 1. istnieje liczba pierwsza p i liczba naturalna c , być może równa 1, taka, że $a = pc$. Tak więc

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1 = pc.$$

Równość ta wyklucza, by p była którąś z liczb p_1, p_2, \dots, p_n . Jeśli bowiem $p = p_k$, a b jest iloczynem pozostałych liczb p_i, \dots , to

$$pb + 1 = pc$$

¹Euklides, (365?-300?p.n.e.), matematyk i fizyk grecki, twórca geometrii – pierwszej aksjomatycznej teorii matematycznej oraz podstaw teorii liczb. Jako pierwszy badał sumę szeregu geometrycznego, o czym pisze w IX księdze swego dzieła "Elementy". Euklides był jednym z pierwszych nauczycieli w Muzeum Aleksandryjskim, założonym ok. roku 300 p.n.e. przez Ptolomeusza I, który zdobył władzę w Egipcie po upadku imperium Aleksandra Wielkiego w roku 323 p.n.e.

czyli $p(c - b) = 1$. Otrzymujemy sprzeczność, p jest większe od 1, a $(c - b)$ co najmniej równe 1. ■

Do znajdowania kolejnych liczb pierwszych służy tzw. **sito Eratostenesa**². Polega to na wykreślaniu z ciągu kolejnych liczb naturalnych po kolei wielokrotności: liczby 2, pozostawiając samą dwójkę. Pierwszą niewykreśloną jest 3, jest to więc liczba pierwsza. Zostawiamy ją i wykreślamy jej wielokrotności. Pierwszą niewykreśloną jest 5 –liczba pierwsza. Zostawiamy ją i wykreślamy jej wielokrotności, itd. Pozostaną same liczby pierwsze. Algorytm ten nadaje się do stosowania przez komputer i znajdowania wszystkich liczb pierwszych z przedziału $[2, N]$, a to, jak duże jest N , zależy od szybkości komputera. Znacznie wcześniej niż powstały komputery, Czebyszew wykazał, że dla każdej liczby $n > 2$ pomiędzy liczbami n i $2n$ znajduje się jakaś liczba pierwsza.

Próbowano znaleźć proste wzory arytmetyczne, które dawałyby liczby pierwsze. Fermat wysunął słynne przypuszczenie, że wszystkie liczby postaci

$$F(n) = 2^{2^n} + 1$$

są liczbami pierwszymi, jednak Euler odkrył rozkład na czynniki liczby

$$2^{2^4} + 1 = 641 \cdot 6700417.$$

Do tej pory nie udowodniono nawet, że dla $n > 4$ którakolwiek z liczb $F(n)$ jest liczbą pierwszą. Liczby Fermata odgrywają istotną rolę przy rozwiązywaniu problemów związanych z konstrukcjami geometrycznymi. Gauss udowodnił na przykład, że n -kąąt foremny wpisany w koło o danym promieniu można skonstruować za pomocą cyrkuła i linijki wtedy i tylko wtedy, gdy $n = 2^m \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k$, gdzie m jest liczbą całkowitą nieujemną a p_1, p_2, \dots, p_k są różnymi liczbami Fermata pierwszymi. Można więc skonstruować trójkąt, czworokąt, pięciokąt, sześciokąt foremny, ale nie można skonstruować siedmiokąta foremnego. Ten ostatni fakt udowodnimy też później inaczej.

Innym ciekawym i prostym wyrażeniem, które daje wiele liczb pierwszych, jest

$$f(n) = n^2 - n + 41$$

Dla $n = 1, 2, \dots, 40$ wyrażenie $f(n)$ jest liczbą pierwszą, jednak $f(41) = 41^2$

Wyrażenie $n^2 - 79n + 1601$ daje liczby pierwsze aż do $n = 79$.

Jak widzieliśmy, łatwo dowieść, że jest nieskończenie wiele liczb pierwszych w ciągu wszystkich liczb naturalnych. Dirichlet udowodnił, że w każdym ciągu arytmetycznym, którego pierwszy wyraz i różnica są liczbami naturalnymi względnie pierwszymi, istnieje nieskończenie wiele liczb pierwszych. Dla niektórych ciągów można to dość łatwo wykazać, w ogólnej wersji jest to trudne twierdzenie. Najprostszym przykładem jest oczywiście ciąg liczb nieparzystych - ciąg arytmetyczny o pierwszym wyrazie 1 i różnicy 2. Zawiera on oczywiście wszystkie liczby pierwsze, czyli nieskończenie wiele. Udowodnimy tw. Dirichleta dla ciągu liczb postaci $4k + 3$ (pierwszy wyraz 3 różnica 4).

- **Twierdzenie 0.3** *Dla każdej liczby naturalnej n istnieje większa od n liczba pierwsza postaci $4k + 3$.*

D o w ó d. Udowodnimy najpierw, że każda liczba postaci $4k+3$ posiada dzielnik pierwszy tej samej postaci.

Liczba $4k+3$ jest swoim własnym dzielnikiem, ma więc przynajmniej jeden dzielnik tej postaci. Bierzemy najmniejszy z takich jej dzielników, $4l + 3$ i sprawdzimy, że jest liczbą pierwszą. Jeżeli liczby t i s są dzielnikami $4l + 3$, to są nieparzyste, przy dzieleniu przez 4 dają więc resztę 1 lub 3. Gdyby było $t = 4n + 1$ i $s = 4m + 1$, to $4k + 3 = ts = 16nm + 4n + 4m + 1$, co jest niemożliwe. Jedna z liczb t, s jest więc postaci $4n + 3$ i oczywiście jest dzielnikiem liczby $4k + 3$, nie większym niż $4l + 3$, a więc $k = l$. Jedynymi dzielnikami liczby $4l + 3$ są 1 i ona sama.

²Eratostenes z Cyreny, (ok.275-ok.194p.n.e.), filozof, astronom, matematyk i geograf grecki, pierwszy dokonał pomiaru długości południka i wyznaczył kąt nachylenia ekliptyki do równika ziemskiego.

Możemy teraz przystąpić do dowodu twierdzenia. Dla $n > 4$ liczba $(n! - 1)$ jest oczywiście postaci $(4k + 3)$. Liczba ta nie dzieli się przez żadną liczbę $\leq n$. Wszystkie dzielniki pierwsze tej liczby są więc większe niż n , w szczególności jej dzielnik pierwszy postaci $4l + 3$ jest większy niż n . Wynika stąd od razu, że ciąg liczb pierwszych postaci $4k + 3$ jest nieograniczony, a więc nieskończony. ■

Podobny dowód można przeprowadzić dla ciągu liczb $6n + 5$, jednak metoda ta nie daje się uogólnić na przypadek innych ciągów arytmetycznych.

Wśród ważniejszych wyników dotyczących rozmieszczenia liczb pierwszych, dających się w miarę elementarnie sformułować, można jeszcze wspomnieć o twierdzeniu Gaussa, które mówi, że ilość liczb pierwszych mniejszych od n (oznaczymy ją tutaj przez A_n) podzielona przez n jest asymptotycznie zbieżna do $(\ln n)^{-1}$. Ściśle

$$\lim_{n \rightarrow \infty} \frac{A_n \cdot \ln n}{n} = 1$$

Kończąc te uwagi o liczbach pierwszych przytoczymy dwa nie rozstrzygnięte dotąd zagadnienia.

Pierwsze z nich to pytanie, czy istnieje nieskończenie wiele par postaci $p, p + 2$, gdzie p i $p + 2$ są liczbami pierwszymi (są to tzw. liczby bliźniacze). Chociaż odpowiedź pozytywna wydaje się być prawdziwa nie uzyskano dotąd w tym kierunku żadnych wyników.

Drugie - to tzw. *hipoteza Goldbacha*. Goldbach zapisał się w historii matematyki wyłącznie postawieniem w roku 1742 pewnego zagadnienia, w liście do Eulera. Dostrzegł mianowicie, że w każdym przypadku, który wypróbował, dowolna liczba parzysta może być przedstawiona jako suma dwu liczb pierwszych. Na przykład

$$4 = 2 + 2, 6 = 3 + 3, 8 = 5 + 3, \dots, 100 = 97 + 3, \dots$$

W roku 1931 matematyk rosyjski Sznilerman udowodnił, że każdą liczbę naturalną można przedstawić jako sumę co najwyżej 300 000 liczb pierwszych. Dowód jest bezpośredni i konstruktywny, chociaż nie daje żadnej praktycznej metody uzyskania rozkładu dowolnej liczby naturalnej na sumę liczb pierwszych. Matematyk radziecki Winogradow zdołał następnie zmniejszyć ilość liczb pierwszych z 300 000 do 4, jednak Winogradow udowodnił twierdzenie jedynie "dla dostatecznie dużych n ", tzn. wykazał, że istnieje liczba naturalna N taka, że każda liczba naturalna $n > N$ daje się przedstawić w postaci sumy co najwyżej 4 liczb pierwszych. Dowód Winogradowa nie pozwala jednak na oszacowanie liczby N , ponieważ jest wprowadzony metodą nie wprost. Winogradow udowodnił, że fałszywe jest przypuszczenie, jakoby istniało nieskończenie wiele liczb całkowitych nie dających się rozłożyć na sumę co najwyżej 4 liczb pierwszych.

Twierdzenie 1. mówi, że każda liczba $n > 1$ jest pierwsza, albo daje się rozłożyć na czynniki pierwsze. Pozostaje pytanie o jednoznaczność tego rozkładu. Podamy dwa dowody jednoznaczności rozkładu na czynniki pierwsze. Historycznie wcześniejszy jest dowód podany jeszcze przez Euklidesa i oparty na jego konstrukcji największego wspólnego dzielnika. Ponieważ temu ostatniemu pojęciu poświęcimy w dalszym ciągu wykładu więcej czasu, podamy najpierw inny dowód. Będzie to dowód niewprost. Załóżmy mianowicie, że istnieje liczba, która ma dwa istotnie różne rozkłady. Na mocy zasady minimum, istnieje najmniejsza taka liczba. Oznaczmy ją przez m . Mamy zatem

$$m = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s,$$

gdzie p_1, p_2, \dots, p_r i q_1, q_2, \dots, q_s są liczbami pierwszymi. Możemy oczywiście założyć, że

$$p_1 \leq p_2 \leq \dots \leq p_r \quad \text{oraz} \quad q_1 \leq q_2 \leq \dots \leq q_s.$$

Zauważmy, że $p_1 \neq q_1$, bo w przeciwnym razie istniałaby liczba mniejsza niż m posiadająca niejednoznaczny rozkład. Zatem $p_1 < q_1$ lub $q_1 < p_1$. Powiedzmy, że $p_1 < q_1$. Niech

$$m' = m - p_1 q_2 \cdots q_s = p_1 (p_2 \cdots p_r - q_2 \cdots q_s) = (q_1 - p_1) q_2 \cdots q_s.$$

Ponieważ $m' \in N$ i $m' < m$ więc m' ma jednoznaczny rozkład na czynniki. Zatem $p_1|(q_1 - p_1)$ lub $p_1|q_2 \cdots q_s$. To ostatnie jest niemożliwe, bo q_i oraz p_1 są liczbami pierwszymi, a p_1 jest ostro mniejsza od wszystkich q_i . Zatem $(q_1 - p_1) = p_1 h$, czyli $q_1 = p_1(h + 1)$, co przeczy temu, że q_1 było liczbą pierwszą.

Otrzymaliśmy zatem

- **Twierdzenie 0.4** (O JEDNOZNACZNOŚCI ROZKŁADU NA CZYNNIKI PIERWSZE) Każda większa od 1 liczba naturalna daje się przedstawić jako iloczyn potęg liczb pierwszych, i to na jeden tylko sposób, z dokładnością do kolejności czynników.
- **Wniosek 0.1** Jeśli p jest liczbą pierwszą i $p|nk$, to $p|n$ lub $p|k$.

W dalszym ciągu symbolem $\Theta(n)$ będziemy oznaczali liczbę wszystkich dzielników liczby n . Z twierdzenia o istnieniu i jednoznaczności rozkładu liczby naturalnej na czynniki pierwsze wynika, że jeżeli

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_s^{\alpha_s},$$

to każdy dzielnik d liczby n jest postaci

$$d = p_1^{\lambda_1} \cdot p_2^{\lambda_2} \cdot \dots \cdot p_s^{\lambda_s},$$

gdzie λ_i są liczbami naturalnymi spełniającymi nierówności

$$0 \leq \lambda_i \leq \alpha_i, \quad \text{dla } i = 1, 2, \dots, s.$$

I na odwrót — jest oczywiste, że każda liczba d powyższej postaci jest dzielnikiem liczby n . Łatwo zatem obliczyć liczbę wszystkich możliwych dzielników liczby n i otrzymujemy

$$\Theta(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \dots \cdot (\alpha_s + 1)$$

0.1 Algorytm Euklidesa.

Jeśli n nie dzieli się przez k , to możemy wykonać **dzielenie z resztą**. Dla dowolnych różnych od 0 liczb n i k istnieją takie liczby d i r , że $n = kd + r$, przy czym $r < k$, d i r są wyznaczone jednoznacznie. d nazywamy **ilorazem**, a r - **resztą** z dzielenia n przez k (jeśli $n < k$, to $d = 0$). Do znalezienia d można się posłużyć zasadą maksimum: d jest największym elementem zbioru $\{l \in N : kl \leq n\}$. Z tego już wynika, że reszta r jest mniejsza niż k .

Geometrycznie operacja ta polega na znalezieniu na prostej przedziału o końcach naturalnych, w którym leży ułamek $\frac{n}{k}$, jest to przedział $[d, d+1)$. Jeszcze inaczej można powiedzieć, że d jest częścią całkowitą liczby wymiernej $\frac{n}{k}$, a $\frac{r}{k}$ - jej częścią ułamkową.

- **Definicja 0.5** Największym wspólnym dzielnikiem liczb n i k , różnych od zera, nazywamy liczbę:

$$NWD(n, k) = \max\{l \in \mathbb{N} : l|n \text{ i } l|k\}.$$

Jej istnienie wynika z zasady maksimum: zbiór wszystkich wspólnych dzielników liczb n i k jest niepusty (należy do niego 1) i ograniczony, np. przez n .

Przy szukaniu największego wspólnego dzielnika nie będziemy się posługiwać, jak w szkole, rozkładem na czynniki pierwsze, zresztą ten sposób wymaga posiadania tablic liczb pierwszych i dla dużych liczb jest to trudne. Wykorzystamy znany od starożytności sposób.

Algorytm Euklidesa:

Niech $0 < n < k$ i wykonajmy dzielenie z resztą n przez k : $n = kd + r$. Wtedy, jeśli $l|n$ i $l|k$, to również $l|r$, bo $r = n - kd$. Podobnie, jeśli $l|r$ i $l|k$, to $l|n$. Tak więc wspólne dzielniki liczb n i k są dokładnie te same, co wspólne dzielniki liczb k i r . W szczególności $NWD(n, k) = NWD(k, r)$. Wykonując więc operację dzielenia z resztą uzyskaliśmy parę mniejszych liczb o tym samym NWD . Jeśli liczby są jeszcze za duże, by zgadywać, możemy tę operację zastosować ponownie, tym razem dzieląc k przez r , itd:

$$\begin{aligned}n &= kd_1 + r_1, & r_1 < k, \\k &= r_1d_2 + r_2, & r_2 < r_1, \\r_1 &= r_2d_3 + r_3, & r_3 < r_2, \\&\vdots\end{aligned}$$

To postępowanie musi się skończyć, bo kolejne reszty tworzą malejący ciąg liczb naturalnych. Przypuścimy, że skończy się na s -tym kroku, tzn. $r_{s+1} = 0$. Ostatnie dwa wiersze naszych obliczeń wyglądają tak:

$$\begin{aligned}r_{s-2} &= r_{s-1}d_s + r_s, & r_{s-1} < r_{s-2} \\r_{s-1} &= r_s d_{s+1} + 0, & 0 < r_{s-1}\end{aligned}$$

Mamy:

$$NWD(n, k) = NWD(k, r_1) = NWD(r_1, r_2) = \dots = NWD(r_{s-1}, r_s) = r_s.$$

A więc ostatnia niezerowa reszta w tym ciągu dzielen z resztą jest największym wspólnym dzielnikiem liczb n i k .

Wyliczmy teraz z pierwszej równości r_1 w zależności od n i k , podstawmy do drugiej równości i wyliczmy r_2 (też w zależności od n i k) itd. Otrzymamy w końcu wyrażenie na r_s . Mianowicie $r_s = pn + qk$, gdzie p i q są liczbami całkowitymi. Udowodniliśmy tym sposobem ważne twierdzenie.

- **Twierdzenie 0.5** *Największy wspólny dzielnik liczb n i k wyraża się jako ich kombinacja o współczynnikach całkowitych;*

$$\forall n, k > 0 \quad \exists p, q \in \mathbf{Z} \quad (NWD(n, k) = pn + qk)$$

Przykład.

Niech $n = 1001$ oraz $k = 357$. Wówczas

$$\begin{aligned}1001 &= 2 \cdot 357 + 287, & \text{więc } 287 &= 1001 - 2 \cdot 357, \\357 &= 1 \cdot 287 + 70, & \text{więc } 70 &= 357 - (1001 - 2 \cdot 357) = 3 \cdot 357 - 1001, \\287 &= 4 \cdot 70 + 7, & \text{więc } 7 &= 287 - 4 \cdot 70 = 2 \cdot 1001 - 5 \cdot 357, \\70 &= 10 \cdot 7 + 0,\end{aligned}$$

Zatem, zgodnie z algorytmem Euklidesa, 7 jest największym wspólnym dzielnikiem liczb 1001 i 357 i przedstawiliśmy go w postaci $7 = 2 \cdot 1001 - 5 \cdot 357$.

Za pomocą ostatniego twierdzenia możemy udowodnić wiele ważnych własności, między innymi (udowodnioną wcześniej) jednoznaczność rozkładu na czynniki pierwsze.

- **Twierdzenie 0.6** (ZASADNICZE TWIERDZENIE ARYTMETYKI) *Jeżeli iloczyn $m \cdot n$ dzieli się przez k i liczba k jest względnie pierwsza z m , to k dzieli n .*

D o w ó d. Dla dowodu posłużymy się przedstawieniem jedynki - największego wspólnego dzielnika liczb m i k jako ich kombinacji o współczynnikach całkowitych: $1 = pm + qk$, a stąd $n = pmn + qkn$. Oba składniki sumy po prawej stronie dzielą się przez k , więc suma także, czyli $k|n$. ■

Ponieważ każda liczba pierwsza jest względnie pierwsza z dowolną liczbą naturalną, więc otrzymujemy natychmiast:

- **Wniosek 0.2** *Jeżeli $NWD(m, n) = 1$ oraz $k|m$, to $NWD(k, n) = 1$.*
- **Wniosek 0.3** *Jeżeli $NWD(m, n) = 1$ oraz $k|n$, to $NWD(m, k) = 1$.*
- **Wniosek 0.4** *Jeżeli p jest liczbą pierwszą i dzieli iloczyn mn , to p dzieli co najmniej jeden z czynników: $p|mn \rightarrow p|m \vee p|n$.*
- **Wniosek 0.5** *Jeżeli liczby m, n podzielimy przez ich największy wspólny dzielnik, to otrzymamy liczby względnie pierwsze.*

Teraz, tak, jak obiecywaliśmy, możemy wrócić jeszcze raz do sprawy jednoznaczności rozkładu. Dowód poprowadzimy metodą niewprost, korzystając z zasady minimum. Przypuśćmy, że istnieją liczby o niejednoznacznym rozkładzie i niech n będzie najmniejszą taką liczbą. Weźmy pod uwagę dwa różne rozkłady liczby n na czynniki pierwsze i uporządkujmy je według wzrostu tych czynników:

$$m = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s, \quad p_1 \leq p_2 \leq \cdots \leq p_r \quad \text{oraz} \quad q_1 \leq q_2 \leq \cdots \leq q_s$$

p i q są (niekoniecznie różnymi) liczbami pierwszymi. Ponieważ liczba pierwsza p_1 dzieli iloczyn po prawej stronie, dzieli któryś z jego czynników, czyli pewną liczbę q_j . Ponieważ q_j jest też liczbą pierwszą, musi być $p_1 = q_j$. Dzieląc n przez tę liczbę pierwszą, otrzymamy mniejszą od n liczbę naturalną o dwóch różnych rozkładach na czynniki pierwsze:

$$p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_{j-1} q_{j+1} \cdots q_s$$

co jest sprzeczne z wyborem liczby n .

Twierdzenie o jednoznaczności rozkładu wydaje się dość oczywiste. Czy możemy znaleźć jakieś przykłady pokazujące, że nie zawsze tak jest? Czy istnieją zbiory liczb, w których taki rozkład jest określony, ale nie musi być jednoznaczny? Są to bardzo interesujące konstrukcje, do których powrócimy w przyszłości.

0.2 Największy wspólny dzielnik i najmniejsza wspólna wielokrotność

0.2.1 Największy wspólny dzielnik i najmniejsza wspólna wielokrotność dwu liczb

- **Definicja 0.6** *Najmniejszą wspólną wielokrotnością liczb a i b jest liczba*

$$NWW(a, b) = \min\{k \in \mathbb{N} : k > 0 \wedge a|k \wedge b|k\}.$$

Jej istnienie wynika z zasady minimum.

Wiedząc, że w zbiorze liczb naturalnych żadna liczba nie posiada dwóch istotnie różnych rozkładów na czynniki pierwsze, możemy posługiwać się tym rozkładem przy poszukiwaniu największego wspólnego dzielnika i najmniejszej wspólnej wielokrotności liczb. Jeśli p występuje w rozkładzie liczby a z wykładnikiem n , a w rozkładzie liczby b z wykładnikiem m , to p występuje w rozkładzie liczby $NWD(a, b)$ z wykładnikiem $\min(n, m)$, a w rozkładzie liczby $NWW(a, b)$ - z wykładnikiem $\max(n, m)$.

Przytoczymy teraz kilka ważniejszych własności NWD i NWW .

- **Własność 1.** Każda wspólna wielokrotność dwóch liczb dzieli się przez ich najmniejszą wspólną wielokrotność.

D o w ó d. Przypuśćmy, że n jest najmniejszą wspólną wielokrotnością liczb a i b , a w jest ich dowolną wspólną wielokrotnością i wykonajmy dzielenie z resztą: $w = qn + r$, gdzie $r < n$. Stąd $r = w - qn$ jest również liczbą podzieloną przez a i przez b . Jeśli jest więc $r > 0$, to r powinna być niemniejsza od n , co nie jest prawdą. Tak więc $r = 0$, czyli w dzieli się przez n .

- **Własność 2.** Każdy wspólny dzielnik dwóch liczb dzieli ich największy wspólny dzielnik.

D o w ó d. Niech d będzie największym wspólnym dzielnikiem liczb a i b , a l - dowolnym ich wspólnym dzielnikiem. Liczby a i b są wspólnymi wielokrotnościami liczb d i l , dzielą się więc, w myśl Własności 1, przez $NWW(d, l)$. Ta ostatnia liczba jest więc wspólnym dzielnikiem a i b , a więc $NWW(d, l) \leq d$, skąd $NWW(d, l) = d$. To oznacza, że d jest wielokrotnością l .

- **Własność 3.** $ab = NWW(a, b) \cdot NWD(a, b)$.

D o w ó d. Liczba ab jest oczywiście wspólną wielokrotnością a i b , więc na mocy Własności 1. mamy $ab = kNWW(a, b)$ dla pewnego k . Niech m i n będą takie, że $NWW(a, b) = ma = nb$. Wtedy: $ab = kma = knb$, skąd $a = kn, b = km$. Zatem k jest więc dzielnikiem wspólnym a i b . Pozostaje pokazać, że jest to ich największy wspólny dzielnik. Niech l będzie dowolnym wspólnym dzielnikiem a i b . Istnieją więc p i q takie, że $a = pl, b = ql$. Stąd $pql = qa = pb$ i jako wspólna wielokrotność liczb a i b , iloczyn pql dzieli się przez $NWW(a, b)$. Mamy więc dla pewnego $t \in N : pql = tNWW(a, b)$, a wtedy:

$$kNWW(a, b) = ab = pql = tl \cdot NWW(a, b), \text{ skąd } k = tl.$$

Zatem k dzieli się przez l , co, wobec dowolności l , daje $k = NWD(a, b)$.

- **Własność 4.** Jeżeli $NWD(a, c) = 1$ i $NWD(b, c) = 1$, to $NWD(ab, c) = 1$.

D o w ó d. Jeśli liczby ab i c mają wspólny dzielnik pierwszy, to dzieli on a i c lub b i c co przeczy założeniu.

0.2.2 Największy wspólny dzielnik i najmniejsza wspólna wielokrotność n liczb

Pojęcie najmniejszej wspólnej wielokrotności i Własność 1. można uogólnić na przypadek dowolnej skończonej ilości liczb naturalnych, a pojęcie największego wspólnego dzielnika i Własność 2. na przypadek dowolnego zbioru liczb naturalnych. Nie można w taki sposób uogólnić Własności 3. Wystarczy zauważyć, że dla $a = 2, b = 3, c = 6$ mamy $abc = 36$ oraz $NWD(a, b, c) = 1, NWW(a, b, c) = 6$, czyli $NWD(a, b, c) \cdot NWW(a, b, c) = 6$.

Niech będzie dane n liczb naturalnych a_1, a_2, \dots, a_n i poszukajmy ich największego dzielnika. Niech

$$d_k = NWD(a_1, a_2, \dots, a_k) \text{ dla } k = 2, 3, \dots, n$$

i zauważmy, że

$$d_k = NWD(d_{k-1}, a_k) \text{ dla } k = 3, 4, \dots, n$$

Dlaczego? Liczba d_k , jako wspólny dzielnik liczb a_1, a_2, \dots, a_{k-1} (w szczególności) dzieli ich największy wspólny dzielnik d_{k-1} . Ale $d_k | a_k$, więc $d_k | NWD(d_{k-1}, a_k)$. Mamy również

$$NWD(d_{k-1}, a_k) | d_{k-1} \text{ oraz } NWD(d_{k-1}, a_k) | a_k,$$

a ponieważ d_{k-1} jest dzielnikiem każdej z liczb a_1, a_2, \dots, a_k , więc

$$NWD(d_{k-1}, a_k) | a_i \text{ dla } i = 1, 2, \dots, k.$$

Stąd $NWD(d_{k-1}, a_k) | d_k$.

Posługując się zasadą indukcji i wykorzystując Twierdzenie 0.5 możemy bez trudu udowodnić następujące jego uogólnienie

- **Twierdzenie 0.7** Dla dowolnych liczb naturalnych a_1, a_2, \dots, a_n , gdzie $n \geq 2$ istnieją liczby całkowite x_1, x_2, \dots, x_n takie, że

$$NWD(a_1, a_2, \dots, a_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n.$$

Podobnie obliczanie najmniejszej wspólnej wielokrotności kilku liczb można sprowadzić do kolejnego obliczania najmniejszej wspólnej wielokrotności dwu liczb. Niech

$$N_k = NWW(a_1, a_2, \dots, a_k) \text{ dla } k = 2, 3, \dots, n$$

i pokażmy, że

$$N_k = NWW(N_{k-1}, a_k) \text{ dla } k = 3, 4, \dots, n$$

Dlaczego? Ponieważ N_k jest wielokrotnością liczb a_1, a_2, \dots, a_{k-1} , więc $N_{k-1} | N_k$. Ponadto $a_k | N_k$, więc N_k jest wspólną wielokrotnością liczb N_{k-1} i a_k . Stąd

$$NWW(N_{k-1}, a_k) | N_k.$$

Ponieważ

$$a_i | N_{k-1} \text{ dla } i = 1, 2, \dots, k-1$$

oraz

$$N_{k-1} | NWW(N_{k-1}, a_k) \text{ i } a_k | NWW(N_{k-1}, a_k),$$

więc $NWW(N_{k-1}, a_k)$ jest wielokrotnością wszystkich a_i dla $i = 1, 2, \dots, k$, skąd wynika, że $N_k | NWW(N_{k-1}, a_k)$.

0.3 Zastosowania algorytmu Euklidesa do rozwiązywania liniowych równań diofantycznych.

Wśród zadań szkolnych spotykamy takie, które prowadzą do jednego równania o dwóch niewiadomych. Informacją dodatkową, umożliwiającą rozwiązanie, jest na ogół ukryty w treści zadania fakt, że rozwiązania mają być liczbami całkowitymi. Mamy wtedy do czynienia z **równaniem diofantycznym**. Jest to równanie algebraiczne, w którym i współczynniki i niewiadome są liczbami całkowitymi. Nazwa pochodzi od nazwiska greckiego matematyka Diofantosa³, który takie równania rozważał w księdze *Arytmetyka*, napisanej w III wieku n.e. W przypadku, gdy jest to równanie liniowe, najczęściej rozwiązujemy je analizując podzielność występujących w nim liczb. Czasami jednak nie widać jak tym sposobem można otrzymać rozwiązanie. Oto przykład takiego zadania:

Zadanie. Na sezonowej wyprzedaży zegarmistrz sprzedał wszystkie, jakie miał, zegarki po 123 złote. Ucieszony tym faktem, zostawił sobie na szczęście jeden złoty, a za resztę zakupił w hurtowni nowocześniejsze zegarki z pozytywką po 377 zł. Ile było jednych i drugich zegarków?

Widać, że zadanie sprowadza się do rozwiązania w liczbach naturalnych równania:

$$123x - 377y = 1$$

Okazuje się, że równanie diofantyczne może nie mieć rozwiązań, może ich mieć skończenie wiele lub nieskończenie wiele. Równanie, które otrzymaliśmy w powyższym zadaniu, jest najprostszym przykładem równania diofantycznego. Jest to tzw **liniowe równanie diofantyczne**.

- **Twierdzenie 0.8** Liniowe równanie diofantyczne $ax + by = c$ ma rozwiązanie w zbiorze liczb całkowitych wtedy i tylko wtedy, gdy $NWD(a, b)$ jest dzielnikiem c .

³Diofantos, (2 połowa III wieku), matematyk grecki.

D o w ó d. Jeśli istnieją $x, y \in Z$ takie, że $ax + by = c$ to oczywiście $NWD(a, b)$ dzieli c , gdyż dzieli a i dzieli b .

Załóżmy teraz, że dla pewnej liczby całkowitej m mamy $c = m \cdot NWD(a, b)$. Jak pamiętamy, z algorytmu Euklidesa wynika, że $NWD(a, b) = ak + bl$ dla pewnych całkowitych k i l . Otrzymujemy zatem

$$m \cdot NWD(a, b) = a \cdot km + b \cdot lm$$

Oczywiście km i lm są szukanymi całkowitymi rozwiązaniami naszego równania. ■

Możemy teraz rozwiązać nasze równanie. Znajdźmy więc największy wspólny dzielnik współczynników: 123 i 377. Zastosujemy tu algorytm Euklidesa:

$$377 = 3 \cdot 123 + 8$$

$$123 = 15 \cdot 8 + 3$$

$$8 = 2 \cdot 3 + 2$$

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

Widzimy, że w ciągu kolejnych dzielen z resztą ostatnią większą od zera resztą jest 1, a więc to jest największy wspólny dzielnik naszych współczynników. Przekształćmy teraz otrzymany ciąg równości, wyliczając kolejne reszty, przy czym dla odróżnienia występujących w dzieleniu wyjściowych liczb i reszt od współczynników dzielenia, te pierwsze będziemy podkreślać.

$$\underline{8} = \underline{377} - 3 \cdot 123$$

$$\underline{3} = \underline{123} - 15 \cdot \underline{8}$$

$$\underline{2} = \underline{8} - 2 \cdot \underline{3}$$

$$\underline{1} = \underline{3} - \underline{2}$$

Teraz dokonujemy podstawień kolejno z pierwszej do drugiej równości, z drugiej do trzeciej, z trzeciej do czwartej, przy czym redukujemy wyrazy podobne, traktując podkreślone liczby jak zmienne w wyrażeniach algebraicznych:

$$\underline{3} = \underline{123} - 15 \cdot (\underline{377} - 3 \cdot 123) = -15 \cdot \underline{377} + 46 \cdot 123$$

$$\underline{2} = \underline{377} - 3 \cdot \underline{123} - 2 \cdot (-15 \cdot \underline{377} + 46 \cdot \underline{123}) = 31 \cdot \underline{377} - 95 \cdot \underline{123}$$

$$\underline{1} = -15 \cdot \underline{377} + 46 \cdot \underline{123} - (31 \cdot \underline{377} - 95 \cdot \underline{123}) = -46 \cdot \underline{377} + 141 \cdot \underline{123}$$

Otrzymaliśmy w końcu rozwiązanie wyjściowego równania: $x = 141, y = 46$ i odpowiedź do zadania: zegarmistrz sprzedał 141 zegarków po 123 zł. i kupił 46 zegarków po 377 zł. Widać też, że gdyby zostawił sobie nie 1 zł. lecz 2 zł. to otrzymane liczby należałoby pomnożyć przez 2 itd. Możemy więc układać podobne zadania, mając pewność, że równanie $ax + by = c$ ma rozwiązanie w liczbach całkowitych, jeśli tylko c jest największym wspólnym dzielnikiem liczb a i b , lub jego wielokrotnością. Oczywiście jeśli c nie spełnia tego warunku, to rozwiązania nie ma: lewa strona dzieli się przez $NWD(a, b)$, prawa nie.

Wracając do zadania rozwiązywanego na początku, można pytać jak znaleźć wszystkie rozwiązania całkowite liniowego równania diofantycznego o 2 niewiadomych. Rozważmy równanie $ax + by = c$ i załóżmy, że a i b są względnie pierwsze (jeśli nie są, to obie strony równania dzielimy przez $d = NWD(a, b)$) i rozwiążmy równanie

$$ax + by = 1$$

Niech x_0, y_0 będzie rozwiązaniem otrzymanym w ostatnio udowodnionym twierdzeniu, a x_1, y_1 niech oznacza jakiegokolwiek inne rozwiązanie. Wtedy oczywiście $a(x_1 - x_0) + b(y_1 - y_0) = 0$ i para: $x_1 - x_0, y_1 - y_0$ stanowi rozwiązanie równania jednorodnego:

$$ax - by = 0$$

Tak więc każde rozwiązanie równania $ax + by = 1$ jest sumą rozwiązania szczególnego (x_0, y_0) tego równania i pewnego rozwiązania równania jednorodnego. Pozostaje nam rozwiązać równanie jednorodne. Oczwistym rozwiązaniem jest $x = b, y = -a$ a wraz z nim wszystkie jego wielokrotności. Okazuje się, że są to wszystkie rozwiązania wyjściowego równania. Jeżeli bowiem $ax = -by$, to a dzieli iloczyn by , a ponieważ a i b są względnie pierwsze, więc a dzieli y . Podobnie b dzieli x . Ostatecznie więc każde rozwiązanie naszego równania jest postaci:

$$x = x_0 + tb, \quad y = y_0 - ta,$$

gdzie t jest dowolną liczbą całkowitą.

Powyższe rozważania pozwalają udowodnić jeszcze jedno ciekawe elementarne twierdzenie.

- **Twierdzenie 0.9** (TWIERDZENIE CHIŃSKIE O RESZTACH) Niech $m \geq 2$ będzie liczbą naturalną. Dla dowolnych liczb naturalnych a_1, a_2, \dots, a_m , z których każde dwie są względnie pierwsze i dowolnych liczb całkowitych r_1, r_2, \dots, r_m istnieją liczby całkowite x_1, x_2, \dots, x_m takie, że

$$a_1x_1 + r_1 = a_2x_2 + r_2 = \dots = a_mx_m + r_m.$$

D o w ó d. Dla $m = 2$ teza pokrywa się z tezą Twierdzenia 0.8, bo liczby a_1, a_2 są względnie pierwsze, więc równanie

$$a_1x_1 - a_2x_2 = r_2 - r_1$$

ma rozwiązanie w liczbach całkowitych. Niech $m \geq 2$ będzie dowolnie ustaloną liczbą naturalną i założmy, że żądana równość zachodzi dla każdych m liczb. Rozważmy dowolne liczby naturalne $a_1, a_2, \dots, a_m, a_{m+1}$, z których każde dwie są względnie pierwsze i dowolne liczby całkowite $r_1, r_2, \dots, r_m, r_{m+1}$. Niech x_1, x_2, \dots, x_m będą liczbami całkowitymi spełniającymi warunki

$$a_1x_1 + r_1 = a_2x_2 + r_2 = \dots = a_mx_m + r_m.$$

Ponieważ każda z liczb a_1, a_2, \dots, a_m jest względnie pierwsza z a_{m+1} , więc

$$NWD(a_1a_2 \cdot \dots \cdot a_m, a_{m+1}) = 1.$$

Zatem istnieją liczby t i u spełniające równanie

$$a_1a_2 \cdot \dots \cdot a_m \cdot t - a_{m+1} \cdot u = r_{m+1} - a_1x_1 - r_1.$$

Niech

$$x'_i = \frac{a_1a_2 \cdot \dots \cdot a_m}{a_i} \cdot t + x_i \text{ dla } i = 1, 2, \dots, m \text{ oraz } x'_{m+1} = u.$$

Łatwo sprawdzić, że liczby $x'_1, x'_2, \dots, x'_{m+1}$ spełniają żądany warunek.

Dla $i = 1, 2, \dots, m$ mamy bowiem

$$\begin{aligned} a_ix'_i + r_i &= a_i \left(\frac{a_1a_2 \cdot \dots \cdot a_m}{a_i} \cdot t + x_i \right) + r_i = a_1a_2 \cdot \dots \cdot a_m \cdot t + a_ix_i + r_i \\ &= a_{m+1} \cdot x'_{m+1} + r_{m+1} - a_1x_1 - r_1 + a_ix_i + r_i = a_{m+1} \cdot x'_{m+1}. \end{aligned}$$

Zgodnie z zasadą indukcji matematycznej, twierdzenie zostało udowodnione. ■

Natychmiastowy jest następujący wniosek z powyższego twierdzenia.

- **Wniosek 0.6** Jeżeli każde dwie spośród $m \geq 2$ liczb naturalnych a_1, a_2, \dots, a_m są względnie pierwsze, to istnieje liczba całkowita N , która przy dzieleniu przez te liczby daje odpowiednio dowolne dane reszty r_1, r_2, \dots, r_m .

Dalej, ponieważ liczba $N + a_1a_2 \cdot \dots \cdot a_m \cdot k$, gdzie k jest dowolną liczbą całkowitą, daje przy dzieleniu przez każdą z liczb a_1, a_2, \dots, a_m tę samą resztę, co liczba N , więc istnieje nieskończenie wiele liczb całkowitych (również – nieskończenie wiele liczb naturalnych), które przy dzieleniu przez a_1, a_2, \dots, a_m dają odpowiednio reszty r_1, r_2, \dots, r_m .

0.4 Równanie Pitagorasa i kilka innych równań diofantycznych wyższych rzędów.

Wyżej rozwiązaliśmy problem wyznaczenia pierwiastków (oczywiście całkowitych!) równania diofantycznego liniowego o 2 niewiadomych. Uogólnienia problemu idą w dwóch kierunkach: zwiększania liczby niewiadomych i podwyższania stopnia równania. Znanym przykładem kwadratowego równania diofantycznego jest **równanie pitagorejskie**⁴:

$$x^2 + y^2 = z^2.$$

Powszechnie znanym jego rozwiązaniem jest trójka: 3, 4, 5, a ogólniej, każda trójka postaci: $3n, 4n, 5n$, gdzie n jest dowolną liczbą naturalną (tradycyjnie mówi się tu o rozwiązaniach dodatnich, gdyż interpretuje się je jako długości boków trójkąta prostokątnego - stąd nazwa równania). Te wszystkie rozwiązania nie różnią się pomiędzy sobą w sposób istotny: opisują one trójkąty podobne. Wystarczy znać jedno z nich. Takie rozwiązanie, którego nie można otrzymać z innego przez pomnożenie przez liczbę całkowitą, nazwiemy **rozwiązaniem pierwotnym**. Zastanówmy się, jak znaleźć wszystkie rozwiązania pierwotne równania pitagorejskiego.

Pierwszym spostrzeżeniem jest fakt, że liczby a, b, c stanowiące takie rozwiązanie, nie mają wspólnego dzielnika większego od 1. Można jednak powiedzieć więcej: każde dwie spośród nich są względnie pierwsze: gdyby bowiem dwie, na przykład a i b miały wspólny dzielnik pierwszy p , to kładąc: $a = a_1p$, $b = b_1p$, mielibyśmy:

$$p^2(a_1^2 + b_1^2) = c^2$$

a więc p , jako liczba pierwsza, musiałaby także dzielić c i rozwiązanie nie byłoby pierwotne. Liczby a, b, c są więc parami względnie pierwsze. W szczególności co najwyżej jedna z nich może być parzysta. Nie mogą jednak wszystkie być nieparzyste, bo dla nieparzystych a i b suma $a^2 + b^2$ jest parzysta. Dokładnie jedna z nich jest więc parzysta. Nie może to być jednak liczba c . Jeśli bowiem $c = 2k$, to $c^2 = 4k^2$ a lewa strona, jako suma kwadratów liczb nieparzystych, nie dzieli się przez 4.

Zalóżmy więc, że a i c są nieparzyste, a b - parzysta i zapiszmy nasze równanie w postaci:

$$b^2 = c^2 - a^2 = (c - a)(c + a)$$

Liczby $c - a$ i $c + a$ są obie parzyste, ale 2 jest ich jedynym wspólnym dzielnikiem (każdy inny dawałby wspólny dzielnik a i c). Przyjmując:

$$b = 2k, \quad c - a = 2l, \quad c + a = 2m,$$

mamy:

$$k^2 = lm,$$

przy czym l i m są względnie pierwsze. Za pomocą rozkładu l i m na czynniki pierwsze stwierdzamy, że liczby te same muszą być pełnymi kwadratami:

$$m = u^2, \quad l = v^2.$$

Ostatecznie więc:

$$(*) \quad c = u^2 + v^2, \quad a = u^2 - v^2, \quad b = 2uv,$$

gdzie liczby u i v są względnie pierwsze, $u > v$ oraz jedna z nich jest parzysta. Ten ostatni fakt wynika z nieparzystości a i c . Udowodniliśmy, że każde rozwiązanie równania pitagorejskiego jest postaci (*)

⁴Pitagoras, (ok.572-ok.497p.n.e.), matematyk i filozof grecki, uważany za twórcę początków teorii liczb. Założył stowarzyszenie filozoficzno religijne, tzw. Związek Pitagorejski, którego motto brzmiało "wszystko jest liczbą". Zachowane tabliczki z pismem klinowym świadczą, że twierdzenie Pitagorasa znali już Babilończycy na długo przed Pitagorasem, jednak dopiero Pitagoras podał jego dowód. Uważa się, że to Pitagoras wymyślił słowo "matematyka", które oznacza "to czego można się uczyć".

dla pewnych u i v . Wykażemy jeszcze, że wszystkie trójki tej postaci są rozwiązaniami pierwotnymi tego równania. Łatwo sprawdzić, że istotnie:

$$(u^2 - v^2) + (2uv)^2 = (u^2 + v^2)$$

a więc jest to rozwiązanie. Ponadto z (*) wynika, że a i c są nieparzyste, b parzysta. Gdyby liczby a, b, c miały wspólny dzielnik pierwszy $p > 2$, to z (*) mielibyśmy $p|2u$ i $p|2v$, a stąd $p|u$ i $p|v$, wbrew założeniu, że u i v są względnie pierwsze. Tak więc rzeczywiście jest to rozwiązanie pierwotne. Udowodniliśmy więc następujące twierdzenie.

- **Twierdzenie 0.10** *Trójka a, b, c jest rozwiązaniem pierwotnym równania pitagorejskiego wtedy i tylko wtedy, gdy jest postaci*

$$(*) \quad c = u^2 + v^2, \quad a = u^2 - v^2, \quad b = 2uv,$$

przy czym liczby u i v są względnie pierwsze, $u > v$ oraz jedna z nich jest parzysta. Wszystkie pozostałe rozwiązania otrzymujemy z pierwotnych, mnożąc je przez liczbę naturalną.

Uogólnieniem równania pitagorejskiego jest równanie:

$$x^n + y^n = z^n$$

o którym słynne tzw. **Wielkie Twierdzenie Fermata**⁵ głosi, że nie ma ono rozwiązań w liczbach naturalnych dla żadnego $n > 2$. Twierdzenie to, sformułowane przez Fermat'a bez dowodu na marginesie dzieła Diofantosa w pełnej ogólności dopiero w 1995 roku doczekało się udowodnienia. Korzystając z wiadomości o równaniu pitagorejskim, można udowodnić twierdzenie Fermata dla przypadku $n = 4$.

- **Twierdzenie 0.11** *Równanie $x^4 + y^4 = z^4$ nie ma rozwiązań w liczbach naturalnych.*

D o w ó d. Aby dowieść, że równanie to nie ma rozwiązań całkowitych dodatnich, zajmiemy się równaniem postaci: $x^4 + y^4 = w^2$ i wykażemy, że jeśli ma ono rozwiązanie $\{x_0, y_0, w_0\}$, to ma również rozwiązanie $\{x_1, y_1, w_1\}$, gdzie $w_1 < w_0$, co doprowadzi nas do sprzeczności z zasadą minimum. Przypuśćmy więc, że liczby naturalne x, y, w spełniają równanie

$$x^4 + y^4 = w^2$$

przy czym w ma najmniejszą możliwą wartość. Oczywiście liczby x^2, y^2, w spełniają równanie pitagorejskie, a zatem możemy przyjąć, że x^2 i w są nieparzyste, y jest parzysta oraz istnieją względnie pierwsze u, v , z których jedna jest parzysta, takie, że

$$x^2 = u^2 - v^2, \quad y^2 = 2uv, \quad w = u^2 + v^2$$

Z pierwszej równości otrzymujemy znowu równanie pitagorejskie $x^2 + v^2 = u^2$ więc x, u są nieparzyste, v jest parzyste i u, v są względnie pierwsze. Zatem także $(u, 2v) = 1$, a ponieważ $y^2 = 2uv = u \cdot 2v$, więc u i $2v$ muszą być pełnymi kwadratami.

$$u = w_1^2, \quad 2v = 4t^2$$

Ponadto istnieją u_1, v_1 względnie pierwsze takie, że

$$x = u_1^2 - v_1^2, \quad v = 2u_1v_1, \quad u = u_1^2 + v_1^2,$$

Równość $v = 2u_1v_1 = 2t^2$ prowadzi do wniosku, że u_1 i v_1 są także pełnymi kwadratami:

$$u_1 = x_1^2, \quad v_1 = y_1^2,$$

⁵Pierre de Fermat, (1601–1665), matematyk francuski, z zawodu prawnik, prekursor rachunku prawdopodobieństwa i rachunku różniczkowego, podał metodę znajdowania ekstremów funkcji, zajmował się teorią liczb i geometrią analityczną.

przy czym $u_1^2 + v_1^2 = u = w_1^2$, co daje:

$$x_1^4 + y_1^4 = w_1^2$$

Znaleźliśmy drugie rozwiązanie równania wyjściowego, przy czym

$$w = u^2 + v^2 = w_1^4 + v^2 > w_1,$$

a nierówność $w_1 < w$ sprzeczna jest z początkowym wyborem liczby w . Sprzeczność ta dowodzi, że wyjściowe równanie nie ma niezerowego rozwiązania w liczbach całkowitych, czyli twierdzenie Fermata dla wykładnika 4 jest udowodnione. Podobnie rozumując można udowodnić, że

- **Twierdzenie 0.12** *Równanie $x^4 - y^4 = z^2$ nie ma rozwiązań w liczbach naturalnych.*

Wspominaliśmy wcześniej, że równanie diofantyczne może mieć bardzo różną ilość rozwiązań. Przykładem równania, które ma skończenie wiele rozwiązań (dokładnie dwa!) jest równanie $x^2 = 2y^2 - 1$. Są to pary $x = 1, y = 1$ i $x = 239, y = 13$. Matematyk norweski W.Ljunggren udowodnił w 1942 roku, że inne rozwiązania nie istnieją. Natomiast równanie $x^2 - 2y^2 = 1$ ma rozwiązań nieskończenie wiele. Łatwo sprawdzić, że jeżeli x, y jest jakimkolwiek rozwiązaniem tego równania, to $x' = 3x + 4y, y' = 2x + 3y$ jest też rozwiązaniem tego równania.

Długo czas nie było żadnej ogólnej teorii równań diofantycznych i rozpatrywano każde równanie z osobna. Na przykład w 1909 roku matematyk norweski Axel Thue udowodnił, że równanie z dwiema niewiadomymi stopnia co najmniej trzeciego ma tylko skończoną ilość rozwiązań.

Zróbmy kilka przykładów.

- **Przykład 0.1** *Wyznaczyć wszystkie trójkąty prostokątne, których boki są kolejnymi liczbami naturalnymi.*

R o z w i ą z a n i e. Szukamy naturalnych rozwiązań równania

$$n^2 + (n + 1)^2 = (n + 2)^2$$

i okazuje się, że jedynym rozwiązaniem jest trójka (3, 4, 5).

- **Przykład 0.2** *Wykazać, że istnieje nieskończenie wiele trójkątów prostokątnych, których boki są kolejnymi wyrazami ciągu arytmetycznego o pierwszym wyrazie i różnicy będących liczbami naturalnymi.*

R o z w i ą z a n i e. Szukamy naturalnych rozwiązań równania

$$n^2 + (n + r)^2 = (n + 2r)^2$$

i otrzymujemy jako jedyny warunek $\frac{n}{r} = 3$. Zatem jest jasne, że takich trójkątów jest nieskończenie wiele.

- **Przykład 0.3** *Dla jakich liczb naturalnych n istnieje trójkąt prostokątny o bokach, których długości są liczbami naturalnymi i jedna z przyprostokątnych równa jest n ?*

R o z w i ą z a n i e. Szukamy naturalnych rozwiązań równania

$$a^2 + n^2 = c^2$$

Zapisując ten warunek w postaci

$$n^2 = (c - a)(c + a)$$

widzimy, że dla $n = 1, 2$ taki trójkąt nie istnieje. Dla parzystych n warunki zadania spełnia trójkąt o bokach

$$a = \left(\frac{n}{2}\right)^2 - 1, \quad c = \left(\frac{n}{2}\right)^2 + 1,$$

zaś dla nieparzystych n — trójkąt o bokach

$$a = \left(\frac{n^2 - 1}{2}\right), \quad c = \left(\frac{n^2 + 1}{2}\right).$$

- **Przykład 0.4** Wyznaczyć wszystkie trójkąty prostokątne, których długości boków są liczbami naturalnymi a pole równe jest obwodowi.

R o z w i ą z a n i e. Szukamy naturalnych rozwiązań układu równań

$$\begin{aligned} x^2 + y^2 &= z^2 \\ x + y + z &= \frac{xy}{2} \end{aligned}$$

Rugując niewiadomą z i przekształcając otrzymane równanie

$$xy - 4(x + y) + 8 = 0$$

do postaci

$$(x - 4)(y - 4) = 8$$

otrzymujemy jako jedyne naturalne rozwiązania trójki $(5, 12, 13)$ oraz $(6, 8, 10)$.

0.5 Kongruencje

0.5.1 Pojęcie i najprostsze własności kongruencji

- **Definicja 0.7** O liczbach naturalnych a i b mówimy, że przystają modulo m , jeśli ich różnica jest liczbą podzieloną przez m :

$$a \equiv b \pmod{m} \iff m \mid (a - b)$$

Dla dowolnego modulu $m \in \mathbb{N}$ relacja przystawania modulo m , zwana **kongruencją**, jest relacją typu równoważności, tzn. jest zwrotna, symetryczna i przechodnia. Pod wieloma względami kongruencje zachowują się podobnie jak równości, można je dodawać i mnożyć (ale nie dzielić!) stronami. Przypuśćmy bowiem, że $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$. Oznacza to, że liczby $(a - b)$ i $(c - d)$ dzielą się przez m , ale wtedy również ich suma dzieli się przez m :

$$m \mid (a + b) - (c + d), \quad \text{czyli} \quad a + b \equiv c + d \pmod{m}.$$

Zamiast o sumie możemy mówić oczywiście także o różnicy. Natomiast dla iloczynu korzystamy z faktu, że wielokrotność liczby podzielnej przez m jest podzielna przez m , więc z naszych założeń wynika, że

$$m \mid ac - bc \quad \text{i} \quad m \mid bc - bd,$$

a stąd $m \mid ac - bd$.

Co do dzielenia, to zauważmy, że z kongruencji: $6 \equiv 2 \pmod{4}$ wcale nie wynika przystawanie 3 do 1 przy module 4.

Przystawanie liczb a i b modulo m oznacza, że dają one tę samą resztę przy dzieleniu przez m . Liczba a przystaje do zera modulo m wtedy i tylko wtedy, gdy $m \mid a$. Mnożąc daną kongruencję przez siebie dochodzimy do wniosku, że kongruencje można również potęgować stronami (ściśle dowód prowadzimy przez indukcję względem wykładnika potęgi). Kombinując te wyniki razem otrzymujemy twierdzenie:

- **Twierdzenie 0.13** Jeśli $f(x)$ jest wielomianem o współczynnikach całkowitych oraz $a \equiv b \pmod{m}$, to również $f(a) \equiv f(b) \pmod{m}$.

Sformułujemy jeszcze i udowodnimy kilka pożytecznych własności kongruencji.

- **Własność 1.** Jeżeli d jest wspólnym dzielnikiem liczb a, b i m , to z kongruencji $a \equiv b \pmod{m}$ wynika kongruencja $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

Do w ó d. Jeżeli istnieje liczba całkowita k taka, że $a - b = k \cdot m$, to $\frac{a}{d} - \frac{b}{d} = k \cdot \frac{m}{d}$, co oznacza, że $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$. ■

- **Własność 2.** Jeżeli d jest dzielnikiem liczby m to z kongruencji $a \equiv b \pmod{m}$ wynika kongruencja $a \equiv b \pmod{d}$.

Do w ó d. Jeżeli istnieje liczba całkowita k taka, że $a - b = k \cdot m$ oraz $m = d \cdot l$ dla pewnej liczby całkowitej l , to $a - b = kl \cdot d$, co oznacza, że $a \equiv b \pmod{d}$. ■

- **Własność 3.** Jeżeli d jest dzielnikiem liczb a i b a liczby d i m są względnie pierwsze, to z kongruencji $a \equiv b \pmod{m}$ wynika kongruencja

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{m}.$$

Do w ó d. Dzieląc równość $a - b = k \cdot m$ stronami przez d otrzymujemy $\frac{a}{d} - \frac{b}{d} = \frac{km}{d}$. Ponieważ lewa strona równości jest liczbą całkowitą a d i m są względnie pierwsze, więc $\frac{k}{d}$ musi być liczbą całkowitą co oznacza, że $\frac{a}{d} \equiv \frac{b}{d} \pmod{m}$. ■

- **Własność 4.** Jeżeli $a \equiv b \pmod{m_i}$ dla $i = 1, 2, \dots, r$, to

$$a \equiv b \pmod{\text{NWW}(m_1, m_2, \dots, m_r)}.$$

Do w ó d. Równość $a - b = k_i \cdot m_i$ prawdziwa dla $i = 1, 2, \dots, r$, oznacza, że $a - b$ jest wspólną wielokrotnością liczb m_1, m_2, \dots, m_r , więc dzieli się przez ich najmniejszą wspólną wielokrotność, co oznacza, że $a \equiv b \pmod{\text{NWW}(m_1, m_2, \dots, m_r)}$. ■

- **Własność 5.** Jeżeli $a \equiv b \pmod{m}$, to $\text{NWD}(a, m) = \text{NWD}(b, m)$

Do w ó d. Po prostu zbiory wspólnych dzielników liczb a i m oraz b i m są takie same. ■

- **Własność 6.** Jeżeli c jest dzielnikiem liczby a , d jest dzielnikiem liczby b , c i m są względnie pierwsze, d i m są względnie pierwsze, $a \equiv b \pmod{m}$ oraz $c \equiv d \pmod{m}$, to $\frac{a}{c} \equiv \frac{b}{d} \pmod{m}$.

Do w ó d. Załóży, że $a = k \cdot c$ oraz $b = l \cdot d$. Ponieważ $c \equiv d \pmod{m}$, więc $kc \equiv kd \pmod{m}$. Stąd

$$kd \equiv kc = a \equiv b = ld \pmod{m},$$

a ponieważ d i m są względnie pierwsze, więc $k \equiv l \pmod{m}$ co oznacza, że

$$\frac{a}{c} \equiv \frac{b}{d} \pmod{m}.$$

■

- **Przykład 0.5** Wykazać, że liczba $2222^{5555} + 5555^{2222}$ jest podzielna przez 7.

R o z w i ą z a n i e. Ponieważ $2222 \equiv 3 \pmod{7}$, więc

$$2222^5 \equiv 3^5 \pmod{7} \text{ oraz } 2222^6 \equiv 3^6 \equiv 1 \pmod{7}.$$

Stąd $2222^{6 \cdot 925} \equiv 1 \pmod{7}$. Mnożąc kongruencje stronami otrzymujemy

$$2222^{5550} \cdot 2222^5 \equiv 3^5 \equiv 5 \pmod{7}.$$

Podobnie licząc mamy kolejno

$$5555 \equiv 4 \pmod{7}, \quad 5555^2 \equiv 2 \pmod{7} \text{ oraz } 5555^6 \equiv 1 \pmod{7}.$$

Podnosząc tę kongruencję do potęgi 370 otrzymujemy

$$5555^{2220} \equiv 1 \pmod{7}, \text{ więc } 5555^{2222} \equiv 2 \pmod{7},$$

co po dodaniu stronami daje

$$2222^{5555} + 5555^{2222} \equiv 5 + 2 \equiv 0 \pmod{7},$$

czyli liczba $2222^{5555} + 5555^{2222}$ jest podzielna przez 7.

- **Przykład 0.6** Dowieść, że dla dowolnej liczby naturalnej n liczba $3^{(6^n)} - 2^{(6^n)}$ jest podzielna przez 35.

R o z w i ą z a n i e. Ponieważ $3^3 \equiv -2^3 \pmod{35}$, więc podnosząc obie strony do parzystej potęgi $3^{n-1} \cdot 2^n$ otrzymujemy

$$3^{3 \cdot 3^{n-1} \cdot 2^n} \equiv 2^{3 \cdot 3^{n-1} \cdot 2^n} \pmod{35} \text{ czyli } 3^{3^n \cdot 2^n} \equiv 2^{3^n \cdot 2^n} \pmod{35},$$

co daje $3^{(6^n)} \equiv 2^{(6^n)} \pmod{35}$.

- **Przykład 0.7** Pokazać, że dla każdej nieparzystej liczby pierwszej p istnieją liczby całkowite x i y , takie, że $p \mid 1 + x^2 + y^2$.

R o z w i ą z a n i e. Rozpatrzmy reszty z dzielenia przez p liczb n^2 dla $n = 0, 1, 2, \dots, \frac{1}{2}(p-1)$. Są one wszystkie różne, gdyż w przeciwnym przypadku p byłoby dzielnikiem liczby $r^2 - s^2$, gdzie r i s są pewnymi różnymi liczbami ze zbioru $A = \{0, 1, 2, \dots, \frac{1}{2}(p-1)\}$. Niech np. $r > s$. Ponieważ $p \mid r^2 - s^2 = (r-s)(r+s)$, więc p , jako liczba pierwsza dzieli $(r-s)$ lub $(r+s)$. Każdy z tych przypadków jest niemożliwy, gdyż

$$0 < r - s \leq \frac{1}{2}(p-1) \text{ i } 0 < r + s \leq 2 \cdot \frac{1}{2}(p-1) = p-1.$$

Liczby $1 + m^2$, gdzie $m \in A$ dają więc $\frac{1}{2}(p-1) + 1 = \frac{1}{2}(p+1)$ różnych reszt z dzielenia przez p . Podobnie jest z liczbami $-n^2$ gdzie $n \in A$. Obydwa te zbiory dają więc $p+1$ reszt, co jest niemożliwe. Zatem pewne liczby $1 + x^2$ oraz $-y^2$ dają tę samą resztę, czyli $p \mid 1 + x^2 + y^2$.

0.5.2 Funkcja Gaussa i Małe Twierdzenie Fermata

W języku kongruencji wygodnie jest formułować i dowodzić klasyczne twierdzenia teorii liczb. Zajmiemy się teraz niektórymi z nich.

Dla dowolnej liczby naturalnej $m > 0$ przez P_m oznaczmy zbiór dodatnich liczb mniejszych od m i względnie pierwszych z m :

$$P_m = \{0 < k < m : NWD(k, m) = 1\}.$$

Dla liczby pierwszej p mamy więc $P_p = \{1, 2, \dots, p-1\}$. Niech $\Phi(m)$ oznacza liczbę elementów zbioru P_m . Funkcja $\Phi(m)$ nazywa się **funkcją Gaussa**⁶. Oznaczmy przez $r_1, r_2, \dots, r_{\Phi(m)}$ wszystkie elementy zbioru P_m , czyli

$$P_m = \{r_1, r_2, \dots, r_{\Phi(m)}\}.$$

Niech a będzie liczbą dodatnią taką, że $NWD(a, m) = 1$. Wówczas reszty $[ar_i]_{(m)}$ z dzielenia iloczynów ar_i dla $i = 1, 2, \dots, \Phi(m)$ przez m wypełniają cały zbiór P_m . Aby to uzasadnić, zauważmy, że te reszty są mniejsze niż m oraz względnie pierwsze z m , bo każdy z iloczynów ar_i jest liczbą względnie pierwszą z m . Wszystkie te reszty są więc elementami zbioru P_m . Równocześnie stwierdzamy, że są one różne między sobą, bo dla $i \neq j$ liczba ar_i nie przystaje do ar_j modulo m . Mamy więc $\Phi(m)$ elementów zbioru P_m , czyli wszystkie jego elementy. Dla każdego $1 \leq i \leq \Phi(m)$ istnieje więc $1 \leq j \leq \Phi(m)$ takie, że

$$ar_i \equiv r_j \pmod{m}$$

Mnożąc te kongruencje stronami otrzymujemy:

$$a^{\Phi(m)} \prod_{i=1}^{\Phi(m)} r_i \equiv \prod_{j=1}^{\Phi(m)} r_j \pmod{m}.$$

Oznaczając przez r iloczyn wszystkich r_i możemy to zapisać:

$$r \equiv ra^{\Phi(m)} \pmod{m}, \quad \text{czyli } m \mid r(a^{\Phi(m)} - 1)$$

Ponieważ liczby m i r są względnie pierwsze, więc $m \mid (a^{\Phi(m)} - 1)$.

Udowodniliśmy w ten sposób tzw. **Twierdzenie Eulera**⁷.

- **Twierdzenie 0.14** (TWIERDZENIE EULERA): Dla każdej liczby całkowitej a pierwszej względem liczby naturalnej m zachodzi kongruencja

$$a^{\Phi(m)} \equiv 1 \pmod{m}.$$

Wnioskiem z niego jest tzw. **Małe twierdzenie Fermata**:

- **Twierdzenie 0.15** (MAŁE TWIERDZENIE FERMATA): Jeżeli p jest liczbą pierwszą i p nie dzieli a , to $a^{p-1} \equiv 1 \pmod{p}$. Stąd $a^p \equiv a \pmod{p}$, czyli $p \mid (a^p - a)$.

⁶Karl Friedrich Gauss, (1777–1855), zwany "księciem matematyków", matematyk niemiecki, uważany za jednego z trzech, obok Archimedesusa i Newtona, największych matematyków świata. Jego prace dotyczą teorii liczb, algebry, rachunku różniczkowego i całkowego, teorii szeregów, statystyki matematycznej, geometrii sferycznej i geometrii nieeuklidesowej. Gauss stworzył także zupełnie nowe gałęzie matematyki, w tym teorię funkcji zespolonych i geometrię różniczkową. Zajmował się też fizyką, geodezją, astronomią.

⁷Leonard Euler, (1707–1783), szwajcarski matematyk, fizyk i astronom, studiował w Bazylei u Johannesa Bernoulli'ego, był profesorem na uniwersytetach w Petersburgu i Berlinie. Euler jest autorem ok. 500 prac z dziedziny matematyki, w których zajmował się m.in. rachunkiem różniczkowym i całkowym, równaniami różniczkowymi, szeregami nieskończonymi i funkcjami zespolonymi. Jest twórcą znacznej części współczesnej notacji matematycznej — wprowadził symbole e, π, i , podał obecnie używane definicje funkcji trygonometrycznych, stosując oznaczenia "sin", "cos". Euler pracował również nad zastosowaniami matematyki w fizyce, mechanice, teorii sprężystości.

- **Przykład 0.8** Pokazać, że dla każdej liczby naturalnej k liczba $(2^{(2^{6k+2})} + 3)$ jest podzielna przez 19.

Ponieważ $2^6 \equiv 1 \pmod{9}$, więc dla każdej liczby naturalnej k

$$2^{6k} \equiv 1 \pmod{9} \quad \text{i} \quad 2^{6k+2} \equiv 2^2 \pmod{9}.$$

Ponieważ obie strony ostatniej kongruencji są parzyste, więc

$$2^{6k+2} \equiv 2^2 \pmod{18},$$

czyli $2^{6k+2} = 18t + 2^2$ dla pewnej liczby naturalnej t . Stąd

$$2^{2^{6k+2}} = 2^{18t+2^2} = 16 \cdot 2^{18t}.$$

Z MTF wynika, że

$$2^{18} \equiv 1 \pmod{19}, \quad \text{więc} \quad 2^{18t} \equiv 1 \pmod{19}.$$

Ponieważ $16 \equiv -3 \pmod{19}$, więc ostatecznie

$$16 \cdot 2^{18t} \equiv -3 \pmod{19}.$$

0.5.3 Pierwiastki kongruencji i Twierdzenie Lagrange'a

Niech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ będzie wielomianem stopnia n o współczynnikach całkowitych. **Pierwiastkiem kongruencji** $f(x) \equiv 0 \pmod{m}$ nazywamy każdą liczbę całkowitą α taką, że $f(\alpha) \equiv 0 \pmod{m}$. Jeżeli α jest pierwiastkiem i $\beta \equiv \alpha \pmod{m}$, to również β jest pierwiastkiem, gdyż z twierdzenia o mnożeniu i dodawaniu kongruencji wynika wówczas, że $f(\alpha) \equiv f(\beta) \pmod{m}$. Takie dwa pierwiastki będziemy uważali za jedno rozwiązanie. Rozwiązaniem kongruencji jest więc cały ciąg liczb $\alpha + lm$, gdzie $k = 1, 2, 3, \dots$. Poszukiwanie rozwiązań sprowadza się do poszukiwania pierwiastków w zbiorze $\{0, 1, \dots, m-1\}$. Mówiąc o liczbie rozwiązań kongruencji, mamy na myśli liczbę jej pierwiastków zawartych między 0 a $m-1$.

● Kongruencje liniowe

Rozważamy wielomian stopnia $n = 1$ i kongruencję

$$(*) \quad ax \equiv b \pmod{m}$$

Oznacza to, że $m|(ax - b)$, a więc istnieje takie y , że $ax - b = my$. Kongruencja sprowadza się więc do równania diofantycznego:

$$ax - my = b.$$

Wiemy, że takie równanie ma rozwiązanie wtedy i tylko wtedy, gdy $d = \text{NWD}(a, m)$ jest dzielnikiem b . Jedno rozwiązanie (x_0, y_0) tego równania znajdujemy wówczas posługując się algorytmem Euklidesa do wyrażenia liczby d , a za nią także b , jako kombinacji liniowej liczb a i m . Wszystkie inne rozwiązania można więc zapisać w postaci:

$$x = x_0 + t \cdot m_1, \quad y = y_0 + t \cdot a_1$$

gdzie $m_1 d = m$ oraz $a_1 d = a$. Jeżeli $t \in \{0, 1, \dots, d-1\}$, to rozwiązania te nie przystają modulo m . Gdyby bowiem dla pewnych $0 \leq i < j \leq d-1$ prawdziwa była zależność $x_0 + i \cdot m_1 \equiv x_0 + j \cdot m_1 \pmod{m}$, to $m_1 d = m|(j-i)m_1$, czyli $d|(j-i)$, co oczywiście nie jest możliwe. Zatem $t \in \{0, 1, \dots, d-1\}$ wyznaczają różne rozwiązania wyjściowej kongruencji. Biorąc $t \geq d$ nie dostaniemy nowych rozwiązań kongruencji. Dlaczego? Przedstawmy t w postaci $t = kd + r$ dla pewnego $r \in \{0, 1, \dots, d-1\}$. Wówczas

$$x = x_0 + t \cdot m_1 \equiv x_0 + r \cdot m_1 \pmod{m},$$

bo $(t - r)m_1 = ldm_1 = lm$. Udowodniliśmy zatem następujące twierdzenie.

- **Twierdzenie 0.16** *Kongruencja liniowa $ax \equiv b \pmod{m}$ ma d rozwiązań postaci $x = x_0 + t \cdot m_1$, gdzie $d = \text{NWD}(a, m)$, $m = dm_1$ oraz $t \in \{0, 1, \dots, d-1\}$.*

Stąd wniosek.

- **Wniosek 0.7** *Jeżeli $d = \text{NWD}(a, m) = 1$, to kongruencja liniowa $ax \equiv b \pmod{m}$ ma dokładnie jedno rozwiązanie.*

W szczególności, jeżeli moduł kongruencji jest liczbą pierwszą, która nie dzieli a , to $d = 1$ i kongruencja:

$$(**) \quad ax \equiv b \pmod{p}$$

ma jedno rozwiązanie. Znajdujemy je korzystając z twierdzenia Fermata. Niech bowiem p będzie liczbą pierwszą, która nie dzieli a . Mamy więc $a^{p-1} \equiv 1 \pmod{p}$. Mnożąc tę ostatnią kongruencję stronami przez b , otrzymujemy

$$ba^{p-1} \equiv b \pmod{p}$$

Przyjmując teraz $x_0 = ba^{p-2}$ mamy $ax_0 \equiv b \pmod{p}$ i reszta z dzielenia x_0 przez p wyznacza jedyne rozwiązanie kongruencji (**).

- **Przykład 0.9** *Kongruencja liniowa $3x \equiv 5 \pmod{4}$ ma jedno rozwiązanie, bo $d = \text{NWD}(3, 4) = 1$.*

Wyznaczamy je rozwiązując równanie diofantyczne $3x - 4y = 5$.

Ponieważ $3 \cdot (-1) + 4 \cdot 1 = 1$, więc $3 \cdot (-5) + 4 \cdot 5 = 5$ i jako jedyne rozwiązanie tej kongruencji otrzymujemy $x = -5 + 4l$.

- **Przykład 0.10** *Wyznaczyć wszystkie rozwiązania kongruencji liniowej*

$$2x \equiv 6 \pmod{4}.$$

Ponieważ $d = \text{NWD}(2, 4) = 2$, więc, zgodnie z udowodnionym wyżej twierdzeniem, oczekujemy dwu rozwiązań — dla $t = 0$ oraz $t = 1$. Rozwiązując równanie diofantyczne $2x - 4y = 6$, otrzymujemy

$$2 \cdot (-1) - 4 \cdot (-1) = 2, \quad \text{więc} \quad 2 \cdot (-3) - 4 \cdot (-3) = 6.$$

Zatem jako rozwiązania tej kongruencji otrzymujemy:

$$x_1 = -3 + 0 \cdot 2 + 4l = -3 + 4l \quad \text{oraz} \quad x_2 = -3 + 1 \cdot 2 + 4l = -1 + 4l.$$

- **Przykład 0.11** *Wyznaczyć wszystkie rozwiązania kongruencji liniowej*

$$8x \equiv 4 \pmod{3}.$$

Ponieważ 3 jest liczbą pierwszą, która nie jest dzielnikiem liczby 8, więc na mocy Małego Twierdzenia Fermata

$$3 \mid 8^2 - 1, \quad \text{czyli} \quad 8^2 \equiv 1 \pmod{3}.$$

Stąd

$$8^2 \cdot 4 \equiv 4 \pmod{3}, \quad \text{więc} \quad 8 \cdot (4 \cdot 8) \equiv 4 \pmod{3}.$$

Rozwiązaniem tej kongruencji jest zatem $x = 32$ i biorąc $x_0 = 2$, czyli resztę z dzielenia 32 przez 3 wyznaczamy rozwiązanie ogólne

$$x = 2 + 3l.$$

Dla kongruencji o module będącym liczbą pierwszą prawdziwe jest twierdzenie o liczbie rozwiązań, analogiczne (i podobnie dowodzone!) do twierdzenia o liczbie pierwiastków wielomianu w zbiorze liczb rzeczywistych.

- **Twierdzenie 0.17** (LAGRANGE⁸): *Jeżeli f jest wielomianem stopnia n o współczynnikach całkowitych, a p - liczbą pierwszą nie dzielącą współczynnika przy x^n , to kongruencja $f(x) \equiv 0 \pmod{p}$ ma nie więcej niż n rozwiązań.*

D o w ó d prowadzimy przez indukcję względem stopnia wielomianu. (i) Dla $n = 1$ mamy kongruencję liniową $ax \equiv b \pmod{m}$ i twierdzenie jest już udowodnione, co jest treścią Wniosku, ponieważ p jest liczbą pierwszą nie dzielącą a .

(ii) Niech $n > 1$ i przypuśćmy, że twierdzenie jest prawdziwe dla wielomianów stopnia $n - 1$. Rozważmy dowolny wielomian:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0.$$

Niech p będzie liczbą pierwszą i nie dzielącą a_n . Rozpatrujemy kongruencję:

$$(*) \quad f(x) \equiv 0 \pmod{p}$$

Jeżeli α jest jej pierwiastkiem, czyli $f(\alpha) \equiv 0 \pmod{p}$, to dla dowolnego x mamy $f(x) \equiv f(x) - f(\alpha) \pmod{p}$, a więc:

$$f(x) = a_n(x^n - \alpha^n) + a_{n-1}(x^{n-1} - \alpha^{n-1}) + \dots + a_1(x - \alpha)$$

Wylączając z prawej strony czynnik $(x - \alpha)$ przed nawias i porządkując według potęg x wyrazy pozostałe w nawiasie otrzymujemy:

$$f(x) = (x - \alpha)g(x)$$

gdzie g jest pewnym wielomianem o współczynnikach całkowitych stopnia $n - 1$, którego współczynnik przy najwyższej potędze x wynosi a_n . Możemy więc do g zastosować założenie indukcyjne. Jeśli β jest pierwiastkiem $(*)$ i $\beta < p$, to

$$0 \equiv f(\beta) \equiv (\beta - \alpha)g(\beta) \pmod{p}$$

czyli $p | (\beta - \alpha)g(\beta)$, ale p nie dzieli $(\beta - \alpha)$, więc $p | g(\beta)$, co oznacza, że $g(\beta) \equiv 0 \pmod{p}$. Zatem β jest pierwiastkiem kongruencji $g(x) \equiv 0 \pmod{p}$. Ponieważ ta kongruencja ma nie więcej niż $(n - 1)$ rozwiązań, kongruencja $(*)$ ma co najwyżej $(n - 1)$ rozwiązań różnych od α , a więc razem ma nie więcej niż n rozwiązań, co kończy rozumowanie indukcyjne.

- **Wniosek 0.8** *Jeżeli kongruencja $f(x) \equiv 0 \pmod{p}$ ma więcej niż n rozwiązań, to jest ona tożsamością, tzn. jest spełniona przez każdą liczbę całkowitą.*

Zauważmy, że nie trzeba tu zakładać, iż p nie dzieli a_n . Niech bowiem

$$k = \max\{i : p \text{ nie dzieli } a_i\}.$$

Jeśli $k < n$, to a_{k+1}, \dots, a_n są podzielne przez p , więc

$$a_n x^n + \dots + a_{k+1} x^{k+1} \equiv 0 \pmod{p}.$$

Kongruencja $(*)$ sprowadza się więc do:

$$a_k x^k + \dots + a_1 x + a_0 \equiv 0 \pmod{p}.$$

Ta zaś kongruencja, w przypadku $k > 0$, może mieć tylko k rozwiązań na mocy tw. Lagrange'a. Ponieważ ma ich więcej niż $n > k$, musi być tożsamością $k = 0$. To z kolei sprowadza $(*)$ do kongruencji $a_0 \equiv 0 \pmod{p}$, która jest spełniona tylko dla a_0 podzielnego przez p . Ostatecznie wszystkie współczynniki wielomianu $f(x)$ dzielą się przez p , a wtedy $f(x) \equiv 0 \pmod{p}$ dla każdego x . ■

Korzystając z ostatniego wniosku, możemy udowodnić charakteryzację liczb pierwszych, podaną przez Wilsona:

⁸Joseph Louis Lagrange, (1736–1813), matematyk francuski, zajmował się teorią liczb, algebrą i mechaniką teoretyczną, której podstawy zawarł w opublikowanym w roku 1788 dziele *Mécanique analytique*

- **Twierdzenie 0.18** (WILSON): Liczba $p > 1$ jest pierwsza wtedy i tylko wtedy, gdy $p \mid (p-1)! + 1$.

D o w ó d. Niech $p > 2$ będzie liczbą pierwszą. Niech

$$f(x) = (x-1)(x-2)\dots(x-(p-1)) - x^{p-1} + 1.$$

Wykonując działania i porządkując wyrazy według potęg x stwierdzamy, że f jest wielomianem stopnia $p-2$ o współczynnikach całkowitych. Rozpatrzmy kongruencję (*) $f(x) \equiv 0 \pmod{p}$. Z twierdzenia Fermata wynika, że dla każdego $x < p$ jest

$$-x^{p-1} + 1 \equiv 0 \pmod{p}.$$

(*) sprowadza się więc do

$$(x-1)(x-2)\dots(x-(p-1)) \equiv 0 \pmod{p}$$

a więc liczby $1, 2, \dots, p-1$ są rozwiązaniami tej kongruencji. Na mocy wniosku z twierdzenia Lagrange'a, (*), jako kongruencja stopnia $p-2$, jest tożsamością, w szczególności jest spełniona przez $x = 0$, co daje:

$$f(0) \equiv (-1)^{p-1}(p-1)! + 1 \pmod{p}$$

czyli $p \mid (p-1)! + 1$ (oczywiście $p-1$ jest parzyste dla $p > 2$, bo p jest liczbą pierwszą). Dla $p=2$ twierdzenie jest oczywiste.

Odwrotnie, przypuśćmy, że $p \mid (p-1)! + 1$. Niech q będzie dowolnym mniejszym niż p dzielnikiem p . Wtedy $q \mid (p-1)! + 1$. Ponieważ jednak $q \in \{1, \dots, p-1\}$, mamy $q \mid (p-1)!$. Stąd $q = 1$. Jedynym mniejszym od p dzielnikiem p jest więc 1, czyli p jest liczbą pierwszą. ■

Podamy teraz kilka przykładów rozwiązywania kongruencji wyższych stopni.

- **Przykład 0.12** Rozwiązać kongruencję $x^4 \equiv 5 \pmod{12}$.

Skorzystajmy z Twierdzenia Eulera. Ponieważ $\Phi(12) = |\{1, 5, 7, 11\}| = 4$, więc dla każdej liczby x względnie pierwszej z 12 mamy $x^4 \equiv 1 \pmod{12}$. Zatem liczby względnie pierwsze z 12 nie spełniają tej kongruencji. Liczby, które nie są względnie pierwsze z 12 też jej oczywiście nie spełniają, bo prawa strona kongruencji jest względnie pierwsza z 12. Stąd wynika, że ta kongruencja nie ma rozwiązań.

- **Przykład 0.13** Rozwiązać kongruencję $x^{13} - x \equiv 0 \pmod{13}$.

Rozwiązaniem tej kongruencji jest każda liczba ze zbioru $\{0, 1, \dots, 12\}$, co wynika z MTF.

- **Przykład 0.14** Rozwiązać kongruencję $x^{100} \equiv 1 \pmod{7}$.

Jeżeli 7 nie dzieli x , to na mocy MTF jest $x^6 \equiv 1 \pmod{7}$. Stąd

$$x^{100} = x^{6 \cdot 16 + 4} \equiv x^4 \equiv 1 \pmod{7}.$$

Ostatnią kongruencję spełniają (co sprawdzamy "na piechotę") tylko 1 i 6. Oczywiście liczby podzielne przez 7 nie spełniają tej kongruencji.

- **Przykład 0.15** Rozwiązać kongruencję $x^5 - 5x^3 + 4x \equiv 1 \pmod{120}$.

Ponieważ $120 = 3 \cdot 5 \cdot 8$ więc wystarczy znaleźć wspólne pierwiastki kongruencji

$$x^5 - 5x^3 + 4x \equiv 0 \pmod{3}, \quad x^5 - 5x^3 + 4x \equiv 0 \pmod{5}, \quad x^5 - 5x^3 + 4x \equiv 0 \pmod{8}.$$

Okazuje się, że każda z nich jest tożsamością. Zatem ta kongruencja ma 120 rozwiązań.

- **Przykład 0.16** Rozwiązać kongruencję $x^7 - x + 1 \equiv 1 \pmod{42}$.

Ponieważ $42 = 2 \cdot 3 \cdot 7$ więc wystarczy znaleźć wspólne pierwiastki kongruencji

$$x^7 - x + 1 \equiv 0 \pmod{2}, \quad x^7 - x + 1 \equiv 0 \pmod{3}, \quad x^7 - x + 1 \equiv 0 \pmod{7}.$$

Okazuje się, że kongruencja $x^7 - x + 1 \equiv 0 \pmod{3}$ nie ma pierwiastków, więc nasza kongruencja nie ma rozwiązań.

Rozwiązując kongruencje liniowe posłużyliśmy się równaniami diofantycznymi. Ale i na odwrót. Kongruencje mogą być bardzo przydatne w rozwiązywaniu równań diofantycznych.

- **Przykład 0.17** Wykazać, że równania $x^3 + y^3 + z^3 = 4$, $x^3 + y^3 + z^3 = 5$ nie mają rozwiązań całkowitych.

Wystarczy zauważyć, że sześciany liczb całkowitych przystają modulo 9 do liczb: 0,1,2,7,8, a suma jakichkolwiek trzech spośród nich nie przystaje modulo 9 ani do 4 ani do 5.

0.6 Cechy podzielności

Cechą podzielności nazywa się twierdzenie, sformułowane w postaci warunku koniecznego i dostatecznego, pozwalające przy pomocy prostych operacji na cyfrach danej liczby sprawdzić czy jest ona podzielna przez ustaloną liczbę. Pożyteczne są cechy podzielności przez liczby pierwsze (podzielność przez złożone do tego się sprowadza) i to - wzięwszy pod uwagę, że operacje mają być nieskomplikowane - przez nieduże liczby pierwsze. Stosuje się je w sytuacjach, gdy nie warto angażować komputera, a czasem w rozważaniach teoretycznych.

Sformułowanie cechy podzielności zależy od liczby, przez którą podzielność badamy, a także od systemu pozycyjnego, w którym zapisujemy liczby (bo różne są cyfry). W systemie dziesiętkowym, oprócz oczywistych cech podzielności przez 10, 2 i 5, łatwo jest sformułować cechę podzielności przez 9 i 3, bo $10^k - (-1)^k$ dzieli się przez 9, oraz przez 11, w zależności od parzystości liczby k . Dowody tych cech podzielności są dostępne dla ucznia szkoły podstawowej, ale chcąc zrozumieć jakie to jest dla niego trudne, powinniśmy sami poszukać jakichś cech podzielności w niedziesiętkowych systemach pozycyjnych, a w dziesiętkowym - cechy podzielności np. przez 7 i 13. Teoretyczną podstawą dla cech podzielności jest pojęcie kongruencji. Jeżeli potrafimy dla pewnej funkcji $f: \rightarrow$ pokazać, że $n \equiv f(n) \pmod{p}$, to w szczególności dotyczy to reszty 0 i można sformułować cechę podzielności przez p : Liczba n dzieli się przez p wtedy i tylko wtedy, gdy $f(n)$ dzieli się przez p . Oczywiście użyteczność takiej cechy podzielności zależy od tego jaka jest funkcja f , czy łatwo obliczyć jej wartości i czy $f(n) < n$. Jeśli tak jest, to taką cechę można stosować wielokrotnie, obliczając $f(f(n))$, $f(f(f(n)))$ itd, aż otrzymamy liczbę dostatecznie małą. Przypomnijmy sobie podstawowe cechy podzielności w systemie o podstawie 10.

Ustalmy oznaczenia:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

Ponieważ $10 \equiv 0 \pmod{2}$, więc

- $a \equiv a_0 \pmod{2}$,

Podobnie, ponieważ

$$10 \equiv 1 \pmod{3}, \quad 10^2 \equiv 1 \pmod{3}, \quad \text{i ogólnie} \quad 10^k \equiv 1 \pmod{3},$$

więc

- $a \equiv a_n + a_{n-1} + \dots + a_2 + a_1 + a_0 \pmod{3}$,

Liczmy dalej w ten sam sposób:

$$10 \equiv 2 \pmod{4} \quad \text{oraz} \quad 10^2 \equiv 0 \pmod{4}$$

więc dla każdego $k > 1$ mamy $10^k \equiv 0 \pmod{4}$, a stąd

- $a \equiv a_1 \cdot 10 + a_0 \pmod{4}$,

Dla kongruencji o module 5 mamy:

$$10 \equiv 0 \pmod{5} \quad \text{więc} \quad 10^k \equiv 0 \pmod{5} \quad \text{dla wszystkich} \quad k > 1.$$

Stąd

- $a \equiv a_0 \pmod{5}$,

Ponieważ $6 = 2 \cdot 3$, więc

- $a \equiv 0 \pmod{6}$, wtedy i tylko wtedy, gdy
 $a_0 \equiv 0 \pmod{2}$ oraz $a_n + a_{n-1} + \dots + a_2 + a_1 + a_0 \equiv 0 \pmod{3}$,

Dla kongruencji o module 8 mamy:

$$10 \equiv 2 \pmod{8}, \quad 10^2 \equiv 4 \pmod{8} \quad \text{oraz} \quad 10^3 \equiv 0 \pmod{8}$$

więc dla każdego $k > 2$ jest $10^k \equiv 0 \pmod{8}$, a stąd

- $a \equiv a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \pmod{8}$,

Podobnie sprawdzamy następne kongruencje.

- $a \equiv a_n + a_{n-1} + \dots + a_2 + a_1 + a_0 \pmod{9}$,

- $a \equiv a_0 \pmod{10}$,

Zajmijmy się teraz jedną z najstarszych cech podzielności przez 7. Sprawdźmy najpierw, jakie są reszty z dzielenia przez 7 kolejnych potęg liczby 10.

$$10^0 = 0 \cdot 7 + 1, \quad \text{czyli} \quad 10^0 \equiv 1 \pmod{7}$$

$$10^1 = 1 \cdot 7 + 3, \quad \text{czyli} \quad 10^1 \equiv 3 \pmod{7}$$

$$10^2 = 14 \cdot 7 + 2, \quad \text{czyli} \quad 10^2 \equiv 2 \pmod{7}$$

$$10^3 = 142 \cdot 7 + 6, \quad \text{czyli} \quad 10^3 \equiv 6 \pmod{7}$$

$$10^4 = 1428 \cdot 7 + 4, \quad \text{czyli} \quad 10^4 \equiv 4 \pmod{7}$$

$$10^5 = 14285 \cdot 7 + 5, \quad \text{czyli} \quad 10^5 \equiv 5 \pmod{7}$$

$$10^6 = 142857 \cdot 7 + 1, \quad \text{czyli} \quad 10^6 \equiv 1 \pmod{7}.$$

Ponieważ każdą liczbę a można zapisać w postaci

$$\begin{aligned} a &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &= b \cdot 10^6 + \left[a_5(14285 \cdot 7 + 5) + a_4(1428 \cdot 7 + 4) + a_3(142 \cdot 7 + 6) \right. \\ &\quad \left. + a_2(14 \cdot 7 + 2) + a_1(1 \cdot 7 + 3) + a_0(0 \cdot 7 + 1) \right] \end{aligned}$$

więc

$$a \equiv b \cdot 10^6 + a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 \pmod{7}.$$

Z b można postąpić podobnie. Zatem liczba a dzieli się przez 7 wtedy i tylko wtedy, gdy podzielna jest przez 7 liczba, którą otrzymujemy dodając do siebie iloczyny cyfr jedności, dziesiątek, ... kolejno przez 1, 3, 2, 6, 4, 5 i powtarzając tę operację tak długo, jak to jest konieczne (to znaczy do momentu wyczerpania cyfr liczby a). Rachunek ten można nieco uprościć. Mianowicie każdy z otrzymanych wcześniej iloczynów można zastąpić resztą z dzielenia go przez 7. Oczywiście jest też, że reszta z dzielenia wyjściowej liczby przez 7 jest taka sama jak reszta z dzielenia ostatnio otrzymanej liczby przez 7.

Podobnie możemy znaleźć cechę podzielności np. przez 13.

$$\begin{array}{ll} 10^0 = 0 \cdot 13 + 1, & \text{czyli } 10^0 \equiv 1 \pmod{13} \\ 10^1 = 1 \cdot 13 + 10, & \text{czyli } 10^1 \equiv 10 \pmod{13} \\ 10^2 = 7 \cdot 13 + 9, & \text{czyli } 10^2 \equiv 9 \pmod{13} \\ 10^3 = 76 \cdot 13 + 12, & \text{czyli } 10^3 \equiv 12 \pmod{13} \\ 10^4 = 769 \cdot 13 + 3, & \text{czyli } 10^4 \equiv 3 \pmod{13} \\ 10^5 = \cdot 13 + 4, & \text{czyli } 10^5 \equiv 4 \pmod{13} \\ 10^6 = \cdot 13 + 1, & \text{czyli } 10^6 \equiv 1 \pmod{13}. \end{array}$$

Postępując tak, jak w przypadku $n = 7$ widzimy, że

$$a \equiv b \cdot 10^6 + a_0 + 10a_1 + 9a_2 + 12a_3 + 3a_4 + 4a_5 \pmod{13}.$$

Postępując z b podobnie, widzimy, że liczba a dzieli się przez 13 wtedy i tylko wtedy, gdy podzielna jest przez 13 liczba, którą otrzymujemy dodając do siebie iloczyny cyfr jedności, dziesiątek, ... kolejno przez 1, 10, 9, 12, 3, 4 i powtarzając tę operację do momentu wyczerpania cyfr liczby a . Rachunek ten można oczywiście uprościć, zastępując każdy z otrzymanych iloczynów resztą z dzielenia go przez 13. Oczywiście jest też, że reszta z dzielenia wyjściowej liczby przez 13 jest taka sama jak reszta z dzielenia ostatnio otrzymanej liczby przez 13.

Jak łatwo się domyślić, podstawa systemu nie odgrywa roli przy szukaniu cech podzielności. Zróbmy to zatem w systemach przy innych podstawach.

W systemie przy podstawie $c = 2$ liczba a ma przedstawienie

$$a = a_n \cdot 2^n + a_{n-1} \cdot 2^{n-1} + \dots + a_2 \cdot 2^2 + a_1 \cdot 2 + a_0, \text{ gdzie } a_0, a_1, \dots, a_n \in \{0, 1\}$$

i oczywiście są kongruencje

$$a \equiv a_0 \pmod{2} \quad a \equiv 2a_1 + a_0 \pmod{4}$$

i ogólnie

$$a \equiv 2^{k-1}a_{k-1} + \dots + 2a_1 + a_0 \pmod{2^k}$$

Łatwo sprawdzić, że w systemie przy dowolnej podstawie c liczba a , o przedstawieniu

$$a = a_n \cdot c^n + a_{n-1} \cdot c^{n-1} + \dots + c_2 \cdot c^2 + a_1 \cdot c + a_0, \text{ gdzie } a_0, a_1, \dots, a_n \in \{0, 1, \dots, c-1\}$$

przystaje modulo c^k do liczby $a_{k-1} \cdot c^{k-1} + \dots + a_1 \cdot c + a_0$. W szczególności jest podzielna przez c^k wtedy i tylko wtedy, gdy

$$a_{k-1} = a_1 = \dots = a_0 = 0$$

Cecha podzielności przez 3 w systemie dwójkowym to szczególny przypadek ostatniego twierdzenia. Poszukajmy cechy podzielności przez 5. Mamy

$$2^0 \equiv 1 \pmod{5}, \quad 2^1 \equiv 2 \pmod{5}, \quad 2^2 \equiv 4 \pmod{5}, \quad 2^3 \equiv 3 \pmod{5}.$$

Ponieważ $2^4 \equiv 1 \pmod{5}$, więc wszystko zaczyna się powtarzać i otrzymujemy

$$a \equiv b \cdot 2^4 + c_0 + 2c_1 + 4c_2 + 3c_3 \pmod{5}.$$

Podobnie, jak w przypadku przedstawienia liczby w systemie dziesiętnym, widzimy, że liczba a dzieli się przez 5 wtedy i tylko wtedy, gdy podzielna jest przez 5 liczba, którą otrzymujemy dodając do siebie iloczyny współczynników przy kolejnych potęgach podstawy 2 kolejno przez 1, 2, 4, 3 i powtarzając tę operację do momentu wyczerpania cyfr liczby a . Oczywiście jest też, że reszta z dzielenia wyjściowej liczby przez 5 jest taka sama jak reszta z dzielenia ostatnio otrzymanej liczby przez 5.

Cecha podzielności przez 7 jest jeszcze prostsza.

$$2^0 \equiv 1 \pmod{7}, \quad 2^1 \equiv 2 \pmod{7}, \quad 2^2 \equiv 4 \pmod{7}, \quad 2^3 \equiv 1 \pmod{7}$$

więc

$$a \equiv b \cdot 2^3 + c_0 + 2c_1 + 4c_2 \pmod{7}.$$

Zatem tym razem widzimy, że liczba a dzieli się przez 7 wtedy i tylko wtedy, gdy podzielna jest przez 5 liczba, którą otrzymujemy dodając do siebie iloczyny współczynników przy kolejnych potęgach podstawy 2 kolejno przez 1, 2, 4 i powtarzając tę operację do momentu wyczerpania cyfr liczby a .

Zamiast dowodzić cechy podzielności przez 11 w systemie o podstawie 10 zajmijmy się ogólnie kongruencją modulo $c+1$ w systemie o podstawie c . Ponieważ

$$c^0 \equiv 1 \pmod{c+1} \text{ oraz } c^1 \equiv -1 \pmod{c+1},$$

więc

$$c^{2k} \equiv 1 \pmod{c+1} \text{ oraz } c^{2k+1} \equiv -1 \pmod{c+1}.$$

Stąd, jeżeli

$$a = a_k \cdot c^k + a_{k-1} \cdot c^{k-1} + \dots + a_2 \cdot c^2 + a_1 \cdot c + a_0,$$

to

$$\bullet a \equiv (a_0 - a_1 + a_2 - a_3 + \dots + (-1)^k \cdot a_k) \pmod{c+1}$$

0.7 Ćwiczenia

(Liczby pierwsze i liczby złożone. Podzielność w zbiorze liczb całkowitych.)

1. Udowodnić, że:

a) jeżeli p jest liczbą pierwszą większą od 3, to $p^2 - 1$ dzieli się przez 24.

b) jeżeli liczby pierwsze p, q są większe od 3, to $p^2 - q^2$ dzieli się przez 24.

2. Pokazać, że suma dwu liczb pierwszych różniących się o 2, z których mniejsza jest większa od 3, jest podzielna przez 12.

3. Znaleźć wszystkie liczby pierwsze p , takie, że $p+2$ i $p+4$ też są liczbami pierwszymi.

3. Udowodnić, że jeżeli p i $p+2$ są liczbami pierwszymi większymi od 3, to liczba $p+1$ jest podzielna przez 6.

4. Udowodnić, że jeżeli liczby p i $4p+1$ są liczbami pierwszymi, to liczba $8p+1$ nie jest liczbą pierwszą.

5. Wykazać, że dla każdej liczby naturalnej n większej od 2 jedna z liczb $2^n - 1$, $2^n + 1$ jest złożona.

6. Udowodnić, że jeżeli liczba $2^n - 1$ jest pierwsza, to n jest liczbą pierwszą.

7. Udowodnić, że jeżeli liczba $(n-1)!+1$ jest większa od 1 i podzielna przez n , to n jest liczbą pierwszą.

8. Pokazać, że dla każdego n liczby $n+1$ oraz $2n+1$ są względnie pierwsze.

9. Pokazać, że dla dowolnej liczby naturalnej n liczba $n+n^2+\dots+n^{100}$ jest podzielna przez $n(n+1)$.

10. Pokazać, że jeżeli liczba naturalna n jest podzielna przez 3 i nie dzieli się przez 6, to liczba n^2+7 jest podzielna przez 8.

11. Udowodnić, że dla dowolnej liczby naturalnej n liczba $(n+1)^n - 1$ jest podzielna przez n^2 .

12. Pokazać, że jeżeli liczby n i k nie są względnie pierwsze, to liczby $n+k$ oraz $n-k$ też nie są względnie pierwsze.

13. Pokazać, że liczby $n!+1$ oraz $(n+1)!+1$ są względnie pierwsze.

14. Wykazać, że dla dowolnych liczb całkowitych a, b, c liczba $a^3+b^3+c^3$ jest podzielna przez 6 wtedy i tylko wtedy, gdy liczba $a+b+c$ jest podzielna przez 6.

15. Wykazać, że co najmniej jedna z liczb $n^3 - n$ i $n^3 + n$ jest podzielna przez 10.

16. Niech $p_1 < p_2 < \dots < p_n$ będzie ciągiem liczb pierwszych. Sprawdzić, czy zawsze liczba $p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$ jest pierwsza.

(Algorytm Euklidesa. Największy wspólny dzielnik i najmniejsza wspólna wielokrotność.)

1. Znaleźć a i b wiedząc, że:

a) $NWD(a, b) = 12$ i $NWW(a, b) = 168$, b) $NWD(a, b) = 20$ i $NWW(a, b) = 385$,

Ile jest rozwiązań?

2. Jeżeli $d = NWD(a, b)$, to liczby $\frac{a}{d}$ i $\frac{b}{d}$ są względnie pierwsze, jeśli tylko żadna z nich nie jest zerem.

3. Jeżeli $NWD(a, b) = 1$, to dla dowolnej liczby naturalnej c zachodzi równość $NWD(ac, bc) = c$.

4. Pokazać, że jeżeli $(a, b) = 1$, $(c, d) = 1$ oraz $\frac{a}{b} + \frac{c}{d}$ jest liczbą całkowitą, to $b = d$.

5. Dowieść, że ułamek dopełniający do 1 dany ułamek nieskracalny właściwy jest też ułamkiem właściwym.

6. Udowodnić, że jeżeli liczby a, b, c są nieparzyste, to

$$NWD(a, b, c) = NWD\left(\frac{a+b}{2}, \frac{b+c}{2}, \frac{c+a}{2}\right).$$

7. Pokazać, że dla dowolnych liczb całkowitych a, b, c zachodzą wzory

a) $NWW(a, NWD(b, c)) = NWD(NWW(a, b), NWW(a, c))$

b) $NWD(a, NWW(b, c)) = NWW(NWD(a, b), NWD(a, c))$

(Równania diofantyczne. Kongruencje.)

1. Podać rozwiązania ogólne następujących liniowych równań diofantycznych:

a) $2x+3y=5$; b) $2x+3y=4$; c) $3x+9y=33$.

2. Wyznaczyć liczbę trzycyfrową, która jest dwanaście razy większa od sumy swoich cyfr.

3. Znaleźć wszystkie całkowite rozwiązania następujących równań:

a) $2x^3+xy-7=0$; b) $(x+1)(y-2)=2$; c) $x(y^2-1)=48$; d) $x^2-y^2=24$;

e) $xy=x+2y$; f) $xy=2x+5y+7$; g) $xy=3x+8y+1$.

4. Znaleźć wszystkie naturalne rozwiązania następujących równań:

a) $y+x^2=27$; b) $y+2x^2=17x$; c) $x+y+z=xyz$.

5. Wiek pewnego obywatela w roku 1887 równał się sumie cyfr roku jego urodzenia. Ile miał on lat?

6. Wykazać, że równanie $15x^2-7y^2=9$ nie ma rozwiązań całkowitych.

7. Dowieść, że równanie $x^2-2y^2+8z=3$ nie ma rozwiązań w liczbach całkowitych.

8. Rozwiązać w liczbach całkowitych równanie $x^3-2y^3-4z^3=0$.

9. Pokazać, że nie ma dwu liczb naturalnych, których suma i różnica kwadratów byłyby kwadratami liczb całkowitych.

10. Pokazać, że nie ma trzech kwadratów liczb naturalnych tworzących postęp arytmetyczny, którego różnica byłaby również kwadratem liczby naturalnej.

(Kongruencje. Cechy podzielności.)

1. Rozwiązać następujące kongruencje:

a) $3x=2 \pmod{5}$; b) $243x+17=101 \pmod{725}$; c) $6x+3=4 \pmod{10}$;

d) $7x=4 \pmod{10}$; e) $4x+3=4 \pmod{5}$; f) $6x+3=1 \pmod{10}$.

2. Znaleźć dwie ostatnie cyfry liczby 2^{999} .

3. Dowieść, że dla m całkowitego $m^2=0, 1$ albo $4, \pmod{8}$.

4. Wykazać, że jeżeli x jest liczbą nieparzystą i niepodzielną przez 3, to $x^2=1 \pmod{24}$.

5. Wyznaczyć wszystkie rozwiązania kongruencji :

a) $x^{1000} \equiv 1 \pmod{13}$, b) $x^{2003} \equiv 1 \pmod{7}$.

6. Udowodnić, że: $10|3^{24}-11^3$; $11 \cdot 31 \cdot 61|20^{15}-1$ oraz $19|2^{2^{6k+2}}+3$

7. Zbadać, dla naturalnych n , która z dwu liczb $a_n=2^{2n+1}-2^{n+1}+1$ oraz $b_n=2^{2n+1}+2^{n+1}+1$ jest, a która nie jest podzielna przez 5

Wsk. Rozpatrzyć przypadki: $n=4k$, $n=4k+1$, $n=4k+2$, $n=4k+3$,

8. Udowodnić, że liczba $55^{37} - 77^{17}$ jest złożona.
9. Dowieść, że jeżeli p jest liczbą pierwszą, to $\binom{p}{k} \equiv 0 \pmod{p}$ dla $k = 0, 1, \dots, p - 1$.
10. Znaleźć wszystkie pary (m, n) , dla których liczba sześciocyfrowa $2547mn$ jest podzielna przez 15 i nie jest podzielna przez 25.
11. Korzystając z Małego Twierdzenia Fermata znaleźć wszystkie liczby pierwsze p takie, że: a) $2^p + 1$ jest podzielne przez p ; b) $12^p + 5$ jest podzielne przez p
12. Udowodnić, że wśród liczb postaci $2p + 1$, gdzie p jest liczbą pierwszą, jest dokładnie jeden sześcian liczby naturalnej.
13. Znaleźć cechę podzielności przez 13 w systemie dziesiętnym.
14. Znaleźć cechę podzielności przez 5, 6, 7 w systemie dwójkowym.
15. Znaleźć cechę podzielności przez n w systemie o podstawie $(n + 1)$.
16. Czy istnieje liczba trzycyfrowa podzielna przez 11, której pierwsza cyfra jest większa od drugiej, a druga od trzeciej.