Arytmetyka elementarna
Notatki z wykładu

Maciej Paluszyński

8 czerwca 2010

Spis treści

Rozdział 1

Podzielność liczb

Dzielniki

Jeżeli dla dwóch liczb całkowitych a, b istnieje trzecia, k, taka że

$$a = k \cdot b$$

to piszemy $b \mid a$ (b dzieli a, lub a jest wielokrotnością b). Zauważmy, że:

- każda liczba całkowita dzieli 0, a 0 dzieli tylko 0. Zero nie jest więc interesujące.
- 1 ma dokładnie 2 dzielniki, 1 i -1.
- $b \mid a \ \leftrightarrow \ (-b) \mid a$. Wystarczy więc rozważać dzielniki naturalne. Niech więc

  $$\theta(a) \ - \text{ ilość naturalnych dzielników } a.$$

  Na przykład $\theta(1) = 1$, $\theta(8) = 4$, $\theta(10) = 4$. Zauważmy, że dla $k \in \mathbf{N}$ $\theta(k)$ jest parzysta (każdy dzielnik ma dzielnik dopełniczy) chyba, że k jest kwadratem, wtedy $\theta(k)$ jest nieparzysta.

Fakt 1.1. *Własność podzielności jest przechodnia, to znaczy jeżeli $b \mid a$ i $c \mid b$ to także $c \mid a$.*

Dowód. $b \mid a$ czyli $a = k \cdot b$ dla pewnego k oraz $c \mid b$ czyli $b = m \cdot c$ dla pewnego m. W takim razie $a = k \cdot b = km \cdot c$, czyli $c \mid a$. □

W skrócie możemy to wyrazić: „dzielnik dzielnika jest dzielnikiem", lub „wielokrotność wielokrotności jest wielokrotnością".

Fakt 1.2. *Dla $n \in \mathbf{N}$ zachodzi $\theta(n) \leq n$.*

Dowód. Każdy dzielnik n jest nie większy od n, a liczba wszystkich liczb naturalnych nie większych od n to właśnie n. □

Typowym zadaniem w elementarnej teorii liczb jest znalezienie wszystkich dzielników danej liczby $n \in \mathbf{N}$. Możemy zrobić to w ten sposób, że badamy podzielność n przez kolejne liczby, począwszy od 2, a skończywszy na największej liczbie naturalnej $\leq \sqrt{n}$. Na przykład znajdziemy wszystkie dzielniki liczby $n = 60$. Widzimy kolejno, że dzielnikami są 1, 2, 3, 4, 5 i 6. 7 nie jest dzielnikiem, i jest ostatnią liczbą, którą musimy sprawdzić. Każdy ewentualny dzielnik większy od 7 ma dzielnik „dopełniczy", nie większy niż 7, który już zidentyfikowaliśmy. Listę dzielników liczby $n = 60$ uzupełniamy o dzielniki „dopełnicze": 60, 30, 20, 15, 12 i 10. Ostatecznie $\theta(60) = 12$.

NWD i NWW

Rozważmy zbiór $\mathcal{A} = \{a_1, a_2, \ldots, a_n, \ldots\} \subset \mathbf{N}$ (niepusty, skończony lub nieskończony). Rozważmy zbiór liczb, które są dzielnikami wszystkich a_i. Ten zbiór jest niepusty (1 do niego należy), i oczywiście skończony: każdy wspólny dzielnik jest w szczególności dzielnikiem a_1, a więc zbiór wszystkich wspólnych dzielników jest podzbiorem zbioru dzielników a_1. Zbiór wszystkich wspólnych dzielników $\mathcal{A}$ jako zbiór niepusty i skończony ma element największy, i element ten nazywamy największym wspólnym dzielnikiem $\mathcal{A}$, a oznaczamy $\mathbf{NWD}(\mathcal{A}) = \mathbf{NWD}(a_1, a_2, \ldots)$. Dla zbioru $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$ skończonego rozważmy zbiór wszystkich wspólnych wielokrotności, czyli liczb naturalnych będących wielokrotnościami każdego elementu $\mathcal{A}$. Jest to zbiór niepusty, gdyż zawiera iloczyn $a_1 \cdot a_2 \cdot \ldots \cdot a_n$. Jako podzbiór zbioru liczb naturalnych zawiera element najmniejszy, który oznaczamy $\mathbf{NWW}(\mathcal{A}) = \mathbf{NWW}(a_1, \ldots, a_n)$ i nazywamy najmniejszą wspólną wielokrotnością $\mathcal{A}$.

Fakt 1.3. *Każda wspólna wielokrotność danego zbioru $\mathcal{A}$ jest podzielna przez* $\mathbf{NWW}(\mathcal{A})$.

Dowód. Niech W będzie wspólną wielokrotnością elementów $\mathcal{A}$. Podzielmy W przez $\mathbf{NWW}(\mathcal{A})$ z resztą:

$$W = k \cdot \mathbf{NWW}(\mathcal{A}) + r, \quad k, r \in \mathbf{Z},\ 0 \leq r < \mathbf{NWW}(\mathcal{A}).$$

Wtedy $r = W - \mathbf{NWW}(\mathcal{A})$ jest wspólną wielokrotnością $\mathcal{A}$, a skoro $r < \mathbf{NWW}(\mathcal{A})$, to musi być $r = 0$. □

Fakt 1.4. *Niech D będzie wspólnym dzielnikiem zbioru $\mathcal{A}$. Wtedy D dzieli* $\mathbf{NWD}(\mathcal{A})$.

Dowód. Weźmy dowolną liczbę $a \in \mathcal{A}$. a jest wspólną wielokrotnością D i $\mathbf{NWD}(\mathcal{A})$, a w takim razie, zgodnie z poprzednim Faktem,

$$\mathbf{NWW}(D, \mathbf{NWD}(\mathcal{A})) \,\big|\, a.$$

Skoro a była dowolną z liczb ze zbioru $\mathcal{A}$, to w takim razie $\mathbf{NWW}(D, \mathbf{NWD}(\mathcal{A}))$ jest wspólnym dzielnikiem liczb ze zbioru $\mathcal{A}$. W takim razie

$$\mathbf{NWW}(D, \mathbf{NWD}(\mathcal{A})) \leq \mathbf{NWD}(\mathcal{A}).$$

Musi więc zachodzić równość $\mathbf{NWW}(D, \mathbf{NWD}(\mathcal{A})) = \mathbf{NWD}(\mathcal{A})$ i w takim razie

$$D \,\big|\, \mathbf{NWD}(\mathcal{A}).$$

□

Fakt 1.5. *Dla dowolnych liczb $a, b \in \mathbf{N}$ zachodzi wzór*

$$a \cdot b = \mathbf{NWD}(a, b)\mathbf{NWW}(a, b).$$

Dowód. $a \cdot b$ jest wspólną wielokrotnością obu swoich czynników, więc zgodnie z Faktem 1.3

$$\mathbf{NWW}(a, b) \,\big|\, a \cdot b,$$

czyli istnieje $n \in \mathbf{N}$ takie, że

$$a \cdot b = n \cdot \mathbf{NWW}(a, b).$$

Z drugiej strony istnieje $k \in \mathbf{N}$ takie, ze $\mathbf{NWW}(a, b) = k \cdot a$, a więc

$$a \cdot b = n \cdot k \cdot a \;\Rightarrow\; b = n \cdot k,$$

czyli n jest dzielnikiem b. Podobnie możemy pokazać, że $n \,\big|\, a$, a więc n jest wspólnym dzielnikiem, czyli, na mocy Faktu 1.4

$$n \,\big|\, \mathbf{NWD}(a, b). \tag{1.1}$$

Z drugiej strony

$$a = r \cdot \mathbf{NWD}(a, b), \quad b = s \cdot \mathbf{NWD}(a, b),$$

czyli $r \cdot s \cdot \mathbf{NWD}(a, b)$ jest wspólną wielokrotnością a i b, a więc

$$r \cdot s \cdot \mathbf{NWD}(a, b) = m \cdot \mathbf{NWW}(a, b),$$

czyli

$$n{\cdot}r{\cdot}s{\cdot}\mathbf{NWD}(a, b) = n{\cdot}m\mathbf{NWW}(a, b) = m{\cdot}a{\cdot}b = m{\cdot}r{\cdot}s\mathbf{NWW}(a, b){\cdot}\mathbf{NWW}(a, b).$$

skracając, otrzymujemy

$$n = m \cdot \mathbf{NWD}(a, b) \;\Rightarrow\; \mathbf{NWD}(a, b) \,\big|\, n,$$

co w połączeniu z (1.1) daje $n = \mathbf{NWD}(a, b)$. □

Liczby względnie pierwsze

Jeżeli $\mathbf{NWD}(a,b) = 1$ to mówimy, że a i b są względnie pierwsze.

Fakt 1.6. *dla dowolnych liczb* $a, b \in \mathbf{N}$ *liczby*

$$k = \frac{a}{\mathbf{NWD}(a,b)}, \qquad l = \frac{b}{\mathbf{NWD}(a,b)}$$

są względnie pierwsze.

Dowód. Niech $d = \mathbf{NWD}(k,l)$. Liczba $d \cdot \mathbf{NWD}(a,b)$ jest wtedy wspólnym dzielnikiem a i b, a skoro $\mathbf{NWD}(a,b)$ jest największy, to $d \leq 1$ czyli $d = 1$. □

Fakt 1.7. *Jeżeli* $\mathbf{NWD}(a,b) = 1$ *i* $c \in \mathbf{N}$*, to* $\mathbf{NWD}(ac,bc) = c$.

Dowód. liczba c jest wspólnym dzielnikiem ac i bc, a więc

$$c \,\big|\, \mathbf{NWD}(ac,bc).$$

Mamy

$$u \cdot c = \mathbf{NWD}(ac,bc) \quad \text{oraz} \quad a \cdot c = k \cdot \mathbf{NWD}(ac,bc),$$

czyli

$$k \cdot u \cdot c = k \cdot \mathbf{NWD}(ac,bc) = a \cdot c \;\Rightarrow\; k \cdot u = a \;\Rightarrow\; u \,\big|\, a.$$

Podobnie $u \,\big|\, b$, a więc u jest wspólnym dzielnikiem a i b, a więc $u = 1$ czyli $c = \mathbf{NWD}(ac,bc)$. □

Fakt 1.8. *Jeżeli* $c \,\big|\, a \cdot b$ *i* $\mathbf{NWD}(a,c) = 1$ *to* $c \,\big|\, b$.

Dowód. c jest wspólnym dzielnikiem ab i bc. Ponieważ $\mathbf{NWD}(a,c) = 1$ to z Faktu 1.7 mamy $\mathbf{NWD}(ab,bc) = b$. Tak więc $c \,\big|\, b$. □

Fakt 1.9 (Zasadnicze twierdzenie arytmetyki)**.** *Jeżeli* $a, b, c \in \mathbf{N}$*,* $\mathbf{NWD}(a,c) = 1$ *oraz* $\mathbf{NWD}(b,c) = 1$ *to także*

$$\mathbf{NWD}(a \cdot b, c) = 1.$$

Dowód. Niech $u = \mathbf{NWD}(a \cdot b, c)$. Wtedy $u \,\big|\, c$ i $u \,\big|\, a \cdot b$. Zauważmy, że u i a muszą być względnie pierwsze: jakikolwiek wspólny dzielnik u i a jest też wspólnym dzielnikiem c i a. Z Faktu 1.8 $u \,\big|\, b$. u jest więc wspólnym dzielnikiem b i c, czyli zgodnie z założeniem $u = 1$. □

Liczby pierwsze

Liczba naturalna $p > 1$ nazywa się liczbą pierwszą, jeżeli $\theta(p) = 2$, czyli jedynymi dzielnikami p są 1 i p. Zauważmy, że 1 nie uważamy za liczbę pierwszą, i najmniejszą liczbą pierwszą jest 2. Jest to także jedyna parzysta liczba pierwsza.

Twierdzenie 1.10. *Każda liczba naturalna $n > 1$ ma przynajmniej jeden dzielnik będą cy liczbą pierwszą.*

Dowód. Skoro $n > 1$ to n ma dzielniki większe od 1, na przykład samo n. Niech p będzie najmniejszym spośród wszystkich dzielników n większych od 1. Liczba p jest albo pierwsza, i wtedy twierdzenie zachodzi, albo sama ma dzielnik d, różny od p i od 1: $1 < d < p$, $d \mid p$. Ale wtedy d jest dzielnikiem n, większym od 1, i mniejszym od p, co jest sprzeczne z wyborem p. Liczba p musi więc być pierwsza. □

Uwaga: W praktyce taki dzielnik może być trudno znaleźć. Na przykład nie znamy żadnego dzielnika pierwszego liczby $2^{257} - 1$. (Liczba ta ma 78 cyfr.)

Fakt 1.11. *Dla każdej liczby naturalnej n istnieje liczba pierwsza większa od niej.*

Dowód. Dowód przeprowadzimy nie wprost. Załóżmy, że wszystkie liczby pierwsze są mniejsze lub równe n. Rozważmy liczbę $m = n! + 1$. Na mocy Twierdzenia 1.10 liczba ta ma dzielnik będący liczbą pierwszą. Ale żaden dzielnik m nie może być mniejszy lub równy n: ponieważ dzielnik taki byłby również dzielnikiem $n!$, a w konsekwencji dzielnikiem 1. □

Wniosek 1.12. *Liczb pierwszych jest nieskończenie wiele.*

n-tą kolejną liczbę pierwszą oznaczamy p_n: $p_1 = 2,\ p_2 = 3,\ p_3 = 5, \ldots$. Miliony początkowych wyrazów tego ciągu są znane, na przykład $p_{100} = 541$. Największa znana liczba pierwsza to $2^{11213} - 1$, ma 3376 cyfr. Miliardowa liczba pierwsza ma 11 cyfr, ale nie potrafimy jej wypisać. W dzisiejszych czasach największym zainteresowaniem, ze względu na zastosowania w kryptografii, cieszą się liczby pierwsze o kilkudziesięciu – kilkuset cyfrach dziesiętnych.

Liczby Fermata

Liczby Fermata to liczby postaci

$$F_n = 2^{2^n} + 1, \qquad n = 0, 1, 2, \ldots$$

May więc $F_1 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 4097, \ldots$ Fermat przypuszczał, że wszystkie liczby F_n są pierwsze, ale okazało się, że tak nie jest, na przykład F_5 nie jest pierwsza. Zagadnienie związane z tymi liczbami są jednak wystarczająco interesujące, i od kilkuset lat są obiektem badań. My udowodnimy prosty fakt dotyczący tych liczb, który wykorzystamy do oszacowania „gęstościżozłożenia liczb pierwszych wśród liczb naturalnych.

Fakt 1.13. *Dla $m \neq n$ liczby Feramata F_m i F_n są względnie pierwsze.*

Dowód. Liczby m i n są różne, i niech m będzie większa: $0 \leq n < m$. Istnieje więc $k \in \mathbf{N}$ taka, że $m = n + k$. Niech

$$\mathbf{NWD}(F_m, F_n) = d.$$

Naszym celem jest pokazanie, że $d = 1$. Załóżmy więc, że $d > 1$, a w takim razie d ma dzielnik pierwszy p. Istnieje więc liczba pierwsza p taka, że $p \,\big|\, F_n$ i $p \,\big|\, F_m$. Istnieje więc $u \in \mathbf{N}$ takie, że

$$F_n = 2^{2^n} + 1 = u \cdot p, \;\Rightarrow\; 2^{2^{n+k}} = 2^{2^n \cdot 2^k} = \left(2^{2^n}\right)^{2^k} = (u \cdot p - 1)^{2^k}.$$

Ale

$$(u \cdot p - 1)^{2^k} = s \cdot p + 1 \tag{1.2}$$

dla pewnej liczby $s \in \mathbf{N}$. Wynika to wprost ze wzoru dwumianowego Newtona:

$$(u \cdot p - 1)^{2^k} = \sum_{l=0}^{2^k} \binom{2^k}{l} t^l p^l (-1)^{2^k - l} = (-1)^{2^k} + \sum_{l=1}^{2^k} \binom{2^k}{l} t^l p^l (-1)^{2^k - l},$$

czyli, skoro potęga 2^k jest parzysta, otrzymujemy (1.2), gdzie

$$s = \sum_{l=1}^{2^k} \binom{2^k}{l} t^l p^{l-1} (-1)^{2^k - l}.$$

Mamy więc

$$2^{2^m} = 2^{2^{k+n}} = (u \cdot p - 1)^{2^k} = s \cdot p + 1,$$

czyli

$$F_m = 2^{2^m} + 1 = s \cdot p + 2.$$

Ponieważ, jak założyliśmy, $p \,\big|\, F_m$, więc także $p|2$ czyli $p = 2$, a to jest niemożliwe, gdyż wszystkie liczby Fermata są nieparzyste. □

Niech q_n będzie najmniejszym pierwszym dzielnikiem liczby F_n. Dla $m \neq n$ q_m i q_n są różnymi liczbami pierwszymi. Ciąg $q_0, q_1, q_2, \ldots, q_{n-1}$ składa się więc z n różnych liczb pierwszych z których każda jest mniejsza od $2^{2^{n-1}}+1 < 2^{2^n}$. Dla dowolnego $n \in en$ istnieje więc co najmniej n liczb pierwszych mniejszych od 2^{2^n}.

Wniosek 1.14.

$$p_n < 2^{2^n}.$$

Uwaga: Można udowodnić, że $p_{n+1} < 2 \cdot p_n$. Wynika stąd, że dla $n > 1$ mamy $p_n < 2^n$.

Sito Eratostenesa

Chcemy wyznaczyć wyznaczyć wszystkie liczby pierwsze nie większe od zadanej liczby naturalnej n. Stosowany w tym celu algorytm to tak zwane sito Eratostenesa. Wypisujemy wszystkie liczby $2, 3, \ldots, n$. Najmniejszą (2) „odkładamy", a z pozostałych na liście wykreślamy wszystkie liczby podzielne przez 2. Operację iterujemy, to znaczy „odkładamy" najmniejszą z pozostałych na liście liczb (w drugim obiegu będzie to 3) i wykreślamy z listy liczby podzielne przez nią. W ten sposób uzyskujemy ciąg liczb „odłożonych", które oczywiście są pierwsze, a na liście pozostaje coraz to mniej liczb. Ponieważ przy każdej iteracji usuwamy („odkładamy") z listy najmniejszą liczbę, to w końcu najmniejsza pozostała na liście liczba spełnia $p > \sqrt{n}$. W tym momencie „odsiewanie" możemy zakończyć – łatwo zauważyć, że wszystkie ewentualnie pozostałe na liście liczby są pierwsze, i można je hurtem „odłożyć".

Badanie pierwszości liczb jest więc zawsze wykonalne. Z reguły nie jest to jednak praktycznie wykonalne, i na przykład do dziś nie wiadomo, czy liczba Fermata F_{17} jest pierwsza. Na tej praktycznej niewykonalności opierają się współczesne metody szyfrowania.

Rozkład na czynniki pierwsze

Liczb naturalna $n > 1$ która nie jest pierwsza nazywa się liczbą złożoną. Innymi słowy liczba złożona to taka, dla której $\theta(n) > 2$.

Fakt 1.15. *Każda liczba naturalna $n > 1$ jest albo pierwsza, albo jest iloczynem liczb pierwszych.*

Dowód. Zastosujemy indukcję. Fakt jest oczywiście prawdziwy dla wszystkich liczb naturalnych $n < 3$: istnieje tylko jedna liczba > 1 i < 3, i jest ona

pierwsza. Niech więc $n \geq 3$, i załóżmy, że Fakt jest prawdziwy dla wszystkich liczb $m < n$. Pokażemy, że jest również prawdziwy dla n. Jeżeli n jest pierwsza, to dowód zakończony. Jeżeli nie jest pierwsza, to ma dzielnik pierwszy p, $n = p \cdot m$, $1 < p, m < n$. Z założenia indukcyjnego m jest albo pierwsza, albo jest iloczynem liczb pierwszych. W obu przypadkach n jest iloczynem liczb pierwszych, czyli krok indukcyjny jest prawdziwy. □

Wydzielając kolejno najmniejsze pierwsze dzielniki otrzymujemy rozkład dowolnej liczby naturalnej m na czynniki pierwsze

$$m = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_s^{a_s}, \tag{1.3}$$

gdzie $a_1, a_2, \ldots, a_s \in \mathbf{N}$, $p_1, p_2, \ldots, p_s$ są pierwsze i $p_1 < p_2 < \cdots < p_s$.

Fakt 1.16. *Rozwinięcie* (1.3) *jest jednoznaczne, to znaczy, jeżeli*

$$p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_s^{a_s} = q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_t^{b_t}, \tag{1.4}$$

gdzie $p_1, \ldots, p_s, q_1 \ldots, q_t$ są pierwsze i uporządkowane rosnąco, czyli $p_1 < p_2 < \cdots < p_s$, $q_1 < q_2 < \cdots < q_t$, to

$$s = t, \qquad \forall\, i = 1, \ldots, s \; p_i = q_i, \; a_i = b_i.$$

Dowód. Jeżeli p_1 jest różna od każdej z liczb $q_1, \ldots, q_t$ to jets z każdą z nich względnie pierwsza. W takim razie, zgodnie z zasadniczym twierdzeniem arytmetyki (Fakt 1.9) jest względnie pierwsza z ich iloczynem, czyli z m. Oczywiście jest to sprzeczność, czyli $p_1 = q_i$ dla pewnego i. p_1 jest z definicji najmniejszym pierwszym dzielnikiem m, a $q_1 \leq q_i$, więc $p_1 = q_1$. Zauważmy, że także $a_1 = b_1$. W przeciwnym razie, jeżeli $a_1 > b_1$, to obie strony (1.4) dzielimy przez $p_1^{b_1}$. Otrzymujemy

$$p_1^{a_1 - b_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_s^{a_s} = q_2^{b_2} \cdot \ldots \cdot q_t^{b_t},$$

Teraz p_1 dzieli lewą stronę, ale jest względnie pierwsze z prawą, co jest niemożliwe. Podobnie gdy $a_1 < b_1$, wtedy obie strony dzielimy przez $p_1^{a_1}$. Musimy więc mieć $a_1 = b_1$. Dzielimy więc obie strony równości (1.4) przez wspólną wartość $p_1^{a_1} = q_1^{b_1}$, i powtarzamy procedurę. Zauważmy, że w końcu także otrzymamy $s = t$. □

Wniosek 1.17. *Jeżeli liczba $m \in \mathbf{N}$ ma rozkład na czynniki pierwsze* (1.3) *to*

$$\theta(m) = (a_1 + 1)(a_2 + 1) \cdots (a_s + 1).$$

Dowód. Jeżeli $d \,\big|\, m$ to dzielniki pierwsze d są też dzielnikami pierwszymi m. Rozkład d na czynniki pierwsze wygląda więc następująco:

$$d = p_1^{n_1} \cdot p_2^{n_2} \cdots p_s^{n_s}, \qquad 0 \le n_i \le a_i, \quad i = 1, \ldots, s. \tag{1.5}$$

Zauważmy, że wszystkich możliwych rozwinięć postaci (1.5) jest dokładnie $(a_1 + 1)(a_2 + 1) \cdots (a_s + 1)$. □

Przykład: Znajdziemy wszystkie liczby m, dla których $\theta(m) = 3$. Liczba 3 ma tylko 2 dzielniki, 1 i 3, więc oczywiście w rozwinięciu (1.3) mamy $s = 1$ oraz $a_1 = 2$. Wynika stąd, że $m = p^2$, gdzie p jest dowolną liczbą pierwszą. Liczby m są więc kwadratami liczb pierwszych: $m = 4, 9, 25, 49, \ldots$.

Wyznaczanie NWD i NWW

Jeżeli znamy rozkłady na czynniki pierwsze

$$m = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_s^{a_s}, \qquad n = q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_t^{b_t}, \tag{1.6}$$

wtedy łatwo wyznaczyć $\mathbf{NWD}(m, n)$ i $\mathbf{NWW}(m, n)$. Największy wspólny dzielnik to iloczyn liczb pierwszych, które występują w obu rozkładach (1.6), w mniejszej z obydwu potęg, a najmniejsza wspólna wielokrotność to iloczyn wszystkich liczb pierwszych występujących w którymkolwiek z rozkładów (1.6), w większej ze swoich potęg. Łatwo to sprawdzić badając podzielność i korzystając z zasadniczego twierdzenia arytmetyki (Fakt 1.9). Powyższe odnosi się również do większej ilości liczb.

Przykład: $a = 360$, $b = 270$, $c = 420$. Mamy więc $a = 2^3 \cdot 3^2 \cdot 5$, $b = 2 \cdot 3^3 \cdot 5$ oraz $c = 2^2 \cdot 3 \cdot 5 \cdot 7$. Tak więc

$$\mathbf{NWD}(a, b, c) = 2 \cdot 3 \cdot 5, \quad \mathbf{NWW}(a, b, c) = 2^3 \cdot 3^3 \cdot 5 \cdot 7 = 8 \cdot 27 \cdot 35 = 7560.$$

Algorytm Euklidesa

Niech $m, n \in \mathbf{N}$. Wyznaczymy $\mathbf{NWD}(m, n)$ nie korzystając z rozkładu na czynniki pierwsze. Postępujemy według następującej procedury. Jeżeli $m = n$ to oczywiście $\mathbf{NWD}(m, n) = m = n$ i koniec. Załóżmy więc, że jedna z liczb jest większa, powiedzmy $m > n$. Wtedy

$$m = k \cdot n + r, \qquad 0 \le r < n.$$

Jeżeli $r = 0$ to oczywiście $n \,\big|\, m$ czyli $\mathbf{NWD}(m, n) = n$ został wyznaczony. Załóżmy więc, że $r > 0$. Każdy wspólny dzielnik m i n jest też dzielnikiem r (gdyż $r = m - k \cdot n$), a więc wspólnym dzielnikiem n i r. Z drugiej strony każdy

wspólny dzielnik n i r jest też dzielnikiem m, a więc wspólnym dzielnikiem m i n pary m, n oraz n, r mają więc te same wspólne dzielniki, więc także

$$\mathbf{NWD}(m,n) = \mathbf{NWD}(n,r).$$

Zagadnienie znalezienia **NWD** dwóch liczb sprowadziliśmy do takiego samego zagadnienia, ale dla dwóch mniejszych liczb. Możemy kontynuować procedurę. Oznaczmy $n_1 = m$, $n_2 = n$, $n_3 = r$. W każdym kolejnym kroku utworzymy nowy element ciągu: jeżeli $n_k \neq 0$ to n_{k+1} jest resztą z dzielenia n_{k-1} przez n_k:

$$n_{k-1} = s \cdot n_k + n_{k+1}, \qquad 0 \leq n_{k+1} < n_k.$$

Powtarzając rozumowanie z poprzedniego akapitu widzimy, że na każdym kroku mamy

$$\mathbf{NWD}(n_{k-1}, n_k) = \mathbf{NWD}(n_k, n_{k+1}).$$

Procedura ta musi się w pewnym momencie urwać, to znaczy ciąg n_k (który jest ściśle malejący) musi w końcu osiągnąć 0. Niech n_s będzie ostatnim niezerowym wyrazem naszego ciągu. Oznacz to, ze $n_s \,\big|\, n_{s-1}$ (gdyż reszta z dzielenia jest równa zero), innymi słowy

$$\mathbf{NWD}(n_{s-1}, n_s) = n_s.$$

Oczywiście, otrzymujemy w końcu największy wspólny dzielnik, którego szukaliśmy:

$$\mathbf{NWD}(m,n) = n_s.$$

Opisana powyżej procedura znajdowania największego wspólnego dzielnika to tak zwany algorytm Euklidesa. Podobna procedura przydaje się w wielu sytuacjach. Algorytm Euklidesa można stosować w przypadku większej ilości liczb. Niech $a_1, a_2, \ldots, a_n$ będą parami różne i uporządkowane $a_1 > a_2 > \cdots > a_n$, $n \geq 2$. Wykonujemy następujące dzielenia z resztą:

$$\begin{aligned} a_1 &= k_1 a_n + r_1, \\ a_2 &= k_2 a_n + r_2, \\ &\vdots \\ a_{n-1} &= k_{n-1} a_n + r_{n-1}, \end{aligned}$$

gdzie $0 \leq r_i < a_n$. Jeżeli wszystkie reszty są zerami $r_1 = r_2 = \cdots = r_{n-1} = 0$, to oczywiście $a_n \,\big|\, a_i$ $i = 1, 2, \ldots, a_{n-1}$ i otrzymujemy

$$\mathbf{NWD}(a_1, a_2, \ldots, a_n) = a_n.$$

Załóżmy więc, że nie wszystkie reszty są zerami. Odrzućmy te, które są zerami, i zatrzymajmy tylko te niezerowe. Oczywiście, jeżeli $r_i = 0$ to znaczy, że $a_n \mid a_i$, czyli odrzucenie takiej liczby z listy nie wpłynie na wspólne dzielniki. Niech więc $r_1, \ldots, r_s$ będą pozostałymi, niezerowymi resztami. Zauważmy, że wspólne dzielniki układu liczb $a_1, a_2, \ldots, a_n$ i układu liczb $r_1, r_2, \ldots, r_s, a_n$ są te same, a więc także

$$\mathbf{NWD}(a_1, a_2, \ldots, a_n) = \mathbf{NWD}(r_1, r_2, \ldots, r_s, a_n).$$

Wykonaliśmy więc redukcyjny krok algorytmu Euklidesa. Wykonując dalej takie kroki z konieczności dojdziemy do momentu, w którym wszystkie reszty z dzielenia będą zerami, i ostatecznie ostatnia na liście liczba będzie szukanym dzielnikiem.

Przykład: Stosując algorytm Euklidesa znajdziemy $\mathbf{NWD}(420, 350, 270, 225)$. Wykonujemy dzielenia:

$$\begin{aligned} 420 &= 1 \cdot 225 + 195 \\ 360 &= 1 \cdot 225 + 135 \\ 270 &= 1 \cdot 225 + 45. \end{aligned}$$

Rozpatrzmy więc $\mathbf{NWD}(225, 195, 135, 45)$. Wykonujemy kolejne dzielenia

$$\begin{aligned} 225 &= 5 \cdot 45 + 0 \\ 195 &= 4 \cdot 45 + 15 \\ 135 &= 3 \cdot 45 + 0. \end{aligned}$$

Pozostają tylko dwie niezerowe liczby $15, 45$. Łatwo zauważyć, że $\mathbf{NWD}(15, 45) = 15$, a więc także

$$\mathbf{NWD}(420, 360, 270, 225) = 15.$$

Ciekawostki

(a) Jak wspomnieliśmy wcześniej (bez dowodu) $p_{n+1} < 2p_n$, gdzie p_n jest n-tą kolejną liczbą pierwszą (uwaga po Wniosku 1.14). Niech m będzie liczbą naturalną większą lub równą 2. Niech p_n będzie największą liczbą pierwszą $\leq m$. Oczywiście taka liczba istnieje, bo zbiór liczb pierwszych nie większych niż m jest skończony. Wtedy kolejna liczba pierwsza p_{n+1} jest większa niż m, a z drugiej strony $p_{n+1} < 2p_n \leq 2m$. Widzimy więc, że dla dowolnej liczby naturalnej $m \geq 2$ istnieje liczba pierwsza pomiędzy m i $2m$. Wyciągniemy stąd wniosek, że dla dowolnej liczby naturalnej n istnieją co najmniej 3 liczby pierwsze mające dokładnie n cyfr dziesiętnych. Wynika to z faktu, że

mamy następujące 4 liczby dokładnie n-cyfrowe: $1 \cdot 10^{n-1}$, $2 \cdot 10^{n-1}$, $4 \cdot 10^{n-1}$ i $8 \cdot 10^{n-1}$. Pomiędzy każdą sąsiadującą parą istnieje liczba pierwsza, i ma dokładnie n cyfr dziesiętnych.

(b) Wiadomo, że liczby pierwsze (poza 2) są nieparzyste. Okazuje się, że w pewnym sensie spośród liczb nieparzystych łatwiej być liczbą pierwszą liczbom postaci $4k+3$ niż liczbom postaci $4k+1$ (zauważmy, że wszystkie liczby nieparzyste mają jedną z tych form, dla jakiegoś całkowitego, nieujemnego k).

Fakt 1.18. *Każda liczba naturalna postaci $n = 4k+3$ ma przynajmniej jeden dzielnik pierwszy tej samej postaci.*

Dowód. Niech p będzie najmniejszym dzielnikiem liczby $n = 4k+3$ tej samej postaci. Zbiór takich dzielników jest niepusty, gdyż na przykład należy do niego sama liczba n. Istnieje więc jego element najmniejszy. Jeżeli liczba p jest pierwsza, to fakt jest udowodniony. Jeżeli nie jest pierwsza, to ma rozkład

$$p = d \cdot e, \qquad 1 < d, e < p.$$

Żaden z czynników d, e nie jest parzysty, gdyż wtedy parzysta byłaby liczba p, a w konsekwencji także n, co jest nieprawdą. Każdy z dzielników d, e ma więc jedną z postaci $4l + 1$ lub $4l + 3$. Zauważmy, że nie mogą oba być pierwszej postaci. Gdyby tak było, to mielibyśmy

$$p = d \cdot e = (4l_1 + 1)(4l_2 + 1) = 4(4l_1l_2 + l_1 + l_2) + 1,$$

co jest sprzeczne z definicją p: p jest postaci $4l + 3$. Jeden z czynników d lub e (łatwo zauważyć, że dokładnie jeden) musi więc być postaci $4l + 3$ co jest sprzeczne z założeniem, że p jest najmniejszym dzielnikiem n tej postaci. □

Wniosek 1.19. *Dla każdej liczby naturalnej n istnieje liczba pierwsza postaci $4k + 3$ większa od n. Liczb pierwszych postaci $4k + 3$ jest więc nieskończenie wiele.*

Dowód. Liczba $n! - 1$ jest postaci $4k + 3$ (dla $n \leq 4$), a więc ma pierwszy dzielnik tej samej postaci. Jednak żaden jej właściwy dzielnik nie może być dzielnikiem $n!$, gdyż wtedy byłby także dzielnikiem 1. Ponieważ wszystkie liczby $\leq n$ są dzielnikami $n!$, więc pierwszy dzielnik n postaci $4k + 3$ musi być większy od n. Ostatnie stwierdzenie wniosku jest w związku z tym oczywiste. □

Powyższą obserwację możemy rozwinąć. Wiemy, że liczby pierwsze > 3 nie są podzielne ani przez 2 ani przez 3. W takim razie reszta z dzielenia takiej liczby przez 6 może wynieść tylko 1 albo 5. Jak pokazuje następujący fakt reszta 5 jest uprzywilejowana.

Fakt 1.20. *Każda liczba naturalna postaci $n = 6k+5$ ma przynajmniej jeden dzielnik pierwszy tej samej postaci.*

Dowód. Dowód jest taki sam, jak dowód Faktu 1.18. Zauważmy, że iloczyn dwóch liczb jest postaci $6k+5$ dokładnie wtedy, gdy jeden z czynników jest postaci $6l+1$ a drugi postaci $6l+5$. Korzystając z tej obserwacji postępujemy dalej tak samo jak w dowodzie Faktu 1.18. □

Fakt ten ma podobny wniosek.

Wniosek 1.21. *Dla każdej liczby naturalnej n istnieje większa od niej liczba pierwsza postaci $6k+5$. Liczb pierwszych tej postaci jest więc nieskończenie wiele.* □

Równania diofantyczne

Równanie nazywa się diofantyczne, jeżeli dotyczy liczb całkowitych, w szczególności jeżeli szukamy tylko całkowitoliczbowych rozwiązań. Przyjrzyjmy się diofantycznemu równaniu liniowemu stopnia 1:

$$a\,x + b\,y = l, \qquad a, b \in \mathbf{N},\ l \in \mathbf{Z}. \tag{1.7}$$

Szukamy rozwiązań $x, y \in \mathbf{Z}$. Zastosujemy algorytm Euklidesa. Przypomnijmy, że mając dwie liczby naturalne $a, b \in \mathbf{N}$, powiedzmy $a > b$ algorytm Euklidesa daje nam ściśle malejący, skończony ciąg

$$n_1 > n_2 > \cdots > n_s > 0,$$

w którym każda kolejna liczba n_i jest resztą z dzielenia n_{i-2} przez n_{i-1}, $a = n_1$, $b = n_2$. Wiemy, że w takiej sytuacji

$$\mathbf{NWD}(n_1, n_2) = \mathbf{NWD}(n_2, n_3) = \cdots = \mathbf{NWD}(n_{s-1}, n_s) = n_s.$$

Niech więc równaniu (1.7) $a > b$ i oznaczmy $n_1 = a$, $n_2 = b$. Ponieważ $n_1 = q_1 \cdot n_2 + n_3$, to mamy

$$n_1 x + n_2 y = l \ \Rightarrow (q_1 \cdot n_2 + n_3)x + n_2 y = l, \tag{1.8}$$

czyli

$$n_2 x_1 + n_3 y_1 = l, \quad \text{gdzie} \quad y_1 = x, \quad x_1 = q_1 x + y. \tag{1.9}$$

Rozwiązanie równania (1.8) daje więc rozwiązanie równania (1.9) i na odwrót, gdyż x, y można odtworzyć z x_1, y_1: $x = y_1$, $y = x_1 - q_1 y_1$. Jeżeli $n_3 \neq 0$ to możemy kontynuować regresję:

$$n_3 x_2 + n_4 y_2 = l \qquad y_2 = x_1, \quad x_2 = q_2 x_1 + y_1.$$

Kontynuując dochodzimy w końcu do

$$n_{s-1}x_{s-2} + n_s y_{s-2} = l,$$

które jest łatwo do rozwiązania. Mamy $n_s \,\big|\, n_{s-2}$, a więc $n_{s-1} = q_{s-1}n_s$, czyli

$$n_s \cdot (q_{s-1} \cdot x_{s-2} + y_{s-2}) = l,$$

lub, podstawiając $x_{s-1} = q_{s-1}x_{s-2} + y_{s-2}$

$$n_s \cdot x_{s-1} = l. \tag{1.10}$$

To ostatnie równanie ma rozwiązanie dokładnie wtedy, gdy $n_s \,\big|\, l$, i w takim przypadku rozwiązanie łatwo obliczyć. Jeżeli rozwiązanie (1.10) istnieje, to możemy odtworzyć wszystkie kolejne pary rozwiązań. W pierwszym kroku możemy przyjąć dowolne całkowite x_{s-2} (na przykład 0) i następnie $y_{s-2} = x_{s-1} - q_{s-1} \cdot x_{s-2}$. Następnie stosujemy zależność ($x_0 = x$, $y_0 = y$)

$$x_{i-1} = y_i, \quad y_{i-1} = x_i - q_i \cdot y_i, \qquad i = (s-1), \ldots, 1. \tag{1.11}$$

Udowodniliśmy w ten sposób następujący wniosek.

Wniosek 1.22. *Rozwiązanie równania* (1.7) *w liczbach całkowitych istnieje wtedy i tylko wtedy, gdy*

$$\mathbf{NWD}(a, b) \,\big|\, l.$$

W szczególności zawsze istnieje rozwiązanie w liczbach całkowitych równania

$$a \cdot x + b \cdot y = \mathbf{NWD}(a, b).$$

□

Przykład: Jako ilustrację procedury znajdowania rozwiązania rozważmy równanie

$$119 \cdot x + 105 \cdot y = 28.$$

Mamy $119 = 1 \cdot 105 + 14$, więc powyższe równanie redukuje się do

$$105 \cdot x_1 + 14 \cdot y_1 = 28.$$

Dalej $105 = 7 \cdot 14 + 7$ i otrzymujemy

$$\begin{aligned} 14 \cdot x_2 + 7 \cdot y_2 &= 28 \\ 7\,(2 \cdot x_2 + y_2) &= 28 \\ 7 \cdot x_3 &= 28 \end{aligned}$$

Rekurencyjnie, stosując zależność (1.11) odtwarzamy teraz rozwiązania poprzednich równań. Z x_3 odtwarzamy parę x_2 i y_2, przy czym mamy dowolność wybory x_2. Weźmy $x_2 = 0$ i otrzymujemy $y_2 = 4$. Stąd $x_1 = y_2 = 4$,

$$y_1 = x_2 - q_2 \cdot x_1 = 0 - 7 \cdot 4 = -28.$$

Dalej $x = y_1 = -28$ oraz

$$y = x_1 - q_1 \cdot y_1 = 4 - 1 \cdot (-28) = 4 + 28 = 32.$$

Mamy więc szukane rozwiązanie.

Wniosek 1.22 można uogólnić na większą liczbę niewiadomych. Zróbmy jeszcze następującą uwagę. Zmiana znaku nie wpływa na podzielność jednej liczby przez drugą. W takim razie zbiory dzielników liczb a i $-a$ są identyczne. Rozważając największy wspólny dzielnik zbioru liczb nie musimy ograniczać się do liczb naturalnych, możemy rozważać dowolne liczby całkowite. Ponieważ każda liczba jest dzielnikiem 0, więc jeżeli chcemy mówić o największym wspólnym dzielniku zbioru liczb całkowitych, to przynajmniej jedna z liczb tego zbioru musi być różna od zera. Zwróćmy uwagę, że co prawda rozważamy liczby całkowite, to bierzemy pod uwagę jedynie dzielniki naturalne, czyli **NWD** jest zawsze liczbą naturalną, i mamy prostą własność:

$$\mathbf{NWD}(a_1, a_2, \ldots, a_n) = \mathbf{NWD}(|a_1|, |a_2|, \ldots, |a_n|).$$

Takie rozszerzenie pojęcia największego wspólnego dzielnika akurat pasuje do poniższego twierdzenia.

Twierdzenie 1.23. *Dla $n > 1$ i liczb całkowitych $a_1, a_2 \ldots, a_n$ z których nie wszystkie sa zerami istnieją liczby całkowite $\xi_1, \xi_2, \ldots, \xi_n$ takie, że*

$$a_1 \cdot \xi_1 + a_2 \cdot \xi_2 + \cdots + a_n \cdot \xi_n = \mathbf{NWD}(a_1, a_2, \ldots, a_n). \tag{1.12}$$

$\mathbf{NWD}(a_1, a_2, \ldots, a_n)$ *jest najmniejszą liczbą naturalną, którą da się przedstawić w tej postaci (dla pewnych $\xi_1, \ldots, \xi_n$).*

Dowód. Rozważmy zbiór $\mathcal{A}$ tych liczb naturalnych m, które da się przedstawić w postaci (1.12). Zauważmy, że jest to zbiór niepusty. Jeżeli $a_k \neq 0$, to albo a_k albo $-a_k$ jest liczbą naturalna, i należy do $\mathcal{A}$:

$$\begin{aligned} a_k &= a_1 \cdot 0 + a_2 \cdot 0 + \cdots + a_k \cdot 1 + a_{k+1} \cdot 0 + \cdots + a_n \cdot 0 \\ (-a_k) &= a_1 \cdot 0 + a_2 \cdot 0 + \cdots + a_k \cdot (-1) + a_{k+1} \cdot 0 + \cdots + a_n \cdot 0 \end{aligned}$$

Niech d będzie najmniejszym elementem zbioru $\mathcal{A}$. Mamy więc, dla pewnych $\xi_1, \xi_2, \ldots, \xi_n$

$$d = a_1 \cdot \xi_1 + \cdots + a_n \cdot \xi_n. \tag{1.13}$$

Załóżmy, że inna liczba naturalna, m, też ma reprezentację tej postaci:

$$m = a_1 \cdot x_1 + \cdots + a_n \cdot x_n. \tag{1.14}$$

Pokażemy, że $d \,\big|\, m$. Liczba m jest większa lub równa d, więc $m = q \cdot d + r$, gdzie $0 \leq r < d$. Obie strony równości (1.13) pomnóżmy przez q i odejmijmy stronami od równości (1.14):

$$\begin{aligned} q \cdot d &= a_1 \cdot q \cdot \xi_1 + \cdots + a_n \cdot q\xi_n \\ q \cdot d + r &= a_1 \cdot x_1 + \cdots + a_n \cdot x_n \\ r &= a_1 \cdot (x_1 - q \cdot \xi_1) + \cdots + a_n \cdot (x_n - q \cdot \xi_n). \end{aligned}$$

Gdyby $r > 0$, to byłoby to sprzeczne z założeniem, że d jest najmniejszą liczbą w $\mathcal{A}$. Musi więc być $r = 0$ czyli istotnie $d \,\big|\, m$. Każda liczba całkowita (niekoniecznie naturalna, gdyż zmiana znaku nie wpływa na podzielność), którą można przedstawić w postaci (1.14) dzieli się więc przez d. Wiemy, że wszystkie niezerowe liczby a_k mają takie przedstawienie, a więc d dzieli każdą liczb a_k:

$$d \,\big|\, a_k, \qquad k = 1, 2, \ldots, n.$$

Liczba d jest więc wspólnym dzielnikiem wszystkich współczynników $a_1, \ldots a_n$. Z drugiej strony, oczywiście, każdy wspólny dzielnik tych współczynników jest też dzielnikiem d, a więc

$$d = \mathbf{NWD}(a_1, \ldots, a_n).$$

□

Uwaga: Zauważmy, że powyższy dowód nie daje praktycznej procedury znalezienia rozwiązania równania (1.12), a jedynie zapewnia istnienie. Natomiast w przypadku $n = 2$ dowód Wniosku 1.22 daje taką praktyczną procedurę.

Wniosek 1.24. *Liczby $a_1, \ldots a_n$ są względnie pierwsze $\Leftrightarrow$ istnieją liczby całkowite $\xi_1, \ldots \xi_n$ takie, że*

$$a_1 \cdot \xi_1 + a_2 \cdot \xi_2 + \cdots + a_n \cdot \xi_n = 1. \quad \square$$

Z Twierdzenia 1.23 możemy wyciągnąć wniosek analogiczny do Wniosku 1.22, który wcześniej udowodniliśmy w przypadku 2 niewiadomych.

Wniosek 1.25. *Równanie*

$$m = a_1 \cdot x_1 + \cdots + a_n \cdot x_n \tag{1.15}$$

gdzie liczby $a_1, a_2, \ldots, a_n$ i m są całkowite (nie wszystkie a_i równe 0), $n \geq 2$ ma rozwiązanie w liczbach całkowitych wtedy i tylko wtedy, gdy m jest podzielna przez $\mathbf{NWD}(a_1, a_2, \ldots, a_n)$.

Dowód. Oznaczmy $d = \mathbf{NWD}(a_1, \ldots, a_n)$. Jeżeli rozwiązanie równania (1.15) istnieje, to wstawiając do niego $a_i = d \cdot b_i$ otrzymujemy

$$m = d \cdot b_1 \cdot x_1 + \cdots + d \cdot b_n \cdot x_n = d \cdot (b_1 \cdot x_1 + \cdots + b_n \cdot x_n), \qquad (1.16)$$

czyli istotnie $d \,\big|\, m$. Z drugiej strony załóżmy, że $d \,\big|\, m$, czyli $m = d \cdot k$. Wiemy, że liczby $b_i = a_i/d$ są względnie pierwsze, czyli w myśl Wniosku 1.24 istnieją liczby całkowite $\xi_1, \ldots, \xi_n$ takie, że

$$b_1 \cdot \xi_1 + b_2 \cdot \xi_2 + \cdots + b_n \cdot \xi_n = 1.$$

Łatwo zauważyć, że liczby $x_i = k \cdot \xi_i$ stanowią rozwiązanie równania (1.15):

$$a_1 \cdot x_1 + \cdots + a_n \cdot x_n = a_1 \cdot k \cdot \xi_1 + \cdots + a_n \cdot k \cdot \xi_n = d \cdot k \cdot (b_1 \cdot \xi_1 + \cdots + b_n \cdot \xi_n) = d \cdot k = m.$$

□

Podamy teraz procedurę, przy pomocy której można rozwiązać równania (1.15) w przypadku $n > 2$. Załóżmy, że istnieje takie rozwiązanie, czyli liczby całkowite $x_1, \ldots x_n$ dla których zachodzi (1.15). Przekształcając (1.15) otrzymujemy

$$a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_{n-1} \cdot x_{n-1} = m - a_n \cdot x_n.$$

Wiemy, że rozwiązanie powyższego równania (czyli liczby $x_1, \ldots, x_{n-1}$ – x_n jest ustalone) istnieje. Jeżeli więc $d = \mathbf{NWD}(a_1, \ldots, a_{n-1})$, to zgodnie z Wnioskiem 1.25 $d \,\big|\, (m - a_n \cdot x_n)$. Istnieje więc liczba całkowita, nazwijmy ją x_{n+1}, taka, że

$$d \cdot x_{n+1} = m = a_n \cdot x_n \;\Rightarrow\; a_n \cdot x_n + d \cdot x_{n+1} = m. \qquad (1.17)$$

Znając a_n, d i m możemy znaleźć x_n oraz x_{n+1} korzystając z procedury opartej o algorytm Euklidesa, opisanej w dowodzie Wniosku 1.22. W ten sposób „nadgryźliśmy" problem znalezienia rozwiązania $x_1, \ldots, x_n$: znaleźliśmy x_n. Pozostaje kontynuować analogicznie, i znaleźć pozostałe liczby x_i.

Przykład Rozwiążemy równanie

$$12 \cdot x + 15 \cdot y + 7 \cdot z = 11.$$

Mamy $\mathbf{NWD}(12, 15, 7) = 1 \,\big|\, 11$, czyli rozwiązanie istnieje, musimy je tylko znaleźć. Obliczamy $\mathbf{NWD}(12, 15) = 3$, i formułujemy równanie (1.17):

$$7 \cdot z + 3 \cdot t = 11.$$

To jest równanie z dwoma zmiennymi, więc rozwiązujemy je zwykłą procedurą stosując algorytm Euklidesa. Mamy $7 = 2 \cdot 3 + 1$, czyli przekształcone równanie ma postać:

$$3 \cdot z_1 + 1 \cdot t_1 = 11, \qquad \text{gdzie} \quad t_1 = z,\ z_1 = 2 \cdot z + t.$$

Widzimy więc, że $3 \cdot z_1 + t_1 = 11$. Możemy wybrać z_1 dowolnie, i oznaczmy nasz wybór k. Wtedy $t_1 = 11 - 3 \cdot k$, czyli $z = 11 - 3 \cdot k$ oraz $t = k - 2 \cdot (11 - 3 \cdot k) = 7 \cdot k - 22$. Pozostało nam do rozwiązania równanie

$$12 \cdot x + 15 \cdot y = 11 - 7 \cdot (11 - 3 \cdot k) = 21 \cdot k - 6 \cdot 11,$$

czyli, po skróceniu przez 3

$$4 \cdot x + 5 \cdot y = 7 \cdot k - 22.$$

Kontynuujemy: $5 = 1 \cdot 4 + 1$, a więc

$$4 \cdot x_1 + 1 \cdot y_1 = 7 \cdot k - 22, \qquad \text{gdzie} \quad y_1 = y,\ x_1 = 1 \cdot x + y.$$

Za x_1 możemy podstawić dowolną liczbę całkowitą, nazwijmy ją l. Wtedy $y_1 = 7 \cdot k - 4 \cdot l - 22$. Wracając do pierwotnych zmiennych otrzymujemy

$$x = -7 \cdot k + 5 \cdot l + 22, \quad y = 7 \cdot k - 4 \cdot l - 22, \quad z = 11 - 3 \cdot k.$$

Równania wyższych stopni

Równanie

$$x^2 + y^2 = z^2 \tag{1.18}$$

nazywa się równaniem Pitagorasa. Szukamy rozwiązań równanie Pitagorasa wśród liczb naturalnych. Łatwo zgadnąć rozwiązanie: $x = 3$, $y = 4$ i $z = 5$. Rozwiązanie nazywamy właściwym, jeżeli wszystkie liczby x, y, z są naturalne a x oraz y są względnie pierwsze. Widać, że wszystkie rozwiązania (naturalne) równania Pitagorasa są postaci dx, dy, dz, gdzie x, y, z jest rozwiązaniem właściwym, a d jest dowolną liczbą naturalną. Następujące twierdzenie wyznacza wszystkie rozwiązania właściwe

Twierdzenie 1.26. *Wszystkie rozwiązania właściwe równania* (1.18) *w których y jest liczbą parzystą maja postać*

$$x = m^2 - n^2, \quad y = 2 \cdot m \cdot n, \quad z = m^2 + n^2, \tag{1.19}$$

gdzie m, n są dowolnymi liczbami naturalnymi względnie pierwszymi, o przeciwnej parzystości, oraz $m > n$.

Uwagi: (a) Zauważmy, że jeżeli x, y, z jest rozwiązaniem właściwym, to x i y nie mogą być jednocześnie parzyste ani jednocześnie nieparzyste. Gdyby obie były parzyste, to nie mogłyby być względnie pierwsze. Gdyby obie były nieparzyste, to z^2 musiałaby mieć postać $4k + 2$, co jest niemożliwe. Jedna z liczb x, y musi więc być parzysta, a druga nieparzysta. Zastrzeżenie w sformułowaniu twierdzenia, że y jest liczbą parzystą nie ogranicza więc ogólności.

(b) Różne pary liczb m, n, spełniające wymagania twierdzenia, dają różne rozwiązania. Wynika to z zależności $2 \cdot m^2 = z + x$ oraz $2 \cdot n^2 = z - x$.

Dowód. Założyliśmy, że y jest parzysta, a więc x musi być nieparzysta. W związku z tym z także jest nieparzysta. Mamy więc, dla pewnych liczb naturalnych a i b, $a > b$

$$z + x = 2 \cdot a, \qquad z - x = 2 \cdot b.$$

Zauważmy, że liczby a i b muszą być względnie pierwsze. Jeżeli bowiem $d \,|\, a$ i $d \,|\, b$, to z zależności $z = a + b$, $x = a - b$ otrzymalibyśmy $d \,|\, x$ oraz $d \,|\, z$. Wtedy $d^2 \,|\, x^2$ i $d^2 \,|\, z^2$, czyli $d^2 \,|\, y^2$, a z tego wynika, że $d \,|\, y$. d jest więc wspólnym dzielnikiem x i y, czyli skoro te dwie liczby sa względnie pierwsze musi być $d = 1$. Z równania (1.18) mamy

$$y^2 = z^2 - x^2 = 4 \cdot a \cdot b.$$

y jest parzysta, więc dla pewnej liczby $c \in \mathbf{N}$ mamy $y = 2 \cdot c$, oraz $c^2 = a \cdot b$. Liczby a i b są względnie pierwsze, więc same muszą być kwadratami liczb naturalnych:

$$a = m^2, \quad b = n^2 \;\Rightarrow\; z = m^2 + n^2, \quad x = m^2 - n^2.$$

Mamy także

$$y = 2 \cdot c = 2 \cdot m \cdot n.$$

Liczby a i b sa względnie pierwsze, więc także m i n muszą być względnie pierwsze. W związku z tym nie mogą być obie parzyste. Nie mogą też obie być nieparzyste, bo wtedy także x byłaby parzysta, a wiemy, że nie jest. m i n mają więc przeciwną parzystość, i, oczywiście $m > n$. Udowodniliśmy więc, że każde rozwiązanie właściwe ma opisaną w twierdzeniu postać. Pozostaje pokazać, że jeżeli liczby naturalne m i n spełniają warunki twierdzenia, to wzór (1.19) daje właściwe rozwiązanie równania (1.18). Podstawiając (1.19) do (1.18) widzimy, że rzeczywiście otrzymujemy rozwiązanie. Z (1.19) oraz z $m > n$ wynika, że wszystkie liczby x, y i z są naturalne, i y jest parzysta. Pozostaje sprawdzić, ze x i y są względnie pierwsze. Niech $d = \mathbf{NWD}(x, y)$.

Zauważmy, że $x = m^2 - n^2$, a więc x nie jest parzysta (bo m i n mają przeciwną parzystość). Nie może więc mieć parzystych dzielników, czyli d musi być nieparzysta. $d \mid x$ i $d \mid y$ więc także, z (1.18) $d \mid z$. Z (1.19) wynika, że $2m^2 = z + x$ oraz $2n^2 = z - x$ więc $d \mid 2m^2$ i $d \mid 2n^2$. Ponieważ d jest nieparzysta, więc $d \mid m^2$ i $d \mid n^2$. Ale m i n sa względnie pierwsze, a z tego wynika, że m^2 i n^2 sa względnie pierwsze. Musimy więc mieć $d = 1$. Udowodniliśmy więc, że x i y są względnie pierwsze, co kończy dowód twierdzenia. □

Zauważmy, że znane rozwiązanie $3, 4, 5$ odpowiada $m = 2$, $n = 1$. Warto jako ciekawostkę wspomnieć następujące twierdzenie:

Twierdzenie 1.27 (Wielkie Twierdzenie Fermata). *Dla $n > 2$ równanie*

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

nie ma rozwiązań będących liczbami naturalnymi.

Twierdzenie to jest jednym z najsłynniejszych twierdzeń, i ma bogatą historię. Pierre de Fermat, który je sformułował w 1637 roku myślał, że umie je udowodnić, i że jest to łatwe. Przypuszczalnie się mylił, ponieważ dowód okazał się trudny. Ostatecznie, po wielu próbach i trudach, twierdzenie zostało udowodnione pod koniec ubiegłego wieku.

Rozdział 2

Kongruencje

Niech $a, b \in \mathbf{Z}$, $m \in \mathbf{N}$. Mówimy, że „a przystaje do b modulo m", i piszemy $a \equiv b \pmod{m}$, jeżeli $m \mid (b - a)$. Na przykład

$$18 \equiv -8 \pmod{13}, \qquad -5 \equiv 5 \pmod{10}.$$

a przystaje do b modulo m jeżeli mają takie same reszty z dzielenia przez m. Przystawanie nazywa się też czasem kongruencją. Łatwo zauważyć następujące własności kongruencji:

1. $a \equiv b \pmod{m}$ (zwrotna),
2. $a \equiv b \pmod{m} \;\Leftrightarrow\; b \equiv a \pmod{m}$ (symetryczna),
3. jeżeli $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$ to także $a \equiv c \pmod{m}$ (przechodnia),
4. kongruencje możemy dodawać, odejmować i mnożyć stronami: jeżeli $a \equiv b \pmod{m}$ oraz $c \equiv d \pmod{m}$ to także

$$a \pm c \equiv b \pm d \pmod{m}, \qquad a \cdot c \equiv b \cdot d \pmod{m}.$$

Z własności 1–3 wynika, że przystawanie modulo m jest relacją równoważności, która rozdziela zbiór liczb całkowitych na klasy abstrakcji – reszty z dzielenia przez m. Z własności 4 natomiast wynika że kongruencje można stronami mnożyć przez stałą, i podnosić do naturalnej potęgi. Nie można jednak stronami dzielić:

$$6 \equiv 2 \pmod{4}, \quad 2 \equiv 2 \pmod{4} \;\not\Rightarrow\; 3 \equiv 1 \pmod{4}.$$

Można łatwo zauważyć jednak, że jeżeli $d \mid a$, $d \mid b$ oraz $d \mid m$, to

$$a \equiv b \pmod{m} \;\Rightarrow\; \frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right).$$

Jeżeli $d \mid m$ to mamy też oczywiście

$$a \equiv b \pmod{m} \;\Rightarrow\; a \equiv b \pmod{d}.$$

Twierdzenie 2.1. *Jeżeli* $a \equiv b \pmod{m}$ *i* $f(x) = \alpha_n x^n + \cdots + \alpha_1 x + a_0$ *jest wielomianem o współczynnikach całkowitych, to* $f(a) \equiv f(b) \pmod{m}$.

Dowód. Dla $i = 0, 1, 2, \ldots, n$ podnosząc kongruencję stronami do potęgi otrzymujemy $a^i \equiv b^i \pmod{m}$, a następnie mnożąc kongruencje stronami przez stałe otrzymujemy $\alpha_i a^i \equiv \alpha_i b^i \pmod{m}$. Dodając stronami wszystkie te kongruencje otrzymujemy tezę. □

Weźmy dowolną liczbę $N \in \mathbf{N}$, i niech jej rozwinięcie dziesiętne ma postać $N = c_n c_{n-1} \cdots c_0$, czyli

$$N = c_0 + 10\, c_1 + 10^2\, c_2 + \cdots + 10^n\, c_n.$$

Ustalmy wielomian $f(x) = c_0 + c_1\, x + c_2\, x^2 + \cdots + c_n\, x^n$. Mamy $c_i \in \mathbf{Z}$ (nawet $c_i \in \{0, 1, \ldots, 9\}$), $f(10) = N$ i $f(1) = c_0 + c_1 + \cdots + c_n$. Oczywiście zachodzi kongruencja

$$10 \equiv 1 \pmod{9}.$$

Z twierdzenia 2.1 mamy więc, że $f(10 \equiv f(1) \pmod{9}$. Możemy stąd wywnioskować tak zwaną cechę podzielności przez 9:

Wniosek 2.2. *Liczba naturalna jest podzielna przez* 9 *wtedy i tylko wtedy gdy suma jej cyfr dziesiętnych jest podzielna przez* 9.

Podobny wniosek możemy sformułować dla 3. Zauważmy, że tak naprawdę udowodniliśmy trochę więcej niż cechę podzielności, mianowicie pokazaliśmy, że reszta z dzielenia przez 9 liczby jest taka sama jak reszta z dzielenia przez 9 sumy jej cyfr. Możemy podobnie udowodnić inne cechy podzielności. Ponieważ $10 \equiv -1 \pmod{11}$, oraz

$$f(-1) = c_0 - c_1 + c_2 - + \cdots \pm c_n, \tag{2.1}$$

a więc

Wniosek 2.3. *Liczba* N *jest podzielna przez* 11 *wtedy i tylko wtedy, gdy suma oscylująca (czyli suma* (2.1)*) jest podzielna przez* 11. □

Przykład: $11 \mid 10^n + 1 \;\Leftrightarrow\; n$ jest parzyste. Zauważmy, że liczbę N możemy także zapisać w postaci

$$N = (c_2 c_1 c_0) + 1000\, (c_5 c_4 c_3) + 1000^2\, (c_8 c_7 c_6) + \ldots.$$

Kolejne trójki cyfr to współczynniki, liczby od 0 do 999. Są to „cyfry" w zapisie „tysiącowym" liczb. Taki system zapewne uważalibyśmy za naturalny gdybyśmy mieli po 1000 palców. Wprowadźmy wielomian

$$g(x) = (c_2c_1c_0) + x\,(c_5c_4c_3) + x^2\,(c_8c_7c_6) + \dots$$

Oczywiście powyższa suma jest skończona, a nie dopisaliśmy jej końca dlatego, że ostatni współczynnik n może wystąpić w różnych miejscach ostatniego trzycyfrowego współczynnika wielomianu. Korzystając z kongruencji

$$1000 \equiv -1 \pmod 7, \qquad 1000 \equiv -1 \pmod{13},$$

otrzymujemy

$$N \equiv (c_2c_1c_0) - (c_5c_4c_3) + (c_8c_7c_6) - \dots \pmod 7, \quad \text{a także } \pmod{13},$$

a więc

Wniosek 2.4. *Liczba N jest podzielna przez 7 wtedy i tylko wtedy, gdy oscylująca suma jej cyfr dziesiętnych (grupowanych po 3) jest podzielna przez 7. Podobna cecha podzielności zachodzi dla 13.*

Przykład: Liczba 10^n jest podzielna przez 7 (i przez 13) wtedy i tylko wtedy, gdy n przy dzieleniu przez 6 daje resztę 3. Łatwo zauważyć, że dokładnie w takim przypadku suma oscylująca daje 0.

Twierdzenie Eulera

Dla $m \in \mathbf{N}$, $m > 1$ niech $\varphi(m)$ oznacza ilość liczb naturalnych nie większych od m, i względnie pierwszych z m. Ustawmy te liczby w porządku rosnącym, i oznaczmy przez

$$r_1, r_2, r_3, \dots, r_{\varphi(m)}.$$

Oczywiście, zawsze mamy $r_1 = 1$, $r_{\varphi(m)} = m - 1$. Weźmy $a \in \mathbf{Z}$, dowolną liczbę względnie pierwszą z m. Niech ρ_k będzie resztą z dzielenia ar_k przez m:

$$a\,r_k = q_k \cdot m + \rho_k, \qquad k = 1, 2, \dots, \varphi(m). \tag{2.2}$$

Fakt 2.5. *Liczby ρ_k to te same liczby co r_k, z dokładnością do numeracji.*

Dowód. Wszystkie liczby ρ_k są mniejsze od m i żadna nie może być zerem (bo m nie dzieli $a \cdot r_k$). Innymi słowy, $1 \le \rho_k < m$. Zauważmy, że liczby ρ_k muszą być względnie pierwsze z m. Wiemy, że m jest względnie pierwsza z a i z r_k, więc z zasadniczego twierdzenia algebry jest względnie pierwsza z

$a \cdot r_k$. Z drugiej strony z (2.5) wynika, że ewentualne wspólne dzielniki m i ρ_k byłyby też wspólnymi dzielnikami m i $a \cdot r_k$. Musi więc w szczególności zachodzić

$$1 = \mathbf{NWD}(m, a \cdot r_k) = \mathbf{NWD}(m, \rho_k).$$

Mamy więc $\varphi(m)$ liczb naturalnych $\rho_1, \ldots \rho_{\varphi(m)}$ mniejszych od m i względnie pierwszych z m. Wystarczy pokazać, że liczby te są wszystkie różne. Załóżmy więc nie wprost, że $\rho_k = \rho_l$ dla pewnych k, l, $1 \leq k < l \leq \varphi(m)$. Wtedy

$$a \cdot r_k = q_k \cdot m + \rho_k, \quad a \cdot r_l = q_l \cdot m + \rho_l \;\Rightarrow\; a \cdot r_k \equiv a \cdot r_l \pmod{m}.$$

W takim razie $m \,\big|\, a(r_l - r_k$ a stąd $m \,\big|\, (r_l - r_k)$, a to jest niemożliwe, bo $1 \leq r_l - r_k < m$. Wszystkie liczby $\rho_1, \ldots \rho_{\varphi(m)}$ są więc różne. □

Twierdzenie 2.6 (Eulera). *Dla każdej pary liczb $a, m \in \mathbf{Z}$, $m > 1$ względnie pierwszych zachodzi kongruencja*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{2.3}$$

Dowód. Oznaczmy

$$M = r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} = \rho_1 \cdot \rho_2 \cdot \ldots \cdot \rho_{\varphi(m)}.$$

Widzimy, że $\mathbf{NWD}(M, m) = 1$, gdyż m jest względnie pierwsze z każdym czynnikiem. Z definicji ρ_k mamy

$$\rho_k \equiv a \cdot r_k \pmod{m} \qquad k = 1, 2, \ldots, \varphi(m),$$

i po pomnożeniu stronami

$$M \equiv a^{\varphi(m)} M \pmod{m} \;\Rightarrow\; m \,\big|\, M(a^{\varphi(m)} - 1).$$

Musi więc zachodzić (2.3). □

Przykład: Dla a liczby nieparzystej $a^4 \equiv 1 \pmod{8}$

Wniosek 2.7 (Małe twierdzenie Fermata). *Jeżeli p jest liczbą pierwszą, $a \in \mathbf{Z}$ nie dzieli się przez p, to*

$$a^{p-1} \equiv 1 \pmod{p}. \quad \square$$

Tajny klucz symetryczny:

Metoda szyfrowania przy pomocy tajnego klucza ma wadę: osoba szyfrująca i osoba odczytująca muszą posługiwać się tym samym kluczem. Szyfrujący może ustalić klucz, a następnie przesłać go do odbiorcy. Ale ten proces przesyłania to słabe ogniwo całego systemu: ktoś może przechwycić klucz w trakcie przesyłki. Okazuje się, że tajnego klucza wcale nie trzeba przesyłać. Dwie osoby mogą ustalić tajny klucz w sprytny sposób, przesyłając pomiędzy sobą jedynie jawne „półprodukty". Odkrycie takiego sprytnego sposobu bezpiecznej generacji tajnego klucz było sensacją, i przełomem w kryptografii. Opiszemy teraz ten sprytny (ale jednocześnie prosty) sposób. Dwie strony w jawny sposób uzgadniają dwie liczby. Jedną z tych liczb, a, nazwiemy podstawą, a drugą, m modułem. Liczba a może być mała, na przykład 2 lub 5, natomiast m powinna być dużą liczbą pierwszą. Od wielkości m zależy długość generowanego tajnego klucza, a jej pierwszość jest ważna dla bezpieczeństwa procedury. Po ustaleniu jawnych liczb a i m każda ze stron dodatkowo ustala sobie tajną liczbę, tak zwany wykładnik. Oznaczmy te dodatkowe, tajne, liczby przez t_1, t_2. Każda ze stron oblicza potęgę a^{t_i}, a następnie jej resztę z dzielenia przez m:

$$a^{t_1} = q_1 \cdot m + r_1, \qquad a^{t_2} = q_2 \cdot m + r_2.$$

Następnie strony przesyłają sobie tak obliczone reszty, w sposób jawny. Następnie każda ze stron podnosi otrzymaną resztę do swojej tajnej potęgi, i ponownie oblicza resztę z dzielenia przez m:

$$r_2^{t_1} = q_3 \cdot m + \rho_1, \qquad r_1^{t_2} = q_4 \cdot m + \rho_2.$$

Zauważmy, że $\rho_1 = \rho_2$:

$$r_2^{t_1} = \left(a^{t_2} - q_2 \cdot m\right)^{t_1} = a^{t_2 \cdot t_1} + m(\ \dots\ )$$
$$r_1^{t_2} = \left(a^{t_1} - q_1 \cdot m\right)^{t_2} = a^{t_1 \cdot t_2} + m(\ \dots\ )$$

czyli $r_2^{t_1} \equiv r_1^{t_2} \pmod{m}$. Wspólna wartość $\rho_1 = \rho_2$ jest tajnym kluczem, który został wygenerowany bez przesyłania tajnych informacji. Osoba podsłuchująca ewentualnie komunikację ma do dyspozycji liczby a, m oraz dwie reszty r_1 i r_2. Nie ma prostej metody (w praktyce oznacza to, że w ogóle nie ma metody) na odtworzenie z tych danych tajnego klucza $\rho_1 = \rho_2$, czy równoważnie potęg t_1, t_2

Przykład: Ustalamy podstawę 2 i moduł 19. To są jawne dane. Pierwszy użytkownik wybiera swoją tajną potęgę 16, a drugi użytkownik 13. Pierwszy użytkownik oblicza

$$2^{16} = 65536 = 3449 \cdot 19 + 5 \equiv 5 \pmod{19},$$

i przesyła 5 jako swoją resztę. Drugi użytkownik tak otrzymaną resztę przetwarza:

$$5^{13} = 1220703125 = 64247532 \cdot 19 + 17 \equiv 17 \pmod{19}.$$

To jest tajny klucz, wygenerowany po stronie drugiego użytkownika. Sprawdźmy, co wygeneruje pierwszy użytkownik. Drugi użytkownik oblicza swoją resztę:

$$2^{13} = 8192 = 431 \cdot 19 + 3 \equiv 3 \pmod{19},$$

i przesyła ją pierwszemu użytkownikowi. Ten dalej oblicza:

$$3^{16} = 43046721 = 2265616 \cdot 19 + 17 \equiv 17 \pmod{19}.$$

Istotnie, pierwszy użytkownik otrzymał ten sam tajny klucz.

Klucz niesymetryczny

Metoda jawnego uzgadniania tajnego klucza opisana powyżej nie zdobyła wielkiej popularności, bo wkrótce po niej odkryto jeszcze lepszą metodę szyfrowania, tak zwaną metodę z kluczem niesymetrycznym. Do szyfrowania używa się jednego klucza (który może być jawny), natomiast do odszyfrowywania potrzebny jest inny klucz, pasujący do klucza szyfrującego. Schemat komunikacji jest taki, że osoba chcąca otrzymywać zaszyfrowane wiadomości generuje parę kluczy – szyfrujący (publiczny, jawny) i odszyfrowujący (prywatny, tajny). Następnie klucz szyfrujący udostępnia wszystkich chętnym. Schemat działa następująco: wybieramy dwie liczby pierwsze p i q, które powinny być duże. Wielkość tych liczb ma wpływ na bezpieczeństwo szyfru. Dodatkowo opisywany schemat wymaga, aby wiadomość do zaszyfrowania (czyli *liczba* – w dzisiejszym elektronicznym cyfrowym świecie wiadomości to liczby), musi być mniejsza od iloczynu $p \cdot q$. Nie jest to poważne ograniczenie, gdyż praktyczne implementacje opisywanego systemu szyfrowania szyfrują w ten sposób tylko tajny klucz. Właściwa wiadomość szyfrowana jest inną metodą, właśnie przy pomocy klucza. Mamy więc wybrane dwie liczby pierwsze, i obliczamy ich iloczyn $P = p \cdot q$. Następnie obliczamy $(p-1)(q-1)$, i wybieramy liczbę k względnie pierwszą z $(p-1)(q-1)$. Para liczb P i k stanowi klucz publiczny. Kluczem tym szyfrujemy wiadomość w następujący sposób. Niech X będzie wiadomością do zaszyfrowania (to jest liczba). Podnosimy X do potęgi k i obliczamy resztę z dzielenia przez P. Tak uzyskana liczba Y to tekst zaszyfrowany. Nie da się go już odszyfrować kluczem publicznym. Do odszyfrowania postępujemy następująco. Wiemy, że $(p-1)(q-1)$ i k są względnie pierwsze, więc istnieją liczby r i μ takie, że

$$r \cdot k + \mu \cdot (p-1)(q-1) = 1. \tag{2.4}$$

Jak wiemy, r i μ można wyznaczyć algorytmem Euklidesa. Para P i r to klucz prywatny. Nie da się odtworzyć r bez znajomości faktoryzacji $P = p \cdot q$. Odszyfrowujemy wiadomość następująco. Wiadomość zaszyfrowaną czyli liczbę Y podnosimy do potęgi r, a następnie obliczamy resztę ρ z dzielenia przez P:

$$Y^r = \theta \cdot P + \rho \;\Rightarrow\; \big(X^k - \theta' \cdot P\big)^r = \theta \cdot P + \rho \;\Rightarrow\; X^{k \cdot r} = \rho + P\,(\,\ldots).$$

Widzimy więc, że $Y^r \equiv X^{k \cdot r} \pmod{P}$. Przypomnijmy funkcję φ. Wiemy, że dla liczby pierwszej p mamy $\varphi(p) = (p-1)$, oraz dla liczb względnie pierwszych p, q mamy $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$. W takim razie $\varphi(P) = (p-1)(q-1)$. Z (2.4) wynika więc, że

$$X^{k \cdot r} = X^1 \big(X^{(p-1)(q-1)}\big)^{-\mu}.$$

Wiemy z twierdzenia Eulera 2.6, że

$$X^{(p-1)(q-1)} = X^{\varphi(P)} \equiv 1 \pmod{P}.$$

Jeżeli $\mu \leq 0$ to od razu mamy

$$X^1 \big(X^{(p-1)(q-1)}\big)^{-\mu} \equiv X \pmod{P},$$

czyli $X^{k \cdot r} \equiv X \pmod{P}$. Jeżeli $\mu > 0$ to pisząc

$$\big(X^{(p-1)(q-1)}\big)^{\mu} \equiv 1 \pmod{P} \;\Rightarrow\; \big(X^{(p-1)(q-1)}\big)^{\mu} X^{k \cdot r} \equiv X^{k \cdot r} \pmod{P},$$

ale lewa strona ostatniej kongruencji to X, tak więc niezależnie od znaku μ otrzymaliśmy

$$X^{k \cdot r} \equiv X \pmod{P} \;\Rightarrow\; \rho \equiv X \pmod{P}.$$

Jeżeli $X < P$, to w takim razie $X = \rho$. Mając resztę ρ potrafimy więc odczytać wiadomość X.

Przykład: Niech $p = 2$ i $q = 11$. Wtedy $P = 22$, a jako k możemy wziąć 3, liczbę względnie pierwszą z $(p-1)(q-1) = 1 \cdot 10 = 10$. Mamy klucz publiczny $(22, 3)$. Powiedzmy, że wiadomość do zaszyfrowania to $X = 16$. Kluczem publicznym szyfrujemy wiadomość:

$$16^3 = 4096 = 186 \cdot 22 + 4 \equiv 4 \pmod{22}.$$

Wiadomość zaszyfrowana to 4. Następnie znajdujemy r i μ takie, że

$$r \cdot 3 + \mu \cdot 10 = 1.$$

Wiemy jak rozwiązać takie równanie, i łatwo znajdujemy, na przykład, $r = 7$, $\mu = -2$. Odszyfrowujemy wiadomość:

$$4^7 = 2^{14} = 16384 = 744 \cdot 22 + 16 \equiv 16 \pmod{22}.$$

Wiadomość została prawidłowo odszyfrowana. Kluczem publicznym była para $(22, 3)$, natomiast kluczem prywatnym para $(22, 7)$.

Na zakończenie tego rozdziału udowodnimy jeszcze tak zwane „chińskie twierdzenie o resztach". Zwróćmy uwagę, że nazwa ta pojawiła się dawno temu, kiedy określenie „chińskie" miało zupełnie inny podtekst. Nazwę twierdzenia należy więc rozumieć w dawnym sensie, jakoś „tajemnicze twierdzenie o resztach", czy „mądre twierdzenie o resztach". Nie należy nazwy twierdzenia interpretować ze współczesnym podtekstem, gdyż twierdzenie to wcale nie jest tandetne.

Twierdzenie 2.8 (Chińskie twierdzenie o resztach). *Niech $m \in N$, $m \geq 2$, a liczby $a_1, a_2, \ldots, a_m \in \mathbf{N}$ niech będą parami względnie pierwsze. Jeżeli $r_1, r_2, \ldots, r_m \in \mathbf{Z}$ będą dowolne, to istnieją liczby całkowite $x_1, x_2, \ldots, x_m$ dla których*

$$a_1 \cdot r_1 = a_2 \cdot r_2 = \cdots = a_m \cdot r_m. \tag{2.5}$$

Dowód. Dowód jest indukcyjny ze względu na m. Dla $m = 2$ twierdzenie jest prawdziwe, bo sprowadza się do rozwiązania równania

$$a_1 \cdot x_1 - a_2 \cdot x_2 = r_2 - r_1,$$

przy czym $\mathbf{NWD}(a_1, a_2) = 1$. Udowodnimy teraz krok indukcyjny. Załóżmy, że twierdzenie jest prawdziwe dla pewnej liczby $m \geq 2$. Weźmy jakieś liczby $a_1, \ldots, a_{m+1}$ parami względnie pierwsze, i $r_1, \ldots, r_{m+1}$ dowolne całkowite. Z założenia indukcyjnego istnieją liczby całkowite $x_1, \ldots x_m$ takie, że zachodzi (2.5). Mamy

$$\mathbf{NWD}(a_1 \cdot a_2 \cdot \ldots \cdot a_m, a_{m+1}) = 1,$$

a więc istnieją liczby $t, u \in \mathbf{Z}$ spełniające

$$a_1 \cdot a_2 \cdot \ldots \cdot a_m \, t - a_{m+1} \, u = r_{m+1} - a_1 \cdot x_1 - r_1.$$

Niech

$$x_i' = \frac{a_1 \cdot a_2 \cdot \ldots \cdot a_m}{a_i} \, t + x_i, \qquad i = 1, 2, \ldots, m, \quad \text{oraz } x_{m+1}' = u.$$

Liczby x_i' są całkowite, oraz

$$a_i x_i' + r_i = a_1 \cdot a_2 \cdot \ldots \cdot a_m \cdot t + a_i \cdot x_i + r_i$$

$$= a_{m+1} \cdot u + r_{m+1} - a_1 \cdot x_1 - r_1 + a_i \cdot x_i + r_i$$
$$= a_{m+1} \cdot u + r_{m+1}$$
$$= a_{m+1} \cdot x'_{m+1} + r_{m+1}.$$

□

Wniosek 2.9. *Jeżeli $m \geq 2$ i liczby $a_1, a_2, \ldots, a_m$ są parami względnie pierwsze, oraz $r_1, r_2, \ldots, r_m$ są dowolnymi resztami ($0 \leq r_i < a_i$), to istnieje liczba naturalna N taka, że reszta z dzielenia N przez a_i jest równa r_i, $i = 1, \ldots, m$.* □

Rozdział 3

Wielomiany

Liczby zespolone

Zbiór liczb zespolonych $\mathbf{C}$ jest większy od zbioru liczb rzeczywistych: $\mathbf{R} \subset \mathbf{C}$. Liczby zespolone możemy interpretować w kilka równoważnych sposobów:

- Jako liczby postaci $a + b\,\mathbf{i}$, gdzie $a, b \in \mathbf{R}$, natomiast $\mathbf{i}$ jest symbolem. Liczby te dodajemy i odejmujemy według wzoru:

  $$(a_1 + b_1\,\mathbf{i}) \pm (a_2 + b_2\,\mathbf{i}) = (a_1 \pm a_2) + (b_1 \pm b_2)\,\mathbf{i},$$

  a mnożymy według wzoru

  $$(a_1 + b_1\,\mathbf{i}) \cdot (a_2 + b_2\,\mathbf{i}) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)\,\mathbf{i}.$$

  Jeżeli $b = 0$ to piszemy po prostu $a + 0\,\mathbf{i} = a$, i takie liczby zespolone utożsamiamy z liczbami rzeczywistymi. Jeżeli $a = 0$ to piszemy po prostu $0 + b\,\mathbf{i} = b\,\mathbf{i}$ i takie liczby nazywamy czysto urojonymi. Jeżeli $b = 1$ to b również nie piszemy, na przykład $0 + 1\,\mathbf{i} = \mathbf{i}$. Rolę 0 pełni po prostu $0 = 0 + 0\,\mathbf{i}$, rolę 1 pełni $1 = 1 + 0\,\mathbf{i}$. Można wyprowadzić wzór na dzielenie. Dowolne liczby można przez siebie dzielić, z wyjątkiem dzielenia przez 0. Zauważmy, że $\mathbf{i}^2 = (0 + 1\,\mathbf{i})(0 + 1\,\mathbf{i}) = -1 + 0\,\mathbf{i} = -1$. $\mathbf{i}$ jest więc pierwiastkiem kwadratowym z -1 (podobnie jak $-\mathbf{i}$).

- Jako pary liczb rzeczywistych (a, b), $a, b \in \mathbf{R}$. Pary takie dodajemy i odejmujemy według wzorów

  $$(a_1, b_1) \pm (a_2, b_2) = (a_1 \pm a_2, b_1 \pm b_2),$$

  a mnożymy według wzoru

  $$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1).$$

Zerem jest para $(0,0)$ a jedynką $(1,0)$. Liczby rzeczywiste a utożsamiamy z parami $(a,0)$. Podobnie jak w powyższej interpretacji takie utożsamienie zachowuje działania na liczbach rzeczywistych.

- Jako punkty płaszczyzny $\mathbf{R}^2 = \{(x,y); x,y \in \mathbf{R}\}$. Ta interpretacja liczb zespolonych łączy się w oczywisty sposób z poprzednią. Liczby rzeczywiste utożsamiamy z prosta poziomą $\{(x,0); x \in \mathbf{R}\}$.

Liczby zespolone to w pewnym sensie najlepszy rodzaj liczb (każdy wielomian rozkłada się na czynniki liniowe), i są bardzo chętnie stosowane także w zastosowaniach.

Kwaterniony

Kwaterniony to zbiór liczb jeszcze większy niż zbiór liczb zespolonych. Jako liczby kwaterniony nie są już tak dobre jak liczby zespolone – mnożenie nie jest przemienne. Nie są więc raczej stosowane (chociaż w niektórych dziedzinach inżynierii używa się kwaternionów), i traktujemy je jako ciekawostkę. Kwaterniony możemy zdefiniować na kilka równoważnych sposobów:

- Jako liczby postaci $a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$, $a,b,c,d \in \mathbf{R}$. Dodawanie, odejmowanie i mnożenie definiujemy w zwykły sposób, mnożąc wszystko przez wszystko, i grupując, oraz

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}.$$

- Jako liczby postaci $z + t\,\mathbf{j}$, gdzie $z,y \in \mathbf{C}$,

- Jako pary (z,t), gdzie $z,t \in \mathbf{C}$ z następująco zdefiniowanym mnożeniem

$$(z_1,t_1)(z_2,t_2) = (z_1\overline{z_2} - t_1\overline{t_2}, z_1\overline{t_2} + t_1\overline{z_2}).$$

- Jako czwórki liczb rzeczywistych (a,b,c,d), $a,b,c,d \in \mathbf{R}$ z odpowiednio zdefiniowanym działaniami.

Wielomiany

Wielomiany to funkcje postaci

$$P(x) = a_n\,x^n + a_{n-1}\,x^{n-1} + \cdots + a_1\,x + a_0.$$

Współczynniki a_i mogą być rzeczywiste lub zespolone, i wielomian P nazywamy odpowiednio wielomianem rzeczywistym lub zespolonym. Jeżeli

$a_n \neq 0$ to wyrażenie $a_n\, x^n$ nazywamy wyrazem wiodącym wielomianu, samo a_n współczynnikiem wiodącym, a n stopniem wielomianu $n = \deg(P)$. Wyraz a_0 nazywa się wyrazem wolnym wielomianu. Podobnie jak liczby całkowite, wielomiany można dodawać, odejmować, mnożyć i, czasami, dzielić. Zauważmy, że stopień sumy i różnicy wielomianów jest nie wyższy niż większy ze stopni składników, natomiast stopień iloczynu wielomianów jest zawsze sumą stopni czynników. Mówimy, że wielomian P dzieli wielomian Q ($P \,\big|\, Q$) jeżeli istnieje wielomian R taki, że $P \cdot R = Q$. Zauważmy, że wtedy musi zachodzić $\deg(P) \leq \deg(Q)$. Mamy też następujący fakt.

Fakt 3.1. *Jeżeli $P \,\big|\, Q$ oraz $Q \,\big|\, P$, to $P = c\,Q$, dla pewnej stałej c.*

Dowód. Kiedy mnożymy dwa wielomiany ich stopnie się dodają. Skoro $P \,\big|\, Q$ to $Q = P \cdot R$ dla pewnego wielomianu R. Z drugiej strony skoro $Q \,\big|\, P$ to $P = Q \cdot S$ dla pewnego wielomianu S. W takim razie $P = S \cdot R \cdot P$, a więc stopnie R i S muszą być równe 0, czyli wielomiany te muszą być stałymi. □

Zauważmy, że wielomian stały $P(x) = a_0 \neq 0$ dzieli każdy inny wielomian. Mówimy, że wielomian Q jest rozkładalny, jeżeli istnieją dwa wielomiany P i R, oba stopnia co najmniej 1 (a więc żaden nie jest stałą), takie, że $Q = P \cdot R$. Jeżeli wielomian nie jest rozkładalny, to nazywamy go nierozkładalnym (nieprzywiedlnym, pierwszym). Zauważmy, że rozkładalność zależy od tego, czy wielomian rozpatrujemy jako rzeczywisty, czy jako zespolony. Na przykład wielomian x^2+1 jest nierozkładalny jako wielomian rzeczywisty, ale rozkłada się $x^2 + 1 = (x + i) \cdot (x - i)$ jako wielomian zespolony. Mamy następujący fakt, stanowiący podstawę algorytmu Euklidesa dla wielomianów.

Fakt 3.2. *Dla każdej pary wielomianów P i S ($\deg(P) > 0$) istnieje dokładnie jedna para wielomianów Q i R taka, że*

$$S = P \cdot Q + R, \qquad \deg(R) < \deg(P).$$

Innymi słowy, wielomiany można zawsze dzielić z resztą. Wielomian Q nazywamy ilorazem, a R resztą dzielenia.

Dowód. Najpierw udowodnimy istnienie pary Q, R. Zastosujemy indukcję względem stopnia wielomianu S, wielomian P traktując jako ustalony. Przypomnijmy, że $\deg(P) > 0$. Jeżeli $\deg(S) < \deg(P)$ to wystarczy wziąć $Q = 0$, $R = S$. Załóżmy, że fakt został już udowodniony (tylko istnienie) dla wielomianów S stopnia mniejszego niż n, i weźmy dowolny wielomian S stopnia n, przy czym $n \geq \deg(P) = m$. Niech a_n będzie współczynnikiem wiodącym S a b_m współczynnikiem wiodącym wielomianu P ($a_n, b_m \neq 0$). Rozpatrzmy wielomian

$$S_1(x) = S(x) - \frac{a_n}{b_m}\, x^{n-m}\, P(x).$$

Łatwo zauważyć że wyrazy wiodące dwóch wielomianów po prawej stronie kasują się, a więc S_1 jest wielomianem stopnia niższego niż $n = \deg(S)$. W takim razie, na mocy założenia indukcyjnego

$$S_1 = Q_1 \cdot P + R, \qquad \deg(R) < \deg(P).$$

Mamy więc

$$\begin{aligned} S(x) &= S_1(x) + \frac{a_n}{b_m}\, x^{n-m}\, P(x) \\ &= (Q_1(x) + \frac{a_n}{b_m}\, x^{n-m})P(x) + R(x) \\ &= Q(x) \cdot P(x) + R(x). \end{aligned}$$

Istnienie ilorazu i reszty zostało więc indukcyjnie udowodnione. Pokażemy teraz jednoznaczność. Niech

$$S = Q_1 \cdot P + R_1 = Q_2 \cdot P + R_2, \qquad \deg(R_i) < \deg(P),\ i = 1, 2.$$

Wynika stąd, że

$$P\,(Q_1 - Q_2) = R_2 - R_1.$$

Stopień prawej strony jest $< \deg(P)$ więc jedyną możliwością jest $Q_1 - Q_2 = 0$ oraz, w konsekwencji $R_1 = R_2$. □

Uwaga: Zauważmy, że powyższy dowód daje nam także procedurę znajdowania ilorazu i reszty – jest to zwykła procedura długiego dzielenia.
Przykład:

Dzięki Faktowi 3.2 możemy udowodnić dla wielomianów wiele twierdzeń, których dla liczb całkowitych dowodziliśmy przy pomocy algorytmu Euklidesa.

NWD i NWW

Zdefiniujemy teraz **NWD** i **NWW** wielomianów. Zauważmy, że musimy ustalić jakąś normalizację. W przypadku liczb całkowitych ograniczyliśmy się do dzielników i wielokrotności dodatnich. W przypadku wielomianów musimy zdecydować się na jakąś stałą.

Definicja 3.3. *Niech P i Q będą wielomianami, z których co najmniej jeden jest niezerowy.* $\mathbf{NWD}(P,Q)$ *to wielomian o następujących własnościach:*

(a) współczynnik wiodący $\mathbf{NWD}(P,Q)$ *jest równy* 1,

(b) $\mathbf{NWD}(P,Q) \,\big|\, P$ *oraz* $\mathbf{NWD}(P,Q) \,\big|\, Q$,

(c) jeżeli jakiś wielomian R dzieli jednocześnie P i Q to także $R \,\big|\, \mathbf{NWD}(P,Q)$.

Uwaga: Bezpośrednio z powyższego sformułowania definicji nie wynika, że $\mathbf{NWD}(P,Q)$ w ogóle istnieje, a nawet jeżeli istnieje, to że jest jedyny. Istnienie udowodnimy za moment, natomiast teraz zauważmy, że jeżeli $\mathbf{NWD}(P,Q)$ istnieje, to może być tylko jeden. Jeżeli dwa wielomiany S_1 i S_2 spełniałyby warunki (a)–(c), to mielibyśmy $S_1 \,\big|\, S_2$ oraz $S_2 \,\big|\, S_1$. W takim razie istniałaby stała $c \neq 0$ taka, że $S_1 = c \cdot S_2$. Z normalizacji (a) wynikałoby wtedy, że $c = 1$. W takim razie największy wspólny dzielnik $\mathbf{NWD}(P,Q)$, jeżeli istnieje, określony jest jednoznacznie.

Definicja 3.4. *Niech P i Q będą niezerowymi wielomianami.* $\mathbf{NWW}(P,Q)$ *to wielomian o następujących własnościach*

(a) współczynnik wiodący $\mathbf{NWW}(P,Q)$ *to iloczyn współczynników wiodących P i Q,*

(b) $P \,\big|\, \mathbf{NWW}(P,Q)$ *oraz* $Q \,\big|\, \mathbf{NWW}(P,Q)$,

(c) jeżeli dla pewnego wielomianu R mamy $P \,\big|\, R$ i $Q \,\big|\, R$ to także $\mathbf{NWW}(P,Q) \,\big|\, R$.

Uwagi: (i) Podobnie jak w przypadku **NWD** możemy zauważyć, że powyższe warunki jednoznacznie określają **NWW**.
(ii) Trzeba jeszcze pokazać, że **NWD** i **NWW** istnieją. Na razie uzasadniliśmy, że oba te wielomiany jeżeli istnieją, to sa jedyne.

Fakt 3.5. *Jeżeli P i Q są wielomianami z których co najmniej jeden jest niezerowy, to istnieje* $\mathbf{NWD}(P,Q)$.

Dowód. Dowód istnienia przeprowadzimy konstruując $\mathbf{NWD}(P,Q)$ wprost. Podobnie jak w przypadku liczb całkowitych wykorzystamy algorytm Euklidesa. Załóżmy, że $P \neq 0$, i że $\deg(P) \geq \deg(Q)$. Jeżeli $Q = 0$ to, jak łatwo sprawdzić, wielomian $\frac{P}{a}$, gdzie a jest współczynnikiem wiodącym P, jest $\mathbf{NWD}(P,Q)$. Rozważmy więc przypadek $Q = neq0$. Jeżeli $\deg(Q) = 0$, czyli Q jest stałą, to oczywiście $\mathbf{NWD}(P,Q) = 1$. Ograniczmy się więc do przypadku $\deg(Q) > 0$. Wtedy dzielimy P przez Q z resztą:

$$P = W \cdot Q + R, \qquad \deg(R) < \deg(Q),$$

i postępujemy dalej rekurencyjnie. Powstaje skończony ciąg wielomianów S_n, taki, że $S_1 = P$, $S_2 = Q$ oraz

$$S_{n-1} = W_n \cdot S_n + S_{n+1}, \qquad \deg(S_{n+1}) < \deg(S_n),$$

jeżeli $\deg(S_n) > 0$, natomiast jeżeli $\deg(S_n) = 0$ to $S_{n+1} = 0$. Dopóki dzielenie daje niezerową resztę procedura toczy się, ale jest jasne, że skoro stopnie wielomianów S_n ściśle maleją, to w końcu dochodzimy do momentu, w którym reszta jest zerem, i procedura kończy się. Niech S_n będzie ostatnim wielomianem różnym od zera w powyższym skończonym ciągu. Czasem nazywa się on ostatnią resztą. Mamy więc

$$S_{n-2} = W_{n-1} \cdot S_{n-1} + S_n, \tag{3.1}$$

$$S_{n-1} = W_n \cdot S_n. \tag{3.2}$$

Zgodnie z (3.2) mamy $S_n \,\big|\, S_{n-1}$, a zgodnie z (3.1) także $S_n \,\big|\, S_{n-2}$. Następnie „cofając się" wzdłuż ciągu $\{S_k\}$ widzimy, że S_n dzieli wszystkie elementy ciągu, w tym $S_n \,\big|\, P$ i $S_n \,\big|\, Q$. Widzimy więc, że S_n spełnia warunek (b) Definicji 3.3. Z drugiej strony, jeżeli jakiś wielomian R dzieli P i Q, to posuwając się "wzdłuż" ciągu $\{S_k\}$ widzimy, że dzieli także wszystkie jego wyrazy, w tym także ostatni, S_n. S_n spełnia więc także warunek (c) definicji **NWD**. W końcu, niech a będzie współczynnikiem wiodącym wielomianu S_n, wtedy oczywiście wielomian

$$\mathbf{NWD}(P,Q) = \frac{1}{a} S_n$$

spełnia wszystkie warunki (a)–(c) Definicji 3.3. □

Dowody następujących faktów są takie same, jak w przypadku liczb całkowitych.

Fakt 3.6. *Niech P i Q będą pewnymi wielomianami. Wtedy istnieją wielomiany S i T takie, że*

$$P \cdot S + Q \cdot T = \mathbf{NWD}(P,Q).$$

Fakt 3.7. *Wielomiany P i Q są względnie pierwsze (to znaczy $\mathbf{NWD}(P,Q) = 1$) wtedy i tylko wtedy gdy istnieją wielomiany S i T takie, że*

$$P \cdot S + Q \cdot T = 1.$$

Fakt 3.8. *Jeżeli wielomiany P i Q są niezerowe, to wielomiany $\frac{P}{\mathbf{NWD}(P,Q)}$ i $\frac{Q}{\mathbf{NWD}(P,Q)}$ są względnie pierwsze.*

Fakt 3.9. *Jeżeli wielomiany P i Q są względnie pierwsze i $P \,\big|\, Q \cdot W$ to $P \,\big|\, W$.*

Udowodnimy teraz istnienie **NWW**.

Twierdzenie 3.10. *Niech P i Q będą niezerowymi wielomianami. Wtedy istnieje $\mathbf{NWW}(P,Q)$ oraz*

$$\mathbf{NWW}(P,Q) = \frac{P \cdot Q}{\mathbf{NWD}(P,Q)}. \tag{3.3}$$

Dowód. Wielomian zdefiniowany wzorem (3.3) spełnia oczywiście warunki (a) i (b) Definicji 3.4. Załóżmy więc, że wielomian R jest wspólną wielokrotnością P i Q czyli $P \,\big|\, R$ i $Q \,\big|\, R$. Mamy więc

$$R = P \cdot S, \qquad R = Q \cdot T.$$

Z drugiej strony mamy

$$P = W \cdot \mathbf{NWD}(P,Q), \qquad Q = V \cdot \mathbf{NWD}(P,Q),$$

oraz wielomiany W i V są zgodnie z Faktem 3.8 względnie pierwsze. W takim razie

$$R = W \cdot S \cdot \mathbf{NWD}(P,Q) = V \cdot T \cdot \mathbf{NWD}(P,Q) \;\Rightarrow\; W \cdot S = V \cdot T.$$

W takim razie $W \,\big|\, V \cdot T$ czyli $W \,\big|\, T$ a stąd $T = W \cdot T_1$, czyli

$$R = V \cdot W \cdot T_1 \cdot \mathbf{NWD}(P,Q) = \frac{P \cdot Q}{\mathbf{NWD}(P,Q)} \cdot T_1 \;\Rightarrow\; \frac{P \cdot Q}{\mathbf{NWD}(P,Q)} \,\big|\, R.$$

Warunek (c) Definicji 3.4 jest więc też spełniony. □

Pierwiastki

Liczba X_0 jest pierwiastkiem wielomianu P jeże li $P(x_0) = 0$. Mamy natychmiast następujący fakt.

Fakt 3.11. *Liczba x_0 jest pierwiastkiem wielomianu p wtedy i tylko wtedy gdy $(x - x_0) \mid P$.*

Dowód. Jeżeli $(x - x_0) \mid P$ to oczywiście x_0 jest pierwiastkiem P. Wystarczy więc udowodnić przeciwną implikację. Załóżmy, że x_0 jest pierwiastkiem P. Oznaczmy

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

Wtedy

$$\begin{aligned}
P(x) &= P(x) - P(x_0) \\
&= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 - \\
&\quad - a_n x_0^n - a_{n-1}x_0^{n-1} - \cdots - a_1 x_0 - a_0 \\
&= a_n(x^n - x_0^n) + a_{n-1}(x^{n-1} - x_0^{n-1}) + \cdots + a_1(x - x_0) \\
&= a_n(x - x_0)(x^{n-1} + x^{n-2}x_0 + \cdots + x x_0^{n-2} + x_0^{n-1}) + \\
&\quad + a_{n-1}(x - x_0)(x^{n-2} + \cdots + x_0^{n-2}) + \cdots + a_1(x - x_0) \\
&= (x - x_0)(a_n(x^{n-1} + x^{n-2}x_0 + \cdots + x x_0^{n-2} + x_0^{n-1}) + \cdots + a_1).
\end{aligned}$$

□

Mówimy, że x_0 jest pierwiastkiem stopnia k (pierwiastkiem k-krotnym) wielomianu P ($k \geq 1$) jeżeli

$$(x - x_0) \mid P \quad \text{ale} \quad (x - x_0)^{k+1} \nmid P.$$

Wniosek 3.12. *Wielomian stopnia n ma co najwyżej n pierwiastków (pierwiastek k-krotny liczony jest jako k pierwiastków.*

Dowód. Dowód jest indukcyjny. Dla $n = 1$ jest dobrze: wielomian stopnia 1, czyli $P(x) = a_1 x + a_0$ ma dokładnie 1 pierwiastek $x_0 = -\frac{a_0}{a_1}$. Załóżmy, że wniosek jest prawdziwy dla pewnego $n \geq 1$ i rozważmy wielomian P stopnia $n+1$. Jeżeli P nie ma pierwiastków to wniosek jest prawdziwy w odniesieniu do P. Natomiast jeżeli P ma pierwiastek x_0 to

$$P(x) = (x - x_0)\, W(x),$$

gdzie $W(x)$ jest wielomianem stopnia n. Pierwiastki P to x_0 lub pierwiastki W, których na mocy założenia indukcyjnego jest nie więcej niż n. W sumie pierwiastków P jest więc nie więcej niż $n + 1$ (z uwzględnieniem krotności). Krok indukcyjny został więc wykonany. □

Podamy bez dowodu tak zwane zasadnicze twierdzenie algebry. Dowód nie jest trudny, ale używa teorii funkcji zmiennej zespolonej.

Twierdzenie 3.13 (Zasadnicze twierdzenie algebry). *Wielomian zespolony stopnia n ma dokładnie n pierwiastków (z uwzględnieniem krotności).*

Wniosek 3.14. *Jedynymi wielomianami zespolonymi nierozkładalnymi (pierwszymi) są wielomiany stopni* 0 *i* 1. *Każdy wielomian stopnia wyższego jest rozkładalny.*

Wniosek 3.15. *Jedynymi wielomianami rzeczywistymi nierozkładalnymi są wielomiany stopni* 0, 1 *lub* 2. *Każdy wielomian stopnia wyższego jest rozkładalny.*

Dowód. Rozważmy wielomian

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_i \in \mathbf{R}.$$

Co prawda wielomian ma współczynniki rzeczywiste, ale możemy potraktować go jako szczególny przypadek wielomianu zespolonego. Jako taki, w myśl Wniosku 3.14, rozkłada się na iloczyn czynników liniowych

$$P(x) = a_n(x - z_1)(x - z_2)\dots(x - z_n), \tag{3.4}$$

gdzie $z_1, \dots, z_n$ są pierwiastkami, być może zespolonymi, i być może powtarzającymi się. Zauważmy, że jeżeli z jest pierwiastkiem P i $z \notin \mathbf{R}$, to także $\overline{z}$ jest pierwiastkiem P:

$$P(\overline{z}) = \overline{P(z)},$$

(gdyż współczynniki $a_n, \dots, a_0$ są rzeczywiste), a $\overline{0} = 0$. W reprezentacji (3.4) pierwiastki można więc pogrupować na rzeczywiste i zespolone w parach sprzężonych:

$$P(x) = a_n(x-x_1)(x-x_2)\dots(x-x_k)(x-z_1)(x-\overline{z_1})(x-z_2)(x-\overline{z_2})\dots(x-z_m)(x-\overline{z_m}).$$

$x_1, \dots, x_k$ to pierwiastki rzeczywiste (których być może w ogóle nie ma), a $z_1, \overline{z_1}, \dots, z_m, \overline{z_m}$ to pierwiastki zespolone we wzajemnie sprzężonych parach (pierwiastków zespolonych też może w ogóle nie być). Niech

$$z_j = \alpha_j + i\,\beta_j, \qquad \alpha_j, \beta_j \in \mathbf{R},$$

wtedy

$$\begin{aligned}(x - z_j)(x - \overline{z_j}) &= x^2 - x\overline{z_j} - xz_j + z_j\overline{z_j} \\ &= x^2 - x(\alpha_j - i\,\beta_j) - x(\alpha_j + i\,\beta_j) + (\alpha_j^2 + \beta_j^2) \\ &= x^2 - 2\,\alpha_j\,x + \alpha_j^2 + \beta_j^2.\end{aligned}$$

Jest to wielomian rzeczywisty stopnia 2. Jest on nierozkładalny, gdyż nie ma pierwiastków rzeczywistych ($\Delta = 4\alpha_j^2 - 4(\alpha_j^2 + \beta_j^2) = -4\beta_j^2 < 0$). □

Wniosek 3.16. *Wielomian rzeczywisty stopnia nieparzystego ma pierwiastek rzeczywisty i dzieli się więc przez czynnik liniowy.*

Znajdowanie pierwiastków

Dla wielomianów stopni $1, 2, 3, 4$ istnieją wzory na pierwiastki. Udowodniono, że dla wielomianów stopni wyższych niż 4 takich wzorów nie ma. Wyprowadzimy wzory na pierwiastki wielomianu stopnia 3, są to tak zwane wzory Cardano. Rozważmy równanie 3 stopnia:

$$a_3x^3 + a_2x^2 + a_1x + a_0 = 0. \tag{3.5}$$

Obie strony możemy podzielić przez a_3, więc przyjmijmy, że $a_3 = 1$. Zróbmy podstawienie $y = x + \frac{a_2}{3}$. Wstawiając $x = y - \frac{a_2}{3}$ do (3.5) otrzymujemy

$$\begin{aligned}
0 &= \left(y - \frac{a_2}{3}\right)^3 + a_2\left(y - \frac{a_2}{3}\right)^2 + a_1\left(y - \frac{a_2}{3}\right) + a_0 \\
&= y^3 - 3y^2\frac{a_2}{3} + 3y\frac{a_2^2}{3^2} - \frac{a_2^3}{3^3} + a_2\left(y^2 - 2y\frac{a_2}{3} + \frac{a_2^2}{3^2}\right) + a_1\left(y - \frac{a_2}{3}\right) + a_0 \\
&= y^3 + y^2(-a_2 + a_2) + y\left(\frac{a_2^2}{3} - \frac{2a_2^2}{3} + a_1\right) - \frac{a_2^3}{27} + \frac{a_2^3}{9} - \frac{a_1a_2}{3} + a_0 \\
&= y^3 + Ay + B,
\end{aligned}$$

gdzie

$$A = a_1 - \frac{a_2^2}{3} = \frac{3a_1 - a_2^2}{3},$$
$$B = \frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0 = \frac{2a_2^3 - 9a_1a_2 + 27a_0}{27}.$$

Równanie 3 stopnia (3.5) zostało więc sprowadzone do postaci bez wyrazu kwadratowego. Oczywiście obie postacie równania są równoważne, związek pomiędzy nimi sprowadza się do prostego przesunięcia $y = x + \frac{a_2}{3}$. Będziemy więc szukali rozwiązań równania

$$y^3 + Ay + B = 0. \tag{3.6}$$

Zróbmy jeszcze jedno podstawienie

$$y = z - \frac{A}{3z}. \tag{3.7}$$

Zauważmy, że odpowiednie z zawsze możemy znaleźć,

$$z = \frac{y \pm \sqrt{y^2 + \frac{4Ay}{3}}}{2}.$$

Podstawiając (3.7) do równania (3.6) otrzymujemy

$$\begin{aligned} 0 &= \left(z - \frac{A}{3z} \right)^3 + A \left(z - \frac{A}{3z} \right) + B \\ &= z^3 - z^2 \frac{A}{z} + z \frac{A^2}{3z^2} - \frac{A^3}{27z^3} + Az - \frac{A^2}{3z} + B \\ &= z^3 + z(-A + A) + \frac{1}{z} \left(\frac{A^2}{3} - \frac{A^2}{3} \right) - \frac{1}{z^3} \frac{A^3}{27} + B \\ &= z^3 - \frac{A^3}{27z^3} + B. \end{aligned}$$

Mnożymy stronami przez z^3, i otrzymujemy

$$z^6 + B\, z^3 - \frac{A^3}{27} = 0. \tag{3.8}$$

Oznaczając $w = z^3$ otrzymujemy dalej

$$w^2 + B\, w - \frac{A^3}{27} = 0. \tag{3.9}$$

Jest to tak zwane „równanie rozwiązujące" lub „rezolwenta". Jest to równanie kwadratowe, i łatwo je rozwiązać. Oznaczmy pierwiastki rezolwenty α_1, α_2 (być może są równe). Zauważmy, że z równania (3.9) wynika, że

$$\alpha_1 \cdot \alpha_2 = -\frac{A^3}{27}. \tag{3.10}$$

Wiemy, że są 3 różne pierwiastki stopnia 3 z α_1. Wybierzmy jeden z nich, $z_1 = \sqrt[3]{\alpha_1}$. Wszystkie pierwiastki 3 stopnia z α_1 dane są wtedy wzorami:

$$z_1, \qquad z_2 = z_1\, e^{i\, 2\pi/3}, \qquad z_3 = z_1\, e^{i\, 4\pi/3} = z_1\, e^{-i\, 2\pi/3}.$$

Niech ξ_1, ξ_2, ξ_3 będą pierwiastkami 3 stopnia z α_2. $z_1, z_2, z_3 xi_1, \xi_2$ oraz ξ_3 to jedyne liczby, które spełniają (3.8). Z równania (3.10) wynika, że liczby

$$-\frac{A}{3\, z_i}, \qquad i = 1, 2, 3$$

są pierwiastkami 3 stopnia z α_2. W takim razie, z dokładnością do numeracji mamy

$$\xi_1 = -\frac{A}{3\, z_1}, \quad \xi_2 = -\frac{A}{3\, z_2} = -\frac{A}{3\, z_1\, e^{i\, 2\pi/3}} = -\frac{A\, e^{-i\, 2\pi/3}}{3\, z_1},$$

$$\xi_3 = -\frac{A}{3\,z_3} = -\frac{A}{3\,z_1\,e^{-i\,2\pi/3}} = -\frac{A\,e^{i\,2\pi/3}}{3\,z_1}.$$

Zauważmy w końcu, że

$$z_i - \frac{A}{3\,z_i} = z_i + \xi_i = \xi_i - \frac{A}{3\,\xi_i}, \quad i = 1, 2, 3.$$

Wracając do zmiennej y w podstawieniu (3.7) widzimy, że znaleźliśmy 3 pierwiastki równania (3.6):

$$\begin{aligned} y_1 &= z_1 - \frac{A}{3\,z_1}, \\ y_2 &= z_2 - \frac{A}{3\,z_2} = z_1\,e^{i\,2\pi/3} - \frac{A\,e^{-i\,2\pi/3}}{3\,z_1}, \\ y_3 &= z_3 - \frac{A}{3\,z_3} = z_1\,e^{-i\,2\pi/3} - \frac{A\,e^{i\,2\pi/3}}{3\,z_1}. \end{aligned} \tag{3.11}$$

Podsumujmy powyższe rozważania:

Wniosek 3.17 (Wzory Cardano). *Pierwiastki równania* 3 *stopnia* (3.5)

$$a_3x^3 + a_2x^2 + a_1x + a_0 = 0$$

dane są wzorami:

$$\begin{aligned} x_1 &= z_1 - \frac{A}{3\,z_1} - \frac{a_2}{3\,a_3}, \\ x_2 &= z_1\,e^{i\,2\pi/3} - \frac{A\,e^{-i\,2\pi/3}}{3\,z_1} - \frac{a_2}{3\,a_3}, \\ x_3 &= z_1\,e^{-i\,2\pi/3} - \frac{A\,e^{i\,2\pi/3}}{3\,z_1} - \frac{a_2}{3\,a_3} \end{aligned}$$

gdzie z_1 jest dowolnym z pierwiastków 3 *stopnia dowolnego z pierwiastków rezolwenty* (3.9)*:*

$$w^2 + B\,w - \frac{A^3}{27} = 0.$$

W powyższym wzorze

$$\begin{aligned} A &= \frac{3\,a_1\,a_3 - a_2^2}{3\,a_3^2}, \\ B &= \frac{2\,a_2^3 - 9\,a_1\,a_2\,a_3 + 27\,a_0\,a_3^2}{27\,a_3^3}. \end{aligned}$$

□

W przypadku gdy równanie (3.5) ma współczynniki rzeczywiste możemy wyciągnąć dodatkowe wnioski. Rezolwenta (3.9) też ma współczynniki rzeczywiste, i w takim razie pierwiastki α_1, α_2 mogą być:

(a) dwa rzeczywiste różne,

(b) jeden rzeczywisty podwójny,

(c) dwa zespolone sprzężone.

Przypomnijmy wzory (3.11):

$$\begin{aligned} y_1 &= z_1 - \frac{A}{3\,z_1}, \\ y_2 &= z_1\, e^{i\,2\pi/3} - \frac{A\, e^{-i\,2\pi/3}}{3\,z_1}, \\ y_3 &= z_1\, e^{-i\,2\pi/3} - \frac{A\, e^{i\,2\pi/3}}{3\,z_1}. \end{aligned}$$

W przypadkach (a) i (b) pierwiastek α_1 jest rzeczywisty i możemy wybrać z_1 rzeczywiste. Wtedy

$$\begin{aligned} y_2 &= \Big(z_1 - \frac{A}{3\,z_1}\Big)\,\cos(2\pi/3) + \Big(z_1 + \frac{A}{3\,z_1}\Big)\,\sin(2\pi/3) \\ &= \Big(-\frac{1}{2}\Big)\Big(z_1 - \frac{A}{3\,z_1}\Big) + i\,\frac{\sqrt{3}}{2}\Big(z_1 + \frac{A}{3\,z_1}\Big), \\ y_3 &= \Big(-\frac{1}{2}\Big)\Big(z_1 - \frac{A}{3\,z_1}\Big) - i\,\frac{\sqrt{3}}{2}\Big(z_1 + \frac{A}{3\,z_1}\Big). \end{aligned}$$

Zauważmy, że $y_2 = \overline{y_3}$ i w przypadku gdy jedna z tych liczb jest rzeczywista to obie są równe. Pamiętamy (3.10):

$$\alpha_1 \cdot \alpha_2 = -\frac{A^3}{27},$$

oraz

$$z_1 + \frac{A}{3\,z_1} = 0 \Leftrightarrow z_1 = -\frac{A}{3\,z_1} \Leftrightarrow z_1^3 = -\frac{A^3}{27\,z_1^3} \Leftrightarrow \alpha_1\alpha_1 = -\frac{A^3}{27} = \alpha_1\alpha_2.$$

Jeżeli $\alpha_1 \neq 0$ to ostatnia równość jest równoważna $\alpha_1 = \alpha_2$. Pokazaliśmy więc, że jeżeli $\alpha_1 \neq 0$ to $z_1 + \frac{A}{3\,z_1} = 0$ jest równoważne $\alpha_1 = \alpha_2$, czyli przypadkowi (b). Zauważmy, że ta równoważność zachodzi również jeżeli $\alpha_1 = 0$. Ten ostatni warunek jest bowiem równoważny $z_1 = 0$ i $A = 0$. Pokazaliśmy więc, że w przypadku (a) mamy dokładnie 1 pierwiastek rzeczywisty

i dwa zespolone sprzężone, a w przypadku (b) mamy wszystkie pierwiastki rzeczywiste, w tym jeden przynajmniej podwójny.

Rozważmy teraz ostatni przypadek (c), to znaczy α_1 i α_2 zespolone sprzężone. Równanie (3.10) przybiera postać

$$|\alpha_1|^2 = -\frac{A^3}{27} \;\Rightarrow\; |z_i| = \sqrt{\frac{-A}{3}},\ i = 1, 2, 3,\ (A < 0).$$

Mamy więc

$$z_1 = \sqrt{\frac{-A}{3}}\, e^{i\,\varphi}, \quad z_2 = \sqrt{\frac{-A}{3}}\, e^{i\,(\varphi + 2\pi/3)}, \quad z_3 = \sqrt{\frac{-A}{3}}\, e^{i\,(\varphi - 2\pi/3)}$$

dla pewnego $\varphi \in (0, 2\pi),\ \varphi \neq \pi$ gdyż $z_i \notin \mathbf{R}$. Zauważmy, że wtedy

$$-\frac{A}{3\,z_1} = \sqrt{\frac{-A}{3}}\, e^{-i\,\varphi} = \overline{z_1},$$

i podobnie

$$-\frac{A}{3\,z_2} = \overline{z_2}, \qquad -\frac{A}{3\,z_3} = \overline{z_3}.$$

W takim razie wszystkie liczby y_i, a więc także pierwiastki x_i są rzeczywiste:

$$\begin{aligned} y_1 &= 2\Re(z_1) = \sqrt{\frac{-A}{3}}\, \cos(\varphi), \\ y_2 &= 2\Re(z_2) = \sqrt{\frac{-A}{3}}\, \cos(\varphi + 2\pi/3), \\ y_3 &= 2\Re(z_3) = \sqrt{\frac{-A}{3}}\, \cos(\varphi - 2\pi/3). \end{aligned}$$

Podsumujmy te obserwacje:

Wniosek 3.18. *Załóżmy, że równanie* (3.5) *ma współczynniki rzeczywiste. Pierwiastki dane przez Wniosek 3.17 mają następujące własności:*

(a) jeżeli rezolwenta (3.9) *ma dwa różne pierwiastki rzeczywiste to równanie* (3.5) *ma jeden rzeczywisty pierwiastek i dwa zespolone sprzężone,*

(b) jeżeli rezolwenta ma jeden podwójny rzeczywisty pierwiastek, to równanie (3.5) *ma tylko rzeczywiste pierwiastki, w tym jeden wielokrotny,*

(c) jeżeli rezolwenta ma dwa zespolone pierwiastki, to (3.5) *ma* 3 *różne rzeczywiste pierwiastki.* □