Wykłady z Algebry

Jarosław Grytczuk

1. Liczby całkowite

Liczby $0, \pm 1, \pm 2, \pm 3, ...$ nazywamy *liczbami całkowitymi*, a zbiór wszystkich takich liczb oznaczamy przez $\mathbb{Z}$. Zbiór liczb całkowitych dodatnich $1, 2, 3, ...$, zwanych również *liczbami naturalnymi*, oznaczamy przez $\mathbb{N}$. Dziedzina zajmująca się badaniem własności liczb całkowitych to *Teoria Liczb*—najstarsza, obok *Geometrii*, dyscyplina matematyczna. O dziwo, wiele najtrudniejszych, dotąd nierozwiązanych problemów matematycznych pochodzi właśnie z Teorii Liczb. W tym rozdziale przypomnimy i pogłębimy szereg zagadnień dotyczących liczb całkowitych, a także przedstawimy kilka najważniejszych problemów, wokół których koncentruje się aktualny nurt badań.

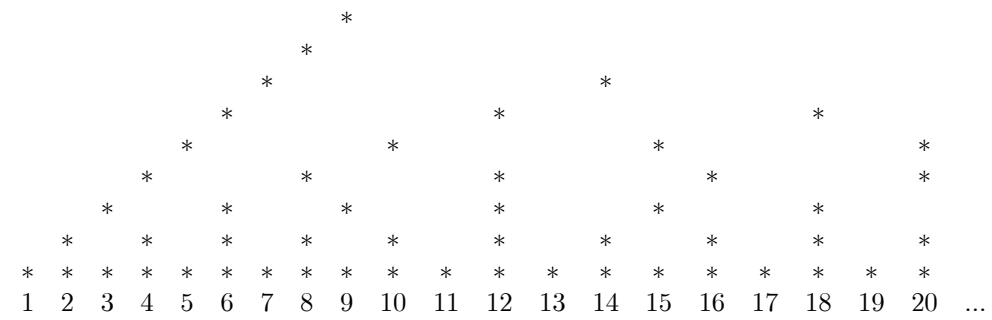
1.1. Algorytm Euklidesa. Tak się wybornie składa, że możemy rozpocząć od przedstawienia pierwszego w historii matematyki algorytmu—*Algorytmu Euklidesa*, służącego znajdowaniu *największego wspólnego dzielnika* dwóch liczb naturalnych. Najpierw przypomnimy niezbędne pojęcia.

Definicja 1. *Niech d i n będą liczbami naturalnymi. Mówimy, że d* ***dzieli*** *n jeśli istnieje taka liczba naturalna k, że $n = dk$. Liczbę d nazywamy wówczas* ***dzielnikiem*** *liczby n.*

Na przykład, 6 dzieli 18 ponieważ $18 = 6 \cdot 3$. Natomiast 6 nie dzieli 20 ponieważ równanie $20 = 6k$ nie ma rozwiązań w liczbach naturalnych k. Fakt podzielności liczby n przez d zapisujemy jako $d \mid n$.

Każda liczba naturalna n ma skończoną liczbę różnych dzielników. Oznaczamy ją przez $\tau(n)$. Na przykład, $\tau(20) = 6$ ponieważ 20 ma sześć różnych dzielników: 1, 2, 4, 5, 10, 20. Liczbę dzielników danej liczby n możemy odczytać z następującego

Diagramu Leibniza:



Liczba gwiazdek widniejących nad n to właśnie liczba jej dzielników $\tau(n)$.

TWIERDZENIE 1. *(O dzieleniu z resztą) Dla dowolnych liczb całkowitych n i d, przy czym $d > 0$, istnieje dokładnie jedna para liczb całkowitych q i r taka, że*

$$n = dq + r, \ \ 0 \leq r < d.$$

PROOF. Przyjmując $q = \left\lfloor \frac{a}{d} \right\rfloor$ i $r = a - d \left\lfloor \frac{a}{d} \right\rfloor$ dostajemy parę spełniającą tezę twierdzenia. Ponadto, warunki twierdzenia określają tę parę jednoznacznie. W istocie, przypuśćmy, że mamy również $a = dq' + r'$ i $0 \leq r' < d$. Wówczas mielibyśmy

$$d(q - q') = r' - r,$$

a to jest możliwe tylko wtedy, gdy $q - q' = 0$. ∎

Liczbę q z powyższego twierdzenia nazywamy *ilorazem*, a r—*resztą* z dzielenia n przez d.

PRZYKŁAD 1. *Jeśli $n = 25$ i $d = 7$, to $q = 3$ i $r = 4$ ponieważ*

$$25 = 7 \cdot 3 + 4, \ 0 \leq 4 < 7.$$

Jeśli $n = -25$ i $d = 7$, to $q = -4$ i $r = 3$, ponieważ

$$-25 = 7 \cdot (-4) + 3, \ 0 \leq 3 < 7.$$

DEFINICJA 2. ***Największym wspólnym dzielnikiem*** *liczb naturalnych m i n nazywamy największą liczbę naturalną dzielącą jednocześnie m i n. Oznaczamy ją przez (m, n).*

Na przykład, $(2002, 770) = 154$ ponieważ 154 dzieli zarówno liczbę 2002 jak i 770 i jest największą liczbą naturalną o tej własności.

Opiszemy teraz zasadę działania *Algorytmu Euklidesa*, pozwalającego dla zadanych liczb naturalnych m i n znaleźć ich największy wspólny dzielnik (m, n). Przypuśćmy, że $m \geq n$. W pierwszym kroku wykonujemy dzielenie m przez n i otrzymujemy, zgodnie z twierdzeniem o dzieleniu z resztą, iloraz q_1 i resztę r_1:

$$m = q_1 n + r_1, 0 \leq r_1 < n.$$

Jeżeli $r_1 \neq 0$ to możemy wykonać drugie dzielenie—n przez r_1, które daje drugi iloraz q_2 i drugą resztę r_2:

$$n = q_2 r_1 + r_2, 0 \leq r_2 < r_1.$$

Jeżeli ponownie $r_2 \neq 0$ to dzielimy znowu r_1 przez r_2 i dostajemy iloraz q_3 i resztę r_3 spełniające warunki

$$r_1 = r_2 q_3 + r_3, 0 \leq r_3 < r_2.$$

I tak dalej:

$$\begin{aligned} r_2 &= r_3 q_4 + r_4, 0 \leq r_4 < r_3, \\ r_3 &= r_4 q_5 + r_5, 0 \leq r_5 < r_4, \\ &\ldots\ldots\ldots\ldots \end{aligned}$$

Jest jasne, że w końcu otrzymamy $r_k = 0$ dla pewnego k naturalnego, ponieważ ciąg liczb całkowitych $r_1 > r_2 > r_3 > ...$ jest z malejący i ograniczony z dołu przez 0. Twierdzimy teraz, że jeżeli $r_k = 0$, to $(m, n) = r_{k-1}$. W istocie, wystarczy zauważyć, że równość

$$m = nq + r$$

pociąga za sobą równość $(m, n) = (q, r)$. Stosując to spostrzeżenie do kolejnych równości otrzymamy $(m, n) = (r_{k-2}, r_{k-1}) = r_{k-1}$.

PRZYKŁAD 2. *Niech $m = 2002$ a $n = 770$. Powtarzając dzielenie z resztą na kolejnych parach dostajemy ciąg równości:*

$$\begin{aligned} 2002 &= 770 \cdot 2 + 462, \\ 770 &= 462 \cdot 1 + 308, \\ 462 &= 308 \cdot 1 + 154, \\ 308 &= 154 \cdot 2. \end{aligned}$$

Zatem, $(2002, 770) = 154$.

Algorytm Euklidesa pozostaje wciąż jedną z najbardziej efektywnych metod wyznaczania największego wspólnego dzielnika. Znajduje on zstosowanie w bujnie rozwijającej się ostatnio *Kryptografii*—dziedzinie zajmującej się szyfrowaniem informacji. O zastosowaniach Teorii Liczb w Kryptografii będzie jeszcze mowa.

1.2. Liczby pierwsze. Każda liczba naturalna $n > 1$ posiada co najmniej dwa różne dzielniki, 1 i n.

DEFINICJA 3. *Liczbę $p > 1$ nazywamy liczbą **pierwszą** jeśli 1 i p są jedynymi jej dzielnikami. Liczbę naturalną $n > 1$, która nie jest pierwszą nazywamy liczbą **złożoną**.*

Liczby pierwsze możemy rozpoznać w Diagramie Leibniza jako te, nad którymi "świecą" dokładnie dwie gwiazdki.

TWIERDZENIE 2. *(Euklides) Liczb pierwszych jest nieskończenie wiele.*

PROOF. Przypuśćmy, że $p_1 = 2 < p_2 = 3 < ... < p_r$ są wszystkimi liczbami pierwszymi. Przyjmijmy $P = p_1 p_2 ... p_r + 1$ i niech p będzie dzielnikiem pierwszym liczby P. Wtedy liczba p nie może być żadną z liczb p_i, gdyż w przeciwnym razie, dzieliłaby różnicę $P - p_1 p_2 ... p_r = 1$, co jest niemożliwe. Zatem $p_1, p_2, ..., p_r$ nie są wszystkimi liczbami pierwszymi. ∎

TWIERDZENIE 3. *Odstępy pomiędzy kolejnymi liczbami pierwszymi mogą być dowolnie duże.*

PROOF. W istocie, niech $n \geq 2$ będzie liczbą naturalną. Rozważmy ciąg $n-1$ kolejnych liczb naturalnych

$$n!+2, n!+3, ..., n!+n.$$

Ponieważ żadna z nich nie może być liczbą pierwszą, twierdzenie jest udowodnione. ∎

Znacznie trudniej udowodnić prawdziwość następującego twierdzenia, znanego jako *Postulat Bertranda*.

TWIERDZENIE 4. *(Postulat Bertranda) W każdym przedziale* $[n, 2n]$, $n = 1, 2, ...$ *znajduje się liczba pierwsza.*

A jeszcze trudniejsze są dowody słynnego Twierdzenia Dirichleta czy Twierdzenia o Liczbach Pierwszych.

TWIERDZENIE 5. *(Twierdzenie Dirichleta) Jeżeli* $(a, b) = 1$, *to ciąg arytmetyczny* $an + b$, $n = 0, 1, 2, ...$ *zawiera nieskończenie wiele liczb pierwszych.*

TWIERDZENIE 6. *(Twierdzenie o Liczbach Pierwszych) Niech* $\pi(N)$ *oznacza liczbę liczb pierwszych w przedziale* $[1, N]$. *Wówczas*

$$\lim_{N\to\infty} \frac{\pi(N)}{\frac{N}{\ln N}} = 1.$$

Mamy wreszcie całą plejadę nierozwiązanych dotąd problemów o liczbach pierwszych. Na przykład wciąż nie wiadomo czy istnieje nieskończenie wiele par *bliźniaków*, czli par liczb pierwszych różniących się o 2.

1.3. Podstawowe Twierdzenie Arytmetyki.

TWIERDZENIE 7. *Każda liczba całkowita* $n > 1$ *rozkłada się na iloczyn liczb pierwszych.*

PROOF. Liczba n albo jest pierwsza albo jest złożona. W pierwszym przypadku teza twierdzenia jest oczywista. Jeśli n jest złożona, to z definicji istnieje liczba d, taka, że $1 < d < n$ i d dzieli n. Niech m oznacza najmniejszy z takich dzielników. Pokażemy, że m musi być liczbą pierwszą. Gdyby m nie było pierwsze, to istniałoby takie naturalne k, że $1 < k < m$ i k dzieliłoby m. Stąd mielibyśmy, że $1 < k < m$ i k dzieli n, a to przeczy wyborowi m. Otrzymana sprzeczność pokazuje, że rzeczywiście m jest liczbą pierwszą. Oznaczając ją przez p_1 możemy więc napisać $n = p_1 r$, gdzie $1 < r < n$. Powtarzając to samo rozumowanie do liczby r otrzymamy $n = p_1 p_2 s$, gdzie $p_1 \leq p_2$ i $1 \leq s < r < n$. Ten proces zakończy się po skończonej liczbie kroków, ponieważ między 1 i n znajduje się tylko skończona liczba liczb naturalnych. W rezultacie otrzymamy rozkład

$$n = p_1 p_2 ... p_t \tag{1.1}$$

gdzie $p_1 \leq p_2 \leq ... \leq p_t$ są liczbami pierwszymi, co kończy dowód twierdzenia. ∎

Zauważmy, że jeżeli $n = ab$, to liczby a i b nie mogą być jednocześnie większe od $\sqrt{n}$. Stąd wynika, że dowolna liczba złożona n posiada dzielnik pierwszy nie przewyższający $\sqrt{n}$.

Oczywiście w rozkładzie (1.1) te same czynniki mogą się powtarzać i możemy je wówczas zapisać jako potęgi. W ten sposób otzrymamy rozkład liczby n na iloczyn potęg różnych liczb pierwszych:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}, \tag{1.2}$$

gdzie $p_1 < p_2 < ... < p_k$ i $\alpha_i > 0$ dla $i = 1, 2, ..., k$. Przedstawienie liczby n w postaci (1.2) nazywamy jej *rozkładem kanonicznym.*

Udowodnimy teraz fundamentalne twierdzenie o jednoznaczności rozkładu na czynniki pierwsze znane jako Podstawowe Twierdzenie Arytmetyki.

TWIERDZENIE 8. *(Podstawowe Twierdzenie Arytmetyki) Rozkład kanoniczny liczby całkowitej $n > 1$ jest jednoznaczny.*

PROOF. Rozkład kanoniczny liczby pierwszej jest oczywiście jednoznaczny. Załóżmy, że pewne liczby całkowite dodatnie, większe od jedynki, mają różne rozkłady kanoniczne i niech N będzie najmniejszą z takich liczb. Mamy więc

$$N = p_1 p_2 ... p_k = q_1 q_2 ... q_m,$$

przy czym każda z liczb p jest różna od każdej z liczb q. W istocie, w przeciwnym razie dzieląc N przez p, otrzymalibyśmy liczbę całkowitą $N' < N$ posiadającą tę samą co i N własność, a to jest niemożliwe wobec wyboru N. Możemy także założyć, że

$$p_1 \leq p_2 \leq ... \leq p_k \text{ i } q_1 \leq q_2 \leq ... \leq q_m$$

i $p_1 < q_1$. Zdefiniujmy teraz liczbę

$$P = p_1 q_2 ... q_m.$$

Z tego, że $p_1 \mid P$ i $p_1 \mid N$ wynika, że $p_1 \mid (N - P)$, gdzie $N - P = (q_1 - p_1) q_2 ... q_m > 1$. Dlatego możemy napisać

$$N - P = p_1 t_1 ... t_h, \tag{1.3}$$

gdzie t_i są liczbami pierwszymi. Jeśli $q_1 - p_1 > 1$, to możemy także zapisać $q_1 - p_1$ w postaci iloczynu liczb pierwszych:

$$q_1 - p_1 = r_1 r_2 ... r_s.$$

Otrzymaliśmy w ten sposób drugi rozkład liczby $N - P$ na czynniki pierwsze, a mianowicie

$$N - P = r_1 r_2 ... r_s q_2 ... q_m. \tag{1.4}$$

Widzieliśmy wcześniej, że żadne p nie jest równe żadnemu q. W szczególności, p_1 nie jest równe żadnemu z q. Dalej jest jasne, że $p_1 \nmid (q_1 - p_1)$ i dlatego p_1 nie jest równe żadnemu z r, tak więc $q_1 - p_1$ nie może zawierać w rozkładzie na czynniki pierwsze p_1. Zatem liczba $N - P$ posiada dwa różne rozkłady (1.3) i (1.4) na czynniki pierwsze. To samo jest słuszne w przypadku, gdy $q_1 - p_1 = 1$. No ale $1 < N - P < N$, a to przeczy minimalności N. Zatem, nie istnieją liczby całkowite $n > 1$ posiadające więcej niż jeden rozkład kanoniczny. ∎

Na przykład, $2002 = 2 \times 7 \times 11 \times 13$ jest jedynym możliwym rozkładem kanonicznym liczby 2002. Podobnie, $52! = 80\,658\,175\,170\,943\,878\,571\,660\,636\,856\,403\,766\,975\,289\,505\,440\,883\,277\,824\,000\,000\,000\,000 = 2^{49} 3^{23} 5^{12} 7^8 11^4 13^4 17^3 19^2 23^2 29 \times 31 \times 37 \times 41 \times 43 \times 47$.

1.4. Funkcja Eulera. Niech N będzie liczbą naturalną. Symbolem $\varphi(N)$ oznaczamy liczbę nieskracalnych ułamków właściwych o mianowniku N. Na przykład, $\varphi(18) = 6$, bo istnieje dokładnie 6 takich ułamków o mianowniku 18:

$$\frac{1}{18}, \frac{5}{18}, \frac{7}{18}, \frac{11}{18}, \frac{13}{18}, \frac{17}{18}.$$

Funkcja $N \mapsto \varphi(N)$ nosi nazwę *Funkcji Eulera*. A oto tabela początkowych wartości funkcji Eulera:

N:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\varphi(N)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6

.

Jest intuicyjnie oczywiste, że wartość $\varphi(N)$ musi zależeć od rozkładu liczby N na czynniki pierwsze. Na przykład, jeżeli $N = p$ jest liczbą pierwszą, to oczywiście $\varphi(p) = p - 1$. Ogólnie, jeśli liczba pierwsza p dzieli N, to należy pominąć wszystkie ułamki, których licznik dzieli się przez p. Ta obserwacja pozwala na znalezienie wzoru na funkcję $\varphi(N)$.

TWIERDZENIE 9. *Niech $N = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$, będzie kanonicznym rozkładem liczby N na czynniki pierwsze. Wówczas*

$$\varphi(N) = N(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_r}) \tag{1.5}$$

PROOF. Rozważmy zbiór U_N wszystkich ułamków właściwych o mianowniku N. Jest ich oczywiście N. Spośród nich dokładnie $\frac{N}{p_1}$ ułamków skraca się przez p_1. Odrzucając każdy taki ułamek pozostanie $N - \frac{N}{p_1} = N(1 - \frac{1}{p_1})$ ułamków. Podobnie, wśród $N(1 - \frac{1}{p_1})$ pozostałych ułamków znajduje się dokładnie $\frac{1}{p_2} N(1 - \frac{1}{p_1})$ takich, których licznik dzieli się przez p_2. Zatem, po ich odrzuceniu pozostanie

$$N(1 - \frac{1}{p_1}) - \frac{1}{p_2} N(1 - \frac{1}{p_1}) = N(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})$$

ułamków. Postępując dalej w ten sam sposób aż do ostatniego czynnika p_r, usuniemy ze zbioru U_N wszystkie ułamki skracalne, a liczba tych, które pozostaną wyniesie dokładnie

$$N(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_r}),$$

co kończy dowód wzoru (1.5). ∎

Wzór (1.5) można podać w nieco innej równoważnej postaci:

$$\varphi(N) = (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1})...(p_r^{k_r} - p_r^{k_r - 1}). \tag{1.6}$$

PRZYKŁAD 3. *Obliczymy wartość funkcji Eulera dla $N = 2002$. Ponieważ*

$$2002 = 2 \times 7 \times 11 \times 13,$$

więc, na mocy wzoru (1.6),

$$\varphi(2002) = 1 \cdot 6 \cdot 10 \cdot 12 = 720.$$

Z Twierdzenia 9 wynika natychmiast, że funkcja Eulera jest *multyplikatywna*.

WNIOSEK 1. *Dla dowonych liczb całkowitych dodatnich M, N takich, że $(M, N) = 1$ zachodzi wzór*

$$\varphi(MN) = \varphi(M)\varphi(N).$$

Funkcja Eulera posiada jeszcze wiele innych ciekawych własności, które poznamy w dalszym ciągu. Zakończymy ten paragraf jedną z nich.

TWIERDZENIE 10. *Dla dowolnej liczby całkowitej $N > 0$*

$$\sum_{d|N} \varphi(d) = N.$$

PROOF. Niech $N = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ będzie rozkładem kanonicznym liczby N. Rozważmy iloczyn

$$P = \prod_{i=1}^{r} (1 + \varphi(p_i) + \varphi(p_i^2) + ... + \varphi(p_i^{k_i})).$$

Korzystając ze wzoru (1.6) otrzymujemy

$$\begin{aligned} P &= \prod_{i=1}^{r} (1 + (p_i - 1) + (p_i^2 - p_i) + ... + (p_i^{k_i} - p_i^{k_i - 1}) \\ &= \prod_{i=1}^{r} p_i^{k_i} = N. \end{aligned}$$

Z drugiej strony, otwierając nawiasy i wykorzystując multyplikatywność funkcji φ otrzymamy

$$\begin{aligned} P &= \sum_{(l_1, l_2, ..., l_r)} \varphi(p_1^{l_1}) \varphi(p_2^{l_2}) ... \varphi(p_r^{l_r}) \\ &= \sum_{(l_1, l_2, ..., l_r)} \varphi(p_1^{l_1} p_2^{l_2} ... p_r^{l_r}), \end{aligned}$$

gdzie sumowanie przebiega po wszystkich układach liczb $(l_1, l_2, ..., l_r)$ takich, że $0 \leq l_i \leq k_i$, $i = 1, 2, ..., r$, przy czym każdy układ występuje w tej sumie dokładnie raz. Wówczas iloczyny postaci $p_1^{l_1} p_2^{l_2} ... p_r^{l_r}$ odpowiadają dzielnikom liczby N, a więc

$$\begin{aligned} P &= \sum_{(l_1, l_2, ..., l_r)} \varphi(p_1^{l_1} p_2^{l_2} ... p_r^{l_r}) \\ &= \sum_{d|N} \varphi(d), \end{aligned}$$

co kończy dowód. ∎

PRZYKŁAD 4. *Obliczmy sumę funkcji Eulera rozciągniętą po wszystkich dzielnikach liczby $N = 18$. Mamy*

$$\begin{aligned} \sum_{d|18} \varphi(d) &= \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(9) + \varphi(18) \\ &= 1 + 1 + 2 + 2 + 6 + 6 = 18. \end{aligned}$$

1.5. Funkcja Möbiusa i Hipoteza Riemanna. Na zakończenie przedstawimy pewną szczególną wersję jednego z najsławniejszych matematycznych problemów wszechczasów, ukazującą jego związek z fenomenem jednoznacznego rozkładu. W tym celu zdefiniujemy jedną z ważniejszych funkcji arytmetycznych, mianowicie funkcję Möbiusa.

DEFINICJA 4. *(Funkcja Möbiusa) Niech* $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ *będzie kanonicznym rozkładem liczby naturalnej* n *na czynniki pierwsze. Wówczas symbol* $\mu(n)$ *oznacza liczbę określoną wzorem*

$$\mu(n) = \begin{cases} 0, & gdy\ \alpha_i > 1\ dla\ pewnego\ 1 \leq i \leq r \\ (-1)^r, & gdy\ \alpha_i = 1\ dla\ wszystkich\ i = 1, ..., r. \end{cases}$$

Ponadto przyjmujemy $\mu(1) = 1$.

Jeśli więc liczba n dzieli się przez jakiś kwadrat większy od 1, to $\mu(n) = 0$, na przykład $\mu(12) = 0$. Natomiast, w przypadku liczb *bezkwadratowych* $\mu(n) = \pm 1$ w zależności od parzystości liczby czynników pierwszych w rozkładzie kanonicznym liczby n. Na przykład, $\mu(15) = 1$, ale $\mu(30) = -1$.

Sama funkcja $\mu(n)$ jest tak samo nieregularna jak nieregularnie rozmieszczone są liczby pierwsze w ciągu liczb naturalnych. Jest więc naturalnym badanie funkcji sumacyjnej określonej wzorem

$$M(n) = \sum_{k=1}^{n} \mu(k).$$

Przez pewien czas sądzono, że jest możliwe aby $|M(n)| \leq \sqrt{n}$, dla wszystkich $n \geq 1$, ale to przypuszczenie zostało w końcu obalone. Pozostała natomiast do rozstrzygnięcia następująca kwestia, która, jak można udowodnić, jest równoważna słynnej *Hipotezie Riemanna*:

dla każdego $\varepsilon > 0$ *istnieje stała* c_ε *taka, że*

$$|M(n)| \leq c_\varepsilon n^{\frac{1}{2}+\varepsilon}.$$

Warto dodać, że za rozwiązanie Hipotezy Riemanna wyznaczono w roku 2000 nagrodę wysokości 1.000.000$.

2. Arytmetyka modulo m

DEFINICJA 5. *Niech* $m > 0$ *będzie ustaloną liczbą całkowitą. Mówimy, że liczby całkowite* a *i* b ***przystają modulo*** m*, co zapisujemy jako*

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

jeżeli reszty z dzielenia a *i* b *przez* m *są takie same.*

Z powyższej definicji wynikają (prawie) natychmiast następujące własności relacji przystawania.

1. $a \equiv b (\mathrm{mod}\, m)$ wtedy i tylko wtedy gdy $m \mid a - b$.
2. Jeżeli $a \equiv b (\mathrm{mod}\, m)$ i $c \equiv d (\mathrm{mod}\, m)$, to
$$\begin{aligned} a + c &\equiv b + d (\mathrm{mod}\, m), \\ ac &\equiv bd (\mathrm{mod}\, m), \\ a^k &\equiv b^k (\mathrm{mod}\, m), \end{aligned}$$
dla dowolnego $k \geq 0$.
3. Relacja przystawania modulo m jest *relacją równoważności*, tzn., dla dowolych liczb całkowitych a, b, c zachodzą własności:
   (1) $a \equiv a (\mathrm{mod}\, m)$
   (2) Jeżeli $a \equiv b (\mathrm{mod}\, m)$, to $b \equiv a (\mathrm{mod}\, m)$.
   (3) Jeżeli $a \equiv b (\mathrm{mod}\, m)$ i $b \equiv c (\mathrm{mod}\, m)$, to $a \equiv c (\mathrm{mod}\, m)$.

Dla liczby $a \in \mathbb{Z}$ oznaczamy przez $[a]_m$ zbiór wszystkich liczb całkowitych przystających do a modulo m:

$$[a]_m = \{x \in \mathbb{Z} : x \equiv a (\mathrm{mod}\, m)\}.$$

Zbiór $[a]_m$ nazywamy *klasą abstrakcji* (lub *klasą równoważności*) elementu a. Innymi słowy, jeżeli r jest resztą z dzielenia a przez m, to $[a]_m$ składa sie z wszystkich liczb dających resztę r przy dzieleniu przez m. Łatwo zobaczyć, że takie klasy mają postać obustronnie nieskończonych ciągów arytmetycznych o różnicy m. Na przykład, dla $m = 3$ mamy trzy klasy:

$$\begin{aligned} [0]_3 &= \{...-6,-3,0,3,6,9,...\} \\ [1]_3 &= \{...-5,-2,1,4,7,10,...\} \\ [2]_3 &= \{...-4,-1,2,5,8,11,...\}, \end{aligned}$$

które można zobrazować jak następuje:

liczba:	...	−8	−7	−6	−5	−4	−3	−2	−1	0	1	2	3	4	5	6	...
reszta 0:	...			0			0			0			0			0	...
reszta 1:	...	1			1			1			1			1			...
reszta 2:	...		2			2			2			2			2		...

Należy podkreślić, że klasy reszt tworzą podział zbioru $\mathbb{Z}$ na rozłączne *warstwy*, z których każda może być reprezentowana przez dowolny ze swoich elementów. Na przykład,

$$[1]_3 = [7]_3 = [-98]_3.$$

Definicja 6. *Zbiór wszystkich klas reszt modulo m oznaczamy symbolem $\mathbb{Z}_m$, a jego elementy nazywamy* ***liczbami całkowitymi modulo*** *m:*

$$\mathbb{Z}_m = \{[0]_m, [1]_m, ..., [m-1]_m\}.$$

Liczby całkowite modulo m, podobnie jak zwykłe liczby całkowite, możemy dodawać i mnożyć.

Definicja 7. *W zbiorze $\mathbb{Z}_m$ określamy działania dodawania i mnożenia modulo m jak następuje:*

$$[a]_m \oplus [b]_m = [a+b]_m, \;\; [a]_m \odot [b]_m = [ab]_m.$$

Zauważmy, że tak określone działania nie zależą od wyboru reprezentantów klas. W istocie, jeżeli $[a]_m = [a']_m$ i $[b]_m = [b']_m$, to wobec własności 2 relacji przystawania modulo m mamy

$$\begin{aligned} [a]_m \oplus [b]_m &= [a+b]_m = [a'+b']_m = [a']_m \oplus [b']_m, \\ [a]_m \odot [b]_m &= [ab]_m = [a'b']_m = [a']_m \odot [b']_m. \end{aligned}$$

Twierdzenie 11. *Niech a, b, c będą dowolnymi elementami zbioru $\mathbb{Z}_m$ i oznaczmy $0 = [0]_m$ i $1 = [1]_m$. Wówczas operacje $\oplus$ i $\odot$ spełniają następujące własności.*

1. $a \oplus b$, $a \odot b \in \mathbb{Z}_m$.
2. $a \oplus b = b \oplus a$, $a \odot b = b \odot a$.
3. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$, $(a \odot b) \odot c = a \odot (b \odot c)$.
4. $a \oplus 0 = a$, $a \odot 1 = a$.
5. $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

6. *Dla każdego $a \in \mathbb{Z}_m$ istnieje element $-a \in \mathbb{Z}_m$ taki, że $a \oplus (-a) = 0$.*

PROOF. Własność 1 jest bezpośrednią konsekwencją definicji działań modulo m. Dla dowodu pierwszej części własności 2 przypuśćmy, że $a = [x]_m$ i $b = [y]_m$. Wówczas

$$\begin{aligned} a \oplus b &= [x]_m \oplus [y]_m = [x+y]_m \\ &= [y+x]_m = [y]_m \oplus [x]_m \\ &= b + a. \end{aligned}$$

Podobne dowody można sporządzić dla drugiej części 2 i dla pozostałych własności 3,4,5. Dla 6 wystarczy przyjąć $-a = [-x]_m$. ∎

W praktyce upraszczamy niewygodną notację $[x]_m$ opuszczając znak $[\cdot]_m$ i używając zwykłych symboli $0, 1, 2, ..., m-1$ na oznaczenie klas

$$[0]_m, [1]_m, ..., [m-1]_m.$$

Podobnie, zamiast pisać $\oplus$ i $\odot$, działania na klasach oznaczamy zwykłymi symbolami dodawania i mnożenia $+$ i $\cdot$. Zazwyczaj jest jasne z kontekstu o jaki moduł m się rozchodzi. Na przykład, jeżeli wiadomo, że $m = 9$, to napiszemy po prostu $7 + 5 = 3$ zamiast $[7]_9 \oplus [5]_9 = [3]_9$.

Widzimy, że operacje dodawania i mnożenia liczb całkowitych modulo m mają podobne własności do zwykłych działań arytmetycznych w zbiorze liczb całkowitych. Istnieje jednak pewien aspekt, w którym występuje diametralna różnica. Otóż, równość $ab = ac$ w $\mathbb{Z}$ pociąga za sobą, przy założeniu $a \neq 0$, równość $b = c$. Tak jednak nie musi być w $\mathbb{Z}_m$. Na przykład w $\mathbb{Z}_6$

$$3 \cdot 1 = 3 \cdot 5$$

i, pomimo tego, że $3 \neq 0$, mamy $1 \neq 5$.

2.1. Elementy odwracalne w $\mathbb{Z}_m$.

DEFINICJA 8. *Element $r \in \mathbb{Z}_m$ nazywamy **odwracalnym** jeśli istnieje taki element $x \in \mathbb{Z}_m$, że $rx = 1$. W takim przypadku x nazywamy odwrotnością elementu r, co zapisujemy jako $x = r^{-1}$.*

Ponieważ $rx = xr$ w $\mathbb{Z}_m$, więc mamy również $xr = 1$ i $r = x^{-1}$.

TWIERDZENIE 12. *Element $r \in \mathbb{Z}_m$ jest odwracalny wtedy i tylko wtedy, gdy r i m są względnie pierwsze w $\mathbb{Z}$. W szczególności, jeśli p jest liczbą pierwszą, to każdy element $\mathbb{Z}_p$, oprócz 0, jest odwracalny.*

PROOF. Przypuśćmy, że r jest odwracalny, równanie $rx = 1$ posiada rozwiązanie w $\mathbb{Z}_m$. Stąd, dostajemy równość $rx - 1 = km$, spełnioną w zbiorze $\mathbb{Z}$, przy pewnym $k \in \mathbb{Z}$, albo inaczej

$$rx - km = 1.$$

Teraz widzimy, że każdy wspólny dzielnik liczb r i m musi także dzielić $rx - km$, co jest równe 1, a więc $(r, m) = 1$.

Na odwrót, przypuśćmy, że $(r, m) = 1$. Wtedy, na mocy Algorytmu Euklidesa, istnieją liczby całkowite x i y takie, że $rx + my = 1$. Stąd dostajemy $rx \equiv 1 (\mathrm{mod}\, m)$, co oznacza, że $rx = 1$ w $\mathbb{Z}_m$, co było wymagane. ∎

Zbiór wszystkich elementów odwracalnych w $\mathbb{Z}_m$ oznaczamy symbolem $\mathbb{Z}_m^*$. Z powyższego twierdzenia i z definicji funkcji Eulera $\varphi(n)$, wynika natychmiast następujący ważny wniosek.

WNIOSEK 2. *Liczba elementów zbioru $\mathbb{Z}_m^*$ wynosi $\varphi(m)$. W szczególności,*

$$\mathbb{Z}_p^* = \{1, 2, ..., p-1\}$$

jeśli p jest liczbą pierwszą.

Na zakończenie przytoczymy klasyczne twierdzenie Teorii Liczb, które ma ważne zastosowania w Kryptografii.

TWIERDZENIE 13. *(Euler) Jeżeli $(a, m) = 1$, to*

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

PROOF. Ponieważ relacja przystawania jest zachowana przy potęgowaniu, więc wystarczy rozważyć przypadek $1 \leq a \leq m$. Niech

$$\mathbb{Z}_m^* = \{r_1, r_2, ..., r_k\}$$

będzie zbiorem wszystkich elementów odwracalnych w $\mathbb{Z}_m$. Oczywiście mamy $k = \varphi(m)$. Rozważmy zbiór

$$a\mathbb{Z}_m^* = \{ar_1, ar_2, ..., ar_k\}.$$

Pokażemy, że $a\mathbb{Z}_m^* = \mathbb{Z}_m^*$. Przede wszystkim zauważmy, że wśród elementów ar_i nie ma dwóch takich samych. Rzeczywiście, gdyby $ar_i = ar_j$, to mielibyśmy $r_i = r_j$, a to ma miejsce tylko wtedy, gdy $i = j$. Ponadto, $ar_i \in \mathbb{Z}_m^*$ dla każdego $i = 1, 2, ..., k$. W istocie, $(ar_i)^{-1} = a^{-1}r_i^{-1}$ jest elementem odwrotnym do ar_i ponieważ

$$(ar_i)(a^{-1}r_i^{-1}) = (aa^{-1})(r_i r_i^{-1}) = 1.$$

Zatem zbiór $a\mathbb{Z}_m^*$ zawiera się w $\mathbb{Z}_m^*$ i ma tyle samo elementów co $\mathbb{Z}_m^*$, co oznacza, że $a\mathbb{Z}_m^* = \mathbb{Z}_m^*$. Stąd otrzymujemy

$$\begin{aligned} (ar_1)(ar_2)...(ar_k) &= r_1 r_2 ... r_k \\ a^k r_1 r_2 ... r_k &= r_1 r_2 ... r_k \\ a^k &= 1, \end{aligned}$$

co kończy dowód. ∎

PRZYKŁAD 5. *Niech $a = 3$ i $m = 2002$. Wówczas $\varphi(2002) = 720$ i $a^{\varphi(m)} = 3^{720} =$* 33 674 673 851 759 750 856 331 497 445 230 897 149 265 186 906 248 357 438 540 530 783 948 648 484 137 983 443 787 634 713 970 636 211 751 301 005 489 461 020 887 861 597 290 789 116 538 204 801 574 376 217 692 873 888 831 937 443 606 603 951 434 000 477 164 925 923 413 761 326 458 870 848 579 927 470 308 375 706 978 838 323 310 798 626 387 523 347 898 424 565 433 142 447 829 264 408 202 854 501 997 556 294 840 092 580 924 401 270 407 824 655 801 038 401*. Pomimo sporego rozmiaru tej liczby możemy być pewni (dzięki Twierdzeniu Eulera), że przy dzieleniu przez* 2002 *zostawi ona resztę* 1.

W przypadku gdy $m = p$ jest liczbą pierwszą dostajemy natychmist następujący wniosek.

WNIOSEK 3. *(Fermat) Jeżeli liczba pierwsza p nie dzieli a, to*

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

2.2. Systemy numeracji o podstawie 10 i 2. Podstawą *dziesiętnego* systemu numeracji jest liczba 10. Oznacza to, że ciąg cyfr

$$c_{n-1}...c_1c_0,$$

gdzie cyfry $c_i \in \{0, 1, ..., 9\}$, jest "kodem" liczby naturalnej

$$N = c_{n-1} \cdot 10^{n-1} + ... + c_1 \cdot 10 + c_0.$$

Analogicznie możemy zapisywać liczby naturalne stosując inne niż 10 podstawy. Na przykład, w systemie dwójkowym podstawą jest 2, a więc zapisanie liczby N w tym systemie polega na rozłożeniu N na sumę potęg dwójki. Na przykład,

$$\begin{aligned} 2002 &= 1024 + 512 + 256 + 128 + 64 + 16 + 2 \\ &= 1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^7 + 1 \cdot 2^6 + \\ &\quad 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 1, \end{aligned}$$

a więc 2002 w zapisie dwójkowym ma postać 11111010010.

Niech $N = c_{n-1}...c_1c_0$ będzie zapisem dziesiętnym liczby N i rozważmy sumę cyfr $S = \sum_{i=0}^{n-1} c_i$ liczby N.

TWIERDZENIE 14. *Niech N będzie dowolną liczbą naturalną i niech S oznacza sumę cyfr (dziesiętnych) liczby N. Wówczas*

$$N \equiv S (\mathrm{mod}\, 9).$$

W szczególności, liczba N jest podzielna przez 9 wtedy i tylko wtedy, gdy S jest podzielna przez 9.

PROOF. Jest jasne, że $10^i \equiv 1 (\mathrm{mod}\, 9)$ dla każdego $i = 1, 2, ...$ Stąd

$$c_i \cdot 10^i \equiv c_i (\mathrm{mod}\, 9).$$

Dodając te relacje stronami dostajemy tezę. ∎

Na przykład, liczba 2002 musi dawać resztę 4 z dzielenia przez 9, ponieważ suma jej cyfr jest równa 4. Podobnie można udowodnić mniej znaną cechę podzielności przez 11.

TWIERDZENIE 15. *Niech $T = \sum_{i=0}^{n-1} (-1)^i c_i$ oznacza naprzemienną sumę cyfr (dziesiętnych) liczby naturalnej N. Wówczas*

$$N \equiv T (\mathrm{mod}\, 11).$$

PROOF. Wystarczy zauważyć, że $10^i \equiv (-1)^i (\mathrm{mod}\, 11)$. ∎

Na przykład, liczba 2002 musi dzielić się przez 11 ponieważ $T = 2-0+0-2 = 0$.

2.3. Kryptosystem RSA. Opiszemy teraz w zarysie zasadę działania najbardziej rozpowszechninego obecnie sposobu szyfrowania informacji, opartego na Twierdzeniu Eulera. Wynaleźli go w 1978 roku Rivest, Shamir i Adleman.

Alicja chce aby listy adresowane do niej były zaszyfrowane tak, aby żaden ewentualny *Intruz* nie mógł ich łatwo odczytać. W tym celu wybiera dwie raczej duże liczby pierwsze p i q (po około 100 cyfr każda) i oblicza ich iloczyn $N = pq$. Następnie znajduje wartość funkcji Eulera $\varphi(N) = (p-1)(q-1)$ i wybiera dwie liczby e i d tak, aby $(e, \varphi(N)) = (d, \varphi(N)) = 1$, oraz $ed \equiv 1 (\mathrm{mod}\, \varphi(N))$. Teraz podaje do publicznej wiadomości swój klucz szyfrujący: parę liczb (N, e). Liczby $\varphi(N)$ i d pozostają utajnione.

Jeżeli *Bogdan* chce zaszyfrować swój list (miłosny) do Alicji, to postępuję według następującego schematu. Najpierw zamienia treść listu na liczbę M spełniającą warunek $(M, N) = 1$, (to zawsze można zrobić) a następnie oblicza $M^e (\mathrm{mod}\, N)$ i wysyła otrzymany wynik. Alicja po odebraniu listu oblicza $(M^e)^d (\mathrm{mod}\, N)$ uzyskując w ten sposób oryginalną wiadomość. Dzieje się tak dlatego, że

$$M^{ed} = M^{\varphi(N)k+1} = (M^{\varphi(N)})^k M \equiv M (\mathrm{mod}\, N),$$

na mocy Twierdzenia Eulera. Intruz, który przechwycił list Bogdana do Alicji, widzi liczbę M^e, ale nie zna klucza do rozszyfrowania, którym jest liczba d. Mógłby ją obliczyć łatwo (z Algorytmu Euklidesa) gdyby znał $\varphi(N)$. Kłopot w tym, że aby obliczyć $\varphi(N)$ musi rozłożyć liczbę N na czynniki pierwsze, a to jest właśnie zadanie o ogromnej skali obliczeniowej, nawet dla najszybszych obecnie komputerów.

PRZYKŁAD 6. *Niech* $N = 438\,345\,710\,960\,029$ *i* $e = 6436\,343$. *Zaszyfrowana wiadomość to pewna data zapisana w postaci liczby ośmiocyfrowej. Jej szyfrogram ma postać* $M^e = 79\,632\,318\,919\,898$. *Czy potrafisz złamać szyfr?*

3. Liczby rzeczywiste

Zajmiemy się teraz jednym z największych wynalazków myśli ludzkiej—*liczbami rzeczywistymi* i spróbujemy przekonać się jak bardzo są one rzeczywiste. Przyjmiemy najprostszą geometryczną interpretację zbioru liczb rzeczywistych $\mathbb{R}$ jako punktów na *osi liczbowej*: na prostej znajdujemy dwa różne punkty i przypisujemy im liczby 0 i 1, następne liczby umiejscawiamy według zasad geometrycznych. Na przykład $\frac{1}{2}$ znajdzie się w środku odcinka o końcach 0 i 1, a 2 w takim punkcie aby środkiem odcinka 02 był punkt 1.

3.1. Liczby wymierne. Zbiór *liczb wymiernych* oznaczamy literą $\mathbb{Q}$. Stanowią go wszystkie możliwe ułamki $\frac{a}{b}$, gdzie a i b są liczbami całkowitymi, przy czym $b \neq 0$. Oczywiście różne ułamki mogą wyrażać tę samą liczbę wymierną, na przykład

$$\frac{2}{3} = \frac{4}{6} = \frac{-10}{-15}.$$

TWIERDZENIE 16. *W każdym odcinku na osi liczbowej znajdują się liczby wymierne.*

PROOF. Niech x i y będą dowolnymi różnymi punktami na prostej i niech d oznacza odległość między x i y. Wybierzmy liczbę naturalną n tak, aby $\frac{1}{n} < 2d$. Wówczas odkładając odcinek o długości $\frac{1}{n}$ odpowiednią liczbę razy, powiedzmy m, dostaniemy liczbę $\frac{m}{n}$ znajdującą się między x a y. ∎

TWIERDZENIE 17. *Liczby wymierne można ustawić w ciąg.*

PROOF. Najpierw ustawimy w ciąg liczby wymierne dodatnie. Można to zrobić na przykład według wzrostu sumy licznika i mianownika:

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{1}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \dots .$$

W ten sposób, każdy ułamek nieskracalny dodatni (czyli każda liczba wymierna dodtnia) ma swoje miejsce w tym ciągu. Ułamki ujemne ustawiamy tak samo i przeplatamy z dodatnimi umieszczając dodatkowo na początku liczbę 0:

$$0, \frac{1}{1}, -\frac{1}{1}, \frac{1}{2}, -\frac{1}{2}, \frac{2}{1}, -\frac{2}{1}, \frac{1}{3}, -\frac{1}{3}, \frac{3}{1}, -\frac{3}{1}, \frac{1}{4}, -\frac{1}{4}, \dots .$$

∎

W starożytności długo uważano, że każdemu punktowi na prostej odpowiada jakaś liczba wymierna. Tak jednak nie jest. Okazuje się, że gdyby ograniczyć się jedynie do punktów wymiernych, to oś liczbowa zostałaby podziurawiona jak sito.

3.2. Liczby niewymierne. Wykażemy istnienie liczb niewymiernych dwoma sposobami. Oto pierwszy z nich.

TWIERDZENIE 18. *Wszystkich punktów z osi liczbowej nie można ustawić w ciąg.*

PROOF. Przypuśćmy jednak, nie wprost, że udało nam się jakoś ustawić *wszystkie* punkty z prostej w ciąg $P_1, P_2, ...$. Niech I oznacza jakikolwiek odcinek na prostej. Wybierzmy odcinek I_1 zawarty w I tak aby punkt P_1 nie należał do I_1. Następnie wybierzmy odcinek $I_2 \subset I_1$, tak aby $P_2 \notin I_2$. Postępując tak dalej otrzymamy ciąg odcinków domkniętych $I_1 \supset I_2 \supset ...$ takich, że $P_i \notin I_i$, dla $i = 1, 2, ...$ Niech P będzie punktem należącym do części wspólnej wszystkich odcinków I_i. Wówczas $P \neq P_i$ dla każdego $i = 1, 2, ...$, co kończy dowód. ∎

TWIERDZENIE 19. *Długość przekątnej kwadratu o boku* 1 *nie może być wyrażona liczbą wymierną.*

PROOF. Niech x oznacza długość przekątnej kwadratu jednostkowego. Przypuśćmy, że jednak jest ona liczbę wymierną, powiedzmy $x = \frac{a}{b}$, dla pewnych liczb naturalnych a i b. Z twierdzenia Pitagorasa dostajemy

$$1^2 + 1^2 = x^2$$

czyli

$$a^2 = 2b^2.$$

To równanie jest jednak niemożliwe, z uwagi na jednoznaczność rozkładu na czynniki pierwsze. W istocie, kwadrat każdej liczby naturalnej zawiera w rozkładzie *parzystą* liczbę dwójek. Zatem liczba dwójek w rozkładzie a^2 jest parzysta, zaś w rozkładzie $2b^2$ nieparzysta. To jest sprzeczne z Podstawowym Twierdzeniem Arytmetyki. ∎

3.3. Liczby algebraiczne i liczby konstruowalne. Liczbę rzeczywistą α nazywamy *algebraiczną* jeżeli jest ona pierwiastkiem pewnego wielomianu o współczynnikach wymiernych. Na przykład, $\alpha = \frac{-1+\sqrt{5}}{2}$ jest liczbą algebraiczną ponieważ spełnia równanie $x^2 - x - 1 = 0$. *Stopniem* liczby algebraicznej nazywam najmniejszy stopień wielomianu (o współczynnikach wymiernych), którego jest ona pierwiastkiem.

TWIERDZENIE 20. *Wszystkie liczby algebraiczne można ustawić w ciąg.*

PROOF. Łatwo zauważyć, że zbiór wszystkich skończonych ciągów liczb naturalnych można ustawić w ciąg, np. według wielkości sumy wyrazów ciągu:

$$1, 11, 2, 111, 12, 21, 3, 1111, 112, 121, 13, 211, 22, 31, 4, ...$$

Stąd, można ustawić w ciąg wszystkie wielomiany o współczynnikach wymiernych, a ponieważ wielomian stopnia n ma co najwyżej n pierwiastków, więc także ich wszystkie pierwiastki. ∎

Z tego twierdzenia wynika w szczególności, że istnieją liczby, które nie są algebraiczne. Nazywamy je liczbami *przestępnymi*. Chociaż wiemy, że musi istnieć nieskończenie wiele liczb przestępnych, to jednak w przypadku konkretnej liczby stwierdzenie czy jest ona przestępna czy nie jest na ogół trudne. Że liczba π jest przestępna udowodnił dopiero Lindemann w roku 1882, a jego dowód rozstrzygnął ostatecznie kwestię słynnej *kwadratury koła*. Problem ten polegał na skonstruowaniu kwadratu o polu równym polu danego koła jednostkowego. Długość boku tego kwadratu powinna wynosić zatem $\sqrt{\pi}$. Jak się okazało znacznie później zadanie to jest niewykonalne.

Przypuśćmy, że dany jest odcinek o długości 1, a chcemy skonstruować (cyrklem i linijką) odcinek o danej długości x. Czy dla każdej liczby rzeczywistej dodatniej x taka konstrukcja istnieje? *Liczby konstruowalne* to długości odcinków, które mogą być skonstruowane geometrycznie. Zatem nasze pytanie brzmi: *czy każda liczba rzeczywista $x > 0$ jest konstruowalna*? Okazuje się, że odpowiedź jest negatywna.

TWIERDZENIE 21. *Liczba rzeczywista $x > 0$ jest konstruowalna wtedy i tylko wtedy, gdy jest liczbą algebraiczną, której stopień jest potęgą dwójki.*

Ponieważ liczba $\sqrt{\pi}$ nie jest nawet algebraiczna więc nie jest również konstruowalna.

3.4. Ciągi rekurencyjne. Ciągi rekurencyje stanowią wyjątkowo wdzięczny obiekt zarówno badań teoretycznych jak i wszelkiego rodzju eksperymentów komputerowych. Często mają one ścisły związek z liczbami algebraicznymi. Przedstawimy teraz kilka słynnych ciągów rekurencyjnych.

3.4.1. *Ciąg Fibonacciego.* Ciąg ten zaczyna się od dwóch jedynek $f_1 = f_2 = 1$, a następnie rozwija się według wzoru

$$f_n = f_{n-1} + f_{n-2}, \;\; n \geq 3.$$

Oto początkowe wyrazy tego ciągu:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, ...$$

Ciąg ten posiada wiele fascynujących własności, z których teraz przytoczymy jedną.

TWIERDZENIE 22. *Niech α i β będą pierwiastkami równania $x^2 - x - 1 = 0$. Wówczas*

$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \; n \geq 1.$$

PROOF. Zauważmy, że ciągi $1, \alpha, \alpha^2, ...$ i $1, \beta, \beta^2, ...$ spełniają zależność rekurencyjną ciągu Fibonacciego. Stąd każdy ciąg postaci $a_n = c_1\alpha^n + c_2\beta^n$ również spełnia wzór $a_n = a_{n-1} + a_{n-2}$ dla dowolnych stałych c_1 i c_2. To kończy dowód ponieważ wzór z tezy twierdzenia jest prawdziwy dla $n = 1, 2$. ∎

Istnieje wiele nierozwiązanych dotąd kwestii dotyczących ciągu Fibonacciego. Jedną z nich jest pytanie czy istnieje w nim nieskończenie wiele liczb pierwszych.

3.4.2. *Kosmologiczny ciąg Conwaya.* Ciąg Conwaya składa się z sekwencji zbudowanych z symboli 1,2,3:

1
11
21
1211
111221
312211
13112221
1113213211
31131211131221
.....

Reguła powstawania kolejnych sekwencji tego ciągu jest wyjątkowo przewrotna, łatwiej ją odgadniemy czytając na głos to co widzimy. Na przykład, w pierwszej sekwencji widzimy *jedną jedynkę*, a więc w następnej sekwencji zapisujemy *"jeden jeden"*, czyli 11. Następnie odczytujemy drugą sekwencję, która zawiera *dwie jedynki*, a zatem trzecia sekwencja to *"dwa jeden"*, czyli 21, itd. Można udowodnić, że długość n-tej sekwencji kosmologicznego ciągu Conwaya jest równa w przybliżeniu α^n, gdzie stała α, równa w przybliżeniu $1,3035772690...$, jest liczbą algebraiczną stopnia 71. A oto wielomian minimalny tej liczby

$$x^{71} - x^{69} - 2x^{68} - x^{67} + 2x^{66} + 2x^{65} + x^{64} - x^{63} - x^{62} - x^{61} - x^{60}$$
$$-x^{59} + 2x^{58} + 5x^{57} + 3x^{56} - 2x^{55} - 10x^{54} - 3x^{53} - 2x^{52} + 6x^{51} + 6x^{50}$$
$$+x^{49} + 9x^{48} - 3x^{47} - 7x^{46} - 8x^{45} - 8x^{44} + 10x^{43} + 6x^{42} + 8x^{41} - 5x^{40}$$
$$-12x^{39} + 7x^{38} - 7x^{37} + 7x^{36} + x^{35} - 3x^{34} + 10x^{33} + x^{32} - 6x^{31} - 2x^{30}$$
$$-10x^{29} - 3x^{28} + 2x^{27} + 9x^{26} - 3x^{25} + 14x^{24} - 8x^{23} - 7x^{21} + 9x^{20}$$
$$+3x^{19} - 4x^{18} - 10x^{17} - 7x^{16} + 12x^{15} + 7x^{14} + 2x^{13} - 12x^{12} - 4x^{11} - 2x^{10}$$
$$+5x^9 + x^7 - 7x^6 + 7x^5 - 4x^4 + 12x^3 - 6x^2 + 3x - 6.$$

3.4.3. *Hipoteza "*$3x + 1$*"*. Niech n będzie liczbą naturalną. Przyjmijmy, że $T(n) = \frac{n}{2}$, jeśli n jest parzyste i $T(n) = 3n + 1$ gdy n jest nieparzyste. Rozważmy ciąg iteracji

$$n, T(n), T(T(n)), T(T(T(n))), ...$$

Czy dla każdej liczby naturalnej n zawsze, prędzej czy później, otrzymamy 1? Na przykład, dla $n = 13$ ciąg iteracji jest następujący:

$$13, 40, 20, 10, 5, 16, 8, 4, 2, 1.$$

A dla $n = 7$ dostajemy liczby:

$$7, 22, 11, 34, 17, 52, 26, 13, ..., 1.$$

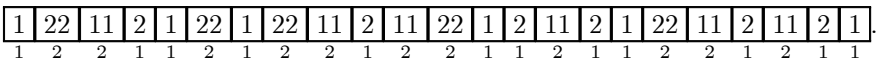
Hipoteza "$3x+1$" to przypuszczenie, że odpowiedź na powyższe pytanie jest pozytywna. Jak dotąd nikomu nie udało się ani potwierdzić ani obalić tego przypuszczenia.

3.4.4. *Ciąg Kolakoskiego.* Ciąg ten zbudowany jest wyłącznie z symboli 1 i 2, a jego początek wygląda następująco:

$$122112122122112112212112122112112 1...$$

Reguła generowania ciągu Kolakoskiego jest równie przewrotna jak w przypadku ciągu Conwaya i uwidoczni się gdy rozbijemy go na bloki złożone z identycznych

symboli:



i napiszemy pod każdym blokiem liczbę określającą jego długość. Otrzymany w ten sposób ciąg jest tym samym ciągiem!

Własności ciągu Kolakoskiego wciąż owiane są tajemnicą. Nie wiadomo na przykład, czy każdy blok pojawiający się w tym ciągu ma w nim swoje "dopełnienie", czyli identyczny blok tym, że jedynki zamieniono na dwójki a dwójki na jedynki.

3.4.5. *Ciąg Hofstadtera.* Ten ciąg określany jest takimi przymiotnikami jak "dziki" czy "chaotyczny" (albo nawet "dziko chaotyczny". Rzeczywiście, ani jedno przypuszczenie co do tego ciągu nie zostało dotąd poparte matematycznym dowodem! Definicja ciągu Hofstadtera jest następująca: $H(1) = H(2) = 1$ oraz

$$H(n) = H(n - H(n-1)) + H(n - H(n-2)),\ n \geq 3.$$

W penym sensie powyższy wzór przypomina regułę ciągu Fibonacciego, tu również następny wyraz jest sumą dwóch wcześniejszych wyrazów, z tym, że które to będą wyrazy, to zależy od dwóch *bezpośrednio* poprzednich wartości $H(n-1)$ i $H(n-2)$.

3.5. Rozwinięcia dwójkowe liczb rzeczywistych. Rozważmy następującą procedurę. Podzielmy odcinek $[0,1]$ na dwa równe odcinki, lewy L i prawy P. Następnie podzielmy każdą z połówek L i P znowu na połowy i oznaczmy je symbolicznie jako LL, LP, PL i PP. I tak dalej. Otrzymujemy w ten sposób *słowa* zbudowane z dwóch liter L i P, a każdemu słowu długości n odpowiada pewien odcinek o długości $\frac{1}{2^n}$.

Niech $x \in [0,1]$ będzie liczbą rzeczywistą i niech S_1, S_2, ... będzie ciągiem słów takich, że każdy z odpowiednich przedziałów zawiera liczbę x. Nie da się ukryć, że zamieniając L na 0 i P na 1 w słowie S_n dostaniemy *rozwinięcie dwójkowe* liczby x z dokładnością do n miejsc po przecinku. Na przykład,

$$\frac{9}{16} \leq \frac{-1+\sqrt{5}}{2} \leq \frac{10}{16}$$

co oznacza, że $\frac{-1+\sqrt{5}}{2} = 0.1001....$

Podobnie ma się rzecz z *rozwinięciami dziesiętnymi*, z tym, że teraz dzielimy odcinki na 10 identycznych części. Właśnie dlatego potrzebujemy aż dziesięciu cyfr do zapisywania takich rozwinięć. Oto kilka przykładów rozwinięć dziesiętnych ważnych stałych matematycznych:

$\frac{-1+\sqrt{5}}{2} = .\,618\,033\,988\,749\,894\,848\,204\,586\,834\,365\,638\,117\,720\,309\,179\,805\,8$
$\sqrt{2} = 1.\,414\,213\,562\,373\,095\,048\,801\,688\,724\,209\,698\,078\,569\,671\,875\,376\,9$
$\pi = 3.\,141\,592\,653\,589\,793\,238\,462\,643\,383\,279\,502\,884\,197\,169\,399\,375\,1$
$e = 2.\,718\,281\,828\,459\,045\,235\,360\,287\,471\,352\,662\,497\,757\,247\,093\,7$
$\ln 2 = .\,693\,147\,180\,559\,945\,309\,417\,232\,121\,458\,176\,568\,075\,500\,134\,360\,26.$

3.6. Ułamki łańcuchowe. Jeszcze jeden sposób zapisu liczb rzeczywistych opiera się na *ułamkach łańcuchowych*. Ułamkiem łańcuchowym nazywamy wyrażenie postaci

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \frac{1}{a_4 + \dots}}}$$

gdzie liczby a_i są liczbami całkowitymi dodatnimi. Jeżeli x jest daną liczbą rzeczywistą, to jej ułamek łańcuchowy znajdujemy ze wzoru $a_n = \lfloor x_n \rfloor$, gdzie $x_1 = x$ oraz

$$x_{n+1} = \frac{1}{x_n - \lfloor x_n \rfloor},\ n \geq 1.$$

Na przykład,

$$\frac{23}{13} = 1 + \cfrac{1}{1 + \frac{1}{3 + \frac{1}{3}}}.$$

Jest jasne, że ułamek łańcuchowy liczby x jest skończony wtedy i tylko wtedy, gdy x jest liczbą wymierną. Oto przykład rozwinięcia liczby niewymiernej:

$$\frac{-1 + \sqrt{5}}{2} = \cfrac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}.$$

Można udowodnić, że jeżeli x jest pierwiastkiem trójmianu kwadratowego, to rozwinięcie x na ułamek łańcuchowy jest okresowe.

4. Liczby zespolone

Rozważmy równanie $x^2 + 1 = 0$. Oczywiście nie ma ono rozwiązań w liczbach rzeczywistych. Wyobraźmy sobie jednak, że, być może na innej planecie, jakaś inna inteligencja stworzyła system matematyczny, w którym takie równanie ma rozwiązanie. Moglibyśmy ową liczbę oznaczyć w naszym świecie przez $\sqrt{-1}$, ale czy to nie jest jakiś nonsens?

4.1. Arytmetyka liczb zespolonych. Dla wygody oznaczmy ów dziwny $\sqrt{-1}$ literą i (od angielskiego "imaginary"). Tak więc i to po prostu liczba jakiej dotąd nie było, liczba, której kwadrat wynosi -1:

$$i^2 = -1.$$

Okazuje się, że dołączając ten obcy element do zbioru liczb rzeczywistych otrzymamy nowy, ale równie sensowny system arytmetyczny *liczb zespolonych*. Nazwa ta bierze się stąd, że każda liczba zespolona może być zapisana w *postaci algebraicznej*

$$x + yi$$

gdzie x i y są liczbami rzeczywistymi, a więc powstaje przez "zespolenie" dwóch liczb rzeczywistych.

Na liczbach zespolonych możemy wykonywać w sposób naturaly wszelkiego rodzju znane dotąd operacje arytmetyczne; mnożenie, dodawanie, dzielenie (byle nie przez 0), itp. Na przykład,

$$\begin{aligned}(1+2i)(-3+i) &= -3 + i - 6i + 2i^2 \\ &= -3 - 5i - 2 \\ &= -5 - 5i.\end{aligned}$$

Zatem, wszystko przebiega zwyczjnie oprócz tego, że $i^2 = -1$.

Z pewnością zasadne jest pytanie po co wprowadzać takie dziwolągi jak $\sqrt{-1}$. Jednym z powodów jest z pewnością następujące Zasadnicze Twierdzenie Algebry udowodnione przez Gaussa (Ziemianina, ...chyba...).

TWIERDZENIE 23. *(Gauss) Każde równanie algebraiczne dowolnego stopnia n ma rozwiązanie w liczbach zespolonych.*

Na przyklad, ujemna Δ nie stanowi już żadnej przeszkody w rozwiązaniu równania kwadratowego, ot choćby takiego jak $x^2 + x + 1 = 0$.

Oprócz tego liczby zespolone okazały się niezwykle przydatne w wielu innych działach matematyki i jej zastosowań. Zbiór liczb zespolonych będziemy oznaczać przez $\mathbb{C}$.

4.2. Geometria liczb zespolonych. Ponieważ liczby zespolone to pary liczb rzeczywistych więc naturalnym jest przypisanie im punktów płaszczyzny według zasady

$$x + yi \longmapsto (x, y).$$

Okaże się, że ten model zbioru $\mathbb{C}$ jest pod wieloma względami bardzo pożyteczny.

Niech $K = a + bi$ będzie ustaloną liczbą zespoloną. Zobaczmy co dzieje się gdy dodajemy liczbę K do innych liczb zespolonych $L = x + yi$. Łatwo zauważyć, że otrzymujemy geometryczny efekt przesunięcia o wektor (a, b).

Nieco trudniej przedstawia się sprawa mnożenia. Aby dokładnie wyjaśnić co dzieje się z punktami K i L podczas mnożenia liczb zespolonych będziemy musieli użyć trygonometrii.

Oznaczmy przez r odległość punktu K od środka układu współrzędnych, a α niech oznacza kąt między odcinkiem KO a dodatnią częścią osi X. Wówczas, z definicji funkcji trygonometrycznych dostajemy

$$K = r(\cos\alpha + i\sin\alpha).$$

Ten zapis liczby K nazywamy *trygonometrycznym*. Liczbę L możemy przedstawić podobnie jako

$$L = s(\cos\beta + i\sin\beta),$$

gdzie znaczenie liter s i β jest analogiczne. Wykonajmy mnożenie $K \cdot L$:

$$\begin{aligned} K \cdot L &= r(\cos\alpha + i\sin\alpha) \cdot s(\cos\beta + i\sin\beta) \\ &= rs\left((\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta)\right). \end{aligned}$$

To ostatnie wyrażenie może być uproszczone, co daje nam elegancki i przydatny wzór

$$K \cdot L = rs(\cos(\alpha + \beta) + i\sin(\alpha + \beta)). \tag{4.1}$$

Widzimy więc jak bardzo naturalne i zarazem podobne do mnożenia liczb rzeczywistych jest mnożenie liczb zespolonych (trzeba mieć rysunek).

Ze wzoru (4.1) wynika natychmiast wzór na potęgowanie liczb zespolonych.

$$K^n = r^n(\cos n\alpha + i\sin n\alpha). \tag{4.2}$$

Możemy w ten sposób obliczać potęgi o wielkich wykładnikach przy niewielkim nakładzie sił. Na przykład obliczmy $(1 + \sqrt{3}i)^{100}$. Mamy tu $r = 2$ i $\alpha = \frac{\pi}{6}$. Wobec

tego

$$(1+\sqrt{3}i)^{100} = 2^{100}(\cos 100 \cdot \frac{\pi}{6} + i \sin 100 \cdot \frac{\pi}{6}).$$

Ale $100 \cdot \frac{\pi}{6} = \frac{50}{3}\pi = 48\pi + \frac{2}{3}\pi$, więc

$$\begin{aligned}(1+\sqrt{3}i)^{100} &= 2^{100}(\cos\frac{2}{3}\pi + i\sin\frac{2}{3}\pi)\\ &= -2^{99} + 2^{99}\sqrt{3}i.\end{aligned}$$

4.3. Pierwiastki z jedynki i wielokąty foremne. *Pierwiastkowanie* w zbiorze $\mathbb{C}$ nie różni się wiele od zwykłego pierwiastkowania i jest operacją odwrotną do potęgowania. Aby obliczyć pierwiastki stopnia n z danej liczby zespolonej K rozwiązujemy po prostu równanie $X^n = K$. Niech $K = r(\cos\alpha + i\sin\alpha)$, a $X = s(\cos\beta + i\sin\beta)$. Wówczas, na mocy wzoru (4.2) otrzymujemy związki

$$\begin{aligned}s &= \sqrt[n]{r},\\ \beta &= \frac{\alpha + 2k\pi}{n},\end{aligned}$$

przy czym ostatni wzór daje różne wrtości β dla $k = 0, 1, ..., n-1$. Zatem wszystkie rozwiązania równania $X^n = K$ wyrażają się wzorami

$$X_k = \sqrt[n]{r}(\cos\frac{\alpha + 2k\pi}{n} + i\sin\frac{\alpha + 2k\pi}{n}),$$

dla $k = 0, 1, ...n-1$. Warto odnotować, że punkty X_k są rozmieszczone *równomiernie* na okręgu o środku w punkcie O i promieniu $\sqrt[n]{r}$.

W szczególnym przypadku, gdy $K = 1$, dostajemy n *pierwiasków z jedynki*

$$E_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}.$$

Pierwiastki z jedynki tworzą ciekawą strukturę. Łatwo zauważyć, że $E_k = G^k$, gdzie $G = E_1$, oraz $E_k \cdot E_l = E_{k+l}$, gdzie dodawanie $k + l$ wykonywane jest modulo n.

Przedstawimy teraz jedno z najbardziej spektakularnych twierdzeń w historii matematyki, w którym własności pierwiastków z jedynki odgrywają kluczową rolę. Chodzi tu o słynne twierdzenie Gaussa rozstrzygające problem konstruowalności wielokątów foremnych.

Liczbę zespoloną $K = x + yi$ nazywamy *konstruowalną* jeżeli liczby rzeczywiste x i y są konstruowalne. Liczby całkowite postaci

$$F_k = 2^{2^k} + 1, k \geq 0,$$

nazywamy *liczbami Fermata*. Pierwszych pięć liczb Fermata to

$$3, 5, 17, 257, 65537.$$

Wszystkie są liczbami pierwszymi. Do dziś nie wiadomo, czy istnieje choćby jeszcze jedna liczba pierwsza Fermata.

TWIERDZENIE 24. *(Gauss) Wielokąt foremny jest konstruowalny wtedy i tylko wtedy, gdy liczba jego wierzchołków N ma postać*

$$N = 2^r p_1 p_2 ... p_s,$$

gdzie $r, s \geq 0$, a $p_1, p_2, ..., p_s$ są różnymi liczbami pierwszymi Fermata.

PROOF. Niech

$$G_N = \cos\frac{2\pi}{N} + i\sin\frac{2\pi}{N}.$$

Można pokazać, że G_N jest liczbą algebraiczną stopnia $\varphi(N)$. Wystarczy więc zobaczyć, że $\varphi(N)$ jest potęgą dwójki wtedy i tylko wtedy, gdy N ma postać opisaną w tezie twierdzenia. Niech $N = 2^r q_1^{r_1}...q_s^{r_s}$ będzie rozkładem liczby N na czynniki pierwsze, w którym $r \geq 0, r_i \geq 1$, a liczby q_i są nieparzyste i parami różne. Wówczas

$$\varphi(N) = \varphi(2^r)\prod_{i=1}^{s} q_i^{r_i-1}(q_i - 1).$$

Stąd $r_i = 1$ i q_i muszą być potęgami dwójki. To kończy dowód. ∎

Z tego tiwerdzenia wynika w szczególności, że nie istnieje konstrukcja geometryczna 9-kąta foremnego, natomiest można skonstruować 17-kąt foremny.