Liczby pierwsze i jednoznaczność rozkładu – ogólniej

Stara Delta

fragmenty artykułu Władysława NARKIEWICZA z *Delty* 9/1979

Twierdzenie o jednoznaczności rozkładu na czynniki pierwsze w zbiorze liczb naturalnych wypowiada się najprościej w następujący sposób: każdą liczbę naturalną różną od jedności możemy przedstawić w postaci iloczynu $p_1p_2\dots p_r$ liczb pierwszych na jeden tylko sposób, o ile rozkłady, różniące się kolejnością czynników, uważać będziemy za równe. Podobne twierdzenie można wysłowić także i dla liczb całkowitych, niekoniecznie dodatnich: *każdą liczbę całkowitą, różną od* $0, 1, -1$, *możemy przedstawić na jeden sposób w postaci iloczynu* $ap_1p_2\dots p_r$, *przy czym* $p_1, \dots, p_r$ *są liczbami pierwszymi, a liczba* a *równa jest* 1 *lub* -1. (Oczywiście i w tym przypadku należy utożsamiać rozkłady, różniące się kolejnością czynników.) Nazwijmy pierścieniem liczbowym każdy zbiór zawarty w zbiorze liczb zespolonych, w którym wykonalne jest dodawanie, odejmowanie i mnożenie. Oczywiście, zbiór $\mathbb{Z}$ liczb całkowitych jest takim pierścieniem. Nasuwa się naturalne pytanie, czy w każdym pierścieniu liczbowym zachodzi twierdzenie analogiczne do wysłowionego przed chwilą w przypadku pierścienia $\mathbb{Z}$.

Rozpatrzmy dla przykładu pierścień liczb całkowitych Gaussa, złożony ze wszystkich liczb zespolonych postaci $A + Bi$, przy czym A, B są liczbami całkowitymi. O tym pierścieniu można udowodnić następujące twierdzenie, analogiczne do twierdzenia o jednoznacznym rozkładzie w $\mathbb{Z}$: jeśli z jest liczbą całkowitą Gaussa, różną od $0, 1, -1, i, -i$, to możemy ją przedstawić w postaci

$$z = P_1 \cdot \ldots \cdot P_r,$$

przy czym liczby P_i są liczbami pierwszymi Gaussa, tj. mają tę własność, że z rozkładu P_i na czynniki, $P_i = xy$, gdzie x, y są liczbami całkowitymi Gaussa, wynika, że jeden z tych czynników jest równy, 1, -1, i lub $-i$.

Jeżeli

$$z = P'_1 \cdot \ldots \cdot P'_s$$

jest innym rozkładem tego typu, to $r = s$, a przy tym po odpowiednim przenumerowaniu liczb $P'_1, \dots, P'_s$ zachodzą równości: $P'_1 = a_1P_1$, $\dots$, $P'_r = a_rP_r$, przy czym każda z liczb a_i jest równa 1, -1, i lub $-i$.

Dla przykładu rozłożymy na czynniki pierwsze w pierścieniu Gaussa liczbę 2: mamy równość: $2 = (1 + i)(1 - i)$, a rozkład ten jest rozkładem na czynniki pierwsze, bo jeśli np. $1 + i = (a + bi)(c + di)$, to $2 = |1 + i| \cdot |1 - i| = |1 + i|^2 = (a^2 + b^2)(c^2 + d^2)$, a zatem $a^2 + b^2 = 1$ lub też $c^2 + d^2 = 1$, co pokazuje, że jedna z liczb $a + bi$, $c + di$ jest równa 1, -1, i lub $-i$.

Możemy przy tym także napisać: $2 = i(1 - i)^2 = (-1)(1 + i)(-1 + i) = -i(1 + i)^2$, co pokazuje, że możliwości podane w sformułowaniu twierdzenia rzeczywiście występują.

By móc sensownie sformułować twierdzenie o jednoznaczności rozkładu dla dowolnego pierścienia liczbowego, należy uprzednio określić, co będziemy rozumieli przez liczby pierwsze w takim pierścieniu i jakie liczby będą grały role liczb $1, -1$ w pierścieniu liczb całkowitych, czy też liczb $1, -1, i, -i$ w pierścieniu Gaussa. W tym celu zauważmy, że odwrotność każdej z liczb $1, -1, i, -i$ również leży w pierścieniu Gaussa.

Rozwiązanie zadania F 809.
Po zwiększeniu masy pierwszego cylindra równowaga nastąpi dopiero, gdy znajdzie się on na dnie naczynia, a cały gaz przejdzie do drugiego cylindra. Ponieważ ciśnienie gazu oraz jego temperatura nie zmieniają się, więc także objętość pozostanie stała. Zatem $S_1h + S_2h = S_2h_1$, gdzie S_1 i S_2 to przekroje wewnętrzne cylindrów, a h_1 to wysokość, na którą wzniesie się drugi tłok. Początkowo ciśnienie gazu w obu naczyniach było jednakowe, tzn. $m_1g/S_1 = m_2g/S_2$, stąd $S_1/S_2 = m_1/m_2$. Zatem

$$h_1 = \left(\frac{m_1}{m_2} + 1\right)h = 0{,}15 \text{ m}.$$

Niech log oznacza logarytm przy naszej ulubionej podstawie.

$$K = \frac{\log 3}{\log 2} \cdot \frac{\log 7}{\log 5}; \quad L = \frac{\log 7}{\log 2} \cdot \frac{\log 3}{\log 5}.$$

Zatem $K = L$.

To podsuwa następujące określenie: jeżeli R jest pierścieniem liczbowym, to liczba a należąca do niego nazywa się odwracalna w R, jeżeli $a \neq 0$ oraz $1/a$ należy do R. (Oczywiście, liczby 1 i -1 są odwracalne w każdym pierścieniu, a przykład pierścienia Gaussa pokazuje, że liczb odwracalnych może być więcej.) Teraz możemy określić liczby pierwsze w pierścieniu R: różną od zera liczbę a pierścienia R nazywamy liczbą pierwszą w R, jeżeli z równości $a = xy$ ($x \in R$, $y \in R$) wynika, że jedna z liczb x, y jest odwracalna w R.

Używając tych definicji, możemy teraz sformułować dla dowolnego pierścienia liczbowego R odpowiednik twierdzenia o jednoznaczności rozkładu: mówimy, że *w R zachodzi twierdzenie o jednoznaczności rozkładu, jeżeli każda liczba $a \in R$, różna od zera i nieodwracalna da się zapisać w postaci*

$$a = P_1 \cdot \ldots \cdot P_r,$$

przy czym liczby $P_1, \ldots, P_r$ są liczbami pierwszymi w R, a przy tym jeżeli $a = P'_1 \cdot \ldots \cdot P'_s$ jest innym takim rozkładem, to $r = s$ i po odpowiednim ponumerowaniu liczb $P'_1, \ldots, P'_r$ zachodzą równości: $P'_1 = c_1 P_1$, $\ldots$, $P'_r = c_r P_r$, przy czym liczby $c_1, \ldots, c_r$ są odwracalne.

Następujący przykład świadczy o tym, że sformułowane powyżej twierdzenie nie we wszystkich pierścieniach liczbowych jest prawdziwe:

rozpatrzmy pierścień R złożony ze wszystkich liczb $a + bi\sqrt{5}$, przy $a, b \in \mathbb{Z}$. (Proponuję Czytelnikowi sprawdzenie, że R w istocie jest pierścieniem.) Liczba 6 ma w R dwa różne rozkłady:

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Nietrudno sprawdzić, że występujące tu czynniki są liczbami pierwszymi w rozważanym pierścieniu. Jeżeli np. $2 = X \cdot Y = (x + yi\sqrt{5})(a + bi\sqrt{5})$, przy czym $x, y, a, b \in \mathbb{Z}$, to $4 = |x + yi\sqrt{5}|^2 |a + bi\sqrt{5}|^2 = (x^2 + 5y^2)(a^2 + 5b^2)$, a więc $x^2 + 5y^2 = a^2 + 5b^2 = 2$ lub też jedna z liczb $x^2 + 5y^2$, $a^2 + 5b^2$ jest równa 1, a druga równa 4. Ponieważ równanie $u^2 + 5v^2 = 2$ nie ma rozwiązań całkowitych, musi zachodzić druga możliwość, a wówczas jedna z liczb X, Y musi być równa 1 lub -1. Podobnie sprawdzamy, że pozostałe czynniki naszych rozkładów są pierwsze. Pozostaje sprawdzić, że ilorazy czynników obu rozkładów nie są odwracalne, ale to wynika z uwagi, że żadna z liczb $\frac{1 \pm i\sqrt{5}}{2}$, $\frac{1 \pm i\sqrt{5}}{3}$ nie leży w R. Widzimy ostatecznie, że w pierścieniu R twierdzenie o jednoznaczności rozkładu nie zachodzi.

Wielomianów postaci $x^2 + x + p$, gdzie p jest liczbą pierwszą, mających tę własność, że dla wartości x z zakresu od 0 do $p - 2$ przyjmują wartości będące liczbami pierwszymi, wcale nie jest dużo. Euler w 1772 roku, oprócz wspomnianego w *Małej Delcie* $x^2 + x + 41$, znał jeszcze cztery wielomiany tego typu:

$$x^2 + x + 3, \quad x^2 + x + 5, \quad x^2 + x + 11, \quad x^2 + x + 17.$$

Okazuje się, że innych nie ma, ale dowód powstał dopiero w 1966 roku.

A dlaczego wartości x, dla których wielomian daje w wyniku liczbę pierwszą, kończą się na $p - 2$? Dla $x = p - 1$ mamy

$$(p-1)^2 + (p-1) + p = (p-1)^2 + 2(p-1) + 1 = (p - 1 + 1)^2 = p^2.$$

M. D.-B.

Rozwiązanie zadania M 1345.
Przypuśćmy przeciwnie, że istnieje liczba całkowita r, dla której $f(r) = 2012$. Korzystając z tego, że $x - y$ dzieli $f(x) - f(y)$, dla dowolnych liczb całkowitych x i y, mamy

$$r - t_j \mid 2003, \qquad j = 1, 2, 3, 4.$$

Liczba 2003 jest pierwsza, więc skoro liczby $r - t_j$ są parami różne, to bez straty ogólności możemy przyjąć, że

$$t_1 = r - 2003, \quad t_3 = r + 1,$$
$$t_2 = r - 1, \quad t_4 = r + 2003.$$

Ponieważ $f(t_j) = 9$, więc po podzieleniu z resztą wielomianu f przez wielomian $(x - t_1)(x - t_2)(x - t_3)(x - t_4)$ mamy

$$f(x) = g(x) \cdot (x - r + 2003)(x - r + 1) \cdot (x - r - 1)(x - r - 2003) + 9,$$

dla pewnego wielomianu g o współczynnikach całkowitych. Podstawiając $x = r$, dostajemy

$$2012 = g(r) \cdot 2003^2 + 9,$$

co przeczy temu, że $g(r)$ jest liczbą całkowitą.

Która liczba jest większa?

$$M = \left(\sqrt{37} - 6\right)^{666} \quad \text{czy} \quad N = \frac{1}{100^{100}}$$