Liczby 1, -1, i, $-i$ są jedynymi elementami odwracalnymi pierścienia $Z[i]$, tj. takimi liczbami $x \in Z[i]$, że dla pewnego $y \in Z[i]$ zachodzi $xy = 1$.

Jednoznaczność rozkładu i liczba klas

Prof. dr Władysław NARKIEWICZ

1. 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 $p_1 p_2 \dots p_r$ 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 $ap_1 \dots p_r$, przy czym $p_1, \dots, p_r$ są liczbami pierwszymi, a liczba a równa jest 1 lub -1. (Oczywiście i w tym wypadku 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 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 Z.

Rozpatrzmy dla przykładu pierścień liczb całkowitych Gaussa, złożony z 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 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: $P_1' = a_1 P_1, \dots, P_r' = a_r P_r$, 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 rolę 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. 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 $P_1, \dots, P_r$ 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 $P_1', \dots, P_r'$ zachodzą równości $P_1' = c_1 P_1, \dots, P_r' = c_r P_r$, przy czym liczby $c_1, \dots, c_r$ są odwracalne.

2. Powstaje naturalne pytanie, w jakich pierścieniach liczbowych sformułowane powyżej twierdzenie jest prawdziwe. Następujący przykład świadczy o tym, że nie we wszystkich: rozpatrzmy pierścień R złożony z wszystkich liczb $a+bi\sqrt{5}$ przy $a, b \in Z$. (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

$x, y, a, b \in Z$, 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.

3. Powyższe przykłady wskazują, że istnieją pierścienie z jednoznacznością rozkładu na czynniki pierwsze, jak i bez tej jednoznaczności. Okazuje się, że można w pewien sposób mierzyć, jak bardzo dany pierścień liczbowy odbiega od pierścienia z jednoznacznością rozkładu. Do tego celu potrzebne nam będzie pojęcie ideału.

Jeżeli R jest pierścieniem liczbowym, to niepusty podzbiór $I \subset R$ nazywamy ideałem, jeśli jest w nim wykonalne dodawanie i odejmowanie oraz mnożenie przez elementy z R (niekoniecznie należące do I). Przykładem ideału w pierścieniu liczb całkowitych jest zbiór liczb parzystych (ale zbiór liczb nieparzystych nie jest ideałem, gdyż suma liczb nieparzystych jest parzysta!), czy też zbiór wszystkich liczb podzielnych przez zadaną liczbę naturalną N. Przykład ostatni można uogólnić: jeżeli a jest dowolnym elementem pewnego pierścienia R, to zbiór wszystkich liczb $x \in R$ dających się zapisać w postaci $x = ba$, przy pewnym $b \in R$ jest ideałem. Ten ideał oznaczamy przez I_a i nazywamy ideałem głównym, wyznaczonym przez a. (Czytelnik zechce spróbować udowodnić, że w pierścieniu Z każdy ideał jest ideałem głównym, wyznaczonym przez pewną liczbę naturalną).

Jeżeli I jest ideałem w R, a x jest pewną liczbą z R, to przez xI oznaczać będziemy zbiór wszystkich liczb $y \in R$, dających się zapisać w postaci $y = zx$ przy pewnym z należącym do I. I tak np. ideał I_a możemy zapisać w postaci $I_a = aR$.

Dwa ideały I, J nazywamy równoważnymi, jeżeli można znaleźć niezerowe liczby $a, b \in R$ takie, że $aI = bJ$. Zauważmy, że dowolne dwa ideały główne, powiedzmy I_a i I_b przy $a, b \neq 0$ są równoważne, gdyż zachodzi równość $bI_a = baR = abR = aI_b$. Zauważmy także, że jeżeli ideały I, J oraz I, J_1 są równoważne, to także i ideały J i J_1 będą równoważne. To pozwala nam podzielić zbiór wszystkich ideałów, różnych od ideału zerowego $\{0\} = I_0$ na klasy, zaliczając dwa ideały do tej samej klasy wówczas, gdy są równoważne. Jeżeli liczba takich klas jest skończona, to nazywamy ją liczbą klas pierścienia R i oznaczamy przez $h(R)$. Liczba ta w wielu wypadkach pozwala mierzyć, jak bardzo własności pierścienia R odbiegają od własności pierścienia z jednoznacznym rozkładem. By móc to sformułować precyzyjniej, ograniczymy teraz klasę rozważanych pierścieni. Rozpatrywać będziemy dwa typy pierścieni liczbowych — pierścienie kwadratowe oraz pierścienie cyklotomiczne.

4. Pierścienie kwadratowe określimy w następujący sposób: jeżeli D jest liczbą całkowitą, niepodzielną przez kwadrat liczby naturalnej, różnej od jedności (tj. $D = p_1 \dots p_r$ lub $D = -p_1 \dots p_r$, gdzie $p_1, \dots, p_r$ są różnymi liczbami pierwszymi), a przy tym D daje resztę 2 lub 3 z dzielenia przez 4, to przez pierścień kwadratowy, wyznaczony przez D, będziemy rozumieli zbiór wszystkich liczb postaci $a+b\sqrt{D}$, przy czym $a, b \in Z$. Jeżeli zaś D daje z dzielenia przez 4 resztę 1, to pierścieniem kwadratowym, wyznaczonym przez nią, będziemy nazywali zbiór wszystkich liczb postaci $\frac{a+b\sqrt{D}}{2}$, gdzie $a, b \in Z$ i są jednakowej parzystości. Otrzymany pierścień oznaczamy przez R_D.
(Niejednolitość podanej definicji może wydać się dziwna. Naturalniej byłoby podać także i w przypadku drugim definicję taką samą jak w pierwszym. Okazuje się jednak, że takie podejście nie prowadzi do przejrzystej teorii.)

Pierścienie cyklotomiczne, które teraz wprowadzimy, zostały zdefiniowane w połowie ubiegłego wieku przez matematyka niemieckiego E. E. Kummera, który je wykorzystał przy badaniu rozwiązalności sławnego równania Fermata: $x^n+y^n = z^n$ przy czym x, y, z są liczbami całkowitymi dodatnimi, a $n \geqslant 3$. (Do dziś zresztą nie wiemy, czy to równanie ma rozwiązania). Wybierzmy liczbę pierwszą nieparzystą p i oznaczmy przez z_p liczbę zespoloną $\cos(2\pi/p) + i\sin(2\pi/p)$. (Jest to p-ty pierwiastek z jedności, gdyż wzór Moivre'a daje $z_p^p = 1$). Przez $R[p]$ oznaczać będziemy zbiór wszystkich liczb zespolonych dających się zapisać w postaci

$$a_0+a_1z_p+a_2z_p^2+ \dots +a_{p-2}z_p^{p-2}+a_{p-1}z_p^{p-1},$$

przy czym $a_0, a_1, \dots, a_{p-2}$ są liczbami całkowitymi. Nietrudno sprawdzić, że $R[p]$ jest pierścieniem. Będzie to właśnie pierścień cyklotomiczny wyznaczony przez p. (Słowo „cyklotomia" oznacza podział okręgu, a użyte jest tutaj z tego względu, że liczby $1, z_p, z_p^2, \dots, z_p^{p-1}$ leżą na okręgu jednostkowym i wyznaczają podział tego okręgu na p równych części).

Czego można się dowiedzieć, mierząc precyzyjnie długość?

W ekspedycji wysłanej z planety Alfa na Ziemię uczestniczył Profesor Omega. Mimo, że wiedza techniczna Alfian stoi (w porównaniu z ziemską) bardzo wysoko, w niemal wszystkich pozostałych dziedzinach (szczególnie w zakresie nauk humanistycznych) nie dostają nam oni nawet do pięt. Profesor Omega postanowił zabrać na Alfę całe encyklopedie, leksykony, tomy powieści i roczniki gazet. Zastanawiano się, w jaki sposób zmieści się to wszystko do niewielkiej rakietki, którą przybyli Alfianie, w dodatku i tak bardzo przeładowanej. Profesor Omega wyciągnął z kieszeni mały kalkulator i długo coś obliczał, wertując kartki książek i strony gazet. Następnie wyjął z rakiety długą linijkę z dziwnego metalu i specjalnym widać nożykiem zrobił na niej kreskę. „To wszystko" powiedział, „możecie zabrać z powrotem swoje książki". Gdy Ziemianie zaczęli się domagać bliższych wyjaśnień, powiedział:

— To bardzo proste. Każdej literze waszego alfabetu przypisałem liczbę (A = 1, B = 2 itd.), każdemu znakowi przestankowemu czy specjalnemu symbolowi — liczbę między 51 a 99. Przepisałem na kalkulatorze wszystkie książki używając liczb zamiast liter. Litery oddzielałem znakiem 000, słowa — 00000, a 000000 znaczy, że następujące cyfry należy czytać jako liczbę. Otrzymałem w ten sposób pewną liczbę. Dość dużą, około 200 milionów cyfr, ale nie przesadnie. Postawiłem przed nią 0 i przecinek dziesiętny, otrzymując liczbę wymierną a/b z przedziału (0, 1). Kreska, którą zrobiłem na mojej linijce, dzieli ją właśnie w stosunku a/b. Gdy wrócę na Alfę, w laboratorium zmierzymy dokładnie obie części linijki, obliczymy a/b, zapiszemy w postaci dziesiętnej i oto mamy wszystko z powrotem.

5. Podamy teraz podstawowe twierdzenia dotyczące wprowadzonych pierścieni i wiążące się z liczbą klas oraz jednoznacznością rozkładu.
Jednym z najważniejszych i najstarszych rezultatów w tej dziedzinie jest następujące twierdzenie, podające związek między liczbą klas a jednoznacznością rozkładu: *W pierścieniu R_D lub $R[p]$ zachodzi twierdzenie o jednoznaczności rozkładu wtedy i tylko wtedy, gdy jego liczba klas równa jest* 1, tj. gdy wszystkie ideały są równoważne.
Twierdzenie to sprowadza zagadnienie jednoznaczności rozkładu do obliczenia liczby klas. Dla konkretnego pierścienia nie jest to zagadnienie trudne, szczególnie przy użyciu maszyn cyfrowych. Znacznie trudniej jest wyznaczyć wszystkie pierścienie o tej własności. Okazuje się, że pierścieni R_D przy D ujemnym, oraz $R[p]$ z jednoznacznością rozkładu jest skończenie wiele. Dla pierścieni R_D z D dodatnim tego nie wiemy. Obliczenia numeryczne skłaniają do przypuszczenia, że takich D jest nieskończenie wiele, ale metody matematyki współczesnej nie są dostatecznie mocne na to, by problem ten rozstrzygnąć.
A oto lista ujemnych D, dla których w R_D zachodzi twierdzenie o jednoznacznym rozkładzie: $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$. Pierwszy dowód tego, że nie ma innych D ujemnych o tej własności podał młody matematyk amerykański, H. M. Stark, w 1967 roku. Dla pierścieni $R[p]$ sytuacja jest podobna. Wiemy, dzięki badaniom K. Uchidy, J. Masleya i H. Montgomery'ego, że jednoznaczność rozkładu zachodzi w $R[p]$ jedynie dla $p = 3, 5, 7, 11, 13, 17$ oraz 19.
Znane są także wszystkie pierścienie cyklotomiczne oraz pierścienie kwadratowe R_D z ujemnym D, dla których liczba klas równa jest 2. Jak zauważył L. Carlitz, w takich pierścieniach zachodzi następujący fakt: *w każdym rozkładzie liczby na czynniki pierwsze wystąpi ta sama ilość czynników pierwszych.* Przy tym własność ta jest charakterystyczna dla pierścieni z liczbą klas równą 2.
Byłoby interesującą rzeczą znalezienie podobnych charakteryzacji dla pierścieni z liczbą klas równą 3, 4, itd., jednakże nie otrzymano tu jeszcze definitywnych rezultatów.

Zadania

Redaguje mgr Krzysztof NOWIŃSKI

M 202. Wykazać, że dla dowolnego $n > 0$ istnieje taki m-kąt, że n jego przekątnych leży wewnątrz niego, a wszystkie pozostałe — na zewnątrz.

Rozwiązanie na str. 8

M 203. „Literą T" nazywamy sumę prostopadłych odcinków AB i CD o długości 1 każdy, przy czym C jest środkiem odcinka AB. Wykazać, że w ograniczonym obszarze płaszczyzny nie można pomieścić nieskończenie wielu rozłącznych „liter T".

Rozwiązanie na str. 12

M 204. Czy sześcian o wymiarach $6 \times 6 \times 6$ może być zbudowany z 27 klocków o rozmiarach $1 \times 2 \times 4$?

Rozwiązanie na str. 5
(Zadanie to nadesłała *Małgorzata TOPER* z Lubienia).

Redaguje dr Halina ABRAMOWICZ

F 68. Wiązka cząstek α o strumieniu N cząstek na jednostkę powierzchni pada na folię metalową o grubości x i gęstości n atomów na jednostkę objętości. W wyniku oddziaływania cząstek α z polem jąder atomów folii następuje odchylenie cząstek w stosunku do kierunku lotu pierwotnego. Odchylenie to zależy od tzw. parametru zderzenia — tzn. odległości między torem cząstki daleko od centrum oddziaływania a prostą równoległą do tego toru przechodzącą przez centrum siły (czyli przez jądro). Znaleźć rozkład kątowy cząstek α po przejściu przez folię, zakładając, że folia jest na tyle cienka, że jedna cząstka α może się „zderzyć" tylko z jednym jądrem, oraz zakładając, że jądro pozostaje nieruchome w wyniku oddziaływania (bardzo duża masa jądra w porównaniu z masą cząstki α).

Rozwiązanie na str. 6

Zmierzyć wysokość wieży za pomocą barometru —

— takie zadanie dano przedstawicielom różnych nauk. Oto jak je rozwiązywali: Matematyk wykorzystał twierdzenie Talesa (i to, że dzień był słoneczny): ustawił barometr pionowo, zmierzył jego długość oraz długość jego cienia i wieży i szybko miał odpowiedź. Fizyk-teoretyk wykorzystał fakt, że ciśnienie maleje wraz z wysokością, fizyk-doświadczalnik przywiązał barometr do sznurka, spuścił z wieży i potem zmierzył długość sznurka. Chemik wylał rtęć z barometru do kolby, doprowadził do stanu wrzenia u stóp i na szczycie wieży i z różnicy temperatur wrzenia obliczył żądaną wysokość. Humanista zaś zapukał do stojącej nieopodal chatki. „Dostanie pan barometr, jeśli powie mi pan, ile ta wieża ma wysokości" powiedział do siwego staruszka, który otworzył mu drzwi.