# Nieco historii matematyki w wykładzie algebry

*Prof. dr Stanisław BALCERZYK, dr Michał SZUREK*

Motto: *Historia est magistra vitae — Historia jest nauczycielką życia*

Piękne twierdzenia, które prezentujemy naszym słuchaczom na wykładach, są jak wspaniałe brylanty iskrzące się wewnętrznym blaskiem; nikt nie potrafi z ich obecnego wyglądu odgadnąć, jak wiele nadziei i trudu towarzyszyło znalezieniu niezbyt efektownego diamentu, który dopiero po żmudnej pracy szlifierza stał się prawdziwym klejnotem.

Słuchacze naszych wykładów są często nawet w gorszej sytuacji niż telewidzowie, którzy mozoły podróży znają tylko z ekranu. Uczący się przeważnie nie mają żadnego wyobrażenia o drodze rozwoju nie tylko teorii matematycznych, ale nawet o losach poszczególnych twierdzeń. Wykładowcy i autorzy podręczników również rzadko zwracają uwagę na dzieje teorii. Maksimum wiedzy to zwykle znajomość przebiegu procesu osłabiania założeń w dążeniu do uzyskania końcowego, eleganckiego wyniku. Pięknym wyjątkiem od tej reguły są książki Nicolasa Bourbaki, zawierające informacje historyczne podane w sposób użyteczny dla studiów nad odpowiednią teorią.

W tym stanie rzeczy pragniemy podzielić się z Czytelnikami pewnymi refleksjami na temat celowości kontaktu z przeszłością matematyki. Oczywiście byłoby nonsensem wzywanie do nauczania matematyki przez prezentowanie kolejnych etapów jej rozwoju. Byłoby to zaprzeczeniem postępu, zmarnowaniem czasu. Jednak całkowite odcięcie się od przeszłości także nie jest dobre. Warto czasem zwrócić się wstecz, aby lepiej ocenić i zrozumieć teraźniejszość, nabrać szacunku dla twórczości i wspaniałej intuicji naszych pradziadów, aby dostrzec, że ich działalność służyła konkretnym zagadnieniom, że zbudowane przez nich teorie były mocno osadzone wśród potrzeb ówczesnej matematyki.

Opowiemy o dziejach powstania podstawowych dzisiaj pojęć algebry — pierścienia przemiennego i ideału na gruncie algebraicznej teorii liczb, w pracach Kummera, Kroneckera i Dedekinda, o ratowaniu zasadniczego twierdzenia arytmetyki o jednoznaczności rozkładu — oraz nieco o dalszych badaniach z tym związanych.

Na ogół w kursach algebry istnienie i jednoznaczność rozkładu elementu (takiego jak liczba całkowita lub wielomian) na iloczyn elementów nierozkładalnych jest traktowana jako „prawidłowość" — jej brak raczej jako osobliwość. Zapewne temu zawdzięczamy słynną notatkę Fermata na marginesie dzieła Diofantesa a właśnie teoria liczb skłania do oceny przeciwnej — jednoznaczność rozkładu jest własnością wyjątkową. Zagadnienie rozwiązalności równania Fermata wystarczy oczywiście badać dla wykładników będących liczbami pierwszymi: jeśli $n = pq$ i $x, y, z$ spełniają równanie $x^n+y^n = z^n$, to $x^q, y^q, z^q$ spełniają równanie $X^p+Y^p = Z^p$. Ustalmy więc liczbę pierwszą $p > 2$ i przypuśćmy, że równanie Fermata ma rozwiązanie składające się z dodatnich liczb całkowitych $x, y, z$, a zatem $x^p+y^p = z^p$. Narzuca się od razu pomysł: prawa strona jest iloczynem $p$ czynników $z^p = z \cdot z \cdot \ldots \cdot z$, dobrze byłoby również i lewą stronę przedstawić w postaci iloczynu czynników nierozkładalnych i próbować znaleźć związek pomiędzy czynnikami po obu stronach. Jednak wyrażenie $x^p+y^p$ możemy rozłożyć na iloczyn jedynie dwóch czynników

$$x^p+y^p = (x+y)(x^{p-1}-x^{p-2}y+ \ldots -xy^{p-2}+y^{p-1}).$$

Dopuszczając jednak czynniki będące liczbami zespolonymi możemy wyrażenie to rozłożyć na iloczyn $p$ czynników.

Oznaczmy przez $\zeta_p$ liczbę zespoloną $\cos\frac{2\pi}{p} + i \sin\frac{2\pi}{p}$, wówczas $(\zeta_p)^p = 1$ i liczby

$$\zeta_p^0 = 1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$$

są wszystkimi zespolonymi pierwiastkami $p$-tego stopnia z 1.

Bardzo łatwo sprawdzić, korzystając z wzoru $(T-1)(T-\zeta_p) \ldots (T-\zeta_p^{p-1}) = T^p-1$, że

$$x^p+y^p = (x+y)(x+\zeta_p y) \ldots (x+\zeta_p^{p-1}y),$$

a zatem równanie Fermata możemy przepisać w postaci

$$(x+y)(x+\zeta_p y) \ldots (x+\zeta_p^{p-1}y) = z \cdot z \cdot \ldots \cdot z$$

Definicje pojęć o których mowa w artykule obok. *Pierścieniem* nazywamy zbiór $A$ wraz z określonymi w nim pewnymi działaniami $\oplus$ oraz $\bigcirc$ spełniającymi następujące warunki 1) „dodawanie" $\oplus$ jest przemienne, łączne i ma element neutralny, tj. taki $\Theta \in A$, że $a \oplus \Theta = a$ przy każdym $a \in A$. Ponadto równanie $a \oplus x = \Theta$ o niewiadomej $x \in A$ ma zawsze rozwiązanie — inaczej mówiąc każdy element $a$ zbioru $A$ ma „przeciwny"; 2) „mnożenie" jest łączne i przemienne; 3) „mnożenie" $\bigcirc$ jest rozdzielne względem „dodawania" $\oplus$:

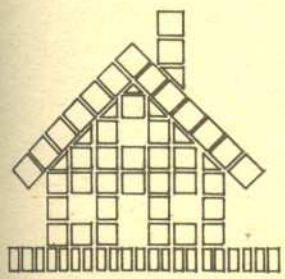
$$a \bigcirc (b \oplus c) = (a \bigcirc b) \oplus (a \bigcirc c),$$

przy dowolnych $a, b, c \in A$.

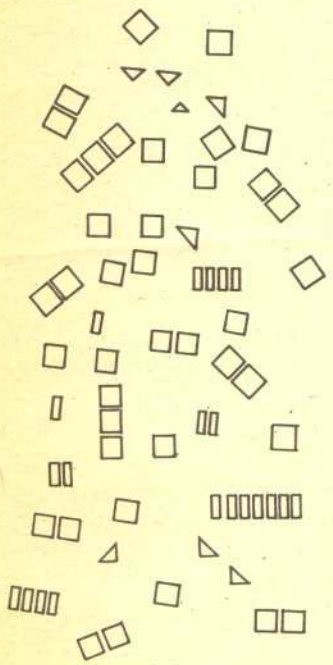
Podzbiór $I \subset A$ nazywa się *ideałem* pierścienia $A$, gdy jest zamknięty ze względu na „dodawanie" tj. $(a \in I, b \in I) \Rightarrow a \oplus b \in I$ oraz gdy spełnia jeszcze warunek $(a \in I, x \in A) \rightarrow a \bigcirc x \in I$.

Najważniejszymi przykładami pierścieni są pierścienie składające się z liczb; $A$ jest pewnym podzbiorem liczb zespolonych, zamkniętym ze względu na zwykłe dodawanie i zwykłe mnożenie liczb. Działania $\oplus$ i $\bigcirc$ określamy wtedy właśnie jako zwyczajne dodawanie i mnożenie. Zbiór liczb naturalnych nie tworzy pierścienia, tworzy go natomiast zbiór wszystkich liczb całkowitych, a także: zbiór $Z$ [i] złożony z liczb $m+ni$ (gdzie $m, n \in Z$), zbiór wszystkich liczb rzeczywistych, zbiór wszystkich liczb zespolonych. Ostatnie z wymienionych pierścieni są też *ciałami*. Tak nazywamy pierścienie $K$, w których „mnożenie" $\bigcirc$ ma też element neutralny $L$ przy czym $L \neq \Theta$ oraz każdy niezerowy element $a \in A$ ma „odwrotny": równanie $a \bigcirc x = L$ ma rozwiązanie dla każdego $a \neq \Theta$. Jeżeli w pierścieniu $A$ $a \bigcirc b = \Theta \Rightarrow a = \Theta$ lub $b = \Theta$ to $A$ nazywamy *dziedziną całkowitości*.

*„Jest niemożliwe rozłożyć sześcian na dwa sześciany, czwartą potęgę na dwie czwarte potęgi i ogólnie potęgę wyższą niż druga na dwie takie potęgi; znalazłem naprawdę zadziwiający dowód tego, jednak margines jest za mały, by go pomieścić".*



Rozwiązanie zadania M 259. Zauważmy, że ponieważ
$x^k - y^k = (x-y)(x^{k-1} + x^{k-2}y + \ldots + xy^{k-2} + y^{k-1})$
dla każdego $k \geqslant 1$, to $p(x) - p(y)$ jest podzielne przez $x-y$ dla każdej pary $x, y \in R$. Gdyby teraz $x_0$ było pierwiastkiem całkowitym wielomianu $p(x)$, to $x_0 - 0 \mid p(x_0) - p(0)$, czyli $x_0 \mid p(0)$ oraz $x_0 - 1 \mid p(x_0) - p(1)$, czyli $x_0 - 1 \mid p(1)$, co jest niemożliwe, ponieważ jedna z liczb $x_0$, $x_0 - 1$ jest parzysta, a zarówno $p(0)$ jak i $p(1)$ są nieparzyste, zgodnie z warunkami zadania. Otrzymana sprzeczność dowodzi, że $x_0$ nie może być pierwiastkiem $p$.



Rozwiązanie zadania M 261. Spośród wszystkich trójkątów o wierzchołkach leżących w wierzchołkach $W$ wybierzmy trójkąt $ABC$ o największym polu. Pokażemy, że jego środek ciężkości $S$ spełnia warunki zadania. Wiemy, że $J_S^{-1/2}(ABC) = A'B'C'$ gdzie $A'$, $B'$, $C'$ są odpowiednio środkami boków $BC$, $AC$ i $AB$. Gdyby teraz $D' = J_S^{-1/2}(D)$ leżał poza trójkątem $ABC$ dla pewnego wierzchołka $D$ wielokąta $W$, to moglibyśmy wskazać wierzchołek $ABC$ (np. $A$) taki, że $D'$ i $A$ leżą po przeciwnych stronach prostej $BC$. Wtedy jednak pole $(A'B'C') <$ pole $(B'C'D')$ i wobec tego pole $(BCD) >$ pole $(ABC)$ wbrew założeniu. Wobec tego obrazy wszystkich wierzchołków $W$ leżą w trójkącie $ABC$, a więc $J_S^{-1/2}(W) \subset ABC \subset W$. Gdy teraz $-\frac{1}{2} \leqslant t < 0$ to $J_S^t(W) \subset J_S^{-1/2}(W) \subset W$, c.b.d.o.

i otrzymujemy rozkład na czynniki należące do pierścienia $Z[\zeta_p]$ składającego się z liczb zespolonych postaci $a_0 + a_1\zeta_p + \ldots + a_{p-1}\zeta_p^{p-1}$, gdzie $a_0, a_1, \ldots, a_{p-1}$ są liczbami całkowitymi.

Liczby $x+y$ i $z$ powinny zatem mieć nietrywialny wspólny dzielnik, a więc ... Otóż nie! W rozumowaniu tym korzystamy bowiem z własności jednoznaczności rozkładu elementów pierścienia $Z[\zeta_p]$ na czynniki nierozkładalne. Wiele błędnych dowodów twierdzenia Fermata (m.in. Gaussa, Eulera, Lagrange'a i prawdopodobnie samego Fermata) polegało właśnie na przyjęciu za oczywistą jednoznaczności rozkładu tam, gdzie nie była ona wcale oczywistą, albo i w ogóle nie miała miejsca.

W XIX wieku najwięcej energii problemowi Fermata poświęcił matematyk niemiecki Ernst Eduard Kummer (1810—1893). Niemal przez całe życie starał się zrealizować ów „naturalny" pomysł — dowód hipotezy Fermata za pomocą rozkładów elementów na czynniki. Pierwszym, który zauważył, że w pewnych pierścieniach liczbowych nie obowiązuje twierdzenie o jednoznaczności rozkładu, był prawdopodobnie Peter Gustav Lejeune Dirichlet (1805—1859). Na przykład w pierścieniu $Z[\sqrt{-5}]$, złożonym z liczb zespolonych postaci $m + n\sqrt{-5} = m + n\sqrt{5}$ i, gdzie $m$, $n$ są całkowite, mamy $6 = 2 \cdot 3 = (1-\sqrt{-5})(1+\sqrt{-5})$ i wszystkie cztery wypisane czynniki są nierozkładalne w rozważanym pierścieniu. To odkrycie stanowiło wielki wstrząs dla Kummera: zawiódł go podstawowy pomysł. Nie załamując się jednak, podjął heroiczny wysiłek znalezienia jakiejś namiastki twierdzenia o jednoznacznym rozkładzie. Stworzył w tym celu pojęcie „idealnego czynnika" i nowatorsko spojrzał na samą relację podzielności. Przymiotnik „idealny" znaczy tu raczej „metafizyczny, duchowy" niż „doskonały". Owe nieziemskie, idealne liczby musiały być przede wszystkim dzielnikami liczb pierwszych całkowitych. Stąd i nazwa — przecież liczby pierwsze nie mają nietrywialnych dzielników w zakresie liczb całkowitych.

Aby opisać „idealne czynniki" Kummera prześledźmy najpierw prostą sytuację, jaka ma miejsce dla pierścienia liczb całkowitych $Z$. W dzisiejszej terminologii waluacją (nieархimedesową) pierścienia $A$ nazywamy określoną na $A$ funkcję $v$ o wartościach całkowitych oraz $\infty$ i taką, że

$$v(xy) = v(x) + v(y),$$

$$v(x+y) \geqslant \min\,(v(x), v(y))$$

dla niezerowych $x, y \in A$ oraz $v(1) = 0$, $v(0) = \infty$ (przyjmujemy, że zawsze $n + \infty = \infty$). Z każdą liczbą pierwszą $p$ można związać pewną waluację pierścienia liczb całkowitych, tzw. waluację $p$-adyczną $v_p$. Dla $n \neq 0$ przyjmujemy $v_p(n) = k$ wtedy i tylko wtedy, gdy $p^k$ dzieli $n$ oraz $p^{k+1}$ nie dzieli $n$. Dla każdej liczby całkowitej $n \neq 0$ istnieje więc tylko skończona ilość waluacji $p$-adycznych, których wartość na $n$ jest różna od zera. Na przykład dla liczby $n = 457380 = 2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^2$ mamy $v_2(n) = 2$, $v_3(n) = 3$, $v_5(n) = v_7(n) = 1$, $v_{11}(n) = 2$, a wszystkie pozostałe waluacje $p$-adyczne przyjmują na $n$ wartość 0. Każda liczba całkowita jest (z dokładnością do czynnika $\pm 1$ — są to jedyne elementy odwracalne w pierścieniu $Z$) wyznaczona przez podanie wartości wszystkich waluacji $p$-adycznych na niej. Dalej, nietrudno wykazać, że poza $p$-adycznymi (i ich wielokrotnościami) pierścień liczb całkowitych $Z$ ma tylko waluację trywialną $v_0$, $v_0(n) = 0$ dla $n \neq 0$.

Owe „idealne czynniki" Kummera były to właśnie waluacje pierścienia $Z[\zeta_p]$. Wykładnik, z jakim taki czynnik wchodzi w rozkład liczby $x \in Z[\zeta_p]$, to po prostu wartość na $x$ owej waluacji.

Ta konstrukcja Kummera jest jednym z najpiękniejszych przykładów abstrakcji — procesu oderwania się od „całkowitoliczbowego terytorium", spojrzenia na zagadnienie z ogólniejszego punktu widzenia (stworzenie arytmetyki pierścieni $Z[\zeta_p]$ — o czym za chwilę) oraz zastosowanie do wyjściowego problemu. W liście do Liouville'a Kummer pisał:

*„Zachęcony przez mojego przyjaciela, p. Lejeune Dirichleta, pozwalam sobie przesłać Panu kilka kopii dysertacji, jaką napisałem trzy lata temu, z okazji jubileuszu stulecia Uniwersytetu w Królewcu, jak również inną dysertację mego przyjaciela i ucznia p. Kroneckera, młodego i wybijającego się geometry. W tych pracach, które zechce Pan przyjąć jako wyraz mego głębokiego szacunku, znajduje się kilka rezultatów dotyczących pewnych zagadnień z teorii liczb zespolonych otrzymanych z pierwiastków z jedności, tj. pierwiastków równania $r^n = 1$, które to rezultaty były ostatnio przedmiotem dyskusji w Pańskiej prześwietnej Akademii, z okazji próby p. Lamé udowodnienia wielkiego twierdzenia Fermata. Co do elementarnego stwierdzenia o tych liczbach, że dowolna złożona liczba zespolona*

— Mówili coś o kolarzach?
— Tak, tak, przed chwilą. Ogromny peleton na czele. Nasi w czołówce. W telewizji właśnie mówili, że do Warszawy przyjadą na wpół do szóstej.
— Aha, to u nas będą koło wpół do piątej.
— Jadą, jadą!!
— Co, już? Dopiero $16^{15}$.
— Widocznie jadą dziś wolniej niż zwykle.
— Jak to? Wolniej jadą, a wcześniej przyjeżdżają?
— Och, zajrzyj na str. 16

*może być rozłożona na czynniki pierwsze w dokładnie jeden sposób, na brak którego zwraca Pan tak słusznie uwagę, a którego brak i w innych sytuacjach, mogę Pana zapewnić, że w ogólności nie jest ono prawdziwe dla liczb zespolonych postaci*

$$a_0 + a_1 r + a_2 r^2 + \ldots + a_{n-1} r^{n-1},$$

*ale można je uratować przez wprowadzenie nowego rodzaju liczb zespolonych, które nazwałem idealnymi liczbami zespolonymi. Wyniki moich badań w tym zakresie przedstawiłem Akademii w Berlinie i wydrukowane są one w sprawozdaniach z jej posiedzeń (marzec 1846); praca na ten sam temat pojawi się wkrótce w Journal für die reine und angewandte Mathematik. Już dawno temu rozpatrywałem zastosowania tej teorii do dowodu twierdzenia Fermata i udało mi się wyprowadzić nierozwiązalność równania $x^n + y^n = z^n$ z dwóch własności liczby pierwszej n, tak że pozostaje tylko zbadać, czy własności te przysługują wszystkim liczbom pierwszym. Gdyby te rezultaty wydawały się Panu godne zainteresowania, może Pan je znaleźć w sprawozdaniach Akademii Berlińskiej z bieżącego miesiąca".*

Dalsza metamorfoza pojęcia „liczby idealnej" dokonana została w pracach Dedekinda. Punktem wyjścia były dwie własności podzielności przez liczbę $p$: (i) jeśli $p$ dzieli $x$, to $p$ dzieli każdą wielokrotność $x$, (ii) jeśli $p$ dzieli $x$ i $y$, to $p$ dzieli $x+y$, które przysługiwały też „liczbom idealnym" Kummera. Richard Dedekind zauważył, że te dwie własności są najbardziej istotne przy badaniu relacji podzielności w sensie Kummera. Doprowadziło go to do ulepszenia pojęcia „idealnej liczby" przez zastąpienie tej „liczby" zbiorem liczb przez nią podzielnych — do sformułowania pojęcia ideału. W dodatku do książki Lejeune Dirichleta o teorii liczb (1871) Dedekind pisał:
... System $\mathfrak{a}$ nieskończonego zbioru liczb należących do $\mathfrak{o}$ [w dzisiejszej terminologii $\mathfrak{o}$ oznaczał dowolny pierścień liczbowy] nazywa się ideałem, jeżeli spełnia on dwa warunki:
1) suma i różnica dwóch liczb z $\mathfrak{a}$ znów jest liczbą z $\mathfrak{a}$;
2) każdy iloczyn liczby z $\mathfrak{a}$ przez liczbę z $\mathfrak{o}$ jest znów liczbą z $\mathfrak{a}$.
... Jeśli $\alpha$ należy do $\mathfrak{a}$ to powiemy, że $\mathfrak{a}$ dzieli $\alpha$, lub że $\mathfrak{a}$ wchodzi [jako czynnik] do $\alpha$ ...
Jeżeli wszystkie liczby pewnego ideału $\mathfrak{a}$ należą także do ideału $\mathfrak{b}$, to $\mathfrak{b}$ składa się z jednej lub kilku klas (mod $\mathfrak{a}$) i powiemy, że $\mathfrak{a}$ jest wielokrotnością $\mathfrak{b}$, albo że dzieli się przez $\mathfrak{b}$, a $\mathfrak{b}$ jest dzielnikiem $\mathfrak{a}$ lub, że wchodzi jako czynnik do $\mathfrak{a}$.
Ideał $\mathfrak{p}$, różny od $\mathfrak{o}$, który nie ma dzielników różnych od $\mathfrak{p}$ i od $\mathfrak{o}$, nazywa się ideałem pierwszym (dziś — maksymalnym).
Jeżeli ideał $\mathfrak{a}$ składa się z wielokrotności jednej ze swoich liczb $\alpha$, to taki ideał nazywa się głównym ...
Te określenia Dedekinda ostatecznie formalizują pojęcie „idealnego czynnika" Kummera i relację podzielności. Nietrudno sprawdzić, że w pierścieniu liczb całkowitych każdy ideał jest główny, że $\mathfrak{a} \subset \mathfrak{b}$ wtedy i tylko wtedy, gdy element $\alpha$ generujący ideał $\mathfrak{a}$ (tzn. $\mathfrak{a}$ składa się z wielokrotności $\alpha$) jest podzielny przez element $\beta$ generujący $\mathfrak{b}$; wreszcie, że ideałami pierwszymi są w tym pierścieniu dokładnie ideały generowane przez liczby pierwsze oraz ideał zerowy. Ponadto z każdą waluacją („idealnym czynnikiem") można związać jej ideał — złożony z tych liczb, na których waluacja przyjmuje wartości dodatnie. Odwrotnie — ideał pierwszy (niezerowy) wyznacza waluację. Zatem mówiąc w gruncie rzeczy o tym samym dochodzimy od mistycznych „idealnych czynników" Kummera (które miały „nieziemski byt" i decydowały o losach „niższych" liczb całkowitych) do sformalizowanego i bardzo prostego pojęcia ideału.
Bardzo łatwe do udowodnienia jest następujące twierdzenie:
*jeżeli każdy ideał dziedziny całkowitości jest główny, to w pierścieniu tym spełnione jest twierdzenie o jednoznaczności rozkładu.* Dla pierścieni postaci $Z[\zeta_p]$ prawdziwe jest także twierdzenie odwrotne: jeśli w pierścieniu takim spełnione jest twierdzenie o jednoznaczności rozkładu, to każdy ideał tego pierścienia jest główny.
Kummerowi potrzebny był jakiś sposób oceny, na ile w danym pierścieniu naruszone jest prawo jednoznaczności rozkładu (dokładniej pisał o tym w Delcie 9/1979 Władysław Narkiewicz). Kummer nazwał ideały $I$ oraz $J$ pierścienia $Z[\zeta_p]$ równoważnymi, o ile istnieją niezerowe elementy $r$, $s$ tego pierścienia takie, że $rI = sJ$. Wszystkie (niezerowe) ideały główne są więc równoważne. Ilość klas równoważności ideałów stanowi pewien miernik niejednoznaczności rozkładu w danym pierścieniu. Kummer udowodnił, że dla pierścieni $Z[\zeta_p]$ liczba klas równoważności ideałów jest skończona, a klasy te stanowią grupę (skończoną) ze względu na naturalne działanie mnożenia.

Analizując bardzo głębokie własności pierścieni $Z[\zeta_p]$ Kummer udowodnił wielkie twierdzenie Fermata dla tych liczb pierwszych $p$ występujących jako wykładniki, które nie dzielą liczby klas ideałów pierścieni $Z[\zeta_p]$. Takie liczby pierwsze są dziś nazywane regularnymi. O tym właśnie rezultacie wspominał w liście do Liouville'a.

Kummer znalazł wzory na liczbę klas ideałów pierścieni $Z[\zeta_p]$ oraz podał kryterium pozwalające rozstrzygać, czy dana liczba pierwsza jest regularna, czy nieregularna. Kryterium to wykorzystuje własności tzw. liczb Bernoulliego $B_0, B_1, B_2, \ldots$ Ten ciąg liczb określił Jacob Bernoulli (1713) jako kolejne współczynniki w szeregu potęgowym

$$\frac{x}{e^x-1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = 1 - \frac{1}{2}x + \frac{1}{6}\cdot\frac{x^2}{2!} - \frac{1}{30}\cdot\frac{x^4}{4!} + \frac{1}{42}\cdot\frac{x^6}{6!} - \ldots$$

Łatwo zauważyć, że $0 = B_3 = B_5 = B_7 = \ldots$, oraz wyprowadzić następujące wzory, pozwalające bezpośrednio wyliczyć kolejne wyrazy tego ciągu

$$B_0 = 1$$
$$\binom{2}{0}B_0 + \binom{2}{1}B_1 = 0$$
$$\binom{3}{0}B_0 + \binom{3}{1}B_1 + \binom{3}{2}B_2 = 0$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\binom{n+1}{0}B_0 + \binom{n+1}{1}B_1 + \ldots + \binom{n+1}{n}B_n = 0$$

(w tablicy tej można oczywiście opuścić składniki zawierające $B_3, B_5, B_7, \ldots$ jako równe zeru); liczby Bernoulliego są więc wymierne.

Zapowiedziane kryterium Kummera orzeka, że liczba pierwsza $p$ jest regularna wtedy i tylko wtedy, gdy $p$ nie dzieli liczników liczb Bernoulliego $B_2, B_4, B_6, \ldots, B_{p-3}$. Istnieje więc metoda pozwalająca sprawdzić, czy dana liczba pierwsza jest, czy nie jest regularna. W ten sposób sprawdzono, że np. wśród liczb pierwszych $< 100$ tylko 37, 59 i 67 nie są regularne (licznik liczby $B_{32}$ jest równy $-37 \cdot 208360028141$). Istnienie nieskończenie wielu liczb pierwszych nieregularnych wykazał Jensen w 1915 roku, a dotychczas nie wiadomo, czy liczb pierwszych regularnych jest nieskończenie wiele.

Choć nie należy to do głównego tematu, wspomnijmy prosty, ale ciekawy wynik Grunerta z 1856 roku: jeżeli dodatnie liczby całkowite $x, y, z$ spełniają równanie Fermata $x^p + y^p = z^p$, to $x, y$ i $z$ są większe od $p$. Można założyć, że $x > y$. Mamy oczywiście $z > x$, więc $x^p + y^p = z^p = [(z-x)+x]^p = x^p + px^{p-1}(z-x) + \ldots$ $\ldots + (z-x)^p > x^p + px^{p-1}$, więc $y^p > px^{p-1} > py^{p-1}$, skąd $y > p$.

Ponieważ $x > y$, więc także $x > p$, zatem $z > p$. Nierozwiązalność równania Fermata wykazana jest dziś dla wszystkich wykładników $p \leqslant 125000$ (Samuel Wagstaff, 1978). Jeżeli zatem jakieś rozwiązanie w ogóle istnieje, to $x > 125000$, a więc dla dojścia do tego rozwiązania musielibyśmy działać na liczbach co najmniej równych $125000^{125000} > 10^{637113}$. Mała jest wobec tego szansa, by na ewentualne rozwiązanie trafić przypadkiem lub przez systematyczne próby, nawet przy użyciu największych komputerów.

Jak to zwykle w matematyce bywa, wprowadzone przez Kummera i Dedekinda pojęcia pierścienia, ideału i grupy klas ideałów zaczęły żyć własnym życiem i — co rzadsze a ważniejsze — znalazły szerokie zastosowanie w innych działach matematyki. Przede wszystkim aż do początku XX wieku wszystkie rozpatrywane pierścienie i ciała były w gruncie rzeczy podciałami lub podpierścieniami ciała liczb zespolonych, bądź ciałami skończonymi. Rolę katalizatora w procesie dalszej (niezbędnej, jak dziś jasno widzimy) abstrakcji odegrały liczby $p$-adyczne (Delta pisała o nich np. w nr. 9/1978) wprowadzone przez Hensela, szeroko stosowane w teorii liczb. Pojęcie ideału stało się podstawowe dla nowoczesnej geometrii algebraicznej.

Przy badaniu pierścieni $Z[\zeta_p]$ Kummer natrafił na szczególnie prostą sytuację. Mówiąc współczesnym językiem powiedzielibyśmy, że rozpatrywał pewne pierścienie Dedekinda. Tak nazywamy dziś te dziedziny całkowitości $A$, w których: (1°) dla każdego ideału $I$ istnieje skończony zbiór generatorów (tzn. takie elementy $b_1, \ldots, b_s \in I$, że każdy element należący do $I$ ma postać $a_1b_1 + \ldots + a_sb_s$ dla pewnych $a_1, \ldots, a_s \in A$), (2°) żaden niezerowy ideał pierwszy (tzn. taki ideał $I$, że jeśli $a, b \in A \setminus I$ to $ab \in A \setminus I$) nie jest zawarty w ideale większym, różnym od $A$, (3°) jeżeli ułamek $a/b$ ($a, b \in A$) jest pierwiastkiem wielomianu o współczynnikach z $A$, którego współczynnik przy najwyższej potędze jest równy 1, to ułamek $a/b$ należy do $A$. Te trzy warunki, okazuje się, decydują o tym, że w takich pierścieniach można „uratować" nieco z własności jednoznaczności rozkładu.

Liczby Bernoulliego pojawiają się w wielu innych sytuacjach, zanotujemy tu tylko następujące wzory prawdziwe dla $|x| < \pi/2$ oraz dla dowolnych liczb naturalnych $m, n$

$$\operatorname{tg} x = \sum_{n=1}^{\infty} (-1)^{n-1} B_{2n} 2^{2n}(2^{2n}-1)\frac{x^{2n-1}}{2n!},$$

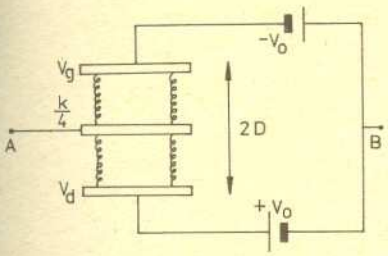
$$1^m + 2^m + 3^m + \ldots + n^m = \frac{n^{m+1}}{m+1} + \frac{n^m}{2} + \frac{1}{2}B_2\binom{m}{1}n^{m-1} + \frac{1}{4}B_4\binom{m}{3}n^{m-3} + \frac{1}{6}B_6\binom{m}{5}n^{m-5} + \ldots;$$

ostatni wyraz po prawej stronie zawiera $n$ lub $n^2$ w zależności od tego, czy $m$ jest parzyste, czy nieparzyste. Oto wartości niektórych liczb Bernoulliego: $B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$, $B_4 = -1/30$, $B_{16} = -3617/510$, $B_{32} = -7709321041217/510$, $B_{120} = -c_{113}/c_{10}$, $B_{122} = c_{107}/6$, gdzie $c_{113}$, $c_{10}$ i $c_{107}$ oznaczają pewne liczby naturalne o 113, 10, 107 cyfrach rozwinięcia dziesiętnego. Wiadomo, że $|B_4| < |B_6| < |B_8| < \ldots$ oraz $\lim_{n\to\infty} \{(-1)^{n-1}B_{2n}/[\sqrt{4\pi n}(n/\pi e)^{2n}]\} = 1$.

Teza twierdzenia Grunerta była tematem zadania nr 4 zawodów III stopnia XXII Olimpiady Matematycznej.

## Kondensator o ujemnej pojemności

Co to jest kondensator — każdy wie. Pojemność kondensatora jest większa od zera, gdyż ładunek i potencjał jednocześnie zmieniają znak. To oczywiste. Tak jednak być nie musi. Można skonstruować kondensator o ujemnej pojemności, tyle, że nie jest to już tak proste urządzenie. Oto ono




Nasz kondensator składa się z trzech płytek połączonych sprężynami, skrajne płytki są zamocowane, środkowa może się poruszać. Dwie baterie zapewniają różnicę potencjałów $V_g - V_d = 2V_0$. Tym samym pole między płytkami ma natężenie $\frac{V_0}{D}$. Jeśli teraz z końcówki $A$ dopłynie na płytkę środkową ładunek $+Q$, to płytka ta dotąd będzie przesuwać się w górę, aż sprężyny zrównoważą siłę elektrostatyczną:

$$k \cdot z = \frac{QV_0}{D} \quad \text{więc} \quad z = \frac{QV_0}{kD}.$$

Wtedy punkt $A$ będzie miał względem $B$ potencjał

$$V_A = -zE = -\frac{V_0^2}{kD^2}Q.$$

Czyli

$$C = -\frac{kD^2}{V_0^2} < 0.$$

Proponuję, by Czytelnik rozważył następujące problemy:

1. Jak zachowują się obwody $RC$, $LC$, $RLC$, gdy $C < 0$?
2. Jak zależy ruch środkowej płytki od częstości zmian napięcia $V_A$? Może warto dodać tłumik oscylacji?

*P. Amsterdamski*

Choć nie jest prawdą, że każdy element pierścienia Dedekinda rozkłada się jednoznacznie na iloczyn elementów nierozkładalnych, to jednak *każdy ideał pierścienia Dedekinda można jednoznacznie przedstawić w postaci iloczynu ideałów nierozkładalnych* (są nimi niezerowe ideały pierwsze). (Iloczynem ideałów $I$, $J$ jest ideał $IJ$ składający się z sum elementów postaci $ab$ gdzie $a \in I$, $b \in J$). Grupy klas pierścieni Dedekinda pojawiających się w teorii liczb były skończone — jak widzieliśmy, znaczy to, że „odchylenie" tych pierścieni Dedekinda od pierścieni z prawem jednoznaczności rozkładu nie jest duże.
W pewnym sensie końcową odpowiedź na pytanie, jak mogą się rozkładać elementy pierścienia Dedekinda, zawiera następujące twierdzenie L. Claborna z 1965 roku:
*każda przemienna grupa abelowa jest grupą klas ideałów pewnego pierścienia Dedekinda.*
Choć wiele na ten temat wiedzieli już Kummer, Dedekind, Kronecker oraz Gauss, dopiero niedawno wyjaśniono do końca, dla jakich liczb pierwszych $p$ pierścienie $Z[\zeta_p]$ mają własność jednoznacznego rozkładu. Jedynymi takimi liczbami są mianowicie 3, 5, 7, 11, 13, 17, 19.
Chociaż ani Kummerowi, ani nikomu innemu do tej pory nie udało się rozstrzygnąć wielkiego problemu Fermata, to jednak stworzone w tym celu pojęcia i metody przydały się i przydają się w całej niemal matematyce, a sztuczne z pozoru określenia wyrosły na bardzo konkretnej problematyce. Jest to jedyna właściwa droga rozwoju pojęć matematycznych.

# Czego nie wiemy o neutrinach? (II)

*Mgr Roman JUSZKIEWICZ*

## CZY NEUTRINA MAJĄ MASĘ?

Przekonanie o tym, że neutrina są cząstkami, pozbawionymi masy spoczynkowej, powstało w latach trzydziestych, kiedy to Wolfgang Pauli, aby uratować bilans energetyczny w reakcji

$$n \to p + e^- + \tilde{\nu}_e \qquad (1)$$

wprowadził hipotezę o ich istnieniu. Przekonanie to dotrwało praktycznie w stanie nienaruszonym do wiosny roku 1980, mimo że nikomu nie udało się podać doświadczalnego dowodu na to, że masa neutrina jest ściśle równa zeru. W roku 1958 Bruno Pontecorvo wysunął przypuszczenie, że jeżeli masa choćby jednego rodzaju neutrin, np. $\nu_e$, jest różna od zera, to powinny wystąpić „oscylacje neutrinowe", tj. przemiany typu $\nu_e \rightleftarrows \nu_\mu$, czy $\nu_e \rightleftarrows \nu_\tau$. Dobrą analogię takiego hipotetycznego procesu stanowią przejścia $K^0 \rightleftarrows \tilde{K}^0$, opisane w artykule M. Święckiego (Delta nr 5/1978). Okres oscylacji zależy od różnicy mas neutrin (z zasady nieoznaczoności wynika, że powinien być on odwrotnie proporcjonalny do tej różnicy). Obserwując takie oscylacje można byłoby zatem zmierzyć różnice mas poszczególnych gatunków neutrin. Całkowity brak oscylacji świadczyłby natomiast o tym, że wszystkie neutrina są cząstkami bezmasowymi. Istnieje również metoda, pozwalająca na bezpośrednie „zważenie" neutrina. Aby tego dokonać, należy zbadać rozkład energii kinetycznej elektronów, uwalnianych w reakcji typu (1). Badając ten rozkład, wyznaczyć można „brakującą" w bilansie energię, która została zużyta na wyprodukowanie masy spoczynkowej neutrina. Latem ubiegłego roku pojawiły się wiadomości, które wywołały prawdziwą sensację. Okazało się mianowicie, że wyniki badań, opartych na obu omówionych metodach, prowadzą do wniosku, że masa neutrina elektronowego jest różna od zera!
Doniesienia te pochodziły od F. Reinesa i C. Cowana z Uniwersytetu Kalifornijskiego, którzy stwierdzili występowanie oscylacji w strumieniu $\nu_e$ z reaktora jądrowego, oraz od W. Lubimowa i jego współpracowników z Instytutu Fizyki Teoretycznej i Doświadczalnej w Moskwie, którym udało się wyznaczyć masę neutrina elektronowego z rozkładu energii kinetycznej elektronów, uwolnionych podczas rozkładu trytu (tryt jest izotopem wodoru o jądrze zbudowanym z dwóch neutronów i jednego protonu). Wartość masy $\nu_e$, wyznaczona przez Lubimowa, wynosi $m(\nu_e) = 30$ eV. Wyniki tych doświadczeń należy jednak traktować z dużą ostrożnością. Zdaniem specjalistów, na ich powtórzenie (i ewentualne potwierdzenie) w innych laboratoriach oraz na usunięcie wszystkich wątpliwości potrzeba co najmniej dwóch lat. A na razie w wyniku naszej niepewności co do masy neutrina „na rozdrożu" znalazły się aż trzy dziedziny fizyki: teoria struktury wewnętrznej gwiazd, kosmologia i teoria oddziaływań cząstek elementarnych.
Jeżeli oscylacje neutrinowe rzeczywiście występują w przyrodzie, to „problem neutrin słonecznych" może uzyskać nieoczekiwanie proste wyjaśnienie. Mianowicie, jest możliwe, że strumień $\nu_e$, rejestrowany przez detektor Davisa stanowi 1/3 wartości przewidywanej przez