O kilku twierdzeniach elementarnej teorii liczb, czyli o tym, skąd się biorą grupy

Czesław BAGIŃSKI, Edmund R. PUCZYŁOWSKI

Pojęcie grupy funkcjonuje w matematyce od prawie 200 lat, a od pewnego czasu jest w niej wszechobecne. Praktycznie w każdym dziale matematyki jest wykorzystywane albo do klasyfikacji, albo do opisu strukturalnych własności obiektów, którymi się ten dział zajmuje. Samo narodzenie pojęcia grupy jest związane ze spektakularnym zastosowaniem go do ostatecznego wyjaśnienia kwestii rozwiązalności przez pierwiastniki równań postaci

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

gdzie $a_1, a_2, \ldots, a_{n-1}$ są liczbami wymiernymi. Dokonał tego zaledwie dwudziestoletni Evariste Galois w 1832 roku. Przez kilkanaście lat osiągnięcie Galois było niedostrzeżone i niedocenione. Nie znaleziono również zadowalającego sposobu przejrzystego przedstawienia rezultatu Galois w krótkim artykule adresowanym do szerokiego audytorium. W tym artykule my również tego nie zrobimy. Chcemy natomiast opowiedzieć o kilku podstawowych twierdzeniach teorii liczb, a właściwie ich dowodach, z których pojęcie grupy (co prawda tylko abelowej) w naturalny sposób samo się wyłania. Odkrycie tych twierdzeń na wiele lat poprzedziło wyniki Galois i mogły się one wydać współczesnym jako obserwacje z pogranicza magii i świata rzeczywistego. Omówimy te wyniki, zanim zdefiniujemy pojęcie grupy.

Wszystkie dalej rozpatrywane liczby są całkowite, natomiast napis $a \mid b$ oznacza, że $a \neq 0$ i a jest dzielnikiem liczby b.

W drugiej połowie osiemnastego wieku John Wilson (matematyk angielski, 1741–1793) zauważył następującą zależność, nazwaną potem twierdzeniem Wilsona. (Uważa się, że tę zależność znał wiele lat wcześniej W.G. Leibniz, 1646–1716.)

Twierdzenie Wilsona.
Dla dowolnej liczby pierwszej p

$$p \mid (p-1)! + 1.$$

Twierdzenie zostało opublikowane po raz pierwszy przez E. Waringa, ale ani Waring, ani Wilson nie znali jego dowodu. Pierwszy dowód został podany przez J.L. Lagrange'a w 1773 roku.

Lagrange udowodnił również twierdzenie odwrotne: *Jeżeli $m > 1$ jest dzielnikiem liczby $(m-1)! + 1$, to m jest liczbą pierwszą.*

Ponad sto lat wcześniej P. Fermat poczynił nie mniej interesującą obserwację:

Małe Twierdzenie Fermata.
Dla dowolnej liczby pierwszej p i dowolnej liczby całkowitej n

$$p \mid n^p - n.$$

Aby udowodnić twierdzenie Wilsona, należy wykazać, że reszta z dzielenia $(p-1)!$ przez p jest równa $p-1$. Z kolei w przypadku twierdzenia Fermata wystarczy wykazać, iż dla dowolnej liczby a, takiej że $1 \leqslant a \leqslant p-1$, reszta z dzielenia a^{p-1} przez p jest równa 1. W dowodach obu faktów wykorzystamy działanie $\odot$ – iloczyn w kółku, jakie wprowadzamy w zbiorze liczb

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

Przyjmujemy mianowicie, że dla dowolnych $a, b \in \mathbb{Z}_p^*$

$$a \odot b = \text{reszta z dzielenia } a \cdot b \text{ przez } p.$$

Nietrudno zauważyć, że dla dowolnych $a, b, c \in \mathbb{Z}_p^*$,

i) $1 \odot a = a$,

ii) $a \odot b = b \odot a$,

iii) $(a \odot b) \odot c = a \odot (b \odot c)$.

Trzecia z tych własności pozwala opuszczać nawiasy w wyrażeniach, które są iloczynami w kółku liczb naturalnych mniejszych od p, natomiast druga – przestawiać ich kolejność.

Zajmiemy się najpierw twierdzeniem Wilsona dla $p = 11$. Mamy wykazać, że $1 \odot 2 \odot 3 \odot \ldots \odot 10 = 10$. Moglibyśmy liczyć kolejno: $1 \odot 2 = 2$, $2 \odot 3 = 6$, $6 \odot 4 = 2$, itd. Wygodniej jest jednak zauważyć, że

$$1 \odot 2 \odot 3 \odot \ldots \odot 10 =$$

$$= 1 \odot (2 \odot 6) \odot (3 \odot 4) \odot (5 \odot 9) \odot (7 \odot 8) \odot 10,$$

i że wyrażenia w nawiasach są równe 1. Stąd natychmiast otrzymujemy, że $1 \odot 2 \odot 3 \odot \ldots \odot 10 = 10$ i dowód jest zakończony.

Podobną metodę można zastosować dla dowolnego p.

Zauważmy, że jeśli $1 \leqslant i < j \leqslant p-1$, to dla dowolnego a, jeśli $1 \leqslant a \leqslant p-1$, to liczba $a(j-i)$ nie jest podzielna przez p. Wynika stąd, że $a \odot i \neq a \odot j$. Zatem, jeśli i przebiega wszystkie liczby od 1 do $p-1$, to również $a \odot i$ przebiega te liczby (tyle że dla $a \neq 1$ w innej kolejności). W efekcie:

iv) dla dowolnego a, jeśli $1 \leqslant a \leqslant p-1$, to istnieje a', takie że $1 \leqslant a' \leqslant p-1$ oraz $a \odot a' = 1$.

Takie a' jest tylko jedno. Istotnie, jeśli $a \odot a'' = 1$, to $a'' = a'' \odot 1 = a'' \odot (a \odot a') = (a'' \odot a) \odot a' = 1 \odot a' = a'$. Zauważmy ponadto, że $a \odot a = 1$ wtedy i tylko wtedy, gdy $p \mid a^2 - 1 = (a-1)(a+1)$. Zatem $a \odot a = 1$ wtedy i tylko wtedy, gdy $a = 1$ lub $a = p-1$. Wynika stąd, że podobnie, jak dla $p = 11$, zbiór $\{2, 3, \ldots, p-2\}$ można rozbić na pary różnych liczb w ten sposób, że dla dowolnej z par a, b, $a \odot b = 1$. W rezultacie otrzymujemy $1 \odot 2 \odot 3 \odot \ldots \odot (p-1) = p-1$ i twierdzenie Wilsona zostało udowodnione.

Niech teraz a będzie dowolną liczbą naturalną mniejszą od p. Jak zauważyliśmy,

$$\{a \odot 1, a \odot 2, \ldots, a \odot (p-1)\} = \{1, 2, \ldots, p-1\}.$$

Zatem

$$\underbrace{(a \odot a \odot \ldots \odot a)}_{p-1 \text{ razy}} \odot (1 \odot 2 \odot \ldots \odot (p-1)) =$$

$$= (a \odot 1) \odot (a \odot 2) \odot \ldots \odot (a \odot (p-1)) =$$

$$= 1 \odot 2 \odot \cdots \odot (p-1)$$

i dalej, korzystając z twierdzenia Wilsona, otrzymujemy

$$\underbrace{(a \odot a \odot \cdots \odot a)}_{p-1 \text{ razy}} \odot (p-1) = p-1,$$

co z kolei po obustronnym pomnożeniu tej równości przez $p-1$ daje

$$\underbrace{(a \odot a \odot \cdots \odot a)}_{p-1 \text{ razy}} \odot (p-1) \odot (p-1) =$$

$$= (p-1) \odot (p-1) = 1.$$

Zatem reszta z dzielenia a^{p-1} przez p jest równa 1, co dowodzi Małego Twierdzenia Fermata.

Pierwszy pełny dowód Małego Twierdzenia Fermata przedstawił L. Euler (1707–1783), czyniąc znacznie ogólniejszą obserwację, której dowód można przeprowadzić tak samo, jak dowód twierdzenia Fermata z dokładnością do pewnych szczegółów. Niech mianowicie m będzie dowolną liczbą naturalną, $m \geqslant 2$. Niech ponadto $\mathbb{Z}_m^*$ będzie zbiorem wszystkich liczb naturalnych mniejszych od m i względnie pierwszych z m, np.

$$\mathbb{Z}_6^* = \{1,5\}, \qquad \mathbb{Z}_7^* = \{1,2,3,4,5,6\},$$

$$\mathbb{Z}_8^* = \{1,3,5,7\}, \quad \mathbb{Z}_9^* = \{1,2,4,5,7,8\}.$$

Na koniec, niech $\varphi(m)$ będzie liczbą elementów zbioru $\mathbb{Z}_m^*$.

Wartości funkcji φ dla małych m są podane w poniższej tabeli.

m	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\varphi(m)$	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

Wówczas zachodzi następujące twierdzenie:

Twierdzenie Eulera.
Dla dowolnej liczby naturalnej a względnie pierwszej z m

$$m \mid a^{\varphi(m)} - 1.$$

Zauważmy, że Małe Twierdzenie Fermata jest szczególnym przypadkiem twierdzenia Eulera. Jeśli bowiem założymy, że $m = p$ jest liczbą pierwszą, to $\varphi(p) = p-1$ (bo przecież $\mathbb{Z}_p^* = \{1,2,3,\ldots,p-1\}$) i otrzymujemy dokładnie treść Małego Twierdzenia Fermata.

Aby udowodnić twierdzenie Eulera, wprowadzimy w zbiorze $\mathbb{Z}_m^*$ działanie, które dla wygody oznaczymy tak samo, jak działanie rozważane wyżej.

Dla różnych wartości m definiowane działania są różne, dlatego bardziej właściwe byłoby oznaczenie go symbolem $\odot_m$

Przyjmiemy mianowicie, że

$$a \odot b = \text{reszta z dzielenia } a \cdot b \text{ przez } m,$$

dla dowolnych $a, b \in \mathbb{Z}_m^*$.

Można łatwo sprawdzić, a jeszcze łatwiej uwierzyć, że to działanie również spełnia warunki i)–iii). Podobnie jak wyżej, sprawdzimy, że spełnia ono także warunek iv). Niech mianowicie $a \in \mathbb{Z}_m^*$. Powtarzając rozumowanie przeprowadzone dla $m = p$, otrzymujemy, że dla $i, j \in \mathbb{Z}_m^*$, $i \neq j$ mamy $a \odot i \neq a \odot j$. Jeżeli zatem $\mathbb{Z}_m^* = \{b_1, \ldots, b_{\varphi(m)}\}$, to

$$\{a \odot b_1, \ldots, a \odot b_{\varphi(m)}\} = \{b_1, \ldots, b_{\varphi(m)}\}.$$

Stąd wynika więc, że istnieje takie $b \in \mathbb{Z}_m^*$, że $a \odot b = 1$, tzn. spełniony jest warunek iv). Mamy ponadto

$$\underbrace{a \odot a \odot \cdots \odot a)}_{\varphi(m) \text{ razy}} \odot (b_1 \odot b_2 \odot \cdots \odot b_{\varphi(m)}) =$$

$$= (b \odot b_1) \odot (b \odot b_2) \odot \cdots \odot (b \odot b_{\varphi(m)}) =$$

$$= b_1 \odot b_2 \odot \cdots \odot b_{\varphi(m)}.$$

Teraz będziemy rozumowali nieco ogólniej niż w dowodzie twierdzenia Fermata. Oznaczmy, mianowicie, przez b prawą stronę ostatniej równości. Mamy więc

$$\underbrace{(a \odot a \odot \cdots \odot a)}_{\varphi(m) \text{ razy}} \odot b = b$$

Na podstawie własności iv) istnieje takie $c \in \mathbb{Z}_m^*$, że $b \odot c = 1$. Jeżeli zatem pomnożymy ostatnią równość stronami przez c, to otrzymamy:

$$\underbrace{(a \odot a \odot \cdots \odot a)}_{\varphi(m) \text{ razy}} \odot (b \odot c) = b \odot c = 1.$$

Zatem reszta z dzielenia $a^{\varphi(m)}$ przez p jest równa 1, co dowodzi twierdzenia Eulera.

Powróćmy na chwilę do twierdzenia Wilsona. Jest ono równoważne temu, że iloczyn w kółku wszystkich elementów z $\mathbb{Z}_p^*$ jest równy $p-1$. Nie jest to prawda, jeśli zastąpimy p dowolną liczbą naturalną m. Rzeczywiście w $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$ mamy

$$1 \odot 2 \odot 4 \odot 7 \odot 8 \odot 11 \odot 13 \odot 14 =$$

$$= (2 \odot 8) \odot (4 \odot 11 \odot 14) \odot (7 \odot 13) = 1.$$

Przyczyną tego jest fakt, że na ogół w $\mathbb{Z}_m^*$ oprócz 1 i $m-1$ istnieją jeszcze inne elementy spełniające warunek $a \odot a = 1$. W $\mathbb{Z}_{15}^*$ są nimi liczby 4 i 11. Zauważmy jednak, że jeśli $\mathbb{Z}_m^* = \{b_1, \ldots, b_{\varphi(m)}\}$, to

$$\left(b_1 \odot b_2 \odot \cdots \odot b_{\varphi(m)}\right) \odot \left(b_1 \odot b_2 \odot \cdots \odot b_{\varphi(m)}\right) = 1.$$

Istotnie, każdy element z wyrażenia w lewym nawiasie można zestawić z elementem z prawego nawiasu tak, aby w iloczynie z nim otrzymać 1. Z tego otrzymujemy

Twierdzenie.
Niech $m > 1$ będzie dowolną liczbą naturalną, natomiast a niech będzie iloczynem wszystkich liczb względnie pierwszych z liczbą m, mniejszych od m. Wówczas

$$m \mid a^2 - 1.$$

Z rozważanych przykładów widać przydatność mnożenia w kółku przy odkrywaniu wielu interesujących własności liczb naturalnych

i ogólniej, całkowitych. Naturalnie, pojawiają się też różne pytania. Oto kilka przykładów.

(a) *Dla jakich liczb naturalnych $n \geqslant 2$ wszystkie elementy zbioru $\mathbb{Z}_n^*$ spełniają warunek $a \odot a = 1$?*

Jest to jedno z 36 zadań-kandydatów wyselekcjonowanych do XLI Międzynarodowej Olimpiady Matematycznej.

(b) *Udowodnić, że dla dowolnej liczby $a \in \mathbb{Z}_{16}^*$ $a \odot a \odot a \odot a = 1$.*

Odpowiedzi na te pytania wraz z Małym Twierdzeniem Fermata oraz pewnymi dodatkowymi argumentami pozwalają wyprowadzić następujące własności liczb naturalnych:

1. Niech m będzie taką liczbą naturalną, że $m \mid a^2 - 1$ dla dowolnej liczby naturalnej a względnie pierwszej z liczbą m. Wówczas m jest dzielnikiem liczby 24.
2. Jeżeli p jest liczbą pierwszą większą od 5, to $240 \mid p^4 - 1$.

Zachęcamy Czytelników do udowodnienia tych własności.

Elementy zbioru $\mathbb{Z}_m^*$ reprezentują wszystkie liczby całkowite względnie pierwsze z m, są w jakimś sensie „cieniami" tych liczb. Działanie mnożenia w kółku, którego własności i)–iv) wykorzystywaliśmy wyżej, jest w pewnym sensie „cieniem" zwykłej operacji mnożenia liczb całkowitych. Własności zbioru i tego działania ujawniają pewną ogólną strukturalną własność zbioru liczb całkowitych i poszczególnych liczb. Zbiór $\mathbb{Z}_m^*$ wraz z działaniem $\odot$ jest przykładem grupy.

Mówiąc ogólnie, **grupę** można zdefiniować jako niepusty zbiór G z działaniem $\circ$, spełniającym warunki

łączności:

(1) $\qquad \forall_{x,y,z \in G}\ (x \circ y) \circ z = x \circ (y \circ z);$

istnienia elementu neutralnego:

(2) $\qquad \exists_{e \in G} \forall_{x \in G}\ e \circ x = x \circ e = x;$

odwracalności każdego elementu:

(3) $\qquad \forall_{x \in G} \exists_{y \in G}\ x \circ y = y \circ x = e.$

Jeżeli do tych warunków dorzucimy jeszcze

przemienność działania:

(4) $\qquad \forall_{x,y \in G}\ x \circ y = y \circ x;$

otrzymamy grupę nazywaną **grupą abelową** albo przemienną. Zbiór $\mathbb{Z}_p^*$ z działaniem $\odot$ jest właśnie grupą przemienną.

Najprostszymi przykładami grup abelowych są:

- zbiór $\mathbb{Z}$ liczb całkowitych ze zwykłym działaniem dodawania;
- dla dowolnej liczby naturalnej n zbiór $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ z działaniem $a \oplus_n b =$ reszta z dzielenia $a + b$ przez n.

Nieco trudniejszą do zauważenia jest obserwacja, że grupą abelową jest również zbiór wszystkich podzbiorów ustalonego zbioru X z działaniem

$$A \div B = (A \cup B) \setminus (A \cap B).$$

Grupa jest obiektem o bardzo regularnej strukturze wewnętrznej, dlatego stwierdzenie, że jakieś działanie wprowadza w ustalonym zbiorze strukturę grupy, niesie istotną informację, której odkrycie metodami elementarnymi bywa trudne.

⋆ ⋆ ⋆

Nasze rozważania kończymy kilkoma zadaniami, wśród których można znaleźć i takie, które powyższe zagadnienia ilustrują.

1. Udowodnić Małe Twierdzenie Fermata przez indukcję ze względu na n i wyprowadzić stąd, w inny sposób, niż przedstawiono w artykule, że dla dowolnej liczby pierwszej p, zbiór Z_p^* jest grupą ze względu na działanie $\odot$.

2. Udowodnić, że niepusty podzbiór X zbioru $\mathbb{Z}$ jest grupą ze względu na dodawanie wtedy i tylko wtedy, gdy dla pewnej nieujemnej liczby całkowitej n, mamy

$$X = \{n \cdot x :\ x \in \mathbb{Z}\}.$$

3. a) Udowodnić, że dla dowolnych liczb naturalnych m, n zbiór

$$\{n \cdot x + m \cdot y :\ x, y \in \mathbb{Z}\}$$

jest grupą ze względu na dodawanie.

b) Na podstawie zadania 2 udowodnić, że istnieją takie liczby całkowite x, y, że $n \cdot x + m \cdot y$ jest największym wspólnym dzielnikiem liczb m i n.

4. Niech n będzie ustaloną liczbą naturalną, $n > 1$.

a) Udowodnić, że zbiór

$$\{a \in \mathbb{Z}_n^* :\ n \mid a^2 - 1\}$$

jest grupą ze względu na działanie $\odot_n$. Udowodnić, że liczba elementów tej grupy jest potęgą liczby 2.

b) Udowodnić analogiczne fakty dla elementów zbioru $\mathbb{Z}_n^*$ spełniających warunek

$$n \mid a^3 - 1.$$

5. (VI Międzynarodowa Olimpiada Matematyczna)

a) Wyznaczyć wszystkie liczby naturalne n, dla których

$$7 \mid 2^n - 1.$$

b) Udowodnić, że nie istnieje liczba naturalna n, dla której

$$7 \mid 2^n + 1.$$