Jest to tekst związany z odczytem wygłoszonym na XLVIII Szkole Matematyki Poglądowej, *Skojarzenia i analogie*, Otwock–Śródborów, styczeń 2012.

Grupy i matematyka szkolna

Kamila MURASZKOWSKA, Edmund PUCZYŁOWSKI, Warszawa

Pojęcie grupy wyłoniło się w długim procesie jako synteza różnych rozumowań, których celem było rozwiązanie konkretnych problemów. Wysławiają się one elementarnie, w języku współczesnej matematyki szkolnej. Kiedyś były jednak problemami, z którymi zmagały się najtęższe umysły i to właśnie im zawdzięczamy wypracowanie pojęć i metod, dzięki którym dzisiaj można wiele tego typu problemów bez trudu rozwiązywać. Powiemy tutaj o kilku z tych problemów. Mamy nadzieję, że one jak i inne przykłady, pokażą jak pojęcie grupy i pewne elementarne jego własności, mogą być użyteczne. Zaczniemy od definicji grupy w postaci, w której ono obecnie funkcjonuje oraz wysłowienia kilku ogólnych jego własności, a następnie pokażemy jak tę wiedzę można wykorzystywać w różnych sytuacjach. W ostatniej części podajemy pewną ilość zadań, na których można samodzielnie przećwiczyć przedstawione informacje.

1. Grupy i ich własności

Grupą nazywamy zbiór G z działaniem „$\circ$”, które każdej uporządkowanej parze elementów a, b należących do G przyporządkowuje element $a \circ b$ z G w taki sposób, że spełnione są warunki:

(1) dla dowolnych a, b, $c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$ (łączność działania),

(2) istnieje taki element $e \in G$, że $g \circ e = e \circ g = g$ dla dowolnego elementu g z G (e nazywamy elementem neutralnym),

(3) dla każdego elementu g z G istnieje taki, element oznaczany przez g^{-1}, że $g \circ g^{-1} = g^{-1} \circ g = e$ (g^{-1} nazywamy elementem odwrotnym do g).

Grupą jest więc para: niepusty zbiór i określone na nim działanie spełniające powyższe warunki. Często jednak wskazujemy tylko zbiór, pamiętając, że słowo grupa mówi też o działaniu. W sytuacjach ogólnych to działanie będziemy oznaczali $\circ$, a w konkretnych przykładach je wskażemy.

Podgrupą grupy G nazywamy dowolny niepusty podzbiór H tej grupy, który jest zamknięty na działanie „$\circ$” oraz na branie elementu odwrotnego względem tego działania, tzn. jeśli h_1, $h_2 \in H$, to również h_1^{-1}, h_2^{-1}, $h_1 \circ h_2 \in H$.

Moc zbioru X oznaczamy $|X|$. W przypadku, gdy X jest grupą lub podgrupą pewnej grupy, $|X|$ nazywamy jej rzędem.

Pojęcia grupy i podgrupy są więc bardzo ogólne, a ich przykłady pojawiają się w bardzo wielu sytuacjach. Z drugiej strony, warunki w definicji są na tyle mocne, że pozwalają uchwycić dość istotne zależności, które zastosowane w konkretnych przykładach, prowadzą do niebanalnych wniosków. Jedną z najogólniejszych własności grup opisuje twierdzenie Lagrange'a. Będzie ono odgrywało kluczową rolę w przedstawionych w następnej części zastosowaniach.

Twierdzenie (Lagrange'a)**.** *Jeśli H jest podgrupą grupy skończonej G, to $|H|$ dzieli $|G|$.*

Idea dowodu tego twierdzenia jest bardzo prosta. Opiera się na obserwacji, że zbiory postaci $g \circ H = \{g \circ h \mid h \in H\}$ są rozłączne lub się pokrywają i, że są one równoliczne z H.

W dalszych rozważaniach będziemy wykorzystywali pewien szczególny przypadek twierdzenia Lagrange'a. Niech G będzie grupą skończoną, a g jej dowolnym elementem. Wtedy istnieje taka liczba naturalna k, że element $\underbrace{g \circ \ldots \circ g}_{k}$, oznaczany w skrócie g^k i nazywany k-tą potęgą g, jest równy elementowi neutralnemu e grupy G. Istotnie, ponieważ grupa G jest skończona, dla pewnych liczb naturalnych $l < m$ mamy $g^m = g^l$. Ale wtedy

$$g^{m-l} = g^m \circ (g^{-1})^l = g^l \circ (g^{-1})^l = e.$$

Najmniejszą taką liczbę naturalną k, że $g^k = e$ nazywamy rzędem elementu g i oznaczamy $o(g)$. Jest jasne, że elementy e, g, g^2, ..., $g^{o(g)-1}$ są parami różne oraz $\{e, g, g^2, \ldots, g^{o(g)-1}\}$ jest podgrupą grupy G (nazywa się ją podgrupą generowaną przez g i oznacza (g)). Zatem $|(g)| = o(g)$ i na mocy twierdzenia Lagrange'a $o(g)$ jest dzielnikiem $|G|$. Zauważmy jeszcze, że jeśli dla pewnej liczby całkowitej m, $g^m = e$, to $o(g)$ dzieli m. Mianowicie, dzieląc m przez $o(g)$ z resztą, otrzymamy, że $m = ko(g) + r$, gdzie k, r są liczbami całkowitymi oraz $0 \leqslant r < o(g)$. Teraz $g^m = (g^{o(g)})^k \cdot g^r = g^r$. Z minimalności $o(g)$ dostajemy, że $r = 0$ czyli, że $o(g)$ dzieli m. Wynika stąd w szczególności, że $g^{|G|} = e$.

2. Przykłady grup i ich zastosowań

W tej części podamy przykłady różnych grup i ich podgrup, które wykorzystamy w dowodach faktów, które mają elementarne sformułowania w języku matematyki szkolnej, ale które wcale nie są proste. Są wśród nich problemy, z którymi zmagali się najwybitniejsi matematycy.

1. Liniowe równania diofantyczne.

Jedną z najprostszych grup jest zbiór liczb całkowitych $\mathbb{Z}$ z działaniem $+$ dodawania tych liczb. Bez trudu zauważamy, że dla dowolnej liczby całkowitej nieujemnej m zbiór $m\mathbb{Z}$ wszystkich liczb całkowitych, które są wielokrotnościami m, jest podgrupą grupy $\mathbb{Z}$. Nietrudno też zauważyć, że dowolna podgrupa H grupy $\mathbb{Z}$ jest tej postaci. Jest to oczywiste w przypadku gdy $H = \{0\}$. Gdy H zawiera liczbę niezerową a, to zawiera też liczbę $-a$. Zatem H zawiera liczbę naturalną. Niech m będzie najmniejszą liczbą naturalną w H. Dowolną liczbę h należącą do H można zapisać w postaci $h = km + r$, gdzie k jest pewną liczbą całkowitą zaś r liczbą całkowitą nieujemną mniejszą od m. Ponieważ H jest podgrupą $\mathbb{Z}$, więc $r = h - km$ należy do H. Z minimalności m wynika więc, że $r = 0$. W efekcie $H = m\mathbb{Z}$.

Pokażemy jak ten fakt można wykorzystać w analizie rozwiązań liniowych równań diofantycznych.

Linowym równaniem diofantycznym nazywa się równanie postaci

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b,$$

gdzie a_1, a_2, ..., a_n, b są liczbami naturalnymi i gdy pytamy o rozwiązania takiego równania w liczbach całkowitych.

Następujące twierdzenie podaje warunki rozwiązalności takiego równania.

Twierdzenie. *Liniowe równanie diofantyczne*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

ma rozwiązanie wtedy i tylko wtedy, gdy największy wspólny dzielnik liczb a_1, a_2, ..., a_n *jest dzielnikiem* b.

Jasne jest, że jeśli równanie ma rozwiązanie w liczbach całkowitych, to największy wspólny dzielnik liczb a_1, a_2, ..., a_n musi dzielić b. Nietrudno też zauważyć, że by udowodnić implikację przeciwną wystarczy wykazać, że jeśli a_1, a_2, ..., a_n są liczbami względnie pierwszymi, to równanie

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = 1$$

ma rozwiązanie w liczbach całkowitych. Pokażemy jak wynika to z opisu podgrup grupy $\mathbb{Z}$.

Zauważmy, że zbiór $H = \{a_1t_1 + a_2t_2 + \ldots + a_nt_n \mid t_1, t_2, \ldots, t_n \in \mathbb{Z}\}$ jest podgrupą grupy $\mathbb{Z}$. Zatem istnieje taka liczba naturalna m, że $H = m\mathbb{Z}$. Oczywiście $m \in H$, więc $m = a_1t_1 + a_2t_2 + \ldots + a_nt_n$ dla pewnych liczb całkowitych t_1, t_2, ..., t_n. Z drugiej strony wszystkie a_i należą do H (bo $a_i = a_1 \cdot 0 + a_2 \cdot 0 + \ldots + a_i \cdot 1 + a_{i+1} \cdot 0 + \ldots + a_n \cdot 0$), więc wszystkie one dzielą się przez m. Założyliśmy jednak, że a_i są liczbami względnie pierwszymi, więc $m = 1$.

2. Twierdzenia Eulera, małe Fermata i Wilsona.

Niech n będzie liczbą naturalną i niech $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. W zbiorze $\mathbb{Z}_n$ określmy działania $a \oplus b =$ reszta z dzielenia $a + b$ przez n. Bez trudu sprawdzamy, że $\mathbb{Z}_n$ jest grupą ze względu na to działanie. Elementem neutralnym jest w tym przypadku 0, a elementem odwrotnym do danego elementu $k \in \mathbb{Z}_n$ jest $n - k$.

Wprowadźmy też w $\mathbb{Z}_n$ działanie $a \odot b =$ reszta z dzielenia ab przez n. Jest to działanie łączne i 1 jest elementem neutralnym, ale nie dla każdego elementu z $\mathbb{Z}_n$ istnieje element odwrotny względem tego działania. Zatem $\mathbb{Z}_n$ nie jest grupą ze względu na to działanie. Zauważmy jednak, że jeśli a, $b \in \mathbb{Z}_n$ są liczbami względnie pierwszymi z n, to również $a \odot b$ jest liczbą względnie pierwszą z n. Zauważmy też, że jeśli $k \in \mathbb{Z}_n$ jest liczbą względnie pierwszą z n, to dla dowolnej różnej od 0 liczby $l \in \mathbb{Z}_n$, $k \odot l \neq 0$. Zatem jeśli $l_1, l_2 \in \mathbb{Z}_n$ oraz $l_1 < l_2$, to $k \odot (l_2 - l_1) \neq 0$, a stąd wynika, że $k \odot l_1 \neq k \odot l_2$. W efekcie podzbiór $\{k \odot l \mid l \in \mathbb{Z}_n\}$ zbioru $\mathbb{Z}_n$ jest n-elementowy, więc jest równy $\mathbb{Z}_n$. Zatem istnieje takie $l \in \mathbb{Z}_n$, że $k \odot l = 1$. Oczywiście l jest liczbą względnie pierwszą z n. Wynika stąd, że zbiór $\mathbb{Z}_n^*$ liczb należących do $\mathbb{Z}_n$, które są względnie pierwsze z n, jest grupą ze względu na działanie $\odot$.

Mamy $|\mathbb{Z}_n^*| = \phi(n)$, gdzie $\phi(n)$ jest liczbą liczb, które są mniejsze od n i są z n względnie pierwsze. Z twierdzenia Lagrange'a wynika więc, że dowolny element z $\mathbb{Z}_n^*$ w potędze $\phi(n)$ jest równy 1. W efekcie uzyskujemy:

Twierdzenie (Eulera)**.** *Dla dowolnych względnie pierwszych liczb naturalnych n, k liczba $k^{\phi(n)} - 1$ jest podzielną przez n.*

Jeśli p jest liczbą pierwszą, to $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ i $\phi(p) = p - 1$. Stosując więc w tym przypadku twierdzenia Eulera otrzymujemy:

Twierdzenie (małe Fermata)**.** *Jeśli p jest liczbą pierwszą, zaś k liczbą naturalną, która nie dzieli się przez p, to liczba $k^{p-1} - 1$ jest podzielna przez p.*

Uwaga. Małe twierdzenie Fermata można też udowodnić przez indukcję, wykorzystując wzór dwumianowy Newtona. W tym celu wygodniej jest wysłowić je w równoważnej postaci, a mianowicie, że dla dowolnej liczby pierwszej p i dowolnej liczby naturalnej k, $k^p - k$ jest liczbą podzielną przez p. Indukcję prowadzimy oczywiście ze względu na k.

Zauważmy przy okazji, że z tego, że $p - 1$ potęga k w $\mathbb{Z}_p^*$ jest równa 1, wynika, że $p - 2$ potęga k w $\mathbb{Z}_p^*$ jest odwrotnością k w tej grupie.

Twierdzenie (Wilsona)**.** *Dla dowolnej liczby pierwszej p, $(p-1)! + 1$ jest liczbą podzielną przez p.*

Dowód. Aby udowodnić to twierdzenie wystarczy wykazać, że w grupie $\mathbb{Z}_p^*$ mamy $1 \odot 2 \odot \ldots \odot (p-2) \odot (p-1) = p - 1$. Zauważmy, że jeśli $k \in \mathbb{Z}_p^*$, to $k \odot k = 1$ wtedy i tylko wtedy gdy $k = 1$ lub $p - 1$. Otrzymujemy stąd, że zbiór $\{2, 3, \ldots, p-2\}$ można przedstawić jako sumę mnogościową rozłącznych zbiorów złożonych z par elementów g, g^{-1}. Przestawiając czynniki iloczynu $1 \odot 2 \odot \ldots \odot (p-2) \odot (p-1)$ tak by obok siebie znalazły się pary g, g^{-1} i skracając ich iloczyny, otrzymamy, że $1 \odot 2 \odot \ldots \odot (p-2) \odot (p-1) = p - 1$, a więc to co mieliśmy udowodnić.

3. Liczby Fermata.

n-tą liczbę Fermata definiujemy za pomocą wzoru $F_n = 2^{2^n} + 1$.

Fermat przypuszczał (lub być może twierdził; historycy nie są tego do końca chyba pewni), że tak zdefiniowane liczby są pierwsze. Zagadnieniem tym zainteresował się Euler i wykazał, że F_5 jest liczbą podzielną przez 641, a więc nie jest liczbą pierwszą. Ten wynik robi wrażenie, no bo czy Euler sprawdzał podzielność F_5 przez kolejne liczby pierwsze aż doszedł do 641 i tutaj mu się

udało? To byłoby chyba nieprawdopodobne. Euler postąpił inaczej, a mianowicie zastanawiał się co można powiedzieć o liczbach pierwszych, które dzielą F_n i odkrył oraz udowodnił następującą ich własność.

Twierdzenie. *Jeśli p jest liczbą pierwszą, która dzieli $2^{2^n}+1$, to $p = 2^{n+1}k+1$ dla pewnej liczby naturalnej k.*

To oczywiście znakomicie ułatwia dojście do tego, że dzielnikiem F_5 jest 641, zwłaszcza gdy się zauważy, że 2^6k+1, dla $k = 1$, 6 dzieli się przez 5 oraz dla $k = 2$, 5, 8 dzieli się przez 3, więc nie jest liczbą pierwszą.

Dowód. Rozpatrzmy grupę $\mathbb{Z}_p^*$ i przyjrzyjmy się rzędowi elementu 2 w tej grupie. Z założenia p dzieli liczbę $(2^{2^n}+1)(2^{2^n}-1) = 2^{2^{n+1}}-1$. Zatem 2^{n+1} potęga 2 w $\mathbb{Z}_p^*$ jest równa 1, a więc rząd $o(2)$ dzieli 2^{n+1}. Ponieważ p dzieli $2^{2^n}+1$, więc p nie dzieli $2^{2^n}-1$. Zatem $2^{2^n} \neq 1$ w $\mathbb{Z}_p^*$, a więc $o(2)$ nie dzieli 2^n. W efekcie $o(2) = 2^{n+1}$. Z drugiej strony $o(2)$ dzieli rząd grupy $\mathbb{Z}_p^* = p-1$, więc dla pewnego naturalnego k, $p-1 = 2^{n+1}k$. Stąd wynika, że $p = 2^{n+1}k+1$.

Widzimy więc, że gdy się więc wykorzysta podstawową wiedzę z teorii grup, to dowód tego twierdzenia jest bardzo prosty. Należy jednak pamiętać, że Euler nie znał ani pojęcia grupy ani twierdzenia Lagrange'a, bo tego wszystkiego wówczas w ogóle nie było. Było wręcz przeciwnie, to między innymi rozumowanie, które zastosował Euler pokazywało, że $\mathbb{Z}_p^*$ jest grupą oraz obejmowało szczególny przypadek twierdzenia Lagrange'a i było jednym z istotnych kroków, które doprowadziły do wyłonienia pojęcia grupy i odkrycia regularności opisanej w twierdzeniu Lagrange'a.

Nieco bardziej zaawansowane rozumowanie pozwala wzmocnić powyższy wynik. Udowodnimy mianowicie:

Twierdzenie. *Jeśli p jest liczbą pierwszą, która dzieli F_n i $n > 1$, to $p = 2^{n+2}m+1$ dla pewnej liczby naturalnej m.*

Dowód. Zauważmy na początek, że z tego co udowodniliśmy w poprzednim twierdzeniu i tego, że $n > 1$, wynika, że p jest postaci $8l+1$, a więc liczba $p-1$ jest podzielna przez 8. Rozpatrzmy iloczyn $\frac{p-1}{2}$ kolejnych liczb parzystych:

$$t = 2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1).$$

Zastanówmy się nad resztą z dzielenia t przez p. Zauważmy, że

$$1 \leqslant p-2i \leqslant \frac{p-1}{2}-1 \text{ wtedy i tylko wtedy gdy } \left(\frac{p-1}{2}+2\right) \leqslant 2i \leqslant p-1.$$

Zatem odwzorowanie $p-2i \to 2i$ przekształca zbiór liczb nieparzystych leżących pomiędzy 1 i $\frac{p-1}{2}-1$ na zbiór liczb parzystych leżących pomiędzy $(\frac{p-1}{2}+2)$ i $p-1$ (odwracając ich kolejność). W efekcie

$$\begin{aligned} &2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1) = \\ &= 2 \cdot 4 \cdot \ldots \cdot \frac{p-1}{2} \cdot \left(p - \left(\frac{p-1}{2}-1\right)\right) \cdot \left(p - \left(\frac{p-1}{2}-3\right)\right) \cdot \ldots \cdot (p-1) = \\ &= (-1)^{\frac{p-1}{4}} \left(\frac{p-1}{2}\right)! + pk = (-1)^{2l} \left(\frac{p-1}{2}\right)! + pk = \left(\frac{p-1}{2}\right)! + pk \end{aligned}$$

dla pewnej liczby naturalnej k. Otrzymaliśmy więc, że reszty z dzielenia t i $\left(\frac{p-1}{2}\right)!$ przez p są równe. Z drugiej jednak strony liczbę t można zapisać jako

$$t = (2 \cdot 1) \cdot (2 \cdot 2) \cdot (2 \cdot 3) \cdot \ldots \cdot \left(2 \cdot \frac{p-1}{2}\right) = 2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!.$$

Stąd i równości reszt, które otrzymujemy przy dzieleniu t i $\left(\frac{p-1}{2}\right)!$ przez p, wynika, że reszta z dzielenia $2^{\frac{p-1}{2}}$ przez p jest równa 1. Zatem $\frac{p-1}{2}$ potęga 2 w grupie $\mathbb{Z}_p^*$ jest równa 1, a więc rząd 2 w grupie $\mathbb{Z}_p^*$, który, jak wiemy jest równy 2^{n+1}, dzieli $\frac{p-1}{2}$. Stąd $p = 2^{n+2}m+1$ dla pewnej liczby naturalnej m.

4. Rozwinięcie dziesiętne odwrotności liczb pierwszych.

W tej części udowodnimy:

Twierdzenie (Gaussa)**.** *Jeśli p jest liczbą pierwszą różną od 2 i 5, to rozwinięcie dziesiętne $1/p$ jest ułamkiem okresowym, którego okres dzieli $p-1$.*

Podobno Gauss, nim odkrył i udowodnił to twierdzenie, policzył rozwinięcia dziesiętne odwrotności wszystkich liczb pierwszych mniejszych niż 1000. Płyną stąd chyba różne inspirujące wnioski, które pozostawiamy indywidualnej rozwadze zainteresowanych.

$$\begin{array}{r|l} 0,c_1c_2c_3\ldots & \\ \hline 10 & p \\ \cline{2-2} -\ldots & \\ \hline a_2 & \\ -\ldots & \\ \hline a_3 & \\ \ldots & \end{array}$$

Dowód. Niech $0,c_1c_2c_3\ldots$ będzie rozwinięciem dziesiętnym liczby $\frac{1}{p}$. Aby znaleźć to rozwinięcie, wyobraźmy sobie, jak przebiega dzielenie pisemne 1 przez p. Liczby a_n, c_n są określone rekurencyjnie za pomocą zależności: $a_1 = 10$, $10 \cdot a_n = p \cdot c_n + a_{n+1}$, $0 < a_{n+1} < p$. Stąd łatwo otrzymujemy, że a_{n+1} jest resztą z dzielenia 10^{n+1} przez p.

Aby ułamek $\frac{1}{p}$ był okresowy, dla pewnych liczb naturalnych k, l musi zachodzić $a_{l+k} = a_k$. Okresem tego ułamka nazywa się najmniejszą liczbę l o tej własności. Istnienie takiej liczby wynika z faktu, że liczba p jest różna od 2 i 5, a zatem reszta r z dzielenia 10 przez p jest niezerowa, a więc należy do $\mathbb{Z}_p^*$. W tej sytuacji $l = o(r)$ jest najmniejszą liczbą, dla której reszta z dzielenia 10^l przez p jest równa 1, a w konsekwencji $a_{l+1} = a_1$. Ułamek $\frac{1}{p}$ jest więc okresowy, a jego okres równy rzędowi $o(r)$ w $\mathbb{Z}_p^*$ i na mocy twierdzenia Lagrange'a dzieli $p-1$.

5. Liczba osi symetrii wielokąta.

Udowodnimy:

Twierdzenie. *Dowolny n-kąt W nie ma żadnej osi symetrii lub ich liczba jest dzielnikiem n.*

Zaczniemy od kilku obserwacji dotyczących izometrii własnych n-kąta W, które są prostymi ćwiczeniami dotyczącymi własności takich izometrii.

1. Zbiór $\mathcal{I}$ izometrii własnych W tworzy grupę ze względu na operację $\circ$ składania przekształceń.

2. Dowolna izometria przekształca wierzchołki W na wierzchołki. Wynika to z faktu, że jeśli obrazami punktów a, b przy izometrii f są punkty $f(a)$, $f(b)$ i s jest środkiem odcinka o końcach a, b, to $f(s)$ jest środkiem odcinka o końcach $f(a)$, $f(b)$ oraz tego, że punkt należący do W (punkty na brzegu wielokąta także traktujemy jako punkty, które do niego należą) jest środkiem odcinka o końcach, które należą do W wtedy i tylko wtedy, gdy nie jest on wierzchołkiem W.

3. Przy dowolnej izometrii W sąsiednie wierzchołki W przechodzą na wierzchołki sąsiednie.

4. Ponumerujmy kolejne wierzchołki wielokąta liczbami od 0 do $n-1$, zgodnie z ruchem wskazówek zegara, zaczynając od dowolnego ustalonego wierzchołka i utożsamimy wierzchołki z tymi liczbami. Każda izometria f permutuje więc liczby (wierzchołki) 0, 1, 2, ..., $n-1$.

Powiemy, że f zachowuje orientację, gdy $f(1) = f(0) + 1$ lub $f(0) = n-1$ i $f(1) = 0$ (oba przypadki można też ująć jednocześnie za pomocą warunku, który mówi, że $f(1)$ oraz $f(0)+1$ dają te same reszty przy dzieleniu przez n).

Oznaczmy przez $\mathcal{N}$ zbiór izometrii własnych W, które zachowują orientację. Zauważmy, że jeśli $f, g \in \mathcal{N}$, to $f \circ g \in \mathcal{N}$ oraz $f^{-1} \in \mathcal{N}$. Zatem $\mathcal{N}$ jest podgrupą $\mathcal{I}$. Jeśli $f \in \mathcal{N}$, to $f(0) = 0$ wtedy i tylko wtedy gdy $f = id$.

Oczywiście symetrie W są izometriami, które nie zachowują orientacji. Okazuje się, że jest i na odwrót. Załóżmy, że f jest izometria W, która nie zachowuje

orientacji. Jeśli $f(0) = 0$, to $f(1) = n - 1$ oraz $f(n - 1) = 1$ i f jest symetrią W względem symetralnej odcinka o końcach $n - 1$ i 1. Jeśli $f(0) = k \neq 0$, to $f(k) = 0$ i f jest symetrią W względem odcinka o końcach 0 i k.

Dowód twierdzenia. Załóżmy, że W ma oś symetrii i s jest symetrią W względem tej osi. Zauważmy, że dla dowolnej izometrii $f \in \mathcal{N}$, $s \circ f$ jest izometrią, która nie zachowuje orientacji, a więc $s \circ f$ jest symetrią. Ponadto $s \circ s \circ f = f$. Jeśli s_1 jest symetrią W, to $s \circ s_1 \in \mathcal{N}$ oraz $s \circ s \circ s_1 = s_1$. Zatem odwzorowanie $f \to s \circ f$ jest bijekcją $\mathcal{N}$ na zbiór symetrii W, a więc liczba osi symetrii W jest równa $|\mathcal{N}|$.

Teraz, jeśli $f \in \mathcal{N}$ i $f(0) = k$, to $f(1) = k \oplus 1$, $f(2) = k \oplus 2$ i ogólnie $f(m) = k \oplus m$. Jeśli więc $g \in \mathcal{N}$ oraz $g(0) = m$, to $f(g(0)) = f(m) = k \oplus m$. To pokazuje, że zbiór $T = \{f(0) \mid f \in \mathcal{N}\}$ jest podgrupą $\mathbb{Z}_n$. Ponadto, jeśli dla pewnych f_1, $f_2 \in \mathcal{N}$, $f_1(0) = f_2(0)$, to $(f_1^{-1} \circ f_2)(0) = 0$, a więc $f_1^{-1} \circ f_2 = id$ i $f_1 = f_2$. Zatem $|T| = |\mathcal{N}|$. Ponieważ T jest podgrupą $\mathbb{Z}_n$, więc z twierdzenia Lagrange'a wynika, że $|T|$ dzieli n. Zatem liczba osi symetrii W dzieli n.

6. Tablica świetlna.

Twierdzenie. *Na pewnej tablicy świetlnej można wyświetlać różne konfiguracje za pomocą danych przełączników. Każdy przełącznik ma ustalony obszar działania. Gdy się go naciśnie, to w jego obszarze działania zgasną wszystkie zapalone żarówki i zapalą się wszystkie te, które się nie paliły. Liczba konfiguracji, które możemy wyświetlić na tej tablicy, jest potęgą* 2.

Niech X będzie pewnym zbiorem. Dla dowolnych podzbiorów A, B zbioru X oznaczmy przez $A \div B$ różnicę symetryczną A i B zdefiniowaną jako

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

Zauważmy, że jeśli $\emptyset$ oznacza zbiór pusty, to $\emptyset \div A = A \div \emptyset = A$ oraz $A \div A = \emptyset$ dla dowolnego podzbioru A zbioru X. Ponadto dla dowolnych podzbiorów A, B, C zbioru X, $(A \div B) \div C = A \div (B \div C)$.

Zatem zbiór 2^X wszystkich podzbiorów zbioru X z działaniem $\div$ jest grupą. Jeśli zbiór X jest n-elementowy, to oczywiście $|2^X| = 2^n$.

Nietrudno stwierdzić, że jeśli P_1, P_2, …, P_k są pewnymi podzbiorami X, to zbiór $\mathcal{P} = \{P_{i_1} \div \ldots \div P_{i_m} \mid i_1, i_2, \ldots, i_m \in \{1, 2, \ldots, k\}\}$ jest podgrupą 2^X. Z twierdzenia Lagrange'a wynika więc, że rząd podgrupy $\mathcal{P}$ dzieli 2^n, a więc jest potęgą 2.

Zauważmy też, że jeśli R jest ustalonym podzbiorem X, to odwzorowanie 2^X w 2^X dane za pomocą wzoru $B \to R \div B$ jest różnowartościowe. Rzeczywiście, jeśli $R \div B_1 = R \div B_2$, to $B_1 = R \div R \div B_1 = R \div R \div B_2 = B_2$. To w szczególności pokazuje, ze moc zbioru $\{R \div B \mid B \in \mathcal{P}\}$ jest potęgą 2.

Dowód twierdzenia. Opisaną w zadaniu tablicę świetlną możemy utożsamiać ze zbiorem X jej żarówek. Konfigurację tablicy utożsamimy z podzbiorem $K \subseteq X$ zawierającym dokładnie te żarówki, które są w tej konfiguracji zapalone. Przełącznikowi o numerze i przyporządkujemy natomiast podzbiór $P_i \subseteq X$ będący obszarem działania tego przełącznika (gdy tablica jest wygaszona, to po naciśnięciu przełącznika i wyświetli się na tablicy konfiguracja P_i. W wyniku naciśnięcia tego przełącznika przy wyświetlonej konfiguracji K otrzymamy konfigurację $K \div P_i$).

Jasne jest teraz, że zbiór konfiguracji, które możemy wyświetlić za pomocą przełączników, których obszarami działania są zbiory P_1, P_2, …, P_k, i gdy startujemy z wygaszonej tablicy, jest równy $\mathcal{P}$. Gdy startujemy z tablicy na której wyświetlona jest konfiguracja R, to zbiór konfiguracji, które możemy uzyskać jest równy $\{R \div B \mid B \in \mathcal{P}\}$. Jak wiemy, moce obu zbiorów są potęgami 2.

3. Zadania

1. Wykazać, że jeśli G jest grupą skończoną z działaniem $\circ$ i H jest takim niepustym podzbiorem G, że dla dowolnych h_1, $h_2 \in H$, $h_1 \circ h_2 \in H$, to H jest podgrupą G.

2. Na tablicy wypisano liczby 1, 2, ..., 2012. Ścieramy dowolne dwie z nich wypisując w zamian wartość bezwzględną ich różnicy. Po wykonaniu 2011 takich operacji ścierania–dopisywania, pozostanie na tablicy jedna liczba. Wykazać, że będzie to zawsze liczba parzysta.

3. Na tablicy narysowano pewną ilość plusów i pewną ilość minusów. Ścieramy dowolne dwa z tych znaków, wpisując w zamian $+$, gdy starte znaki miały ten sam znak, i $-$, gdy miały znaki przeciwne. Wykazać, że bez względu na to jak wykonujemy te operacje, na końcu otrzymamy ten sam znak.

4. Na tablicy narysowano pewna liczbę kół, kwadratów i trójkątów. ściera się dowolne dwie spośród tych figur rysując w zamian:

− koło, gdy starliśmy dwa koła lub koło i trójkąt;

− trójkąt, gdy starliśmy dwa kwadraty lub koło i trójkąt;

− kwadrat, w innych przypadkach.

Operację tę się powtarza aż do momentu gdy na tablicy pozostanie tylko jedna figura. Wykazać, że bez względu na to jak nie będziemy postępowali, zawsze ta figura będzie taka sama.

5. Wykazać, że z danych n liczb całkowitych można wybrać pewną ich ilość w ten sposób by suma wybranych liczb była podzielna przez n.

6. Na okręgu znajduje się 101 liczb naturalnych, których suma jest równa 300. Wykazać, że istnieje taki łuk tego okręgu, że suma wszystkich spośród danych liczb, które znajdują się na tym łuku, jest równa 200.

7. Wykazać, że dla dowolnej liczby pierwszej p oraz liczby naturalnej $i < p-1$ liczba $1^i + 2^i + \ldots + (p-1)^i$ jest podzielna przez p.

Wskazówka. Wykazać, że istnieje takie $a \in \mathbb{Z}_p^*$, że $a^i \neq 1$ oraz zauważyć, że w $\mathbb{Z}_p$, $a^i \odot (1^i \oplus 2^i \oplus \cdots \oplus (p-1)^i) = 1^i \oplus 2^i \oplus \cdots \oplus (p-1)^i$.

8. Dane liczby naturalne n, m są względnie pierwsze wtedy i tylko wtedy gdy względnie pierwsze są liczby $2^n - 1$ i $2^m - 1$.

9. Dla dowolnych różnych liczb naturalnych n, m liczby $2^n + 1$ i $2^m + 1$ są względnie pierwsze.

10. Liczby $10^n + 1$ i $10^m + 1$ nie są względnie pierwsze wtedy i tylko wtedy gdy $n = k \cdot l$, $n = k \cdot t$ dla pewnej liczby naturalnej $k > 1$ oraz nieparzystych liczb naturalnych l, t.