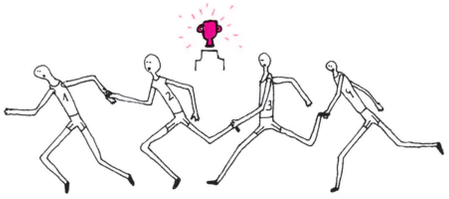


# Cztery zadania, jedno rozwiązanie

*Kamila MURASZKOWSKA*[*], *Edmund PUCZYŁOWSKI*[*]

Spójrzmy na cztery z pozoru zupełnie niezwiązane zadania.

**Zadanie 1.** $n$-tą liczbę Fermata definiujemy wzorem $F_n = 2^{2^n} + 1$. Wykaż, że jeśli $p$ jest liczbą pierwszą, która dzieli $F_n$, to $p = 2^{n+1}k + 1$ dla pewnej liczby naturalnej $k$.

**Zadanie 2.** Udowodnij, że jeśli $p$ jest liczbą pierwszą różną od 2 i 5, to rozwinięcie dziesiętne $1/p$ jest ułamkiem okresowym, którego okres dzieli $p - 1$.

**Zadanie 3.** Udowodnij, że liczba osi symetrii $n$-kąta jest równa 0 lub dzieli $n$.

**Zadanie 4.** Na pewnej tablicy świetlnej można wyświetlać różne konfiguracje za pomocą przełączników. Każdy przełącznik ma ustalony obszar działania. Gdy się go naciśnie, to w jego obszarze zgasną wszystkie zapalone żarówki i zapalą się wszystkie te, które się nie paliły. Wykaż, że liczba konfiguracji, które możemy wyświetlić na tej tablicy, jest potęgą 2.

Może się wydawać, że byłoby bardzo trudno wskazać jakieś wspólne elementy tych problemów. Okazuje się jednak, że rozwiązania wszystkich czterech opierają się na tym samym spostrzeżeniu – fundamentalnej własności pewnych obiektów algebraicznych, o których opowiemy dalej. Spróbujemy odkryć tę własność, rozwiązując ostatnie zadanie.

Tablica świetlna składa się ze zbioru $n$ żarówek $Z = \{z_1, \ldots, z_n\}$. Konfigurację tablicy utożsamimy z podzbiorem $K \subseteq Z$ zawierającym dokładnie te żarówki, które są w tej konfiguracji zapalone. Przełącznikowi natomiast przyporządkujemy podzbiór $P \subseteq Z$ będący obszarem jego działania. W wyniku naciśnięcia przełącznika $P$ przy wyświetlonej konfiguracji $K$ otrzymamy konfigurację odpowiadającą różnicy symetrycznej

$$K \oplus P = (K \cup P) \setminus (K \cap P)$$

zbiorów $K$ i $P$. Liczba konfiguracji, które możemy wyświetlić, jest więc równa liczbie różnych podzbiorów zbioru $Z$, które możemy otrzymać ze zbiorów odpowiadających przełącznikom, stosując operację „$\oplus$”.

Przyjrzyjmy się kilku własnościom tej operacji. Wprost z własności różnicy symetrycznej zbiorów wynika, że dla dowolnych konfiguracji:

i. $\emptyset \oplus K = K \oplus \emptyset = K$,
ii. $K \oplus K = \emptyset$,
iii. $(K_1 \oplus K_2) \oplus K_3 = K_1 \oplus (K_2 \oplus K_3)$ (dzięki temu możemy pomijać nawiasy).

Zamiast pojedynczych konfiguracji rozpatrzymy teraz pewne ich zbiory. Niech $\mathcal{P}$ będzie zbiorem przełączników, a $\mathcal{K}$ – zbiorem wszystkich konfiguracji możliwych do otrzymania za ich pomocą z konfiguracji pustej $\emptyset$ (wszystkie żarówki początkowo zgaszone). Oczywiście, jeśli dwie konfiguracje $K_1$ i $K_2$ należą do zbioru $\mathcal{K}$, to również konfiguracja $K_1 \oplus K_2$ należy do $\mathcal{K}$.

Załóżmy teraz, że naszą konfiguracją początkową jest pewna niepusta konfiguracja $R$. Wtedy zbiór

$$R \oplus \mathcal{K} = \{R \oplus K : K \in \mathcal{K}\}$$

opisuje wszystkie konfiguracje możliwe do uzyskania za pomocą przełączników ze zbioru $\mathcal{P}$, zaczynając od konfiguracji początkowej $R$. Zastanówmy się nad związkiem między zbiorami $R \oplus \mathcal{K}$ i $S \oplus \mathcal{K}$ dla różnych konfiguracji początkowych $R$ i $S$. Naturalnym pytaniem jest, czy za pomocą przełączników ze zbioru $\mathcal{P}$ można uzyskać tę samą konfigurację, zaczynając od dwóch różnych konfiguracji początkowych. Załóżmy więc, że zbiory $R \oplus \mathcal{K}$ i $S \oplus \mathcal{K}$ mają niepustą część wspólną, to znaczy pewna konfiguracja możliwa jest do uzyskania zarówno z konfiguracji początkowej $R$, jak i z $S$. Innymi słowy, $R \oplus K_R = S \oplus K_S$ dla pewnych konfiguracji $K_R, K_S \in \mathcal{K}$. Wtedy na mocy własności dodawania konfiguracji $R = R \oplus K_R \oplus K_R = S \oplus K_S \oplus K_R$.

[*]Instytut Matematyki,
Uniwersytet Warszawski

Mamy więc $R \in S \oplus \mathcal{K}$, a zatem konfigurację $R$ można uzyskać z konfiguracji $S$ za pomocą przełączników z $\mathcal{P}$. Analogicznie dowodzimy, że $S = R \oplus K_R \oplus K_S \in R \oplus \mathcal{K}$, a stąd $R \oplus \mathcal{K} = S \oplus \mathcal{K}$.

Okazuje się więc, że dla różnych stanów początkowych tablicy zbiory konfiguracji możliwych do uzyskania za pomocą przełączników ze zbioru $\mathcal{P}$ są takie same lub rozłączne. Zbiór wszystkich możliwych konfiguracji tablicy dzieli się zatem na sumę rozłącznych zbiorów $R_1 \oplus \mathcal{K}, \ldots, R_m \oplus \mathcal{K}$ dla pewnych konfiguracji początkowych $R_1, \ldots, R_m$. Wykorzystamy jeszcze prostą obserwację, że każdy ze zbiorów $R_i \oplus \mathcal{K}$ ma tyle samo elementów co $\mathcal{K}$. Stąd liczba wszystkich możliwych konfiguracji tablicy jest wielokrotnością liczby zbiorów w $\mathcal{K}$. Oczywiście, liczba wszystkich konfiguracji tablicy jest równa $2^n$ (każda z $n$ żarówek może być zgaszona lub zapalona), a więc liczba elementów zbioru $\mathcal{K}$ musi być potęgą dwójki.

Decydującą rolę w powyższym rozumowaniu odegrały własności (i)–(iii) operacji $\oplus$ oraz to, że dla dowolnych $K_1, K_2$ z $\mathcal{K}$ również $K_1 \oplus K_2$ jest w $\mathcal{K}$. Okazuje się, że podobne rozumowanie można zastosować w wielu innych sytuacjach – w szczególności w rozwiązaniach pozostałych zadań. Podobnie bowiem dowodzi się twierdzenia Lagrange'a dotyczącego grup, które stanowi tutaj kluczowy element rozumowań.

Rozpatrzmy zbiór $G$, w którym określone jest działanie „$\circ$". Zbiór ten nazwiemy *grupą*, jeśli działanie „$\circ$" spełnia następujące warunki:

(1) jest łączne, czyli $(a \circ b) \circ c = a \circ (b \circ c)$,
(2) ma element neutralny, oznaczany jako $e$, spełniający $g \circ e = e \circ g = g$ dla dowolnego elementu $g$ z $G$,
(3) dla każdego elementu $g$ z $G$ istnieje element (oznaczany przez $g^{-1}$) odwrotny do niego, czyli taki, że $g \circ g^{-1} = g^{-1} \circ g = e$.

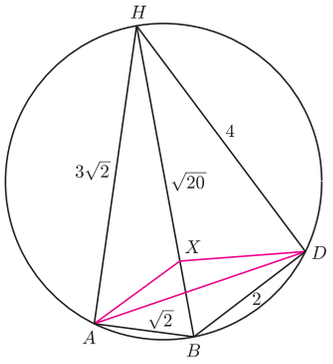
Oczywiście, każda z podgrup danej grupy sama też jest grupą.

*Podgrupą* grupy $G$ nazywamy podzbiór $H \subseteq G$ zamknięty na działanie „$\circ$" oraz na branie elementu odwrotnego względem tego działania. To znaczy, że jeśli elementy $h_1$ i $h_2$ należą do zbioru $H$, to należą do niego również elementy $h_1^{-1}$, $h_2^{-1}$ i $h_1 \circ h_2$. Liczbę elementów grupy $G$ nazywamy jej rzędem i oznaczamy $|G|$.

**Rozwiązanie zadania M 1369.**
Odpowiedź: minimalna wartość wyrażenia $AX + XD$ wynosi $\sqrt{10}$.

Zauważmy, że określony powyżej zbiór konfiguracji tablicy świetlnej wraz z operacją „$\oplus$" jest grupą. Konfiguracja pusta $\emptyset$ jest tu elementem neutralnym, a każda konfiguracja $K$ jest swoją odwrotnością, gdyż $K \oplus K = \emptyset$. Łatwo również sprawdzić, że zbiór konfiguracji możliwych do uzyskania za pomocą danego zbioru przełączników (gdy startuje się z konfiguracji $\emptyset$) jest podgrupą tej grupy.

Rysując trójkąty prostokątne $HAB$ i $HDB$ na jednej płaszczyźnie, dostajemy czworokąt $HABD$ wpisany w okrąg.




Wspomniane wyżej twierdzenie Lagrange'a brzmi następująco:

**Twierdzenie** (Lagrange'a)**.** *Jeśli zbiór $G$ wraz z działaniem „$\circ$" jest skończoną grupą, a $H$ jej podgrupą, to $|H|$ dzieli $|G|$.*

Idea dowodu tego twierdzenia opiera się na pomyśle przedstawionym w rozwiązaniu zadania: zbiór elementów $G$ można podzielić na rozłączne podzbiory postaci $gH = \{gh : h \in H\}$, równoliczne z $H$.

Zastosowanie tego twierdzenia do grupy konfiguracji tablicy świetlnej i jej podgrupy konfiguracji, otrzymywanych za pomocą podanego zbioru przełączników, daje natychmiastowe rozwiązanie zadania 4.

W dalszych rozważaniach będzie użyteczny pewien szczególny przypadek twierdzenia Lagrange'a. Niech $G$ będzie grupą skończoną, a $g$ jej dowolnym elementem. Wtedy istnieje taka liczba naturalna $k$, że element

$$\underbrace{g \circ \ldots \circ g}_{k}$$

(co zapisujemy w skrócie $g^k$) jest równy elementowi neutralnemu grupy $G$. Istotnie, ponieważ grupa $G$ jest skończona, to dla pewnych liczb naturalnych $l < m$ musi zachodzić $g^m = g^l$. Ale wtedy $g^{m-l} = g^m \circ (g^{-1})^l = g^l \circ (g^{-1})^l = e$.

Oczywiście, $AX + XD \geqslant AD$. Równość zachodzi wtedy i tylko wtedy, gdy $X$ jest punktem przecięcia przekątnych tego czworokąta. Szukana minimalna wartość wyrażenia $AX + XD$ to długość odcinka $AD$, którą możemy obliczyć z twierdzenia Ptolemeusza:

$$4 \cdot \sqrt{2} + 2 \cdot 3\sqrt{2} = AD \cdot \sqrt{20},$$

więc $AD = \sqrt{10}$.

Najmniejszą liczbę $k$, taką że $g^k = e$, nazywamy rzędem elementu $g$ i oznaczamy $o(g)$. Jest jasne, że elementy $e, g, g^2, \ldots, g^{o(g)-1}$ 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 $m$ zachodzi równość $g^m = e$, to $o(g)$ dzieli $m$, oraz że $g^{|G|} = e$.

Przyjrzymy się teraz przykładowi – grupie, którą wykorzystamy w rozwiązaniach zadań 1 i 2.

Niech $p$ będzie liczbą pierwszą. Rozpatrzmy zbiór $\{1, 2, \ldots, p-1\}$ z działaniem „$\odot$" określonym dla dowolnych $n, m \in \{1, 2, \ldots, p-1\}$ za pomocą wzoru

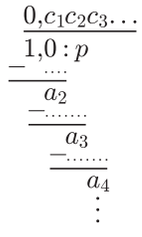
$$n \odot m = nm \bmod p.$$

Nietrudno sprawdzić, że jest to grupa. Łączność działania „$\odot$" wynika z łączności mnożenia, a elementem neutralnym jest 1. Istnienie elementu odwrotnego do danego elementu $n$ można uzasadnić następująco. Dla różnych liczb $k, l \in \{1, 2, \ldots, p-1\}$ reszty z dzielenia $nk$ i $nl$ przez $p$ są różne i niezerowe. W przeciwnym razie mielibyśmy, że $p \mid n(k-l)$, a stąd $p \mid n$ lub $p \mid (k-l)$, co jest niemożliwe. Dla pewnego $m \in \{1, 2, \ldots, p-1\}$ reszta z dzielenia $nm$ przez $p$ jest więc równa 1, czyli $n \odot m = 1$.

Grupę tę nazywamy *grupą multiplikatywną reszt modulo $p$* i oznaczamy ją przez $\mathbb{Z}_p^*$. Rząd $\mathbb{Z}_p^*$ jest, oczywiście, równy $p-1$, a więc z tego, co wiemy o własności rzędów elementów, wynika, że w $\mathbb{Z}_p^*$ dla dowolnego $r \in \mathbb{Z}_p^*$ mamy $r^{p-1} = 1$. Mamy stąd natychmiast Małe Twierdzenie Fermata, które mówi, że dla dowolnej liczby całkowitej $n$ i dowolnej liczby pierwszej $p$ liczba $n^p - n$ jest podzielna przez $p$.

Teraz możemy już rozwiązać pozostałe zadania.

**Zadanie 1.** Załóżmy, że liczba pierwsza $p$ dzieli $2^{2^n}+1$. Rozpatrzmy grupę $\mathbb{Z}_p^*$ i przyjrzyjmy się rzędowi elementu 2 w tej grupie. Z założenia $p$ dzieli liczbę $2^{2^{n+1}} - 1 = (2^{2^n}+1)(2^{2^n}-1)$. Zatem 2 podniesiona do potęgi $2^{n+1}$ w $\mathbb{Z}_p^*$ daje w wyniku 1, a więc $o(2)$ dzieli $2^{n+1}$. Ponieważ jednak 2 do potęgi $2^n$ w $\mathbb{Z}_p^*$ to $-1$, więc $o(2)$ nie dzieli $2^n$. Wiemy zatem, że $o(2) = 2^{n+1}$. Ponadto $o(2)$ dzieli rząd grupy $\mathbb{Z}_p^*$ równy $p-1$, więc dla pewnego naturalnego $k$ zachodzi równość $p - 1 = 2^{n+1}k$. Stąd wynika, że $p = 2^{n+1}k + 1$.




**Zadanie 2.** Niech $0{,}c_1c_2c_3\ldots$ będzie rozwinięciem dziesiętnym liczby $\frac{1}{p}$. Aby wyznaczyć to rozwinięcie, wyobraźmy sobie, jak przebiega dzielenie pisemne 1 przez $p$. Widać, że $n$-ta cyfra $c_n$ jest wynikiem dzielenia całkowitego $a_n$ przez $p$, gdzie liczba $a_n$ określona jest rekurencyjnie jako reszta z dzielenia $a_{n-1}$ przez $p$ pomnożona przez 10. Mamy więc $a_{n+1} = (a_n \bmod p) \cdot 10$, przy czym $a_1 = 10$. Stąd łatwo otrzymujemy jawny wzór $a_{n+1} = (10^n \bmod p) \cdot 10$.

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

**Zadanie 3.** Zbiór izometrii wielokąta składa się z symetrii osiowych o osiach przechodzących przez jeden punkt i obrotów względem tego punktu. Można wykazać, że wraz z działaniem składania przekształceń tworzy on grupę (jej elementem neutralnym jest obrót o zerowy kąt). Wynika to z następujących geometrycznych własności:

(1) złożenie dwóch obrotów jest obrotem,
(2) złożenie obrotu z symetrią lub symetrii z obrotem jest symetrią,
(3) złożenie symetrii względem przecinających się osi jest obrotem.

Wykażemy najpierw, że jeśli wielokąt ma co najmniej jedną oś symetrii, to w grupie jego izometrii jest tyle samo symetrii i obrotów. Niech $O$ będzie zbiorem obrotów,

$S$ – zbiorem symetrii, a $s$ – pewną ustaloną symetrią danego wielokąta. Wtedy składając $s$ z dowolnym obrotem, otrzymamy symetrię. Łatwo też udowodnić, że symetrie $s \circ o_1$ i $s \circ o_2$ będą różne dla różnych $o_1, o_2 \in O$, a więc $|O| \leqslant |S|$. Analogicznie, składając $s$ z dowolną symetrią, otrzymamy obrót, a ponadto $s \circ s_1 \neq s \circ s_2$ dla różnych $s_1, s_2 \in S$. Stąd $|O| \geqslant |S|$, a zatem $|O| = |S|$.

Powodem, dla którego wygodniej rozpatrywać zbiór obrotów $O$, jest zamkniętość tego zbioru na działanie składania przekształceń. Zbiór obrotów z tym działaniem ma więc strukturę grupy. Jak obroty zmieniają zbiór wierzchołków wielokąta? Każdy obrót powoduje pewne cykliczne przesunięcie wierzchołków. Jeśli ponumerujemy kolejne wierzchołki od $w_0$ do $w_{n-1}$, to $k$-te przesunięcie cykliczne $F_k$ przeprowadza wierzchołek $w_i$ na $w_{(i+k) \bmod n}$. Nietrudno sprawdzić, że zbiór $\{F_0, \ldots, F_{n-1}\}$ przesunięć cyklicznych z działaniem składania tworzy grupę. Zbiór obrotów $O$ tworzy więc podgrupę tej grupy, a zatem rząd $O$ (równy liczbie symetrii danego $n$-kąta) dzieli $n$.

# Jak zostać wynalazcą?

*Stanisław BEDNAREK*
Wydział Fizyki i Informatyki Stosowanej, Uniwersytet Łódzki

Wielu z nas marzyło zapewne o momencie, w którym chce się zakrzyknąć *Eureka!*, bo oto nasze działania doprowadziły do powstania nowej wiedzy, metody lub urządzenia. Część szczęśliwców lub osób z większym doświadczeniem na pewno taką chwilę z własnego życia pamięta. Mogła ona być kulminacją szeregu żmudnych prób w większości zakończonych porażkami, jak u Thomasa Edisona usiłującego skonstruować żarówkę.

Czasami odkrycia są dziełem przypadku, o czym przekonał się japoński badacz Hideki Shirakawa, pracujący nad ulepszeniem metody otrzymywania polietylenu: przy kolejnej próbie pomylił naczynia z substratem i katalizatorem, dodając tego ostatniego tysiąc razy za dużo. Otrzymana przez Shirakawę folia nie nadawała się do pakowania kanapek, ale za to świetnie przewodziła prąd elektryczny. Warto wiedzieć, że opisane tu odkrycie było początkiem drogi Shirakawy do Nagrody Nobla z chemii w 2000 roku.

Kiedy jednak mija początkowa euforia związana ze stworzeniem czegoś nowego, warto zastanowić się, co dalej. Przepisy prawa stwarzają możliwości uzyskania korzyści przez wynalazców, czyli osoby, które dokonały wynalazku. Powszechnie przyjmuje się, że wynalazek to dokonane przez człowieka rozwiązanie pewnego problemu związanego z ludzką egzystencją, które spełnia trzy podstawowe kryteria: nowości, poziomu wynalazczego i stosowalności przemysłowej. Takie sformułowanie wyklucza spośród wynalazków odkrycia naukowe, m.in. zjawisk, praw przyrody, procesów czy nowych gatunków organizmów żywych, ponieważ nie są one wytworzone przez człowieka, lecz istnieją albo zachodzą samoistnie. Wynalazkami nie są też sformułowania tych praw za pomocą wzorów matematycznych, a także teorie naukowe, wyjaśniające duże grupy zjawisk w oparciu o przyjęte założenia i modele, np. mechanika kwantowa. Wynalazkami nie są też wytwory ludzkiej działalności o charakterze czysto estetycznym czy informacyjnym, a więc wszelkiego rodzaju dzieła sztuki: rzeźby, powieści, utwory muzyczne, a także roczniki, kroniki itd. Wynalazkami mogą być natomiast sposoby wytwarzania różnego rodzaju przedmiotów czy otrzymywania związków chemicznych.

Czy zatem z grona wynalazców wykluczeni są automatycznie odkrywcy, teoretycy, matematycy i artyści? Niekoniecznie. Odkrywca może zbudować przyrząd wykorzystujący stwierdzone przez siebie zjawisko, a artysta może być twórcą choćby specjalnego podnośnika eksponującego jego dzieło sztuki. Na przykład Roger Penrose, badający ongiś pewne układy wielokątów całkowicie pokrywających płaszczyznę w sposób aperiodyczny, stwierdził, że przy odpowiednio dobranej kolorystyce mają one zachęcające walory estetyczne i mogą służyć do pokrywania ścian lub podłóg. Opatentował zatem te układy, znane dziś jako kafelki Penrose'a, a później wygrał nawet batalię sądową z firmą Kimberly-Clark, produkującą pokryty podobnym wzorem papier toaletowy. Z kolei Rogerowi Schlafly'emu udało się opatentować nawet… dwie bardzo duże liczby pierwsze, co wzbudziło ożywioną dyskusję o granicach stosowalności prawa patentowego.

Dla lepszego wyjaśnienia definicji wynalazku warto dokładniej przedyskutować trzy wymienione w niej kryteria. **Kryterium nowości** oznacza, że istotne cechy rozwiązania przedstawionego przez twórcę jako wynalazek nie mogą występować w innych rozwiązaniach służących do tego samego celu i znanych z wszelkich dostępnych i sprawdzalnych źródeł informacji. Te źródła to przede wszystkim: bazy danych urzędów patentowych, podręczniki, artykuły, katalogi, prospekty, strony internetowe, a także produkty występujące na rynku. Spełnienie **kryterium poziomu wynalazczego**, zwanego też niekiedy **kryterium nieoczywistości**, polega na tym, że nowe rozwiązanie nie może w sposób oczywisty wynikać ze znanych rozwiązań i dostępnej wiedzy, która ich dotyczy. Nie będzie więc wynalazkiem dźwignia dwustronna o wydłużonym ramieniu przykładanej przez nas siły, ułatwiająca podnoszenie dużych ciężarów. Jest bowiem jasne, że wartość siły działającej na ciało na końcu ramienia dźwigni jest odwrotnie proporcjonalna do długości tego ramienia. **Kryterium stosowalności przemysłowej** jest dość zrozumiałe, a jego spełnienie oznacza możliwość produkcji wynalezionego przedmiotu lub zastosowania sposobu, stanowiącego przedmiot wynalazku, na szerszą skalę. Kryterium to powinno dać się spełnić przy obecnych możliwościach technicznych naszej cywilizacji.