

*Dowód:* Skorzystamy ze znanego twierdzenia: jeśli liczby  $a$  i  $n$  są względnie pierwsze, to istnieje taka liczba naturalna  $r$ , że

$$a^r \equiv 1 \pmod{n}.$$

Stosujemy powyższe twierdzenie do  $a = 2$ . Niech  $r$  będzie najmniejszą liczbą całkowitą dodatnią spełniającą kongruencję

$$2^r \equiv 1 \pmod{n}.$$

Jeśli  $r$  jest parzyste, to z założenia minimalności  $r$  mamy  $2^{r/2} \not\equiv 1 \pmod{n}$ , a ponieważ  $2^{r/2} \equiv \pm 1 \pmod{n}$ , zatem musi być  $2^{r/2} \equiv -1 \pmod{n}$ . Wystarczy więc przyjąć  $k = r/2$ .

Jeśli natomiast  $r$  jest nieparzyste, to mamy  $(-2)^r \equiv -1 \pmod{n}$ , wystarczy więc przyjąć  $a = n - 2$  oraz  $k = r$ .

JWR

## MIEDZY NAMI OSZUSTAMI (21)

**TWIERDZENIE:** Dla dowolnej liczby nieparzystej  $n > 3$  istnieją takie liczby całkowite  $a$  i  $k$ , że  $1 \leq a \leq n - 2$ ,  $k > 1$  oraz

$$a^k \equiv -1 \pmod{n}.$$

## MIEDZY NAMI OSZUSTAMI (20'')

*Wyjaśnienie oszustwa (20'):* Oczopląs oczopląsem, a błędne wzory na początku rozwiązania pozostały. Prawdziwa jest jednak równość podana w treści zadania! Najmniejsza wspólna wielokrotność jest wprawdzie równa iloczynowi podzielonemu przez największy wspólny dzielnik, ale tylko dla dwóch liczb. Dla trzech liczb odpowiedni wzór jest bardziej złożony

$$[a, b, c] = \frac{abc \cdot (a, b, c)}{(a, b) \cdot (b, c) \cdot (c, a)}.$$

Poprawne rachunki wyglądają więc następująco

$$\frac{[a, b] \cdot [b, c] \cdot [c, a]}{[a, b, c]^2} = \frac{\frac{ab}{(a, b)} \cdot \frac{bc}{(b, c)} \cdot \frac{ca}{(c, a)}}{a^2 b^2 c^2 \cdot \frac{(a, b, c)^2}{(a, b) \cdot (b, c) \cdot (c, a)}} = \frac{ab \cdot bc \cdot ca}{a^2 b^2 c^2} \cdot \frac{(a, b)^2 \cdot (b, c)^2 \cdot (c, a)^2}{(a, b, c)^2 \cdot (a, b) \cdot (b, c) \cdot (c, a)} = \frac{(a, b) \cdot (b, c) \cdot (c, a)}{(a, b, c)^2}.$$

JWR

## GRY (11)

Oto dalsze własności sumy gier, prowadzące do pojęcia gier równoważnych.

Podstawowe znaczenie ma obserwacja, że dla dowolnej gry  $G$  w grze  $G \oplus G$  wygrywa drugi gracz. Łatwo bowiem podać jego strategię postępowania. Wystarczy, aby kopiował on ruchy gracza rozpoczynającego. Na czym polega to kopiowanie? Otóż gra  $G \oplus G$  w pozycji wyjściowej składa się z dwóch egzemplarzy tej samej gry. Pierwszy gracz wybiera jeden z tych egzemplarzy, a następnie wykonuje na nim legalny ruch. Gracz drugi wykonuje ten sam ruch na pozostałym egzemplarzu. Znowu pierwszy gracz ma wykonać ruch, i znowu bieżąca pozycja jest sumą dwóch egzemplarzy tej samej gry. W ten sposób gracz drugi zawsze będzie miał odpowiedź na ruch gracza pierwszego. A ponieważ gra zakończyć się musi, przegra gracz pierwszy. Prześledź to, Drogi Czytelniku, na przykładzie gry *Nim* z dwoma stosami równej liczności. A w wolnym czasie obejrzyj film *Mistrz zawsze traci* z cyklu *Parada oszustów*.

Z kolei przyjrzyjmy się równości  $0 \oplus G = G \oplus 0 = G$ . Dodanie gry  $0$  (końcówki) jest niezauważalne, bo nie stwarza żadnej dodatkowej możliwości ruchu. Powstaje jednak pytanie, jakie gry można dodać bez wpływu na ostateczny wynik rozgrywki. Okazuje się, że jest tak dla gier, w których drugi gracz wygrywa. Niech bowiem  $H$

będzie grą o strategii wygrywającej dla drugiego gracza. Posadźmy dwóch graczy do gry  $G \oplus H$ . Co się wówczas stanie? Jeden z graczy zorientuje się, że ma strategię wygrywającą w grze  $G$ . Powie sobie: *Chcę grać tylko w grę G*. Jednak jego przeciwnik ma pełne prawo wykonać ruch także w grze  $H$ . Strategia wygrywająca w grze  $G \oplus H$  dla gracza mającego strategię wygrywającą w grze  $G$  jest następująca: grać w grę  $G$  zgodnie z regułami strategii wygrywającej w tej grze. Jeśli jednak przeciwnik wykona ruch w grze  $H$ , to natychmiast na ten ruch odpowiedzieć. Wnikliwy Czytelnik dostrzeże, że jakkolwiek obecność gry  $H$  zmienia przebieg rozgrywki, to nie wpłynie na jej ostateczny wynik.

Ponieważ interesuje nas nie tyle sam przebieg gier, co ich ostateczny wynik, uzasadnione staje się pisanie  $H \equiv 0$  dla gier  $H$  o strategii wygrywającej dla drugiego gracza.

Będziemy także pisać  $G \equiv H$  dla dowolnych takich gier  $G$  i  $H$ , że  $G \oplus H \equiv 0$ .

Nie będziemy podawać formalnie własności relacji równoważności gier, powiemy tylko, że gry równoważne we wszystkich rozważanych przez nas okolicznościach można utożsamiać.

Czytelnik zechce sprawdzić, że prawdziwe są równoważności  $\{1\} \equiv 0$  oraz  $\{1, \{1\}, 2\} \equiv 3$ .

JWR