(3) Od Koła Fortuny do ... Małego Twierdzenia Fermata

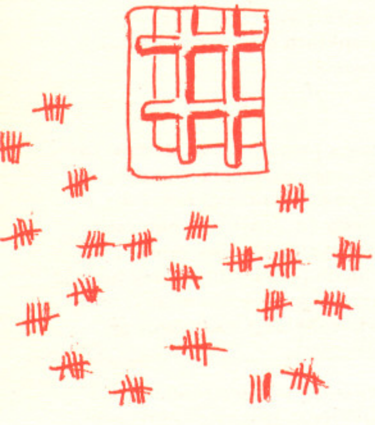
Każdy, kto choć raz oglądał w telewizji (niekoniecznie polskiej) teleturniej „Koło Fortuny" (a tym bardziej, jeśli miał „szczęście" wziąć w nim udział) wie, co to za koło.

Jest ono podzielone na ileś tam równych różnokolorowych sektorów.

Załóżmy, że tych sektorów jest p, gdzie p to ustalona liczba pierwsza, i każdy z nich chcemy pomalować na jeden z n kolorów. I tutaj powstaje

Pytanie: Ile jest wszystkich takich pokolorowań koła, jeśli dwa pokolorowania, z których jedno po obrocie koła o kąt $k \cdot \frac{360°}{p}$, gdzie $k = 0, 1, 2, 3, \ldots, p-1$, staje się drugim, uznajemy za identyczne?

Odpowiedź na to pytanie nie wydaje się trudna.



Każdy sektor malujemy na jeden z n kolorów. Zatem wszystkich pokolorowań tego koła jest n^p (tyle, ile wszystkich funkcji określonych na zbiorze p-elementowym i przyjmujących jedną z n wartości). Wśród tych pokolorowań jest n jednobarwnych i $n^p - n$ niejednobarwnych. Lecz każde niejednobarwne pokolorowanie tego koła jest w liczbie $n^p - n$ liczone p razy, gdyż..., no właśnie, dlaczego? Zatem istotnie różnych pokolorowań niejednobarwnych naszego koła jest $\frac{n^p - n}{p}$, a wszystkich nieidentycznych pokolorowań mamy:

$$n + \frac{n^p - n}{p}.$$

Liczba ta jest więc, przy każdym naturalnym n oraz dla dowolnej liczby pierwszej p, całkowita. Stąd wynika z kolei, że dla każdego naturalnego n oraz dla każdej liczby pierwszej p liczba $\frac{n^p - n}{p}$ jest całkowita, czyli że p dzieli $n^p - n$.

Łatwo spostrzec, że podzielność $p|(n^p - n)$ zachodzi też dla dowolnego n całkowitego ujemnego; jeśli bowiem $n < 0$, to $-n > 0$ i $p|((-n)^p - (-n))$ a więc $p|((-1) \cdot (n^p - n))$, gdy $2 \not| p$. Stąd $p|(n^p - n)$.

Gdy $p = 2$, to podzielność $2|(n^2 - n)$ jest oczywista.

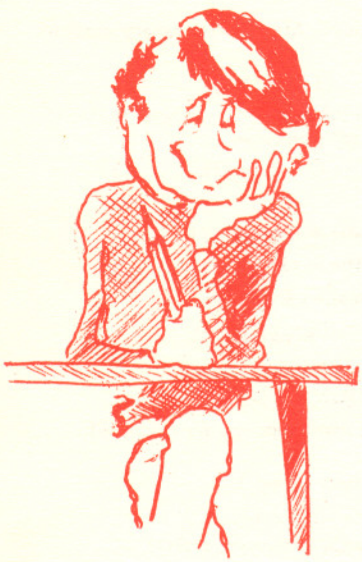
Zatem mamy $p|(n^p - n)$, dla każdego całkowitego n oraz dla każdej liczby pierwszej p.

Ponieważ $n^p - n = n(n^{p-1} - 1)$, więc z podzielności $p|(n^p - n)$, czyli $p|(n(n^{p-1} - 1))$, przy dodatkowym założeniu, że $p \not| n$ otrzymujemy podzielność $p|(n^{p-1} - 1)$, a więc zachodzi

Małe Twierdzenie Fermata

Jeśli n jest liczbą całkowitą niepodzielną przez liczbę pierwszą p, to

$$p|(n^{p-1} - 1).$$



A oto kilka nietrudnych zadań olimpijskich, które łatwo rozwiązuje się z zastosowaniem Małego Twierdzenia Fermata.

1. Udowodnić, że jeżeli liczby $a_1, a_2, \ldots, a_k$ są całkowite, p zaś jest liczbą pierwszą, to

$$p|(a_1^p + a_2^p + \ldots + a_k^p) \Leftrightarrow p|(a_1 + a_2 + \ldots + a_k).$$

2. Wiadomo, że liczba pierwsza p dzieli liczbę $\underbrace{11\ldots1}_{p}$. Udowodnić, że $p = 3$.

3. Niech a i b będą liczbami naturalnymi, p zaś liczbą pierwszą. Udowodnić, że jeżeli liczba $a^p - b^p$ jest podzielna przez p, to jest również podzielna przez p^2.

4. Udowodnić, że dla dowolnej liczby pierwszej p liczba

$\underbrace{11\ldots1}_{p}\underbrace{22\ldots2}_{p}\underbrace{33\ldots3}_{p}\ldots\underbrace{99\ldots9}_{p} - 123456789$ jest podzielna przez p.

Henryk PAWŁOWSKI