Niezależność twierdzenia Goodsteina

Redakcja zażądała ode mnie, abym opisał twierdzenie, które łatwo sformułować, ale które „nie ma elementarnego dowodu". Mówiąc „nie ma elementarnego dowodu" mamy przeważnie na myśli, że wszystkie **znane** dowody są trudne i zrozumienie któregokolwiek z nich wymaga znajomości jakiejś zaawansowanej teorii. Oczywiście nie wyklucza to, że w przyszłości ktoś mądry odkryje dowód krótki i operujący jedynie pojęciami znanymi ze szkoły podstawowej.

Chciałbym potraktować żądanie redakcji dosłownie i przedstawić twierdzenie Goodsteina, o którym można **udowodnić**, że nie ma dowodu elementarnego. W tym celu skonstruujmy najpierw, przez indukcję, liczby naturalne G_n^k dla $k, n = 1, 2, \ldots$

Niech $G_1^k = k$. Jeśli $G_n^k = 0$, to $G_{n+1}^k = 0$. Załóżmy, że mamy $G_n^k > 0$. Wykonujemy następujące operacje: rozwijamy $G_n^k - 1$, przy podstawie $n+1$, w taki sposób, aby w rozwinięciu tym występowały wyłącznie liczby nie większe od $n+1$. Potem zamieniamy wszystkie $n+1$ na $n+2$. Tak utworzona liczba jest szukanym G_{n+1}^k.

Brzmi to nieco zawile, ale przykłady wyjaśnią, mam nadzieję, wszystko.

$G_1^{16} = 16$. Teraz obliczamy G_2^{16}. Najpierw rozwijamy $G_1^{16} - 1$, przy podstawie 2. Mamy: $G_1^{16} - 1 = 15 = 2^3 + 2^2 + 2 + 1 = 2^{2+1} + 2^2 + 2 + 1$. A terazzamieniamy dwójki na trójki: $G_2^{16} = 3^{3+1} + 3^3 + 3 + 1 = 112$. Obliczamy dalej: $G_2^{16} - 1 = 111 = 3^{3+1} + 3^3 + 3$, $G_3^{16} = 4^{4+1} + 4^4 + 4 = 1284$, $G_3^{16} - 1 = 4^{4+1} + 4^4 + 3$, $G_4^{16} = 5^{5+1} + 5^5 + 3 = 18753$, itd.

Łatwo obliczyć, że $G_{16}^{16} = 17^{17+1} + 7 \cdot 17^7 + 7 \cdot 17^6 + 7 \cdot 17^5 + 7 \cdot 17^4 + 7 \cdot 17^3 + 7 \cdot 17^2 + 6 \cdot 17 + 15$.

Inny przykład: ponieważ $G_1^{1041} - 1 = 2^{10} + 2^4 = 2^{2^{2+1}+2} + 2^{2^2}$, to $G_2^{1041} = 3^{3^{3+1}+3} + 3^{3^3}$.

Widać, jak sądzę, że ciąg $(G_n^k)_{n=1}^{\infty}$ rośnie bardzo szybko. Naprawdę jednak ciąg ten zachowuje się jak kozak Makar w anegdocie Franca Fiszera: skacze bardzo wysoko, a potem b a r d z o w o l n o opada.

Goodstein udowodnił, że dla każdego k istnieje takie n, że $G_n^k = 0$.

Jedyny znany mi dowód tego twierdzenia nie jest bardzo trudny i do zrozumienia go wystarczy znajomość arytmetyki liczb porządkowych. Zauważmy jednak, że twierdzenie Goodsteina mówi o liczbach naturalnych, zatem rozsądnym wyjściem jest nazwać elementarnym dowód, w którym używamy jedynie prostych własności dodawania, mnożenia i porządku liczb naturalnych oraz zasady indukcji.

Teoria aksjomatyzująca te pojęcia nazywa się arytmetyką Peano. Otóż udowodniono następujące twierdzenie: jeśli arytmetyka Peano jest niesprzeczna, to nie można w niej udowodnić twierdzenia Goodsteina. I to jest właśnie ścisłe sformułowanie braku „elementarnego dowodu".

Powyższy fakt wydaje mi się znacznie ciekawszy niż samo twierdzenie Goodsteina. Znane dowody tego faktu nie są łatwe i wymagają stosowania teorii modeli lub teorii dowodu, ale to już zupełnie inna historia.

dr Adam KRAWCZYK

Mamy daną tablicę świetlną zbudowaną z lampek, z których każda może znajdować się w jednym z dwóch stanów: być zapalona lub zgaszona. Mamy też układ przełączników, z których każdy działa na pewną ustaloną część lampek w ten sposób, że po jego przełączeniu lampki palące się (w obszarze działania przełącznika) gasną, a zgaszone zapalają się. Wykazać, że liczba układów, które możemy na tej tablicy wyświetlić, jest potęgą dwójki.

Niech $\mathcal{G}$ będzie zbiorem wszystkich podzbiorów (łącznie ze zbiorem pustym) zbioru lampek. Moc $\mathcal{G}$ jest równa 2^s, gdzie s jest liczbą lampek. Działanie przyporządkowujące każdym dwóm zbiorom $A, B \in \mathcal{G}$ ich różnicę symetryczną $A \div B = A \cup B \setminus A \cap B$ spełnia warunki:

$$A \div B = B \div A, \quad (A \div B) \div C = A \div (B \div C), \quad A \div \emptyset = A, \quad A \div A = \emptyset.$$

Zbiór $\mathcal{G}$ z działaniem $\div$ jest więc grupą przemienną.

Zauważmy teraz , że jeśli D_w oznacza zbiór, na który działa wyłącznik w, to startując z wygaszonej tablicy i przełączając wyłączniki $w_1, \ldots, w_n$ zapalimy lampki dokładnie ze zbioru $D_{w_1} \div D_{w_2} \div \ldots \div D_{w_n}$. Oznacza to, że startując z wygaszonej tablicy możemy wyświetlić dokładnie tyle układów, ile jest elementów w najmniejszej podgrupie $\mathcal{P}$ grupy $\mathcal{G}$, której elementami są wszystkie zbiory D_w. Jeżeli startujemy w sytuacji, gdy na tablicy zapalone są lampki ze zbioru A, to liczba układów, które możemy wyświetlić, jest równa mocy warstwy grupy $\mathcal{G}$ względem podgrupy $\mathcal{P}$ wyznaczonej przez A (czyli mocy zbioru $\{A \div B : B \in \mathcal{P}\}$, która jest, oczywiście, równa mocy podgrupy $\mathcal{P}$). Z twierdzenia Lagrange'a (rząd podgrupy dzieli rząd grupy) wynika więc, że ta liczba jest dzielnikiem rzędu grupy $\mathcal{G}$, a więc jest to potęga dwójki.

doc. dr Edmund PUCZYŁOWSKI

Rozwiązanie zadania M 509.

Liczby n, $n-1$, $n-2, \ldots, n-p+1$ dają przy dzieleniu przez p reszty $0, 1, \ldots, p-1$. Jedna z tych liczb, m, dzieli się przez p. Zatem $\left[\frac{n}{p}\right] = \frac{m}{p}$. Mamy teraz

$$\frac{n(n-1)\ldots(n-p+1)}{m} \equiv (p-1)! \pmod{p},$$

skąd po pomnożeniu obu stron przez $\frac{m}{p}$ dostajemy

$$\frac{n(n-1)\ldots(n-p+1)}{p} \equiv \frac{(p-1)!m}{p} \pmod{p},$$

i po podzieleniu przez liczbę $(p-1)!$, względnie pierwszą z p, otrzymujemy

$$\frac{n!}{p!(n-p)!} \equiv \frac{m}{p} \pmod{p},$$

co kończy dowód.