Metoda kongruencji w teorii liczb

Marcin MAZUR, Warszawa

Jednym z najstarszych działów teorii liczb jest teoria podzielności. Stosunkowo elementarne metody i bardzo eleganckie wyniki czynią tę dziedzinę atrakcyjną i dostępną szerokiemu gronu miłośników matematyki oraz pozwalają na samodzielne badania już na wstępnym etapie edukacji matematycznej. Niestety brak tej tematyki w programie szkolnym zdecydowanie utrudnia młodzieży poznanie dziedziny, która poprzez swoje piękno i siłę mogłaby przyczynić się do poszerzenia grona miłośników matematyki. Jeden z wybitniejszych matematyków naszego stulecia, G. H. Hardy, powiedział, że „elementarna teoria liczb powinna być uważana za jeden z najwłaściwszych przedmiotów w początkach wykształcenia matematycznego. Wymaga ona bardzo mało uprzedniej wiedzy, a przedmiot jej jest uchwytny i znajomy, metody rozumowania, które stosuje, są proste, ogólne i nieliczne i nie ma sobie równej, wśród nauk matematycznych, w odwoływaniu się do naturalnej ludzkiej ciekawości". Mam nadzieję, że artykuł ten będzie ilustracją słów G. H. Hardy'ego. Pragnę w nim przybliżyć podstawowe fakty dotyczące kongruencji i ukazać ich użyteczność w rozwiązywaniu problemów teorii liczb.

Na wstępie przypomnijmy sobie podstawowy fakt arytmetyki

Twierdzenie 1: *Każdą liczbę całkowitą $N \neq 0, \pm 1$ można jednoznacznie przedstawić w postaci:*

$$N = \pm p_1^{n_1}, \ldots p_k^{n_k}$$

gdzie $p_1 < p_2 < \ldots < p_n$ są liczbami pierwszymi, $k, n_1, \ldots, n_k$ – liczbami naturalnymi.

Twierdzenie powyższe jest punktem wyjścia do dalszych rozważań, ale zanim do nich przejdziemy uczynię kilka uwag notacyjnych. Zgodnie z tradycją teorioliczbową 0 nie uważa się za liczbę naturalną. Jeśli liczba a dzieli liczbę b, to będziemy pisali $a \mid b$, w przeciwnym razie $a \nmid b$. Jeśli α jest największym wykładnikiem takim, że $p^\alpha \mid N$ (p – liczba pierwsza) to będziemy pisali $p^\alpha \parallel N$. Zapis $(a, b) = d$ oznacza, że d jest największym wspólnym dzielnikiem liczb a i b. Po tych uwagach sformułujemy wniosek z Twierdzenia 1, który będziemy używali dalej wielokrotnie:

Wniosek 1: *Jeśli a, b, c są liczbami całkowitymi, $(a, b) = 1$ oraz $a \mid b \cdot c$, to $a \mid c$.*

Uzasadnienie tego wniosku pozostawiam Czytelnikowi.

W swoim wielkim dziele poświęconym teorii liczb zatytuowanym „Disquisitiones Arithmeticae" K. F. Gauss wprowadził następującą notację: jeśli $m \mid a - b$ to piszemy $a \equiv b \pmod m$ i mówimy, że liczby całkowite a i b przystają do siebie (są kongruentne) według modułu m. Relację $a \equiv b \pmod m$ nazywamy właśnie kongruencją. Okazuje się, że używając pojęcia kongruencji można mówić o problemach związanych z podzielnością w sposób niezwykle efektywny i prosty. Czytelnik zapewne zdaje sobie sprawę jak istotne jest posiadanie odpowiedniego języka do mówienia o pewnych rzeczach. Chcąc porozumiewać się w sposób jak najbardziej efektywny człowiek stworzył olbrzymi zasób słów, choć wiadomo, że bez wielu z nich można by się obejść (ale wówczas wiele myśli byłoby o wiele trudniej wyrazić). Podobnie język kongruencji wydaje się być najwłaściwszy do mówienia o problemach dotyczących podzielności. (Studiując matematykę Czytelnik niejednokrotnie przekona się, jak istotne dla rozwoju matematyki było stworzenie odpowiedniego języka.) Cóż więc jest takiego użytecznego w pojęciu kongruencji? Otóż kongruencjami można „manipulować" jak zwykłymi równaniami. Jeśli moduł jest ustalony, to kongruencje można dodawać i mnożyć stronami:

$$\text{jeśli} \quad a \equiv b \pmod m \quad \text{i} \quad A \equiv B \pmod m, \text{ to}$$
$$a + A \equiv b + B \pmod m \quad \text{i} \quad a \cdot A \equiv b \cdot B \pmod m.$$

Natomiast nie zawsze wolno kongruencje dzielić stronami (podobnie jak równości nie wolno dzielić przez równość $0 = 0$). Jeśli jednak $(A, m) = 1$ oraz $a \equiv b \pmod m$ i $a \cdot A \equiv b \cdot B \pmod m$ to $A \equiv B \pmod m$. Proponuję Czytelnikowi udowodnienie tych własności oraz następujących wniosków:

Wniosek 2: *Jeśli f jest wielomianem o współczynnikach całkowitych i $a \equiv b \pmod m$, to $f(a) \equiv f(b) \pmod m$.*

Wniosek 3: *Jeśli m jest liczbą naturalną o zapisie dziesiętnym $a_0 + a_1 \cdot 10 + \ldots + a_n \cdot 10^n$ oraz $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, to z wniosku 2 wobec kongruencji $10 \equiv 1 \pmod 9$ i $10 \equiv -1 \pmod{11}$ otrzymujemy znane cechy podzielności przez 9 i 11 (jakie?).*

Możemy teraz rozwiązać pierwsze zadanie, tzn. udowodnić następujące

Stwierdzenie 1: *Nie istnieje wielomian dodatniego stopnia o współczynnikach całkowitych, którego wartość dla każdej liczby naturalnej jest liczbą pierwszą.*

Dowód: Załóżmy przeciwnie, że taki wielomian f istnieje. Zatem $f(1) = p$ jest liczbą pierwszą. Niech $b_k = 1 + k \cdot p$, $k \in \mathbb{N}$ (przez $\mathbb{N}$ oznaczać będziemy zbiór liczb naturalnych). Mamy $b_k \equiv 1 \pmod p$. Stąd wobec wniosku 2 otrzymujemy

$$f(b_k) \equiv f(1) = p \equiv 0 \pmod p$$

Wobec tego $p \mid f(b_k)$, a że $f(b_k)$ jest liczbą pierwszą więc $p = f(b_k)$. Tym samym pokazaliśmy, że wielomian f przyjmuje wartość p nieskończenie wiele razy, co wobec podstawowych własności wielomianów jest niemożliwe (dlaczego?) ■

Udowodniony fakt wiąże się z bardzo starym zagadnieniem poszukiwania wzorów na liczby pierwsze. Wykazaliśmy mianowicie, że nie istnieją wzory wielomianowe na liczby pierwsze. Stosując trochę inną metodę, opartą na fakcie, że jeśli różne liczby pierwsze p, q dzielą wartości wielomianu w pewnych liczbach naturalnych, to liczba $p \cdot q$ też dzieli wartość tego wielomianu w pewnej liczbie naturalnej można udowodnić fakt mocniejszy. W związku z tym proponuję Czytelnikowi uściślenie tej metody i rozwiązanie następującego zadania:

Zadanie dla Czytelnika: Dowieść, że nie istnieje wielomian dodatniego stopnia o współczynnikach całkowitych, który dla każdej liczby naturalnej przyjmuje wartość będącą potęgą liczby pierwszej.

W dalszym ciągu litera p będzie używana dla oznaczenia liczby pierwszej.

Przed przystąpieniem do rozwiązania następnego zadania rozwiniemy trochę teorii.

Lemat 1. $\binom{p}{i} \equiv 0 \pmod p$ *dla* $1 \leq i \leq p-1$, *gdzie* $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ *jest symbolem Newtona.*

Dowód: Ponieważ $\binom{p}{i} = p \cdot \frac{(p-1)!}{i!(p-i)!}$ jest liczbą naturalną, więc $i!(p-1)! \mid p(p-1)!$ Ale oczywiście $(i!(p-i)!, p) = 1$ (dlaczego?), więc wobec wniosku 1 mamy
$i!(p-i)! \mid (p-1)!$, a zatem liczba $\frac{(p-1)!}{i!(p-i)!}$ jest naturalna. Jest więc $p \mid \binom{p}{i}$ tzn. $\binom{p}{i} \equiv 0 \pmod p$. ■

Uwaga. Prawdziwe jest również twierdzenie odwrotne.

Udowodnijmy teraz bardzo użyteczne twierdzenie

Małe twierdzenie Fermata (MTF): *Dla dowolnej liczby naturalnej a jest*

$$a^p \equiv a \pmod p$$

Dowód: Dowód przeprowadzimy metodą indukcji matematycznej. Dla $a = 1$ jest to oczywiste. Załóżmy, że MTF jest prawdziwe dla pewnego $a \geq 1$. Wówczas $a^p \equiv a \pmod p$, skąd $a^p + 1 \equiv a + 1 \pmod p$.

Przyjrzyjmy się teraz liczbie $(a+1)^p$. Otóż z wzoru dwumianowego mamy:

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \ldots + \binom{p}{p-1}a + 1 = a^p + 1 + \sum_{i=1}^{p-1}\binom{p}{i}a^i.$$

Wobec lematu 1 mamy $\sum_{i=1}^{p-1}\binom{p}{i}a^i \equiv 0 \pmod p$ (dlaczego?). Stąd wobec faktu, że $a^p + 1 \equiv a + 1 \pmod p$ (wykazaliśmy to wyżej) mamy

$$(a+1)^p = a^p + 1 + \sum_{i=1}^{p-1}\binom{p}{i}a^i \equiv a^p + 1 \equiv a + 1 \pmod p$$

tzn. MTF jest prawdziwe dla $a+1$. Na mocy zasady indukcji matematycznej twierdzenie zostało udowodnione. ■

Następujący wniosek również znany jest pod nazwą – małe twierdzenie Fermata

Wniosek 4: *Jeśli $p \nmid a$ to $a^{p-1} \equiv 1 \pmod p$.*

Dowód: Wobec MTF mamy $p \mid a(a^{p-1}-1)$, a wobec założenia $(p,a) = 1$. Na mocy wniosku 1 otrzymujemy więc, że $p \mid a^{p-1} - 1$, tzn. $a^{p-1} \equiv 1 \pmod p$.

Inna metoda to zastosowanie możliwości dzielenia kongruencji. Mianowicie $a \equiv a \pmod p$ oraz $a \cdot a^{p-1} \equiv 1 \pmod p$ i $(a,p) = 1$, więc $a^{p-1} \equiv 1 \pmod p$. ■

Nieco inną metodą można udowodnić twierdzenie ogólniejsze, które pozostawiam bez dowodu.

Zadanie dla Czytelnika: Udowodnić twierdzenie Eulera, że dla każdej liczby całkowitej a względnie pierwszej z n prawdziwa jest kongruencja

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n),$$

gdzie $\varphi(n)$ – ilość liczb naturalnych mniejszych od n i względnie pierwszych z n (φ zwana jest funkcją Eulera).

Wniosek 5: *Dla każdego całkowitego a takiego, że $p \nmid a$ istnieje dokładnie jedno b takie, że $1 \le b \le p-1$ oraz $a \cdot b \equiv 1 \pmod p$.*

Dowód: Z wniosku 4 mamy $a \cdot a^{p-2} \equiv 1 \pmod p$. Jeśli b jest resztą z dzielenia a^{p-2} przez p to oczywiście $a^{p-2} \equiv b \pmod p$ oraz $1 \le b \le p-1$. Zatem $1 \equiv a \cdot a^{p-2} \equiv a \cdot b \pmod p$. Tym samym wykazaliśmy istnienie b.

Co się tyczy jednoznaczności to zauważmy, że jeśli b_1, b_2 spełniają tezę wniosku, to $a(b_1 - b_2) \equiv 0 \pmod p$, a że $(a,p) = 1$, więc $b_1 - b_2 \equiv 0 (\mathrm{mod}\, p)$ i wobec $1 \le b_i \le p-1$ mamy $b_1 = b_2$ (dlaczego?). ■

Jedyną liczbę b z wniosku 5 będziemy dalej oznaczać przez h_a. Warto tu podkreślić wagę ostatniego wniosku, który pozwala odwracać liczby całkowite modulo p. Jest to równie istotne dla teorii liczb jak odwracanie liczb wymiernych, a liczba h_a jest analogiczna do liczby $\frac{1}{a}$ w zwykłej arytmetyce liczb wymiernych.

Czas już rozwiązać następne zadanie, które zilustruje użyteczność wprowadzonych pojęć.

Zadanie (twierdzenie Wolstenholme, 1862 r.): *Niech $1 + \frac{1}{2} + \ldots + \frac{1}{p-1} = \frac{m}{n}$, gdzie $p \ge 5$ oraz $(m,n) = 1$. Dowieść, że $p^2 \mid m$.*

Rozwiązanie: Sprowadzimy najpierw zadanie do liczb naturalnych. W tym celu zauważmy, że $(p-1)!(1 + \frac{1}{2} + \ldots + \frac{1}{p-1}) = \frac{(p-1)!}{1} + \ldots + \frac{(p-1)!}{p-1} = \frac{(p-1)!m}{n}$ jest liczbą naturalną ($(p-1)!$ jest iloczynem mianowników rozpatrywanych ułamków). Wobec tego $n \mid (p-1)!m$, a że $(n,m) = 1$, więc z wniosku 1 mamy $n \mid (p-1)!$, tzn. $\frac{(p-1)!}{n}$ jest liczbą naturalną i w dodatku niepodzielną przez p (bo $p \nmid (p-1)!$). Zatem $p^2 \mid m$ wtedy i tylko wtedy, gdy $p^2 \mid \frac{(p-1)!m}{n}$, a więc wystarczy wykazać, że $p^2 \mid S = \frac{(p-1)!}{1} + \ldots + \frac{(p-1)!}{p-1}$. Zauważmy, że mianowniki i-tego i $(p-i)$-tego ułamka dają w sumie p. Ta prosta uwaga podpowiada, by

rozpatrywać sumę

$$2S = \sum_{i=1}^{p-1} \left(\frac{(p-1)!}{i} + \frac{(p-1)!}{p-i} \right) = \sum_{i=1}^{p-1} p \cdot \frac{(p-1)!}{i(p-1)} = p \cdot \sum_{i=1}^{p-1} \frac{(p-1)!}{i(p-1)}$$

(oczywiście $p^2 \mid S$ wtedy i tylko wtedy, gdy $p^2 \mid 2S$, bo $p \geq 5$, więc na pewno $p \neq 2$). Liczby $b_i = \frac{(p-1)!}{i(p-1)}$ są dla $i = 1, \ldots, p-1$ naturalne (bo $i \neq p-i$), więc $p \mid 2S$ oraz $\frac{2S}{p} = \sum_{i=1}^{p-1} b_i$. Zatem całe zadanie sprowadza się do wykazania, że $p \mid \frac{2S}{p}$, tzn. $\sum_{i=1}^{p-1} b_i \equiv 0 \pmod p$. W tym celu wykorzystamy wniosek 5. Otóż z określenia liczb b_i wynika, że $i(p-i)b_i = (p-1)!$, a że $i \cdot (p-i) \equiv -i^2 \pmod p$ więc otrzymujemy

$$(*) \qquad -i^2 b_i \equiv (p-1)! \pmod p.$$

Ale nas interesuje samo b_i. Wobec tego musimy ostatnią kongruencję pomnożyć stronami przez „odwrotność" $-i^2$ (patrz uwagi po wniosku 5). W tym celu zauważmy, że wobec $ih_i \equiv 1 \pmod p$ mamy $i^2 h_i^2 \equiv 1 \pmod p$, tzn. $(-i^2)(-h_i^2) \equiv 1 \pmod p$. Zatem mnożąc kongruencję $(*)$ stronami przez $-h_i^2$ otrzymamy

$$-i^2 b_i(-h_i^2 \equiv (p-1)! h_i^2 \pmod p),$$

tzn.

$$b_i \equiv -(p-1)! h_i^2 \pmod p.$$

Zatem $\sum_{i=1}^{p-1} b_i \equiv -(p-1)! \sum_{i=1}^{p-1} h_i^2 \pmod p$ i dla zakończenia rozwiązania wystarczy dowieść, że $\sum_{i=1}^{p-1} h_i^2 \equiv 0 \pmod p$.

Przyjrzyjmy się więc dokładniej liczbom $h_1, \ldots, h_{p-1}$. Otóż, jak łatwo zauważyć, dla $1 \leq i \leq p-1$ jest $h_{h_i} = i$ (bo $h_i \cdot i \equiv 1 \pmod p$), a więc jeśli $h_i = h_j$ to $i = j$ (dlaczego?). Zatem ciąg $(p-1)$ liczb $h_1, \ldots, h_{p-1}$ składa się z parami różnych liczb naturalnych z przedziału $\langle 1, p-1 \rangle$, a więc jest permutacją ciągu $1, 2, \ldots, p-1$ (dlaczego?). Wobec tego mamy $\sum_{i=1}^{p-1} h_i^2 = \sum_{i=1}^{p-1} i^2$. Przypomnijmy teraz następujący wzór

$$1^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6},$$

którego dowód (najłatwiej indukcyjny) pozostawiam Czytelnikowi.

W szczególności $\sum_{i=1}^{p-1} i^2 = \frac{(p-1)p(2p-1)}{6}$ i wobec $(6, p) = 1$ mamy $p \mid \sum_{i=1}^{p-1} i^2$. Tym samym wykazaliśmy, że $\sum_{i=1}^{p-1} h_i^2 \equiv 0 \pmod p$, co kończy dowód. ■

Przed następnym zadaniem udowodnimy mały lemacik, który przyda nam się w przyszłości. Otóż z małego twierdzenia Fermata wiemy, że dla każdego a niepodzielnego przez p jest $a^{p-1} \equiv 1 \pmod p$. Niech $\omega_p(a)$ będzie najmniejszą liczbą naturalną taką, że

$$a^{\omega_p(a)} \equiv 1 \pmod p.$$

Liczbą $\omega_p(a)$ nazywamy wykładnikiem do jakiego należy a według modułu p. Udowodnimy:

Lemacik: *Jeśli* $a^m \equiv 1 \pmod p$, *to* $\omega_p(a) \mid m$.

Dowód: Niech $m = k \cdot \omega_p(a) + r$, gdzie $0 \leq r < \omega_p(a)$ (dzielenie z resztą). Zatem $1 \equiv a^m = a^{k \cdot \omega_p(a) + r} = (a^{\omega_p(a)})^k \cdot a^r \equiv 1^k \cdot a^r = a^r \pmod p$. Ale wobec minimalności $\omega_p(a)$ i nierówności $r < \omega_p(a)$ musi być $r = 0$, tzn. $\omega_p(a) \mid m$. ■

Wniosek 6: *Jeśli* $a^m = 1 \pmod p$ *i* $a^n \equiv 1 \pmod p$, *to* $a^{(m,n)} \equiv 1 \pmod p$.

Dowód pozostawiam Czytelnikowi.

Możemy teraz przejść do następnego zadania.

Zadanie: Niech $A = 10^{10^{10}} + 1$. Dowieść, że

(1) A ma co najmiej 11 różnych dzelników pierwszych,

(2) każdy dzielnik pierwszy A jest większy od 10^4.

Rozwiązanie: (1) Głównym pomysłem, jaki tu zastosujemy, będzie rozłożenie liczby A na iloczyn 11 czynników i wykazanie, że są one parami względnie pierwsze. W tym celu przypomnijmy znaną zapewne Czytelnikowi tożsamość:

$$x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + x^{n-3} \ldots + 1),$$

gdzie n jest nieparzystą liczbą naturalną.

Jeśli teraz zauważymy, że $10^{10} = 2^{10} \cdot \underbrace{5 \cdot 5 \cdot \ldots \cdot 5}_{10 \text{ razy}}$, oraz przyjmiemy w naszej tożsamości $n = 5$ otrzymując tożsamość

$$\frac{x^5+1}{x+1} = x^4 - x^3 + x^2 - x + 1$$

(z której wynika, że jeśli n jest liczbą naturalną, to $\frac{n^5+1}{n+1}$ też), to możemy napisać, że

$$A = 10^{10^{10}} + 1 = (10^{2^{10} \cdot 5^9})^5 + 1 = (10^{2^{10} \cdot 5^9} + 1) \cdot A_9,$$

gdzie liczby $A_i = \frac{(10^{2^{10} \cdot 5^i})^5 + 1}{10^{2^{10} \cdot 5^i} + 1}$, $i = 0, 1, \ldots$, są liczbami naturalnymi.

Podobnie $10^{2^{10} \cdot 5^9} + 1 = (10^{2^{10} \cdot 5^8})^5 + 1 = (10^{2^{10} \cdot 5^8} + 1) \cdot A_8$, itd. Stąd otrzymujemy rozkład liczby A na iloczyn 11 czynników:

$$A = (10^{2^{10}} + 1) \cdot A_0 \cdot A_1 \cdot \ldots \cdot A_9 .$$

Pozostaje sprawa względnej pierwszości czynników. Powróćmy przeto na chwilę do naszej tożsamości, z której wynika, że jeśli $n \equiv -1 \pmod p$, to $\frac{n^5+1}{n+1} = n^4 - n^3 + n^2 - n + 1 \equiv 5 \pmod p$, a stąd jedynym wspólnym dzielnikiem pierwszym liczb $n+1$ i $\frac{n^5+1}{n+1}$ może być 5 (dlaczego?). W szczególności, jeśli $5 \nmid n+1$, to liczby $n+1$ i $\frac{n^5+1}{n+1}$ są względnie pierwsze. Biorąc za n liczbę $10^{2^{10} \cdot 5^i}$ otrzymujemy, że $(10^{2^{10} \cdot 5^i} + 1, A_i) = 1$. Ale jeśli $i > j$, to $A_j \mid 10^{2^{10} \cdot 5^{j+1}} + 1 \mid 10^{2^{10} \cdot 5^i} + 1$ (dlaczego?), więc również $(A_i, A_j) = 1$. Zatem w iloczynie

$$A = (10^{2^{10}} + 1) \cdot A_0 \cdot A_i \cdot \ldots \cdot A_9$$

każde dwa czynniki są względnie pierwsze i większe od 1. Każdy z tych czynników daje więc co najmniej jeden dzielnik pierwszy liczby A i każdy inny, wobec czego A ma co najmniej 11 różnych dzielników pierwszych.

(2) Niech $p \mid A$. Postaramy się pokazać, że liczba $p-1$ ma duży dzielnik. W tym celu zauważmy, że $10^{2^{10} \cdot 5^{10}} \equiv -1 \pmod p$, skąd $10^{2^{11} \cdot 5^{10}} \equiv 1 \pmod p$ (podnieśliśmy stronami do kwadratu). Oczywiście $(p, 10) = 1$, więc z małego twierdzenia Fermata mamy również $10^{p-1} \equiv 1 \pmod p$. Przypomnijmy teraz sobie udowodniony lemacik. Niech $\omega = \omega_p(10)$. Zatem $\omega \mid p-1$ i $\omega \mid 2^{11} \cdot 5^{10}$ (dzielnik liczby $p-1$ już mamy!). Z ostatniej podzielności wnosimy, że $\omega = 2^\alpha \cdot 5^\beta$, gdzie $0 \le \alpha \le 11$ i $0 \le \beta \le 10$. Gdyby $\alpha \le 10$ to podnosząc kongruencję $10^{2^\alpha \cdot 5^\beta} \equiv 1 \pmod p$ stronami do potęgi $2^{10-\alpha} \cdot 5^{10-\beta}$ otrzymalibyśmy kongruencję: $10^{2^{10} \cdot 5^{10}} \equiv 1 \pmod p$, co przeczy kongruencji $10^{2^{10} \cdot 5^{10}} \equiv -1 \pmod p$ (bo $p \neq 2$). Zatem musi być $\alpha = 11$, skąd $\omega = k \cdot 2^{11}$. Tym samym, wobec $\omega \mid p-1$, mamy $p - 1 = N \cdot 2^{11}$ dla pewnego N, tzn. $p = 2048N + 1$. Podstawiając $N = 1, 2, 3, 4, 5$ otrzymujemy liczby złożone (podzielne odpowiednio przez $3, 17, 5, 3, 7$ – proszę sprawdzić!). Zatem $N \ge 6$ i $p \ge 2048 \cdot 6 + 1 > 10^4$, czego należało dowieść. Okazuje się, że liczba $2048 \cdot 6 + 1$ jest pierwsza. Proponuję Czytelnikowi rozstrzygnąć, czy dzieli ona liczbę A (być może z pomocą komputera?!). ■

Przejdźmy teraz do następnego zadania, najtrudniejszego moim zdaniem, którego rozwiązanie, aczkolwiek nie potrzebuje niczego więcej ponad to, co już zostało powiedziane, jednakże wymaga nieco subtelniejszego rozumowania.

Zadanie to ma dosyć ciekawą historię. Było ono jednym z problemów konkursowych na Polsko-Austriackich Zawodach Matematycznych w 1987 roku. Nikt z uczestników nie zdołał rozwiązać tego zadania. Co ciekawsze, okazało się, że rozwiązanie autorskie było błędne i do końca zawodów nie udało się znaleźć poprawnego rozwiązania.

Zadanie: Niech u będzie kwadratem liczby naturalnej, której każdy dzielnik pierwszy ma w zapisie dziesiętnym parzystą ilość cyfr. Wykazać, że wielomian $f(x) = x^n - 1987x$ jest różnowartościowy dla liczb wymiernych, tzn. dla dowolnych liczb wymiernych w_1, w_2 jeśli $f(w_1) = f(w_2)$, to $w_1 = w_2$.

Rozwiązanie: Spróbujemy metody sprowadzania do sprzeczności. Załóżmy przeto, że istnieją różne liczby wymierne $\omega_1 = \frac{a}{c}$ i $\omega_2 = \frac{b}{d}$, gdzie $c > 0$, $d > 0$ i $(a, c) = 1 = (b, d)$, (a, b, c, d – liczby całkowite) takie, że $f(\omega_1) = f(\omega_2)$. Mamy zatem

$$\frac{a^n}{c^n} - 1987\frac{a}{c} = \frac{b^n}{d^n} - 1987\frac{b}{d},$$

skąd

$$(*) \qquad a^n - d^n - 1987ac^{n-1}d^n = b^nc^n - 1987bd^{n-1}c^n.$$

W szczególności $c^n \mid d^n(a^n - 1987ac^{n-1})$, a że $(c^n, a^n - 1987ac^{n-1}) = 1$ (gdyby $p \mid c^n$ i $p \mid a^n - 1987ac^{n-1}$, to $p \mid c$ i $p \mid a$ wbrew temu, że $(a, c) = 1$), więc $c^n \mid d^n$. Analogicznie wykazujemy, że $d^n \mid c^n$, skąd $c^n = d^n$ (bo są to liczby dodatnie), a stąd $c = d$. Tym samym równość $(*)$ przyjmuje postać (po podzieleniu obu stron przez $c^n = d^n$)

$$a^n - 1987ac^{n-1} = b^n - 1987bc^{n-1},$$

tzn.

$$a^n - b^n = 1987c^{n-1}(a - b).$$

Aby uzyskać sprzeczność wystarczy więc wykazać, że równanie

$$x^n - y^n = pz^{n-1}(x - y)$$

nie ma rozwiązań w liczbach całkowitych x, y, z takich, że $x \neq y$ dla $p = 1987$, (1987, jak łatwo sprawdzić, jest liczbą pierwszą, a ponadto liczba $p - 1 = 1987 - 1 = 2 \cdot 3 \cdot 331$ ma dzielniki pierwsze mające nieparzystą ilość cyfr, skąd wobec założenia o n mamy $(p - 1, n) = 1$).

Wykażemy, że równanie to nie ma rozwiązań x, y, z takich, że $x \neq y$ przy ogólniejszym założeniu, że p jest nieparzystą liczbą pierwszą taką, że $(p - 1, n) = 1$, a $n > 1$ jest kwadratem liczby naturalnej. Ale jak to zrobić? Spróbujmy badać podzielność przez p obu stron rozpatrywanego równania. Obliczymy więc, w jakiej potędze p dzieli $x^n - y^n$, w jakiej $pz^{n-1}(x - y)$ i z porównania tych potęg otrzymamy (miejmy nadzieję) sprzeczność. Aby zrealizować powyższy plan udowodnimy następujący lemat:

Lemat: *Niech p będzie liczbą pierwszą, n – liczbą naturalną, a, b – liczbami całkowitymi. Wówczas*

1° *Jeśli $p \nmid a - b$ i $(p - 1, n) = 1$ to $p \nmid a^n - b^n$*

2° *Jeśli $p \nmid n$, $p^\alpha \parallel a - b$, $\alpha \geq 1$ oraz $p \nmid a \cdot b$ to $p^\alpha \parallel a^n - b^n$*

3° *Jeśli $2 \neq p$, $p \nmid a \cdot b$ i $p^\alpha \parallel a - b$, $\alpha \geq 1$ to $p^{\alpha+1} \parallel a^p - b^p$.*

Dowód: Jeśli $p \mid a \cdot b$ (tzn. $p \mid a$ lub $p \mid b$) to wobec $p \nmid a - b$ liczba p dzieli dokładnie jedną z liczb a, b, zatem $p \nmid a^n - b^n$. Jeśli natomiast $p \nmid a$ i $p \nmid b$, to gdyby $p \mid a^n - b^n$, tzn. $a^n \equiv b^n \pmod p$, wówczas (mnożąc ostatnią kongruencję stronami przez h_b^n – patrz wniosek 5) otrzymamy $(a \cdot h_b)^n \equiv 1 \pmod p$. Ale wobec małego twierdzenia Fermata mamy również $(ah_b)^{p-1} \equiv 1 \pmod p$. Zatem korzystając z wniosku 6 otrzymujemy

$$(ah_b)^{(p-1,n)} \equiv 1 \pmod p.$$

Ale $(p - 1, n) = 1$, więc $ah_b \equiv 1 \pmod p$, a że $bh_b \equiv 1 \pmod p$, więc mamy $(a - b)h_b \equiv 0 \pmod p$ i wobec $p \nmid h_b$ otrzymujemy $p \mid a - b$, wbrew założeniu.

2° Mamy równość $a^n - b^n = (a-b)\sum_{i=0}^{n-1} a^i b^{n-1-i}$. Wobec kongruencji $a \equiv b \pmod p$ mamy $a^i \equiv b^i \pmod p$, a stąd $a^i b^{n-1-i} \equiv a^i a^{n-1-i} = a^{n-1} \pmod p$. Zatem $\sum_{i=0}^{n-1} a^i b^{n-1-i} \equiv \sum_{i=0}^{n-1} a^{n-1} = na^{n-1} \pmod p$, a że $p \nmid n$ i $p \nmid a$ więc $p \nmid \sum_{i=0}^{n-1} a^i b^{n-1-i}$. Wobec tego oczywiście $p^\alpha \parallel a^n - b^n$.

3° Niech $a - b = k \cdot p^\alpha$. Zatem $a = b + kp^\alpha$ i $p \nmid k$. Korzystając z wzoru dwumianowego otrzymujemy: $a^p = b^p + p \cdot b^{p-1} \cdot kp^\alpha + \sum_{i=2}^{p} \binom{p}{i} b^{p-i} k^i p^{\alpha i}$. Ale, jak pamiętamy, dla $1 \le i \le p-1$ jest $p \mid \binom{p}{i}$ (lemat 1), tzn. $\binom{p}{i} = p \cdot \omega_i$, skąd otrzymujemy równość (pamiętajmy, że $p \ge 3$):

$$a^p - b^p = p^{\alpha+1}\left(kb^{p-1} + \sum_{i=2}^{p-1} \omega_i b^{p-i} k^i p^{\alpha(i-1)} + k^p p^{(p-1)\alpha-1}\right).$$

Wobec założenia $p \nmid kb^{p-1}$ oraz oczywiście $p \mid \sum_{i=2}^{p-1} \omega_i b^{p-i} k^i p^{\alpha(i-1)} + k_p^{p(p-1)\alpha-1}$ (bo p dzieli każdy składnik; tu wykorzystujemy założenie, że $p \ge 3$, skąd $p-1 \mid \alpha - 1 \ge 1$). Zatem p nie dzieli sumy w nawiasie, a stąd $p^{\alpha+1} \parallel a^p - b^p$. ■

Dla pełności dodamy tu jeszcze, że jeśli $p = 2$ i $\alpha \ge 2$, to 3° również zachodzi, co łatwo wynika z powyższego dowodu.

Z części 3° lematu wynika następujący wniosek:

Wniosek: *Przy założeniach jak w 3° mamy*

$$p^{\alpha+k} \parallel a^{p^k} - b^{p^k}$$

Przeprowadzenie prostej indukcji pozostawiam Czytelnikowi. Proponuję też rozpatrzenie przypadku $p = 2$.

Możemy teraz przejść do rozwiązania zadania. Jak pamiętamy, chcemy udowodnić, że równanie

$$x^n - y^n = pz^{n-1}(x-y)$$

nie ma rozwiązań w liczbach całkowitych takich, że $x \ne y$ (tutaj p jest nieparzystą liczbą pierwszą taką, że $(p-1, n) = 1$ oraz $n > 1$ jest kwadratem liczby naturalnej). Załóżmy bowiem, że $x = a$, $y = b$, $z = c$ jest rozwiązaniem oraz $a \ne b$ i a, b, c nie mają wspólnego dzielnika (jeśli a, b, c mają wspólny dzielnik to skracając przez największy wspólny dzielnik otrzymamy rozwiązanie spełniające nasze wymagania). Gdyby $p \mid a$ lub $p \mid b$, to wobec $p \mid a^n - b^n$ mielibyśmy $p \mid a$ i $p \mid b$ oraz $c^{n-1}p = \frac{a^n - b^n}{a-b} = \sum_{i=0}^{n-1} a^i b^{n-1-i}$ byłoby podzielne przez p^{n-1}. Zatem $p^{n-2} \mid c^{n-1}$, a że $n \ge 4$, więc stąd $p \mid c$, co przeczy względnej pierwszości a, b, c. Tym samym wykazaliśmy, że $p \nmid a \cdot b$. Jak już zauważyliśmy $p \mid a^n - b^n$. Wobec punktu 1° lematu wynika stąd, że $p \mid a - b$. Niech zatem $p^\alpha \parallel a - b$ i $n = p^{2\beta} \cdot n_1$, gdzie $\alpha \ge 1$, $\beta \ge 0$ i $p \nmid n_1$.

Wobec punktu 2° mamy $p^\alpha \parallel a^{n_1} - b^{n_1}$, a wobec wniosku mamy $p^{\alpha+2\beta} \parallel (a^{n_1})^{p^{2\beta}} - (b^{n_1})^{p^{2\beta}} = a^n - b^n$. Z drugiej strony, jeśli $p^\gamma \parallel c$, $\gamma \ge 0$, to $p^{\alpha+\gamma(n-1)+1} \parallel c^{n-1}p(a-b)$. Zatem musi być $p^{\alpha+\gamma(n-1)+1} = p^{\alpha+2\beta}$, skąd $\gamma(n-1) + 1 = 2\beta$. Musi więc być $\gamma \ge 1$ skąd $2\beta \ge n$. Ale stąd wynika, że $n = p^{2\beta \cdot n_1} \ge p^n$, co jest ewidentnie nieprawdą, bo $p^n > n$ (dlaczego?). Tym samym uzyskaliśmy w końcu upragnioną sprzeczność. Widać tu jak daleka jest czasem droga od pomysłu do pełnego rozwiązania. Swoją drogą bardzo ciekawe, że tak niewielkie środki pozwalają osiągnąć tyle wyników. Sytuacja przypomina tu trochę malarstwo, gdzie za pomocą prostego zestawu farbek można malować bardzo złożone obrazy.

Na zakończenie jeszcze jedno zadanie by podkreślić użyteczność ostatniego lematu. Zadanie to było zadaniem nr 3 na 31 Międzynarodowej Olimpiadzie Matematycznej. Za rozwiązanie tego zadania można było uzyskać od 0 do 7

punktów, natomiast średnia ocena uzyskana za to zadanie wyniosła 2,1. Zadanie to brzmi następująco:

Zadanie: Znaleźć wszystkie liczby naturalne $n > 1$ takie, że $n^2 \mid 2^n + 1$.

Rozwiązanie: Załóżmy, że $n^2 \mid 2^n + 1$. Co można powiedzieć o n? Przede wszystkim, ponieważ $2 \nmid 2^n + 1$, więc $2 \nmid n$. Niech p będzie dzielnikiem pierwszym n. Wówczas $p \mid 2^n + 1$ skąd $p \mid 2^{2n} - 1$. Wobec tego $\omega_p(2) \mid 2n$ (patrz lemacik). Ponadto, wobec małego twierdzenia Fermata, $p \mid 2^{p-1} - 1$ (bo $p \neq 2$), więc $\omega_p(2) \mid p - 1$. Stąd $\frac{\omega_p(2)}{(\omega_p(2),2)} \mid n$ i $\frac{\omega_p(2)}{(\omega_p(2),2)} < p$ (dlaczego?). Tym samym dla każdej liczby pierwszej dzielącej n znaleźliśmy dzielnik n mniejszy od tej liczby. W szczególności, jeśli p_1 jest najmniejszym dzielnikiem pierwszym n, to musi być $\frac{\omega_{p_1}(2)}{(\omega_{p_1}(2),2)} = 1$ (dlaczego?), a stąd $\omega_{p_1}(2) = 2$ (bo $\omega_p(2) > 1$ dla dowolnego p). Zatem $p_1 \mid 2^2 - 1 = 3$, skąd $p_1 = 3$. Niech więc $3^\alpha \parallel n$. Ponieważ $3^1 \parallel 2 - (-1)$ więc wobec punktu 2° lematu i wniosku po nim mamy $3^{1+\alpha} \parallel 2^n - (-1)^n = 2^n + 1$ (bo $2 \nmid n$). Ponieważ jednak $n^2 \mid 2^n + 1$, więc $3^{2\alpha} \mid 2^n + 1$, a stąd $2\alpha \leq 1 + \alpha$, tzn. $\alpha = 1$. Tym samym $3 \parallel n$. Najmniejszy dzielnik pierwszy n został więc rozpracowany. Jeśli n nie ma innych dzielników pierwszych, to $n = 3$ i wówczas rzeczywiście $3^2 \mid 2^3 + 1$. W przeciwnym razie niech p_2 będzie najmniejszym dzielnikiem pierwszym n większym od 3. Z dotychczasowych rozważań wiemy, że $n = 3n_1$, $3 \nmid n_1$ oraz $\frac{\omega_{p_2}(2)}{(\omega_{p_2}(2),2)} < p_2$ jest dzielnikiem n. Ponieważ każdy dzielnik pierwszy n_1 jest nie mniejszy od p_2, więc $\frac{\omega_{p_2}(2)}{(\omega_{p_2}(2),2)}$ jako mniejsze od p_2 musi dzielić 3. Stąd $\omega_{p_2}(2) \in \{2, 3, 6\}$ (dlaczego?). Gdyby $\omega_{p_2}(2) = 3$, to mielibyśmy $2^3 \equiv 1 \pmod{p_2}$, skąd $2^{3 \cdot n_1} = 2^n \equiv 1 \pmod{p_2}$, a że $2^n \equiv -1 \pmod{p_2}$, więc otrzymujemy sprzeczność. Jeśli $\omega_{p_2}(2) = 2$, to $p_2 \mid 2^2 - 1 = 3$, co jest niemożliwe, bo $p_2 > 3$. Jeśli w końcu $\omega_{p_2}(2) = 6$, to $p_2 \mid 2^6 - 1 = 63 = 7 \cdot 9$ i $p_2 \nmid 2^3 - 1 = 7$, skąd $p_2 \mid 9$, co również jest niemożliwe. Uzyskana we wszystkich przypadkach sprzeczność dowodzi, że n nie może mieć dzielników pierwszych większych od 3. Tym samym jedyną liczbą spełniającą warunki zadania jest $n = 3$.

Mam nadzieję, że choć w niewielkim stopniu udało mi się przekonać Czytelnika o prawdziwości słów G. Hardy'ego zawartych we wstępie. Wydaje mi się, że tematyka poruszona w tym artykule znakomicie nadaje się na zajęcia kółka matematycznego i w dzisiejszej trudnej sytuacji matematyki szkolnej może być dobrym przykładem pięknej matematyki urzekającej uczniów i przekonującej ich o nieprzeciętnych walorach dyscypliny, która z jednej strony zwana jest królową nauk, z drugiej zaś jest postrachem uczniów i ich rodziców.

By ułatwić uzupełnienie i pogłębienie wiadomości i rozwiązanie zawartych w artykule zadań podaję niewielką bibliografię, której pozycje powinny znajdować się w bibliotekach szkolnych.

Literatura

1. Wacław Sierpiński, „Arytmetyka teoretyczna", Biblioteka Matematyczna t. 7, PWN, Warszawa 1959.
2. Wacław Sierpiński: „250 zadań z elementarnej teorii liczb", Biblioteka Matematyczna t. 17, WSiP, Warszawa 1987.
3. Wacław Sierpiński, „Co wiemy a czego nie wiemy o liczbach pierwszych", Biblioteka Matematyczna, PZWS, Warszawa 1961.
4. Wacław Sierpiński, „Wstęp do teorii liczb", Biblioteka Matematyczna, WSiP, Warszawa 1987.
5. Wacław Sierpiński, „Teoria liczb", Monografie Matematyczne, PWN, Warszawa–Wrocław, 1950.
6. Wacław Sierpiński, „Teoria liczb, część II", Monografie Matematyczne tom 38, PWN, Warszawa 1959.