21. *Udowodnij, że dla dowolnej liczby całkowitej dodatniej n, równanie*

$$x^n + y^{n+1} = z^{n+2}$$

ma rozwiązanie w liczbach całkowitych dodatnich x, y, z.

Rozwiązanie

Rozpatrzymy dwa przypadki.

1° Liczba n jest nieparzysta.

W tym przypadku liczby n, $n+1$ oraz $n+2$ są parami względnie pierwsze (ponieważ wspólny dzielnik dwóch liczb dzieli również ich różnicę).

Poszukamy rozwiązania, przy którym dane w zadaniu równanie przyjmuje postać

$$2^r + 2^r = 2^{r+1}.$$

Na mocy chińskiego twierdzenia o resztach istnieje taka nieujemna liczba całkowita r, że

$$r \equiv 0 \pmod{n}, \quad r \equiv 0 \pmod{n+1} \quad \text{oraz} \quad r \equiv -1 \pmod{n+2}.$$

Wówczas liczby

$$a = \frac{r}{n}, \quad b = \frac{r}{n+1}, \quad c = \frac{r+1}{n+2}$$

są całkowite nieujemne i dla uzyskania rozwiązania równania wystarczy przyjąć $x = 2^a$, $y = 2^b$, $z = 2^c$.

2° Liczba n jest parzysta.

W tym przypadku x^n oraz z^{n+2} są kwadratami liczb naturalnych, więc ich iloraz jest kwadratem liczby wymiernej. Wyjdziemy więc od równości $1+3=4$, w której iloraz sumy przez pierwszy ze składników jest kwadratem liczby wymiernej. Następnie przemnożymy tę równość przez potęgi czynników pierwszych występujących w jej wyrazach, w tym wypadku 2 i 3.

Szukamy więc rozwiązania, przy którym dane w zadaniu równanie przyjmuje postać

$$2^p \cdot 3^q + 2^p \cdot 3^{q+1} = 2^{p+2} \cdot 3^q.$$

Rozwiązaniem jest wówczas trójka liczb

$$x = 2^{p/n} \cdot 3^{q/n}, \quad y = 2^{p/(n+1)} \cdot 3^{(q+1)/(n+1)}, \quad z = 2^{(p+2)/(n+2)} \cdot 3^{q/(n+2)},$$

o ile wszystkie wykładniki są liczbami całkowitymi. To z kolei wymaga spełnienia następujących kongruencji:

$$p \equiv 0 \pmod{n}, \quad p \equiv 0 \pmod{n+1}, \quad p \equiv -2 \pmod{n+2},$$

a także

$$q \equiv 0 \pmod{n}, \quad q \equiv -1 \pmod{n+1}, \quad q \equiv 0 \pmod{n+2}.$$

Powyższe układy kongruencji mają rozwiązania p i q będące liczbami całkowitymi nieujemnymi na mocy następującej ogólnej wersji chińskiego twierdzenia o resztach:

Niech m_1, m_2, ,m_3, …, m_k będą liczbami całkowitymi dodatnimi oraz niech liczby r_1, r_2, ,r_3, …, r_k będą całkowite. Załóżmy, że dla dowolnych $1 \leqslant i < j \leqslant k$ liczba $r_i - r_j$ jest podzielna przez NWD(m_i, m_j). Wówczas układ kongruencji

$$a \equiv r_i \pmod{m_i}, \quad i = 1, 2, 3, \ldots, k$$

ma rozwiązanie a będące liczbą całkowitą nieujemną.

W naszym przypadku NWD$(n, n+1)$ =NWD$(n+1, n+2) = 1$ oraz NWD$(n, n+2) = 2$.

---

22. *Udowodnij, że istnieje taka liczba całkowita dodatnia n, że dla dowolnej liczby całkowitej a liczba*

$$\left(a^5\right)^n - a$$

jest podzielna przez 9991.

Rozwiązanie

Zauważmy, że

$$9991 = 100^2 - 3^2 = 97 \cdot 103,$$

a przy tym liczby 97 i 103 są pierwsze.

Z małego twierdzenia Fermata wynika (zob. rozwiązanie zad. 7 z serii II), że dla dowolnej liczby całkowitej a oraz liczb naturalnych s, t

$$a^{96s+1} \equiv a \pmod{97} \quad \text{oraz} \quad a^{102t+1} \equiv a \pmod{103}.$$

Po podstawieniu $s = 17k$ oraz $t = 16k$, powyższe kongruencje przyjmują odpowiednio postać

$$a^{1632k+1} \equiv a \pmod{97} \quad \text{oraz} \quad a^{1632k+1} \equiv a \pmod{103},$$

skąd

$$a^{1632k+1} \equiv a \pmod{9991}$$

dla dowolnej liczby naturalnej k.

W szczególności dla $k = 2$ otrzymujemy

$$a^{3265} \equiv a \pmod{9991},$$

wobec czego warunki zadania spełnia $n = 3265/5 = 653$, gdyż $\left(a^5\right)^n = a^{5n}$.

Uwaga

Pozornie dziwne sformułowanie zadania, gdzie występuje $\left(a^5\right)^n$ zamiast bardziej naturalnego a^{5n}, wynika z kryptograficznej interpretacji udowodnionego faktu:

Operacją odwrotną do podnoszenia do piątej potęgi *modulo* 9991, jest podnoszenie do potęgi 653 *modulo* 9991.

W ogromnym uproszczeniu, zagadnienie kryptograficzne dotyczy następującej sytuacji. Wyobraźmy sobie, że chcemy otrzymać od naszego współpracownika tajną wiadomość a, będącą liczbą całkowitą z zakresu od 0 do 9990, jednak nie dysponujemy sekretnym kanałem komunikacji. W szczególności nie mamy możliwości przekazania partnerowi w sposób poufny instrukcji dotyczących sposobu zaszyfrowania informacji. Co robimy? Ogłaszamy publicznie przepis na szyfrowanie wiadomości a kierowanej do nas: *Prześlij mi resztę z dzielenia a^5 przez 9991, czyli a podniesione do piątej potęgi modulo 9991.* Aby odszyfrować taką informację, należy odwrócić operację podnoszenia do piątej potęgi *modulo* 9991. W rozwiązaniu

zadania uzyskaliśmy przepis, jak to zrobić, a mianowicie wystarczy otrzymaną zaszyfrowaną wiadomość podnieść do potęgi 653 *modulo* 9991. Wykładnik 653, będący kluczem do rozszyfrowania wiadomości, jest naszą tajemnicą. Uzyskaliśmy go znając rozkład liczby 9991 na czynniki pierwsze. Znalezienie tego rozkładu jest równoznaczne ze złamianiem szyfru. Liczba 9991 jest na tyle mała, że rozłożenie jej na czynniki pierwsze nie nastręcza specjalnych trudności. Gdyby jednak zamiast liczby 9991 użyć liczby $m = pq$, gdzie p i q są odpowiednio wybranymi kilkusetcyfrowymi liczbami pierwszymi, to według obecnego stanu wiedzy można bezpiecznie przyjąć, że znalezienie czynników p i q przy znajomości liczby m jest w praktyce niewykonalne.

Wedle najlepszej wiedzy autora zadania, zagadnienie numerycznego rozwiązania kongruencji

$$a^5 \equiv r \pmod{9991}$$

przy ustalonym r, w ogólnym przypadku nie daje się rozwiązać istotnie szybciej niż przez kolejne sprawdzanie $a = 0, 1, 2, 3, \ldots, 9990$, jeżeli nie wykorzystamy znajomości rozkładu liczby 9991 na czynniki pierwsze — bez znajomości tego rozkładu nie bylibyśmy w stanie znaleźć *magicznego* wykładnika 653.

---

23. *Dana jest liczba całkowita dodatnia n. Udowodnij, że pewna jej wielokrotność ma w zapisie dziesiętnym tylko cyfry mniejsze od 3, a przy tym cyfr tych jest nie więcej niż $(n+1)/2$.*

Rozwiązanie

Rozważmy liczby

$$0,\ 1,\ 2,\ 12,\ 22,\ 122,\ 222,\ 1222,\ 2222,\ 12222,\ 22222,\ \ldots,\ 222\ldots22,$$

gdzie ostatnia liczba jest zapisana za pomocą $[(n+1)/2]$ dwójek ($[x]$ oznacza część całkowitą liczby x, czyli największą liczbę całkowitą nie większą od x). Dla parzystych n mamy $[(n+1)/2] = n/2$, natomiast dla nieparzystych n zachodzi $[(n+1)/2] = (n+1)/2 > n/2$. Rozpatrywanych liczb jest w takim razie

$$2 \cdot [(n+1)/2] + 1 \geqslant 2 \cdot (n/2) + 1 = n + 1 > n.$$

Zatem pewne dwie liczby dają przy dzieleniu przez n tę samą resztę.

Różnica większej i mniejszej z nich jest więc podzielna przez n, a ponadto nie ma ona w zapisie dziesiętnym cyfr innych niż 0, 1, 2, gdyż przy wyborze dowolnych dwóch z wypisanych na początku liczb, odejmowanie mniejszej od większej odbywa się *bez przeniesienia*.

---

24. *Okrąg, którego średnicą jest wysokość AH trójkąta ABC, przecina boki AB i AC odpowiednio w punktach D i E. Niech O będzie środkiem okręgu opisanego na trójkącie ABC. Wykaż, że prosta OA jest prostopadła do prostej DE.*

Rozwiązanie

Z równoramienności trójkąta AOC, sumy jego kątów, twierdzenia o kącie środkowym i wpisanym oraz z sumy kątów w trójkącie ABH otrzymujemy

$$\sphericalangle EAO = \frac{1}{2}(180^\circ - \sphericalangle AOC) = \frac{1}{2}(180^\circ - 2 \cdot \sphericalangle ABC) = 90^\circ - \sphericalangle ABC = \sphericalangle BAH.$$

Ponieważ AH jest średnicą okręgu opisanego na czworokącie $ADHE$, mamy

$$\sphericalangle AED = \sphericalangle AHD = 90^\circ - \sphericalangle DAH = 90^\circ - \sphericalangle BAH.$$

W takim razie kąt pomiędzy prostymi DE i AO wynosi $180^\circ - \sphericalangle EAO - \sphericalangle AED = 90^\circ$.

---

25. *Pewien wielościan wypukły ma n wierzchołków. Oblicz sumę kątów płaskich wszystkich jego ścian.*

Rozwiązanie

Niech k oznacza liczbę krawędzi naszego wielościanu, $S=\{s_1,s_2,\ldots,s_m\}$ niech będzie zbiorem jego ścian, zaś $k(s_i)$ niech oznacza liczbę krawędzi ściany s_i dla $i=1,2,\ldots,m$. Wówczas $k(s_1)+k(s_2)+\ldots+k(s_m)=2k$, ponieważ każda krawędź wielościanu leży w dokładnie dwóch jego ścianach.

Suma kątów płaskich wszystkich ścian wielościanu wynosi

$$(k(s_1)-2)\cdot 180^\circ+(k(s_2)-2)\cdot 180^\circ+\ldots+(k(s_m)-2)\cdot 180^\circ=180^\circ\cdot(2k-2m)=360^\circ\cdot(k-m).$$

Ze wzoru Eulera wiemy, że $k-m=n-2$. W takim razie szukana suma wynosi $360^\circ\cdot(n-2)$.

Urszula Pastwa
Kierownik naukowy obozu