Liga Zadaniowa, Edycja V, Seria 6 (waga 3), Rozwiązania

Zadanie 561. Funkcja $f:\mathbb{R}\to\mathbb{R}$ jest siedmiokrotnie różniczkowalna na całej prostej rzeczywistej, a ponadto

$$f(0)=f'(0)=f''(0)=f'''(0)=f(1)=f'(1)=f''(1)=f'''(1)=0\,.$$

Czy stąd wynika istnienie takiej liczby rzeczywistej c, że $f^{(7)}(c)=0$?

Rozwiązanie:

Korzystając wielokrotnie z twierdzenia Rolle'a udowodnimy, że z założeń o funkcji f wynika istnienie takiej liczby c.

1° Z warunku

$$f(0)=f(1)$$

wynika istnienie takiej liczby $t\in(0,1)$, że

$$f'(t)=0\,.$$

2° Z warunku

$$f'(0)=f'(t)=f'(1)$$

oraz nierówności $0<t<1$ wynika istnienie takich liczb $x_1\in(0,t)$ oraz $x_2\in(t,1)$, że

$$f''(x_1)=f''(x_2)=0\,.$$

3° Z warunku

$$f''(0)=f''(x_1)=f''(x_2)=f''(1)$$

oraz nierówności $0<x_1<x_2<1$ wynika istnienie takich liczb $y_1\in(0,x_1)$, $y_2\in(x_1,x_2)$ oraz $y_3\in(x_2,1)$, że

$$f'''(y_1)=f'''(y_2)=f'''(y_3)=0\,.$$

4° Z warunku

$$f'''(0)=f'''(y_1)=f'''(y_2)=f'''(y_3)=f'''(1)$$

oraz nierówności $0<y_1<y_2<y_3<1$ wynika istnienie takich liczb $z_1\in(0,y_1)$, $z_2\in(y_1,y_2)$, $z_3\in(y_2,y_3)$ oraz $z_4\in(y_3,1)$, że

$$f^{(4)}(z_1)=f^{(4)}(z_2)=f^{(4)}(z_3)=f^{(4)}(z_4)=0\,.$$

5° Z warunku

$$f^{(4)}(z_1)=f^{(4)}(z_2)=f^{(4)}(z_3)=f^{(4)}(z_4)$$

oraz nierówności $z_1<z_2<z_3<z_4$ wynika istnienie takich liczb $a_1\in(z_1,z_2)$, $a_2\in(z_2,z_3)$ oraz $a_3\in(z_3,z_4)$, że

$$f^{(5)}(a_1)=f^{(5)}(a_2)=f^{(5)}(a_3)=0\,.$$

6° Z warunku

$$f^{(5)}(a_1)=f^{(5)}(a_2)=f^{(5)}(a_3)$$

oraz nierówności $a_1<a_2<a_3$ wynika istnienie takich liczb $b_1\in(a_1,a_2)$ oraz $b_2\in(a_2,a_3)$, że

$$f^{(6)}(b_1)=f^{(6)}(b_2)=0\,.$$

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

7° Z warunku

$$f^{(6)}(b_1) = f^{(6)}(b_2)$$

oraz nierówności $b_1 < b_2$ wynika istnienie takiej liczby $c \in (b_1, b_2)$, że

$$f^{(7)}(c) = 0\,,$$

co kończy rozwiązanie zadania.

Zadanie 562. Funkcja $f : \mathbb{R} \to \mathbb{R}$ jest ośmiokrotnie różniczkowalna na całej prostej rzeczywistej, a ponadto

$$f(0) = f'(0) = f''(0) = f'''(0) = f(1) = f'(1) = f''(1) = f'''(1) = 0\,.$$

Czy stąd wynika istnienie takiej liczby rzeczywistej c, że $f^{(8)}(c) = 0$?

Rozwiązanie:

Nie wynika. Rozważmy bowiem funkcję f zdefiniowaną wzorem

$$f(x) = x^4 \cdot (x-1)^4\,.$$

Wówczas pierwsze trzy pochodne funkcji f można zapisać w postaci

$$f'(x) = x^3 \cdot (x-1)^3 \cdot f_1(x)\,,$$
$$f''(x) = x^2 \cdot (x-1)^2 \cdot f_2(x)\,,$$
$$f'''(x) = x \cdot (x-1) \cdot f_3(x)\,,$$

gdzie f_1, f_2, f_3 są funkcjami wielomianowymi. Stąd otrzymujemy

$$f(0) = f'(0) = f''(0) = f'''(0) = f(1) = f'(1) = f''(1) = f'''(1) = 0\,.$$

Ponieważ funkcja f jest wielomianem ósmego stopnia o współczynniku 1 przy x^8, jej pochodna ósmego rzędu jest funkcją stałą, a dokładniej

$$f^{(8)}(x) = 8! = 40320\,.$$

Zatem ósma pochodna funkcji f nie ma miejsc zerowych.

Zadanie 563. Dowieść, że równanie

$$(m^m \cdot n^n)^2 = k^k$$

ma nieskończenie wiele rozwiązań w liczbach całkowitych dodatnich k, m, n.

Rozwiązanie:

Przyjmijmy, że $k = 2n$. Wówczas dane równanie sprowadza się do

$$m^{2m} \cdot n^{2n} = 2^{2n} \cdot n^{2n}\,,$$

czyli

$$m^m = 2^n\,.$$

Jeżeli m jest potęgą dwójki, powiedzmy $m = 2^q$, to

$$m^m = 2^{q \cdot 2^q}\,,$$

skąd wynika, że można przyjąć $n = q \cdot 2^q$ oraz $k = q \cdot 2^{q+1}$.

Odpowiedź: Przykładem nieskończonej rodziny rozwiązań danego równania jest $m = 2^q$, $n = q \cdot 2^q$, $k = q \cdot 2^{q+1}$, gdzie q przebiega liczby całkowite dodatnie.

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Zadanie 564. Interesują nas rozwiązania równania

$$(m^m \cdot n^n)^2 = k^k$$

w takich liczbach całkowitych dodatnich k, m, n, że liczba k nie jest podzielna ani przez m, ani przez n.

Rozstrzygnąć, czy:

a) takie rozwiązania nie istnieją,

b) takie rozwiązania istnieją, ale jest ich skończenie wiele,

c) takich rozwiązań jest nieskończenie wiele.

Rozwiązanie:

Wykażemy, że dane równanie ma nieskończenie wiele rozwiązań spełniających warunki zadania.

Przyjmując $x = m/k$ oraz $y = n/k$ otrzymujemy odpowiednio $m = kx$ oraz $n = ky$. Wówczas dane równanie przyjmuje kolejno postać

$$\left((kx)^{kx} \cdot (ky)^{ky}\right)^2 = k^k\,,$$

$$k^{2kx+2ky} \cdot x^{2kx} \cdot y^{2ky} = k^k\,,$$

$$k^{2x+2y} \cdot x^{2x} \cdot y^{2y} = k\,,$$

$$x^{2x} \cdot y^{2y} = k^{1-2x-2y}\,.$$

Podstawienie

$$p = 2^t - 1, \quad x = \frac{p}{2^{t+2}} \quad \text{oraz} \quad y = \frac{2^{t-2}}{p}\,,$$

gdzie t jest liczbą naturalną większą od 1, prowadzi do

$$x^{2x} \cdot y^{2y} = \left(\frac{p}{2^{t+2}}\right)^{p/2^{t+1}} \cdot \left(\frac{2^{t-2}}{p}\right)^{2^{t-1}/p} = p^{p/2^{t+1} - 2^{t-1}/p} \cdot 2^{(t-2)\cdot 2^{t-1}/p - (t+2)\cdot p/2^{t+1}}\,.$$

Upraszczając wykładniki otrzymujemy

$$\frac{p}{2^{t+1}} - \frac{2^{t-1}}{p} = \frac{p^2 - 2^{t+1}\cdot 2^{t-1}}{p\cdot 2^{t+1}} = \frac{2^{2t} - 2^{t+1} + 1 - 2^{2t}}{p\cdot 2^{t+1}} = -\frac{2^{t+1}-1}{p\cdot 2^{t+1}}$$

oraz

$$\frac{(t-2)\cdot 2^{t-1}}{p} - \frac{(t+2)\cdot p}{2^{t+1}} = \frac{(t-2)\cdot 2^{t-1}\cdot 2^{t+1} - (t+2)\cdot p^2}{p\cdot 2^{t+1}} =$$

$$= \frac{(t-2)\cdot 2^{2t} - (t+2)\cdot(2^{2t} - 2^{t+1} + 1)}{p\cdot 2^{t+1}} =$$

$$= \frac{t\cdot 2^{2t} - 2^{2t+1} - t\cdot 2^{2t} + t\cdot 2^{t+1} - t - 2^{2t+1} + 2^{t+2} - 2}{p\cdot 2^{t+1}} = \frac{-2^{2t+2} + t\cdot 2^{t+1} - t + 2^{t+2} - 2}{p\cdot 2^{t+1}}\,.$$

Ponadto

$$1 - 2x - 2y = 1 - \frac{p}{2^{t+1}} - \frac{2^{t-1}}{p} = \frac{p\cdot 2^{t+1} - p^2 - 2^{t+1}\cdot 2^{t-1}}{p\cdot 2^{t+1}} =$$

$$= \frac{2^{2t+1} - 2^{t+1} - 2^{2t} + 2^{t+1} - 1 - 2^{2t}}{p\cdot 2^{t+1}} = -\frac{1}{p\cdot 2^{t+1}}\,.$$

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Zatem dane równanie przyjmuje postać

$$p^{-\left(2^{t+1}-1\right)/\left(p\cdot 2^{t+1}\right)}\cdot 2^{-\left(2^{2t+2}-t\cdot 2^{t+1}+t-2^{t+2}+2\right)/\left(p\cdot 2^{t+1}\right)}=k^{-1/\left(p\cdot 2^{t+1}\right)},$$

skąd, po obustronnym podniesieniu do potęgi $-p\cdot 2^{t+1}$, otrzymujemy

$$k=p^{2^{t+1}-1}\cdot 2^{2^{2t+2}-t\cdot 2^{t+1}+t-2^{t+2}+2}.$$

W konsekwencji

$$m=k\cdot\frac{p}{2^{t+2}}=p^{2^{t+1}-1}\cdot 2^{2^{2t+2}-t\cdot 2^{t+1}+t-2^{t+2}+2}\cdot\frac{p}{2^{t+2}}=p^{2^{t+1}}\cdot 2^{2^{2t+2}-t\cdot 2^{t+1}-2^{t+2}}$$

oraz

$$n=k\cdot\frac{2^{t-2}}{p}=p^{2^{t+1}-1}\cdot 2^{2^{2t+2}-t\cdot 2^{t+1}+t-2^{t+2}+2}\cdot\frac{2^{t-2}}{p}=p^{2^{t+1}-2}\cdot 2^{2^{2t+2}-t\cdot 2^{t+1}+2t-2^{t+2}}.$$

Zauważmy, że dwójka występuje z najmniejszym wykładnikiem w liczbie m i dla $t\geqslant 2$ wykładnik ten jest dodatni, gdyż

$$2^{2t+2}-t\cdot 2^{t+1}-2^{t+2}=2^{t+1}\cdot\left(2^{t+1}-t-2\right),$$

a dodatniość drugiego czynnika ostatniego iloczynu wynika z nierówności

$$2^{t+1}=(1+1)^{t+1}=\sum_{i=0}^{t+1}\binom{t+1}{i}>\sum_{i=0}^{t+1}1=t+2.$$

Otrzymaliśmy więc rodzinę rozwiązań danych wzorami

$$m=p^{2^{t+1}}\cdot 2^{2^{2t+2}-t\cdot 2^{t+1}-2^{t+2}},\quad n=p^{2^{t+1}-2}\cdot 2^{2^{2t+2}-t\cdot 2^{t+1}+2t-2^{t+2}},$$
$$k=p^{2^{t+1}-1}\cdot 2^{2^{2t+2}-t\cdot 2^{t+1}+t-2^{t+2}+2},$$

gdzie $p=2^t-1$, a t przebiega liczby naturalne większe od 1.

Jeżeli t jest liczbą naturalną większą od 2, to ilorazy

$$\frac{k}{m}=\frac{1}{x}=\frac{2^{t+2}}{p}=\frac{2^{t+2}}{2^t-1}\quad\text{oraz}\quad\frac{k}{n}=\frac{1}{y}=\frac{p}{2^{t+2}}=\frac{2^t-1}{2^{t+2}}$$

nie są liczbami całkowitymi, a zatem liczba k nie jest podzielna ani przez m, ani przez n.

Uwagi:

Rozwiązanie zadania 564 rozwiązuje zadanie 563, jednak znalezienie rozwiązań danego równania spełniających dodatkowy warunek narzucony w zadaniu 564 jest o wiele trudniejsze niż znalezienie rodziny rozwiązań podanej w rozwiązaniu zadania 563.

Istnieją rozwiązania danego równania nienależące do żadnej z rodzin zaprezentowanych w rozwiązaniach zadań 563 i 564. Przykłady takich rozwiązań możemy otrzymać stosując podstawienie podane w zadaniu 564 do następujących wartości (x, y) :

$$(1/3, 1/3),\quad (1/3, 1/4),\quad (1/3, 1/5),\quad (1/3, 3/17),\quad (2/7, 1/4).$$

Jednak nietrudno zauważyć, że w każdym z powyższych przykładów co najmniej jedna z liczb $1/x=k/m$, $1/y=k/n$ jest całkowita, a więc uzyskane w ten sposób rozwiązania nie spełniają warunków zadania 564.

Najmniejsze z uzyskanych przez nas rozwiązań spełniających warunki zadania 564 dostajemy dla $t=3$. W rozwiązaniu tym liczba k ma 68 cyfr, a liczby m i n po 67 cyfr.

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

W poniższej tabeli podajemy wybrane przykłady rozwiązań danego równania.

m	n	k	$x=m/k$	$y=n/k$	Uwagi
2	$1\cdot 2$	$1\cdot 2^2 = 4$	$1/2$	$1/2$	$q=1$
2^2	$2\cdot 2^2$	$2\cdot 2^3 = 16$	$1/4$	$1/2$	$q=2$
2^3	$3\cdot 2^3$	$3\cdot 2^4 = 48$	$1/6$	$1/2$	$q=3$
3^3	3^3	$3^4 = 81$	$1/3$	$1/3$	
2^4	$4\cdot 2^4$	$4\cdot 2^5 = 128$	$1/8$	$1/2$	$q=4$
2^5	$5\cdot 2^5$	$5\cdot 2^6 = 320$	$1/10$	$1/2$	$q=5$
2^6	$6\cdot 2^6$	$6\cdot 2^7 = 768$	$1/12$	$1/2$	$q=6$
2^7	$7\cdot 2^7$	$7\cdot 2^8 = 1792$	$1/14$	$1/2$	$q=7$
2^8	$8\cdot 2^8$	$8\cdot 2^9 = 4096$	$1/16$	$1/2$	$q=8$
$2^6\cdot 3^3$	$2^4\cdot 3^4$	$2^6\cdot 3^4 = 5184$	$1/3$	$1/4$	
2^9	$9\cdot 2^9$	$9\cdot 2^{10} = 9216$	$1/18$	$1/2$	$q=9$
2^{10}	$10\cdot 2^{10}$	$10\cdot 2^{11} = 20480$	$1/20$	$1/2$	$q=10$
2^{11}	$11\cdot 2^{11}$	$11\cdot 2^{12} = 45056$	$1/22$	$1/2$	$q=11$
2^{12}	$12\cdot 2^{12}$	$12\cdot 2^{13} = 98304$	$1/24$	$1/2$	$q=12$
2^{13}	$13\cdot 2^{13}$	$13\cdot 2^{14} = 212992$	$1/26$	$1/2$	$q=13$
2^{14}	$14\cdot 2^{14}$	$14\cdot 2^{15} = 458752$	$1/28$	$1/2$	$q=14$
2^{15}	$15\cdot 2^{15}$	$15\cdot 2^{16} = 983040$	$1/30$	$1/2$	$q=15$
2^{16}	$16\cdot 2^{16}$	$16\cdot 2^{17} = 2097152$	$1/32$	$1/2$	$q=16$
2^{17}	$17\cdot 2^{17}$	$17\cdot 2^{18} = 4456448$	$1/34$	$1/2$	$q=17$
2^{18}	$18\cdot 2^{18}$	$18\cdot 2^{19} = 9437184$	$1/36$	$1/2$	$q=18$
2^{19}	$19\cdot 2^{19}$	$19\cdot 2^{20} = 19922944$	$1/38$	$1/2$	$q=19$
2^{20}	$20\cdot 2^{20}$	$20\cdot 2^{21} = 41943040$	$1/40$	$1/2$	$q=20$
$2^7\cdot 7^7$	$2^4\cdot 7^8$	$2^6\cdot 7^8 = 368947264$	$2/7$	$1/4$	
$3^9\cdot 5^6$	$3^{10}\cdot 5^5$	$3^{10}\cdot 5^6 = 922640625$	$1/3$	$1/5$	
$2^{32}\cdot 3^8$	$2^{36}\cdot 3^6$	$2^{36}\cdot 3^7 = 150\ldots$ (15 cyfr)	$3/16$	$1/3$	$t=2$
$3^{15}\cdot 17^{18}$	$3^{17}\cdot 17^{17}$	$3^{16}\cdot 17^{18} = 605\ldots$ (30 cyfr)	$1/3$	$3/17$	
$2^{176}\cdot 7^{16}$	$2^{182}\cdot 7^{14}$	$2^{181}\cdot 7^{15} = 145\ldots$ (68 cyfr)	$7/32$	$2/7$	$t=3$
$2^{832}\cdot 15^{32}$	$2^{840}\cdot 15^{30}$	$2^{838}\cdot 15^{31} = 527\ldots$ (289 cyfr)	$15/64$	$4/15$	$t=4$
$2^{3648}\cdot 31^{64}$	$2^{3658}\cdot 31^{62}$	$2^{3655}\cdot 31^{63} = 166\ldots$ (1195 cyfr)	$31/128$	$8/31$	$t=5$

Zaprezentowana w rozwiązaniu zadania 564 metoda, po podstawieniu

$$p=2^t-1,\quad x=\frac{p}{2^{t+1}}\quad\text{oraz}\quad y=\frac{2^{t-1}}{p},$$

może posłużyć do znalezienia nieskończonej rodziny rozwiązań równania

$$m^m\cdot n^n=k^k.$$

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Zadanie 565. Dla liczby pierwszej p, na potrzeby tego zadania, *dobrą resztą* nazwiemy każdą taką liczbę całkowitą nieujemną $r<p$, że

$$(r+1)^p \equiv r^p+1 \pmod{p^2}.$$

Dowieść, że dla dowolnej liczby pierwszej p, liczba dobrych reszt nie jest podzielna przez 3.

Rozwiązanie:

Zanim przystąpimy do rozwiązania zadania, przyjrzyjmy się pewnym tożsamościom. Niech $f:\mathbb{R}\setminus\{0\}\to\mathbb{R}$ i $g:\mathbb{R}\to\mathbb{R}$ będą funkcjami określonymi wzorami

$$f(x)=\frac{1}{x} \quad \text{i} \quad g(x)=-x-1.$$

Każda z tych funkcji jest odwrotna do samej siebie, tzn. $f(f(x))=x$ oraz $g(g(x))=x$ dla każdej liczby rzeczywistej x leżącej w dziedzinie odpowiedniej funkcji.

Interesują nas zbiory liczb rzeczywistych zamknięte na działanie funkcji f i g – w tym celu prześledzimy trajektorię liczby rzeczywistej x poddanej działaniu obu tych funkcji. Ponieważ dwukrotne złożenie tej samej funkcji jest identycznością, wystarczy zbadać, co dzieje się z liczbą x po wielokrotnym działaniu tymi funkcjami na przemian.

Otrzymujemy kolejno

$$f(g(x))=\frac{1}{-x-1}=-\frac{1}{x+1},$$

$$g(f(g(x)))=-\left(-\frac{1}{x+1}\right)-1=\frac{1}{x+1}-1=\frac{1-x-1}{x+1}=-\frac{x}{x+1}$$

oraz

$$g(f(x))=-\frac{1}{x}-1=-\frac{x+1}{x},$$

$$f(g(f(x)))=-\frac{x}{x+1}.$$

Otrzymaliśmy więc równość

$$f(g(f(x)))=g(f(g(x)))$$

prawdziwą dla każdej liczby rzeczywistej x, dla której w powyższych rachunkach nie wystąpiło dzielenie przez zero, czyli dla $x\notin\{-1,0\}$.

Schematycznie możemy to zapisać jako

$$-\frac{x}{x+1} \overset{f}{\longleftrightarrow} -\frac{x+1}{x} \overset{g}{\longleftrightarrow} \frac{1}{x} \overset{f}{\longleftrightarrow} x \overset{g}{\longleftrightarrow} -x-1 \overset{f}{\longleftrightarrow} -\frac{1}{x+1} \overset{g}{\longleftrightarrow} -\frac{x}{x+1}.$$

Oznacza to, że rozpoczynając od prawie dowolnej liczby rzeczywistej iterowanie na przemian funkcji f i g, po sześciu iteracjach wrócimy do punktu wyjścia. Zatem zbiór liczb rzeczywistych, z drobnymi wyjątkami, można podzielić na sześcioelementowe podzbiory niezmiennicze na działanie funkcji f i g, w których to podzbiorach z każdej liczby można otrzymać każdą inną przez działanie funkcjami f i g.

Ponieważ przedział $(1,+\infty)$ jest przekształcany przez funkcję f na przedział $(0,1)$, ten z kolei przez funkcję g na przedział $(-2,-1)$ i dalej kolejno przez funkcję f na $(-1,-1/2)$, przez g na $(-1/2,0)$, przez f na $(-\infty,-2)$ i wreszcie przez g z powrotem na $(1,+\infty)$, każda wyżej opisana szóstka liczb zawiera po jednym elemencie z każdego z sześciu wymienionych przedziałów.

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Wyjątki stanowi 5 liczb będących końcami przedziałów. Z liczb tych można stworzyć dwa zbiory.

Zbiór $\{-1, 0\}$ zawiera dwie liczby przekształcane na siebie nawzajem przez funkcję g, liczba 0 jest poza dziedziną funkcji f, a ponadto $f(-1) = -1$. Możemy to schematycznie zapisać jako

$$\textbf{poza dziedziną} \overset{f}{\longleftrightarrow} 0 \overset{g}{\longleftrightarrow} -1 \overset{f}{\longleftrightarrow} -1 \overset{g}{\longleftrightarrow} 0 \overset{f}{\longleftrightarrow} \textbf{poza dziedziną}.$$

Natomiast zbiór $\{-2, -1/2, 1\}$, w którym $f(1) = 1$ oraz $g(-1/2) = -1/2$, możemy przedstawić jako trajektorię długości 6, w której występują powtórzenia, a mianowicie:

$$\mathbf{1} \overset{f}{\longleftrightarrow} 1 \overset{g}{\longleftrightarrow} -2 \overset{f}{\longleftrightarrow} -\frac{1}{2} \overset{g}{\longleftrightarrow} -\frac{1}{2} \overset{f}{\longleftrightarrow} -2 \overset{g}{\longleftrightarrow} \mathbf{1}.$$

Zatem zbiór liczb rzeczywistych podzielony został na sześcioelementowe podzbiory oraz parę i trójkę liczb.

Dokonamy podobnego podziału zbioru reszt modulo p, gdzie p jest dowolną liczbą pierwszą większą od 3. W zbiorze $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ będziemy wykonywać działania modulo p. Zauważmy, że oprócz dodawania, odejmowania i mnożenia, dopuszczalne jest także dzielenie przez resztę różną od zera, gdyż każda niezerowa reszta jest odwracalna.

Zdefiniujmy funkcje $f_p : \mathbb{Z}_p \setminus \{0\} \to \mathbb{Z}_p \setminus \{0\}$ oraz $g_p : \mathbb{Z}_p \to \mathbb{Z}_p$ warunkami

$$f_p(r) = r^{-1} \quad \text{oraz} \quad g_p(r) \equiv -r - 1 \pmod{p},$$

gdzie r^{-1} oznacza resztę odwrotną do r modulo p, czyli jedyną liczbę r^{-1} ze zbioru $\mathbb{Z}_p \setminus \{0\}$ spełniającą kongruencję

$$r \cdot r^{-1} \equiv 1 \pmod{p}.$$

Wówczas każda z tych funkcji jest odwrotna do samej siebie, a ponadto dla dowolnego $r \in \mathbb{Z}_p \setminus \{0, p-1\}$ mamy

$$f_p(g_p(r)) = (-r-1)^{-1} \equiv -(r+1)^{-1} \pmod{p},$$

$$g_p(f_p(g_p(r))) \equiv -\left(-(r+1)^{-1}\right) - 1 = (r+1)^{-1} - 1 \equiv (r+1)^{-1} - (r+1) \cdot (r+1)^{-1} =$$

$$= -(r+1)^{-1} \cdot r \pmod{p},$$

$$g_p(f_p(r)) \equiv -r^{-1} - 1 \equiv -r^{-1} - r \cdot r^{-1} = -r^{-1} \cdot (r+1) \pmod{p},$$

$$f_p(g_p(f_p(r))) = \left(-r^{-1} \cdot (r+1)\right)^{-1} \equiv -r \cdot (r+1)^{-1} \pmod{p}.$$

Powyższe wyniki możemy przedstawić na następującym schemacie, gdzie wszystkie operacje należy rozpatrywać modulo p:

$$\mathbf{R} \overset{f_p}{\longleftrightarrow} -r^{-1} \cdot (r+1) \overset{g_p}{\longleftrightarrow} r^{-1} \overset{f_p}{\longleftrightarrow} r \overset{g_p}{\longleftrightarrow} -r-1 \overset{f_p}{\longleftrightarrow} -(r+1)^{-1} \overset{g_p}{\longleftrightarrow} \mathbf{R}.$$

Powyżej przyjęto oznaczenie $\mathbf{R} = -r \cdot (r+1)^{-1}$.

Zbiór $\mathbb{Z}_p$ możemy więc podzielić następująco:

1° Cykle złożone z sześciu różnych elementów.

2° Elementy, dla których iterowanie funkcji f_p i g_p powoduje problem z dziedziną funkcji f_p. Są to dwa elementy 0 i $p-1$, dla których trajektoria iteracji wygląda następująco:

$$\textbf{poza dziedziną} \overset{f_p}{\longleftrightarrow} 0 \overset{g_p}{\longleftrightarrow} p-1 \overset{f_p}{\longleftrightarrow} p-1 \overset{g_p}{\longleftrightarrow} 0 \overset{f_p}{\longleftrightarrow} \textbf{poza dziedziną}.$$

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

3° Cykle długości 6, w których występuje element powtórzony na kolejnych miejscach (czyli punkt stały funkcji f_p lub g_p). Funkcja f_p ma dwa punkty stałe: 1 oraz $p-1$, przy czym ten drugi został już uwzględniony w przypadku 2°. Funkcja g_p ma jeden punkt stały, a mianowicie $(p-1)/2$. To prowadzi do trójki elementów 1, $(p-1)/2$ i $p-2$, które układają się następująco:

$$\mathbf{1} \overset{f_p}{\longleftrightarrow} 1 \overset{g_p}{\longleftrightarrow} p-2 \overset{f_p}{\longleftrightarrow} \frac{p-1}{2} \overset{g_p}{\longleftrightarrow} \frac{p-1}{2} \overset{f_p}{\longleftrightarrow} p-2 \overset{g_p}{\longleftrightarrow} \mathbf{1}\,.$$

Cykle długości 6, w których występuje element powtórzony na miejscach odległych o 3 zostały już uwzględnione, gdyż taki powtórzony element r musiałby spełniać kongruencję

$$r \equiv -(r+1)^{-1} \cdot r \pmod{p}\,,$$

czyli

$$\begin{gathered} r \cdot (r+1) \equiv -r \pmod{p}\,, \\ r^2 + r \equiv -r \pmod{p}\,, \\ r^2 + 2r \equiv 0 \pmod{p}\,, \\ r \cdot (r+2) \equiv 0 \pmod{p}\,, \end{gathered}$$

skąd $r = 0$ lub $r = p-2$, a te przypadki już rozpatrzyliśmy.

4° Cykle długości 6, w których występuje element powtórzony na miejscach odległych o 2, czyli cykle złożone z dwóch różnych elementów r, r^{-1}.

$$\mathbf{r} \overset{g_p}{\longleftrightarrow} r^{-1} \overset{f_p}{\longleftrightarrow} r \overset{g_p}{\longleftrightarrow} r^{-1} \overset{f_p}{\longleftrightarrow} r \overset{g_p}{\longleftrightarrow} r^{-1} \overset{f_p}{\longleftrightarrow} \mathbf{r}\,.$$

Aby taka konfiguracja miała miejsce, reszta r musi spełniać kongruencję

$$r^{-1} \equiv -r - 1 \pmod{p}\,,$$

czyli

$$\begin{gathered} 1 \equiv -r^2 - r \pmod{p}\,, \\ r^2 + r + 1 \equiv 0 \pmod{p}\,, \\ \left(r^2 + r + 1\right) \cdot (r-1) \equiv 0 \pmod{p}, \quad r \neq 1\,, \\ r^3 - 1 \equiv 0 \pmod{p}, \quad r \neq 1\,, \\ r^3 \equiv 1 \pmod{p}, \quad r \neq 1\,. \end{gathered}$$

To oznacza, że r jest różnym od 1 pierwiastkiem sześciennym z jedności modulo p.

Zatem w przypadku, gdy $p \equiv 5 \pmod{6}$, taki cykl nie istnieje, natomiast w przypadku $p \equiv 1 \pmod{6}$ taki cykl jest dokładnie jeden i składa się z dwóch pierwotnych pierwiastków sześciennych z jedności modulo p.

Podsumujmy: Jeżeli $p = 6k+5$ lub $p = 6k+7$, to zbiór $\mathbb{Z}_p$ rozkłada się na następujące trajektorie względem działania funkcji f_p i g_p:

1° k cykli sześcioelementowych,

2° dwa elementy 0 i $p-1$,

3° cykl zawierający trójkę elementów: 1, $(p-1)/2$ i $p-2$,

4° dwuelementowy cykl złożony z pierwiastków sześciennych z jedności – tylko w przypadku $p = 6k+7$.

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Przechodzimy do rozwiązania zadania.

Łatwo sprawdzić, że dla $p=2$ dobrą resztą jest 0, a dla $p=3$ dobrymi resztami są 0 i 2. Zatem teza zadania jest w tych przypadkach prawdziwa.

W dalszym ciągu załóżmy, że p jest liczbą pierwszą większą od 3 i udowodnijmy dwa lematy.

Lemat 1: Jeżeli a, b są takimi liczbami całkowitymi, że

$$a \equiv b \pmod{p},$$

to

$$a^p \equiv b^p \pmod{p^2}.$$

Dowód lematu:

Niech $a = b + kp$. Wtedy

$$a^p = (b+kp)^p = \sum_{i=0}^{p} \left(\binom{p}{i} \cdot b^{p-i} \cdot k^i \cdot p^i \right) \equiv \sum_{i=0}^{1} \left(\binom{p}{i} \cdot b^{p-i} \cdot k^i \cdot p^i \right) =$$

$$= \binom{p}{0} \cdot b^p \cdot k^0 \cdot p^0 + \binom{p}{1} \cdot b^{p-1} \cdot k^1 \cdot p^1 = b^p + p \cdot b^{p-1} \cdot k \cdot p \equiv b^p \pmod{p^2}.$$

Wniosek: Jeżeli rozszerzymy pojęcie dobrej reszty na wszystkie liczby całkowite, to liczba przystająca do dobrej reszty modulo p jest dobrą resztą – czyli bycie dobrą resztą zależy tylko od reszty z dzielenia przez p, pomimo że w definicji dobrej reszty występuje kongruencja modulo p^2.

Lemat 2: Funkcje f_p i g_p przekształcają dobre reszty na dobre reszty.

Dowód lematu:

Niech $r \in \mathbb{Z}_p$ będzie dobrą resztą.

Wtedy kongruencja

$$(r+1)^p \equiv r^p + 1 \pmod{p^2}$$

jest kolejno równoważna kongruencjom

$$-(r+1)^p \equiv -r^p - 1 \pmod{p^2},$$

$$(-r-1)^p \equiv (-r)^p - 1 \pmod{p^2},$$

$$(-r-1)^p + 1 \equiv (-r-1+1)^p \pmod{p^2}.$$

Stąd wynika, że liczba $-r-1$ jest dobrą resztą, a tym samym dobrą resztą jest liczba $g_p(r) \equiv -r-1 \pmod{p}$.

W przypadku, gdy $r \neq 0$, oznaczmy przez r^{-1} resztę odwrotną do r modulo p^2. Wówczas przemnożenie stronami kongruencji

$$(r+1)^p \equiv r^p + 1 \pmod{p^2}$$

przez $(r^{-1})^p$ prowadzi do

$$\left(r \cdot r^{-1} + r^{-1}\right)^p \equiv \left(r \cdot r^{-1}\right)^p + \left(r^{-1}\right)^p \pmod{p^2},$$

czyli

$$\left(1 + r^{-1}\right)^p \equiv 1 + \left(r^{-1}\right)^p \pmod{p^2}.$$

Stąd wynika, że $f_p(r) \equiv r^{-1} \pmod{p}$ jest dobrą resztą.

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Z lematu 2 wynika, że każdy ze zbiorów, na które rozłożyliśmy $\mathbb{Z}_p$, albo zawiera same dobre reszty, albo nie zawiera żadnej. Prześledźmy dokładnie te zbiory.

1° Cykle sześcioelementowe.
Niektóre mogą składać się z dobrych reszt, a niektóre nie. Trudno to kontrolować (bo bardzo często takich cykli złożonych z dobrych reszt nie ma wcale, ale np. dla $p = 36847$ są aż cztery), ale liczba cykli sześcioelementowych złożonych z dobrych reszt nie wpływa na tezę zadania. W tym przypadku otrzymujemy

liczbę dobrych reszt podzielną przez 6.

2° Elementy 0 oraz $p-1 \equiv -1 \pmod{p}$.
Są dobrymi resztami, bo $(-1)^p = -1$, $0^p = 0$ oraz $1^p = 1$. W tym przypadku otrzymujemy

2 dobre reszty.

3° Trójka elementów: 1, $(p-1)/2$ i $p-2$.
Nie wpływa na tezę zadania. W tym przypadku otrzymujemy

3 dobre reszty albo żadnej.

Uwaga: Ta trójka składa się z dobrych reszt wtedy i tylko wtedy, gdy p jest liczbą pierwszą Wiefericha – obecnie znane są dwie takie liczby: 1093 i 3511.

4° Dwuelementowy cykl złożony z pierwiastków sześciennych z jedności – tylko w przypadku $p \equiv 1 \pmod{6}$.
Okazuje się nie mieć wpływu na tezę zadania. W tym przypadku otrzymujemy

2 dobre reszty albo żadnej.

Uwaga: Można udowodnić, że dla każdej liczby pierwszej $p \equiv 1 \pmod{6}$ te dwie reszty są dobrymi resztami, jednak nie jest to potrzebne dla rozwiązania zadania. Dowód opiera się na spostrzeżeniu, że jeżeli q i r są różnymi pierwotnymi pierwiastkami sześciennymi z jedności modulo p, to q^p i r^p są różnymi pierwotnymi pierwiastkami sześciennymi z jedności modulo p^2, a zatem spełniają kongruencję $q^p + r^p + 1 \equiv 0 \pmod{p^2}$.

Teza zadania wynika z podsumowania liczb dobrych reszt występujących w powyższych czterech przypadkach.

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego