



Równania Diofantyczne

Antoni Łuczak

Modulo

Często podczas rozwiązywania równania diofantycznego warto rozpatrzyć je modulo pewną liczbę.

Ćwiczenie 1. Rozwiązać w liczbach całkowitych równanie

$$(x+1)^3 - x^3 = 2y^2$$

W wielu przypadkach nie tak łatwo dobrać odpowiednie modulo. Pomaga w tym następujące twierdzenie:

Twierdzenie 1 (Jakie modulo wybrać?)

Dana jest liczba pierwsza p oraz liczba naturalna k . Wtedy liczby

$$1^k, 2^k, \dots, (p-1)^k$$

generują dokładnie $\frac{p-1}{\text{NWD}(k, p-1)}$ reszt modulo p .

Dowód. Niech g będzie generatorem modulo p . Wtedy ciąg liczb wypisany powyżej jest permutacją ciągu

$$1, g^k, g^{2k}, \dots, g^{(p-2)k}.$$

Widać, że ten ciąg jest okresowy i jego okres to liczba różnych reszt. Jest on równy najmniejszej takiej liczbie a , że

$$g^{ak} \equiv_p 1 \iff p-1 \mid ak.$$

Najmniejszą taką liczbą jest oczywiście $\frac{p-1}{\text{NWD}(k, p-1)}$. □

Ćwiczenie 2. Rozwiązać w liczbach całkowitych równanie

$$x^5 = y^2 + 4.$$

Schodzenie Fermata

Założmy, że szukamy rozwiązań (x, y, z) pewnego jednorodnego równania diofantycznego. Jeżeli uda nam się pokazać, że dla dowolnego rozwiązania liczby x, y, z są podzielne przez pewną liczbę naturalną d , to otrzymamy nowe rozwiązanie $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$. W ten sposób będziemy w stanie dostawać dowolnie małe rozwiązania, co doprowadzi do sprzeczności.

Ćwiczenie 3. Udowodnić, że liczba $\sqrt{2}$ jest niewymierna.

Zadania

Zadanie 1. Znaleźć wszystkie rozwiązania równania

$$8x^4 + 4y^4 + 2z^4 = t^4$$

w liczbach całkowitych.

Zadanie 2. Znaleźć wszystkie rozwiązania równania

$$x^2 + y^2 + z^2 + t^2 = 2xyzt$$

w liczbach całkowitych.

Zadanie 3. Udowodnić, że liczby 7 nie da się przedstawić w postaci sumy trzech kwadratów liczb wymiernych.

Zadanie 4. Udowodnić, że liczba postaci $4^n(8k+7)$, gdzie n i k są dodatnimi liczbami całkowitymi, nie jest sumą jednego, dwóch ani trzech kwadratów liczb całkowitych.

Zadanie 5. Znaleźć wszystkie takie liczby wymierne a, b , że

$$a^2 + ab + b^2 = 2.$$

Zadanie 6. Dane są takie liczby całkowite a, b, c, d , że jedynym rozwiązaniem równania

$$ax^2 + by^2 + cz^2 + dt^2 = 0$$

w liczbach całkowitych x, y, z, t jest $x = y = z = t = 0$. Czy oznacza to, że liczby a, b, c, d mają ten sam znak?

Zadanie 7. Rozwiązać w liczbach całkowitych równanie

$$x^4 + y^4 + z^4 = 9u^4.$$

Zadanie 8 (OM 2 etap). Dany jest taki wielomian W o współczynnikach całkowitych, że dla dowolnych różnych liczb wymiernych r_1, r_2 zachodzi $W(r_1) \neq W(r_2)$. Czy ten warunek implikuje, że dla dowolnych różnych liczb rzeczywistych t_1, t_2 zachodzi $W(t_1) \neq W(t_2)$?

Rozwiązania ćwiczeń

Rozwiązanie 1. Lewa strona równania jest nieparzysta, natomiast prawa parzysta. W takim razie równanie nie ma rozwiązań.

Rozwiązanie 2. Aby otrzymać jak najmniej reszt postaci x^5 oraz y^2 , nasuwa się rozpatrywanie równania modulo 11. Widać, że x^5 może przyjmować 3 wartości $-1, 0, 1$, natomiast y^2 6 wartości, którymi są $0, 1, 4, 9, 5, 3$. Widać, że niezależnie od wyboru y , prawa strona równania nigdy nie daje reszty $-1, 0$ lub 1 , zatem nasze równanie nie ma rozwiązań.

Rozwiązanie 3. Załóżmy wbrew tezie, że $\sqrt{2} = \frac{a}{b}$. Podnosząc do kwadratu i wymnażając stronami otrzymujemy $a^2 = 2b^2$. Skoro prawa strona jest parzysta, to a jest parzyste, zatem $a = 2a_1$ dla pewnego a_1 . Podstawiając mamy $2a_1^2 = b^2$. Zauważmy, że para (b, a_1) jest nowym rozwiązaniem równania $x^2 = 2y^2$, którego suma wartości bezwzględnych jest mniejsza niż suma wartości bezwzględnych pary (a, b) . Powtarzając takie rozumowanie odpowiednio dużo razy otrzymamy parę, której suma modułów jest ujemna, co daje sprzeczność.

Rozwiązania zadań

Rozwiązanie 1. Należy postępować analogicznie jak w rozwiązaniu ćwiczenia 3. Skoro liczba t jest parzysta, to możemy ją zastąpić liczbą $2t_1$. Dzieląc przez 2 widzimy, że z również jest parzyste i możemy je zastąpić przez $2z_1$. Powtarzając to rozumowanie kilka razy otrzymamy nowe rozwiązanie równania (x_1, y_1, z_1, t_1) o mniejszej sumie modułów (o ile co najmniej jedna liczba jest niezerowa). To ponownie prowadzi do sprzeczności, zatem równanie to nie ma rozwiązań poza czwórką $(0, 0, 0, 0)$.

Rozwiązanie 2. Zauważmy, że gdyby wszystkie liczby x, y, z, t były nieparzyste, to lewa strona dawałaby resztę 4 modulo 8, natomiast prawa resztę 2. Bez straty ogólności założymy, że t jest parzyste. Wtedy również pewna inna liczba musi być parzysta, założymy, że jest to z . Gdyby x oraz y były nieparzyste, to lewa strona dawałaby resztę 2 modulo 4, natomiast prawa resztę 0. W takim razie również x oraz y są parzyste i dzieląc wszystkie liczby przez 2 otrzymujemy nowe, mniejsze rozwiązanie. Podobnie jak w poprzednim zadaniu, oznacza to, że jedynym rozwiązaniem jest czwórka $(0, 0, 0, 0)$.

Rozwiązanie 3. Załóżmy, że teza jest nieprawdziwa. Możemy założyć, że nasze liczby wymierne są postaci $a/d, b/d, c/d$. Wtedy otrzymamy zapis

$$7d^2 = a^2 + b^2 + c^2.$$

Jeżeli d jest nieparzyste, to lewa strona daje resztę 7 modulo 8, natomiast łatwo zauważyć, że prawa strona takiej reszty osiągnąć nie może. W takim razie d jest parzyste. Łatwo zauważyć, że jeśli suma kwadratów trzech liczb jest podzielna przez 4, to każda z nich musi być parzysta. To daje sprzeczność, podobnie jak w poprzednich zadaniach.

Rozwiązanie 4. Załóżmy wbrew tezie, że liczba $4^n(8k+7)$ jest sumą trzech kwadratów (zakładamy, że niektóre z nich mogą być zerowe). Jeżeli $n > 0$, to dostajemy sumę trzech kwadratów podzielnych przez 4. W takim razie każdy z tych kwadratów jest podzielny przez 4 i dzieląc obustronnie otrzymujemy, że $4^{n-1}(8k+7)$ również jest sumą trzech kwadratów. Możemy kontynuować aż $n = 0$. Wtedy dostajemy zapis $8k+7$ jako sumę trzech kwadratów, ale znowu porównując modulo 8 widzimy, że nie jest to możliwe.

Rozwiązanie 5. Zapiszmy $a = x/z, b = y/z$. Wtedy

$$x^2 + xy + y^2 = 2z^2.$$

Widzimy, że zarówno x jak i y muszą być parzyste, natomiast po podzieleniu obustronnie przez 2 widzimy, że również z jest parzyste. Dzieląc ponownie przez 2 otrzymujemy mniejsze rozwiązanie, co prowadzi do sprzeczności.

Rozwiązanie 6. Oczywiście tak nie musi być. Wystarczy ustalić $a = b = c = 1$ oraz $d = -7$. Na mocy zadania 3, jedynym rozwiązaniem jest czwórka $(0, 0, 0, 0)$, natomiast znak d jest różny od znaków a, b, c .

Rozwiązanie 7. Rozpatrzmy to równanie modulo 5. Na mocy MTF, każda czwarta potęga daje resztę 0 lub 1. Jednak wtedy po lewej stronie mamy resztę 0, 1, 2 lub 3, natomiast po prawej resztę 0 lub 4. Widać, że wszystkie liczby są podzielne przez 5 co daje nam nowe rozwiązanie i prowadzi do sprzeczności, o ile początkową czwórką nie było $(0, 0, 0, 0)$.

Rozwiązanie 8. Pokażemy, że tak nie jest. Weźmy wielomian $W(x) = x^3 - 2x$. Jeżeli $r_1 \neq r_2$ są takimi liczbami, że $W(r_1) = W(r_2)$, to

$$r_1^3 - 2r_1 = r_2^3 - 2r_2 \iff (r_1 - r_2)(r_1^2 + r_1r_2 + r_2^2 - 2) = 0.$$

Skoro $r_1 \neq r_2$, to drugi nawias musi być zerowy. Jednak na mocy zadania 5 nie jest to możliwe. W takim razie W spełnia warunki zadania. Mimo tego istnieją takie liczby rzeczywiste t_1, t_2 , że $t_1^2 + t_1t_2 + t_2^2 = 2$.