Równanie Mordella

Maciej Zalewski

18 czerwca 2014

Spis treści

Wstęp

Równanie postaci

$$y^2 = x^3 + k, \quad dla \quad k \in Z \setminus \{0\} \tag{1}$$

nazywamy równaniem Mordella.
Jako pierwszy równanie takiej postaci rozważał Fermat. Postawił on tezę, że jedynym rozwiązaniem równania $y^2 + 2 = x^3$ jest $x = 3,\ y = \pm 5$. W 1920 roku L.J. Mordell udowodnił, że równanie 1 ma co najwyżej skończenie wiele rozwiązań. Dowód twierdzenia Mordell'a bazuje na formach binarnych i twierdzeniu Thue'ego, zostanie to opisane w rozdziale pierwszym. W drugim i trzecim rozdziale zostaną przedstawione przykłady równań, które mają, bądź też nie, rozwiązania całkowite. Czwarty i ostatni rozdział zawiera omówienie wyników dotyczących oszacowania na wysokosć rozwiązań całkowitych równania 1 w zależnosci od parametru k.

1 Formy binarne i twierdzenie Mordella

Definicja 1. *Formą binarną nazywamy wielomian dwóch zmiennych. Ogólna postać formy binarnej stopnia n wygląda następująco*

$$a_0X^n + a_1X^{n-1}Y + a_2X^{n-2}Y^2 + \cdots + a_{n-1}XY^{n-1} + a_nY^n$$

Definicja 2. *Dwie formy binarne $f(X,Y), g(X,Y)$ nazywamy równoważnymi jeżeli istnieją p,q,r,s spełniające $ps - qr = 1$ takie, że*

$$g(X,Y) = f(pX + qY, rX + sY)$$

.

W naszych rozważaniach ograniczymy się do całkowitych form binarnych, czyli takich, że $a_0, a_1, \ldots, a_n \in Z$. W takim przypadku wyróżnik formy jest liczbą całkowitą. Dwie całkowite formy binarne nazywamy $SL(2,Z)$-równoważnymi (równoważnymi), gdy istnieją $p,q,r,s \in Z$, $ps - qr = 1$ takie, że $g(X,Y) = \pm f(pX + qY, rX + sY)$.

Twierdzenie 1.1. *Liczba klas równoważnosci całkowitych form binarnych o ustalonych stopniu i wyróżniku jest skończona.*

Dla form kwadratowych istnieje prosta procedura, z której wynika skończonosć liczy klas równoważnosci dla wyróżnika D. Zacznijmy od dowlonej formy kwadratowej $aX^2 + 2bXY + cY^2$, oznaczmy ją jako $[a,b,c]$. Zauważmy, że współczynnik przy XY jest parzysty. Takie formy nazywamy parzystymi i na nich się skupimy.
Procedura ta wygląda następująco. Jeżeli $|b| > |a|/2$, wybieramy k takie, że $|b + ka|y \leqslant |a|/2$. Wykonujemy podstawienie $(X,Y) \to (X + kY, Y)$. Dostajemy w ten sposóbofrmę $[a,b,c] := [a, b + ka, c + 2bk + ak^2]$. Jeżeli $|c| < |a|$, podstawiamy $(X,Y) \to (-Y,X)$. Wynikiem tego podstawienia jest forma $[a,b,c] := [c,-b,a]$. Wynikiem iteracji tej procedury jest forma $[a,b,c]$ równoważna formie wyjsciowej, spełniająca nierównosci $|2b| \leqslant |a| \leqslant |c|$. Dostajemy stąd, że $|D| \geqslant |ac| - b^2 \geqslant 3b^2$. $|b|$ jest więc ograniczony przez $\sqrt{|D|/3}$. Daje to skończenie wiele wyborów na b. To i równość $b^2 - ac = D$ implikuje skończenie wiele wyborów na a i c.

Przykład 1. *Opiszemy wszystkie klasy równoważnosci form $aX^2 + 2bXY + cY^2$ o wyróżniku $D = 17$. Z powyższej procedury wystarczy rozpatrzyć b spełniające $|b| \leqslant \sqrt{17/3}$. Mamy więc, że $b = 0, \pm 1, \pm 2$. Współczynniki a i c*

dostajemy z równosci $b^2 - ac = 17$ *oraz nierównosci* $|c| \geqslant |a| \geqslant |2b|$. *Ostatecznie dostajemy następującą listę możliwosci dla* $a > 0$,

$$X^2 - 17Y^2$$
$$2X^2 \pm 2XY - 9Y^2$$
$$3X^2 \pm 2XY - 6Y^2$$

Przejdziemy teraz do form szesciennych. Niech $f(X,Y) = aX^3 + 3bX^2Y + 3cXY^2 + dY^3$. Hesjan tej formy wygląda następująco,

$$H(X,Y) = -\frac{1}{36}\begin{vmatrix} f_{XX} & f_{XY} \\ f_{XY} & f_{YY} \end{vmatrix}$$

można go również zapisać następująco $H(X,Y) = (b^2-ac)X^2+(bc-ad)XY+(c^2-bd)Y^2$. Zdefiniujmy również formę szescienną

$$G(X,Y) = \frac{1}{3}\begin{vmatrix} f_X & f_Y \\ H_X & H_Y \end{vmatrix}.$$

Formy H, G są nazywane niezmiennikami f stopnia 2 i 3. Wyróżnik formy f wynosi $27D_1$, gdzie $D_1 = -a^2d^2 + 6abcd + 3b^2c^2 - 4ac^3 - 4db^3$. Wyróżnik formy H wynosi $-D_1$.

Lemat 1. *Przy powyższych oznaczeniach zachodzi następująca równosć*

$$G^2 + D_1 f^2 = 4H^3$$

Możemy teraz poczynić następującą obserwację. Niech f będzie szescienną formą o wyróżniku $D_1 = 4k$ taką, że $f(x,y) = 1$ ma rozwiązanie x_0, y_0. Wtedy równanie Mordell'a $y^2 + k = x^3$ ma rozwiązanie $y = G(x_0,y_0)/2, x = H(x_0,y_0)$. Okazuje się, żę przeciwna implikacja jest również prawdziwa.

Twierdzenie 1.2. *Załóżmy, żę równanie* $y^2 + k = x^3$ *ma rozwiązanie* (p,q). *Wtedy forma szescienna* $f(x,y) = x^3 - 3pxy^2 + 2qy^3$ *ma wyróżnik* $D_1 = 4k$ *oraz* $p = H(1,0), q = G(1,0)/2$. *Ponadto* $H(X,Y) = pX^2 - 2qXY + p^2Y^2$, *więc H jest formą parzystą. Mamy również* $G(X,Y) = 2(-qX3 + 3p^2X^2Y - 3pqXY^2 + (-p^3 + 2q^2)Y^3)$, *w szczególnosci* $G(X,Y)/2$ *jest formą całkowitą.*

Twierdzenie 1.3 (Thue, 1909)**.** *Niech f będzie całkowitą formą binarną taką, że* $f(x,1)$ *ma przynajmniej 3 różne pierwiastki. Niech* $m \in Z \setminus \{0\}$. *Wówczas równanie* $f(x,y) = m$ *ma co najwyżej skończenie wiele rozwiązań.*

Na podstawie twierdzeń 1.2 oraz 1.3 łatwo wywnioskować następujące twierdzenie.

Twierdzenie 1.4 (Mordell, 1922)**.** *Niech $k \in Z \setminus \{0\}$. Wówczas równanie $y^2 + k = x^3$ ma co najwyżej skończenie wiele rozwiązań całkowitych.*

W celu rozwiązania równania Morell'a wystarczy znaleźć reprezentanta każedj z klas równoważnosci całkowitych form szesciennych o wyróżniku $108k$. Dla każdej takiej formy f rozwiązujemy równanie $f(x, y) = 1$ w liczbach całkowitych.

2 Przykłady bez rozwiązań całkowitych

Do pokzania braku rozwiązań całkowitych równania $y^2 = x^3+k$, dla pewnych k, wykorzystamy kongruencje oraz następujący fakt:

$$\begin{aligned} -1 \equiv \square \mod p &\iff p \equiv 1 \mod 4 \\ 2 \equiv \square \mod p &\iff p \equiv 1, 7 \mod 8, \\ -2 \equiv \square \mod p &\iff p \equiv 1, 3 \mod 8. \end{aligned}$$

Twierdzenie 2.1. *Równanie $y^2 = x^3 + 7$ nie ma rozwiązań całkowitych.*

Dowód. Załóżmy, że istnieje rozwiązaanie całkowity (x, y). Jeżeli x jest paryszty, to $y^2 \equiv 7 \mod 8$ ale 7 nie jest kwadratem $\mod 8$. Więc x jest nieparzysty. Zapiszmy $y^2 = x^3 + 7$ jako

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4).$$

Drugi czynnik, $x^2 - 2x + 4 = (x - 1)^2 + 3$, jest dodatni. Ponieważ, x jest nieparzysty $(x-1)^2+3 \equiv 3 \mod 4$. Dostajemy, że $(x-1)^2+3$ jest podzielne przez liczbę pierwszą $p \equiv 3 \mod 4$. Ponieważ$p|(x^2 - 2x + 4)$, p musi dzielić $y^2 + 1$, więc $y^2 + 1 \equiv 0 \mod p$. Więc $-1 \equiv \square \mod p$, co jest sprzeczne z $p \equiv 3 \mod 4$.

Twierdzenie 2.2. *Równanie $y^2 = x^3 - 6$ nie ma rozwiązań całkowitych.*

Dowód. Załóżmy, że istnieje rozwiązanie całkowite (x, y). Jeżeli x jest parzyste, to $y^2 \equiv -6 \equiv 2 \mod 8$, ale $2 \mod 8$ nie jest kwadratem. Mamy więc, że x jest nieparzysty, a więc i y, oraz $x^3 \equiv y^2+6 \equiv 7 \mod 8$. Ponadtio $x^3 \equiv x \mod 8$, więc $x \equiv 7 \mod 8$. Zapiszmy $y^2 = x^3 - 6$ jako

$$y^2 - 2 = x^3 - 8 = (x - 2)(x^2 + 2x + 4),$$

gdzie $x^2+2x+4 \equiv 7^2+2*7+4 \equiv 3 \mod 8$. Ponieważ $x^2+2x+4 = (x+1)^2+3$ jest dodatnie, musi mieć dzielnik pierwszy $p \equiv \pm 3 \mod 8$. Niech p będzie takim dzielnikiem. Ponieważ p dzieli $x^2 + 2x + 4$, p dzieli również $y^2 - 2$. Dostajemy, że $2 \equiv \square \mod p$, więc $p \equiv \pm 1 \mod 8$, sprzeczność.

Twierdzenie 2.3. *Równanie $y^2 = x^3 + 6$ nie ma rozwiązań całkowitych.*

Dowód. Załóżmy, że istnieje rozwiązanie całkowite (x, y). Jeżeli x jest parzyste, to $y^2 \equiv 6 \mod 8$, co jest niemożliwe. Z nieparzystosci x, wynika nieparzystość y. Mamy również $x^3 = y^2 - 6 \equiv -5 \equiv 3 \mod 8$ oraz $x \equiv 3 \mod 8$. Zapiszmy $y^2 = x^3 + 6$ jako

$$y^2 + 2 = x^3 + 8 = (x + 2)(x^2 - 2x + 4),$$

gdzie $x^2 - 2x + 4 \equiv 3^2 - 2 * 3 + 4 \equiv 7 \mod 8$. Dla dowolnej liczby pierwszej p dzielącej $x^2 - 2x + 4$, $y^2 + 2 \equiv 0 \mod p$, więc $-2 \equiv \square \mod p$, czyli $p \equiv 1, 3 \mod 8$. Ponieważ $x^2 - 2x + 4 = (x - 1)^2 + 3$ jest dodatnie, $x^2 - 2x + 4 \equiv 1, 3 \mod 8$. Pokazalismy wczesniej, że $x^2 - 2x + 4 \equiv 7 \mod 8$, sprzeczność.

3 Przykłady z rozwiązaniami całkowitymi

Twierdzenie 3.1. *Jedynymi rozwiązaniami całkowitymi równania $y^2 = x^3 + 16$ są $(x, y) = (0, \pm 4)$.*

Dowód. Zapiszmy to wórnanie w następującej postaci, $x^3 = y^2 - 16 = (y + 4)(y - 4)$. Jeżeli y byłoby nieparzyste, to $(y + 4, y - 4) = 1$, więc $y + 4$ i $y - 4$ byłyby szescianami. Różnica między nimi wynosi 8, a nie istnieją nieparzyste szesciany różniące się o 8. Więc y jest parzyste, a z tego wynika parzystość x. Prawa strona równania $y^2 = x^3 + 16$ jest podzielna przez 8, więc $4|y$. Niech $y = 4y'$, $16y'^2 = x^3 + 16$. Dostajemy, że $4|x$. Niech $x = 4x'$. Wówczas $y'^2 = 4x'^3 + 1$, czyli y' jest nieparzyste. Zapiszmy $y' = 2m + 1$, więc $m^2 + m = x'^3$. Z faktu, że jedynymi kolejnymi szescianami są $-1, 0$ lub $0, 1$, oraz $(m, m + 1) = 1$ wynnika ,że $m = 0$ lub $m + 1 = 0$. W obu przypadkach dostajemy, że $x' = 0$, więc $x = 0$ i $y = \pm 4$.

W dowodzie następnego twierdzenie wykorzystamy jednoznaczność rozkładu w pierscieniu $\mathbb{Z}[i]$.

Twierdzenie 3.2. *Jedynym rozwiązaniem całkowitym równania $y^2 = x^3 - 1$ jest para $(x, y) = (1, 0)$.*

Dowód. Załóżmy, że x jest parzyste, wtedy $y^2 + 1 = x^3 \equiv 0 \mod 8$. To by znaczyło, że $-1 \equiv \square \mod 8$, sprzeczność. Dostajemy, że x jest nieparzysty, a y parzysty. Równanie $x^3 = y^2 + 1$ w $\mathbb{Z}[i]$ faktoryzuje się następująco

$$x^3 = (y + i)(y - i).$$

Jeżeli dwa czynniki po prawej stronie równania są względnie pierwsze w $\mathbb{Z}[i]$, to z faktu, że ich produkt jest szescianem wynika, że każdy z nich musi być szescianem z dokładnoscią do mnożenia przez jednosć, Wynika to z jednoznacznosci rozkładu w $\mathbb{Z}[i]$. Ponadto w $\mathbb{Z}[i]$ wszystkie jednosci są szescianami. Z powyższych rozważań wynika, że jeżeli $y+i$ i $y-i$ są względnie pierwsze, to są one szescianami. Pokażemy, że $y+i$ i $y-i$ są zględnie pierwsze. Niech δ będzie ich wspólnym dzielnikiem. Ponieważ δ dzieli $(y+i)-(y-i)=2i$, $N(\delta)$ dzieli $N(2i)$. Ponadto $N(\delta)$ dzieli $N(y+1)=y^2+1=x^3$, co jest nieparzyste. Dostajemy, że $N(\delta)=1$, czyli δ jest jednoscią. Z wczesniejszych rozważań wynika, że

$$y+i=(m+ni)^3$$

dla pewnych $m,n\in Z$. Wymnarzając i porównując częsci rzeczywiste i urojone dostajemy,

$$y=m^3-3mn^2=m(m^2-3n^2),\quad 1=3m^2n-n^3=n(3m^2-n^2).$$

Drugie równanie mówi nam, że $n=\pm 1$. Jeżeli $n=1$, to $1=3m^2-1$, czyli $3m^2=2$, a równanie to nie ma rozwiązań całkowitych. Jeżeli $n=-1$, to $1=-(3m^2-1)$, czyli $m=0$. Dostajemy, że $y=0$, co daje $x^3=y^2+1=1$, czyli $x=1$.

Twierdzenie 3.3. *Jedynymi rozwiązaniami całkowitymi równania* $y^2=x^3-2$ *są* $(x,y)=(3,\pm 5)$

Dowód. Załóżmy, że x jest parzyste, wtedy $y^2\equiv -2 \mod 8$, ale -2 nie jest kwadratem $\mod 8$. Dostajemy, że x,y są nieparzyste. W $\mathbb{Z}[\sqrt{-2}]$, równanie możemy zapisać następująco

$$x^3=(y+\sqrt{-2})(y-\sqrt{-2}).$$

Pokażemy, że czynniki po prawej stronie są względnie pierwsze. Niech δ będzie ich dzielnikiem. Wówczas δ dzieli ich różnicę, czyli $N(\delta)$ dzieli $N((y+\sqrt{-2})-(y-\sqrt{-2}))=N(2\sqrt{-2})=8$. Równoczesnie $N(\delta)$ dzieli $N(y+\sqrt{-2})=y^2+2$, co jest nieparzyste. Dostajemy więc, że $N(\delta)=1$ czyli δ jest jednoscią. Z jednoznacznosci rozkładu w $\mathbb{Z}[\sqrt{-2}]$ dsotajemy, że $y+\sqrt{-2}$ i $y-\sqrt{-2}$ są szescianami z dokładnoscią do mnożenia przez jednosć. W $\mathbb{Z}[\sqrt{-2}]$ jedynymi jednosciami są ± 1, które są szescianami. Więc $y+\sqrt{-2}$ i $y-\sqrt{-2}$ są szescianami. Niech

$$y+\sqrt{-2}=(m+n\sqrt{-2})^3$$

dla pewnych $m,n\in Z$. Wynika stąd, że

$$y=m^3-6mn^2=m(m^2-6n^2), 1=3m^2n-2n^3=n(3m^2-2n^2).$$

Z drugiego równania wynika, że $n = \pm 1$. Dla $n = 1$ mamy $1 = 3m^2 - 2$, więc $m = \pm 1$. Wtedy $x = 3, y = \pm 5$. Gdy $n = -1$ mamy, że $1 = (-3m^2 - 2)$, czyli $1 = 3m^2$, a to równanie nie ma rozwiązań całkowitych.

4 Ograniczenia na rozwiązania

Wiemy już, że zbiór rozwiązań równania $y^2 = x^3 + k$ w zbiorze liczb całkowitych jest skończony. Nie znamy jednak algorytmu rozwiązywania takiego równania. Pierwsze kroki w tym kierunku bazują na technice form liniowych w logarytmach, opisanej przez A. Baker'a w 1966. Praca ta zapewniła Baker'owi medal Fields'a. Poniższe twierdzenie bazuje na metodach Baker'a.

Twierdzenie 4.1 (Sprindzuk, 1982)**.** *Istnieje efektywnie obliczalna stała $C > 0$ taka, że dla każdego rozwiązania $x, y \in \mathbb{Z}$ równania $y^2 + k = x^3$, $k \in Z \setminus \{0\}$, zachodzi*

$$|x|, |y| \leqslant \exp\left(C|k|(\log|k| + 1)^6\right).$$

Warto odnotować, że stała C w powyższym twierdzeniu jest w rzeczywistosci bardzo duża. W związku z tym możnaby oczekiwać, że zachodzi lepsze szacowanie. Podejrzenie to bazuje na następującej hipotezie.

Hipoteza 1 (Hall, 1971)**.** *Dla dowolnego $\epsilon > 0$ istnie dodatnia liczba rzeczywista $c(\epsilon)$ taka, że*

$$|y^2 - x^3| > c(\epsilon)x^{\frac{1}{2}-\epsilon}$$

dla dowolnych $x, y \in \mathbb{Z}_{>0}$, $y^2 \neq x^3$.

Z powyżeszej hipotezy wynika, że $|x|, |y| \leqslant c_1(\epsilon)|d|^{2+\epsilon}$. Innymi słowy, oczekiwane ograniczenia na x,y są wielomianowe w $|d|$.

Literatura

[1] L. J. Mordell, A Statement by Fermat, Proceedings of the London Math. Soc. 18 (1920), v-vi.

[2] Keith Conrad, Examples of Mordell's equation.

[3] F. Beukers, Diophantine equations.

[4] David A. Cox, Primes of the form $x^2 + ny^2$.

[5] L. J. Mordell, Diophantine equations.