Ciągi trzech kwadratów i krzywe eliptyczne

Radosław Żak

30 kwietnia 2019

Streszczenie

Tematem pracy są ciągi kwadratów liczb wymiernych postaci x, $x+a$, $x+b$, w szczególności zaś ich liczba dla danych a, b. Udowodnię, że jeśli ta liczba jest skończona, to jest mniejsza od trzech.

1 Wprowadzenie

W pracy zajmuję się następującym problemem: dane są liczby wymierne a, b, oraz pewne q wymierne takie, że $q^2 + a$ i $q^2 + b$ są kwadratami liczb wymiernych. Czy można znaleźć więcej takich q? Jeśli tak, to ile? W rozdziale 2 wprowadzam definicje z zakresu geometrii algebraicznej, które przydają się w rozstrzygnięciu tego problemu. W rozdziale 3 przekształcam go do postaci pytania o punkty wymierne na pewnej krzywej eliptycznej. W rozdziale 4 konstruuję przykłady krzywych, dla których liczba możliwych q wynosi 1 i 2. Rozdział 5 zawiera rezultaty dla przypadku, gdy stosunek $\frac{a}{b}$ jest całkowity.

2 Krzywe eliptyczne – podstawy

Krzywą eliptyczną nad ciałem $\mathbb{F}$ nazwiemy krzywą opisaną równaniem

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_6$$

Takie równanie nazywamy *postacią Weierstrassa*, dla $\mathbb{F} = \mathbb{Q}$ może być ona sprowadzona do $E : y^2 = x^3 + ax^2 + bx + c$. Zbiór punktów wymiernych tej krzywej oznaczamy $E(\mathbb{Q})$.

Najważniejszą własnością krzywych eliptycznych jest to, że ich punkty tworzą strukturę grupy — można je dodawać. Biorąc dwa punkty P, Q na krzywej eliptycznej E, prosta PQ przecina E w jeszcze jednym punkcie (jeśli $P = Q$, bierzemy styczną w P). Zdefiniujemy wtedy $P + Q$ jako odbicie tego trzeciego punktu względem osi x.

Należy przy tym zwrócić uwagę na to, że E zawiera jeden punkt w nieskończoności, o współrzędnych jednorodnych $(0, 1, 0)$. Ten punkt będzie elementem neutralnej tej, jak się okazuje, grupy punktów $E(\mathbb{Q})$ z wyżej zdefiniowanym dodawaniem. Elementem przeciwnym do punktu P będzie jego odbicie względem osi x, w szczególności punkty rzędu 2 będą na niej leżeć. Łączność tego działania także można wykazać, jednak nie jest to trywialne (dowód można znaleźć między innymi w [1]). Za to przemienność wynika wprost z definicji, jest to więc grupa abelowa.

Twierdzenie 1. *(Mordell)* Grupa $E(\mathbb{Q})$ jest skończenie generowana.

Oznacza to, że $E(\mathbb{Q})$ ma formę $E(\mathbb{Q})_{tor} \oplus \mathbb{Z}^r$, gdzie $E(\mathbb{Q})_{tor}$ to podgrupa wszystkich punktów skończonego rzędu. Liczbę r nazywamy rangą E i oznaczamy $\mathrm{rank}(E)$. Podgrupa $E(\mathbb{Q})_{tor}$ jest dobrze opisana: istnieją algorytmy na znalezienie jej elementów dla danego E [2], ponadto zachodzi następujące

Twierdzenie 2. *(Mazur)* [3] Grupa $E(\mathbb{Q})_{tor}$ ma jedną z form

- $\mathbb{Z}_n$ dla $1 \leqslant n \leqslant 10$ lub $n = 12$,
- $\mathbb{Z}_{2n} \times \mathbb{Z}_2$ dla $1 \leqslant n \leqslant 4$.

O części $\mathbb{Z}^r$ matematykom wiadomo dużo mniej: nie wiadomo, jakie r są rangami krzywych eliptycznych (największa znana ranga to 28), a jedyne znane i efektywne algorytmy do wyznaczania jej opierają się na nieudowodnionej hipotezie Bircha i Swinnertona-Dyera. Na twierdzeniu Mazura oprzemy analizę hipotezy.

3 Przekształcenie problemu

Dla $a = 0$, $b = 0$ lub $a = b$ teza jest prosta do udowodnienia, przyjmiemy więc, że żadna z tych możliwości nie zachodzi, i $b > a > 0$.

Niech k, l, m będą takimi liczbami wymiernymi, że $l^2 = k^2 + a$ i $m^2 = k^2 + b$. Zatem $-a = (k - l)(k + l)$ oraz $b - a = (m - l)(m + l)$. Oznaczmy

$x = m + l$, wtedy $m - l = \frac{b-a}{x}$, czyli $l = \frac{x - \frac{b-a}{x}}{2}$. Analogicznie dla $y = k + l$ mamy $l = \frac{y - \frac{-a}{y}}{2}$. Zatem

$$x - \frac{b-a}{x} = y + \frac{a}{y},$$

i dla każdej pary (x, y) spełniającej to równanie znajdziemy odpowiednie k, l, m. Ponadto zauważmy, że jeśli para (x, y) spełnia to równanie, to pary $(-x, -y)$, $(-\frac{b-a}{x}, y)$, $(x, \frac{a}{y})$ także. W ten sposób z jednego punktu możemy wygenerować siedem innych, chyba, że $b - a = x^2$ bądź $a = y^2$ (wtedy tylko trzy), ale wiemy, że pierwsza z tych możliwości jest niemożliwa, gdyż lewa strona równania byłaby równa 0, prawa zaś jest niezerowa. Jeśli zaś $a = y^2$, równanie to przybierze postać $(x - y)^2 = b$, zatem b także będzie kwadratem liczby wymiernej. Obliczając dla jednej krotki par odpowiednie k zobaczymy, że uzyskamy zbiór postaci $\{k, -k\}$, przy czym $k = 0 \Leftrightarrow$ krotka ma tylko cztery pary. Kontynuując przekształcenia:

$$x^2y - (b-a)y = xy^2 + ax,$$

co we współrzędnych jednorodnych ma formę

$$xy(x - y) = (b-a)yz^2 + axz^2$$

Dokonując zamiany zmiennych $x \to x$, $y \to \frac{z-ax}{b-a}$, $z \to \frac{y}{b-a}$, dostajemy:

$$x\frac{z-ax}{b-a}(x - \frac{z-ax}{b-a}) = \frac{y^2}{(b-a)^2}((b-a)\frac{z-ax}{b-a} + ax),$$

czyli

$$x(1-ax)(bx-1) = y^2.$$

Dokonując jeszcze jednej zamiany zmiennych $x \to \frac{-x}{ab}$, $y \to \frac{y}{ab}$ i mnożąc obustronnie przez a^2b^2 ostatecznie otrzymujemy

$$x(x+a)(x+b) = y^2.$$

To równanie ma już postać krzywej eliptycznej, możemy więc zastosować narzędzia do badania ich poznane w poprzednim rozdziale. Nazwijmy tę krzywą E. Jeśli E ma niezerową rangę, musi zawierać nieskończenie wiele punktów wymiernych, więc hipoteza będzie zachodzić. Załóżmy więc, że $\text{rank}(E) = 0$. To oznacza, że $E(\mathbb{Q}) = E(\mathbb{Q})_{tor}$. $E(\mathbb{Q})$ ma trzy punkty rzędu

2: $(0,0)$, $(-a,0)$, $(-b,0)$, zatem grupa $E(\mathbb{Q})_{tor}$ nie jest cykliczna. Ponadto te trzy punkty wraz z elementem neutralnym tworzą podgrupę $E(\mathbb{Q})$, oznaczmy ją przez H. Ósemki i czwórki punktów, o których wspominaliśmy wcześniej, staną się sumą warstw postaci $P + H \cup -P + H$, dla pewnych punktów P.

Załóżmy, że a lub b nie jest kwadratem liczby wymiernej. Wtedy nie wystąpią żadne czwórki, więc $|E(\mathbb{Q})|$ będzie postaci $8t + 4$, dla $t > 1$. Zatem z twierdzenia Mazura $E(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_6$. Jeśli natomiast a i b będą kwadratami liczb wymiernych, punkty na krzywej utworzą jedną czwórkę odpowiadającą $k = 0$, oraz być może pewną liczbę ósemek. Z twierdzenia Mazura $E(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$ lub $E(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_8$, więc takich ósemek będzie najwyżej jedna.

Dosyć ogólna postać krzywej, jaką otrzymaliśmy, sugeruje, że każda z możliwości przewidzianych przez twierdzenie Mazura jest osiągalna. W następnym rozdziale skonstruujemy przykłady takich krzywych. Z powyższych rozważań wynika natomiast

Twierdzenie 3. Dane są dodatnie liczby wymierne a, b. Jeśli $q^2 + a$ i $q^2 + b$ są kwadratami liczb wymiernych dla dwóch $q \in \mathbb{Q}_+$, to takich q jest nieskończenie wiele.

Dowód. Każdej ósemce punktów odpowiada jedno dodatnie k. Skoro dla krzywej skończonej rangi ósemek jest najwyżej jedna, to krzywa odpowiadająca a i b musi mieć dodatnią rangę, zatem ma nieskończenie wiele punktów wymiernych. □

4 Przykłady

Nieuchwytność rangi krzywej, o której wspomniano w rozdziale 2, jest najpoważniejszą przeszkodą w znajdywaniu przykładów takich a, b, że możliwych q jest jedno lub dwa, ponieważ krzywe o danej podgrupie torsyjnej da się nietrudno sklasyfikować. Z pomocą przychodzą tablice krzywych, sporządzone przez prof. Johna Cremonę z Uniwersytetu w Warwick [4]. Pierwszą krzywą o randze zero i podgrupie torsyjnej rzędu 8, 12 lub 16, jest krzywa oznaczona 15a1 o wzorze

$$y^2 + xy + y = x^3 + x^2 - 10x - 10,$$

co po zamianie $y \to y - \frac{x+1}{2}$ i $x \to x + 3$ daje

$$y^2 = x(x + 4)(x + \frac{25}{4})$$

Odpowiada ona wartościom $a = 4$, $b = \frac{25}{4}$. Jedyne wymierne punkty na niej to $(0,0)$, $(-4,0)$, $(-\frac{25}{4},0)$, $(8,\pm\frac{25}{2})$, $(-2,\pm\frac{5}{2})$ (oraz oczywiście punkt w nieskończoności). Z wcześniejszych rozważań wynika, że jedynym wymiernym q dla którego q^2+a i q^2+b są kwadratami liczb wymiernych, jest $q=0$. To daje pierwszy przykład takich a, b, że odpowiednie q jest tylko jedno.

Podobnie krzywą 210e2 o równaniu $y^2+xy = x^3-1070x+7182$ i grupie torsyjnej izomorficznej z $\mathbb{Z}_2\times\mathbb{Z}_8$ można przekształcić ($y\to y+\frac{x}{2}$ oraz $x\to x+28$) do postaci $y^2 = x(x+\frac{81}{4})(x+64)$. Dla $a=\frac{81}{4}$ i $b=64$ istnieją dwie nieujemne wartości q. Punkty wymierne na tej krzywej to: $(0,0)$, $(\frac{81}{4},0)$, $(64,0)$, $(-54,\pm135)$, $(-36,\pm126)$, $(-24,\pm60)$, $(6,\pm105)$, $(36,\pm450)$, $(216,\pm3780)$. Możliwe wartości q to 0 oraz 6.

Uzyskanie tych rezultatów bardziej „klasycznymi" sposobami jest prawdopodobnie możliwe, ale skomplikowane do uogólnienia. Tymczasem tą metodą, mając dostęp do odpowiednich danych, możemy szybko zweryfikować istnienie q dla dowolnych a, b.

5 Szczególne przypadki

Mimo iż, jak widzieliśmy, nie da się w prosty sposób określić liczby właściwych q dla danych a, b, to da się to zrobić, jeśli ich iloraz $\frac{a}{b}$ ma określone własności, w szczególności jest całkowity.

Twierdzenie 4. Dana jest liczba $k\in\mathbb{Q}_+$ niebędąca kwadratem liczby wymiernej, taka że wielomian $R_k(x) = 3x^4+4(k+1)x^3+6kx^2-k^2$ nie ma pierwiastków wymiernych. Wtedy dla dowolnego $a\in\mathbb{Q}_+$ jeśli q^2+a i q^2+ka są kwadratami liczb wymiernych dla pewnego $q\in\mathbb{Q}$, to takich q jest nieskończenie wiele.

Dowód. Przyjmijmy nie wprost, że dla pewnych k, a teza nie zachodzi. W rozdziale trzecim udowodniliśmy, że wtedy dla krzywej $E: y^2 = x(x+a)(x+ka)$ mamy $E(\mathbb{Q})\simeq\mathbb{Z}_2\times\mathbb{Z}_{2n}$ dla $n=4$, 8 lub 6, przy czym pierwsze dwa przypadki mogą zachodzić jedynie gdy a oraz ka są kwadratami liczb wymiernych. Ten przypadek nie może zachodzić, gdyż wtedy $\frac{ka}{a}=k$ musiałoby także być kwadratem liczby wymiernej. Zatem $E(\mathbb{Q})\simeq\mathbb{Z}_2\times\mathbb{Z}_6$. Wtedy na E istnieje punkt $P=(x_0,y_0)$ rzędu 3. Styczna w P przecina E trzykrotnie, tzn. P jest punktem przegięcia tej krzywej. To oznacza, że druga pochodna

$y(x) = \sqrt{x(x+a)(x+ka)}$ ma zero w punkcie x_0. Ponieważ

$$y''(x) = \frac{3x^4 + 4a(k+1)x^3 + 6a^2kx^2 - a^4k^2}{4(x(x+a)(x+ka))^{\frac{3}{2}}},$$

to wielomian $R(x) = \frac{y''(ax)}{a^4} = 3x^4 + 4(k+1)x^3 + 6kx^2 - k^2$ ma wymierny pierwiastek $\frac{x_0}{a}$, co przeczy założeniom. □

Przykład. Weźmy $k = 2$. Oczywiście k nie jest kwadratem liczby wymiernej, pozostaje więc zweryfikować, czy $R_k(x) = 3x^4 + 12x^3 + 12x^2 - 4$ ma pierwiastek wymierny. Jednak wtedy mielibyśmy $(x^2 + 2x)^2 = \frac{4}{3}$, zaś $\frac{4}{3}$ nie jest kwadratem liczby wymiernej, sprzeczność.

Uwaga. Przypadek $k = 2$ jest przydatny w kontekście liczb *kongruentnych*, tj. takich całkowitych liczb bezkwadratowych d, że $x - d$, x, $x + d$ są kwadratami liczb wymiernych dla pewnego x. Przykład mówi nam, że takich x możemy znaleźć nieskończenie wiele dla każdej liczby kongruentnej d.

Twierdzenie 5. Jeśli $k \in \mathbb{Z}$ i $k \neq 0, 1$, to wielomian $R_k(x)$ nie ma pierwiastków wymiernych.

Dowód. Wielomian $R_k(x)$ ma pierwiastek wymierny wtedy i tylko wtedy, gdy ma go $27R_k(\frac{x}{3}) = x^4 + 4(k+1)x^3 + 18kx^2 - 27k^2$. Z twierdzenia o pierwiastkach wymiernych, każdy jego pierwiastek wymierny jest całkowity. Rozważając ten wielomian jako funkcję k, otrzymamy trójmian kwadratowy $-27k^2+(4x^3+18x^2)k+(x^4+4x^3)$ o wyróżniku $(4x^3+18x^2)^2+4\cdot27\cdot(x^4+4x^3) = 16x^6 + 144x^5 + 432x^4 + 432x^3 = 16(x^2 + 3x)^3$, zatem

$$k = \frac{4x^3 + 18x^2 \pm 4\sqrt{x(x+3)}^3}{54},$$

w szczególności $x(x + 3)$ jest kwadratem liczby wymiernej. Skoro x jest całkowite, to $x(x + 3)$ także. Jeśli $3 \nmid x$, to $\mathrm{nwd}(x, x + 3) = \mathrm{nwd}(x, 3) = 1$, więc zarówno x jak i $x+3$ są kwadratami liczb całkowitych, co jak łatwo sprawdzić zachodzi tylko dla $x = 1$ oraz $x = -4$. Pierwsza z tych wartości daje $k = 1$ lub $k = -\frac{5}{27}$, druga zaś $k = 0$ lub $k = \frac{32}{27}$ – wszystkie cztery dają sprzeczność. Jeśli $3 \mid x$, to $\mathrm{nwd}(\frac{x}{3}, \frac{x}{3} + 1) = 1$, $x = 0$ lub $x = -3$. Pierwsza możliwość daje sprzeczność (gdyż nie ma dwóch kwadratów niezerowych liczb całkowitych odległych o 1), druga daje $k = 0$, trzecia $k = 1$, czyli także sprzeczności. To kończy dowód.

Wniosek. Niech k będzie liczbą naturalną niebędącą kwadratem, zaś a liczbą wymierną. Jeśli istnieje takie $q \in \mathbb{Q}$, że q^2+a oraz q^2+ka są kwadratami liczb wymiernych, to takich q jest nieskończenie wiele.

Literatura

[1] Andrew Sutherland, *Elliptic curves*, https://math.mit.edu/classes/18.783/2015/LectureNotes2.pdf

[2] Karl Rubin i Alice Silverberg, *Ranks of elliptic curves*, https://www.ams.org/journals/bull/2002-39-04/S0273-0979-02-00952-7/

[3] Barry Mazur, *Modular curves and the Eisenstein ideal*, Publ. math. IHES 47 (1977), 33-186. MR 80c:14015, https://mathscinet.ams.org/mathscinet-getitem?mr=80c:14015

[4] John Cremona, *Elliptic curve data*, http://johncremona.github.io/ecdata/ oraz https://raw.githubusercontent.com/JohnCremona/ecdata/master/allgens/allgens.00000-09999

[5] A. Wiman, *Über den Rang von Kurven* $y^2 = x(x + a)(x + b)$, Acta Math. 76 (1945), 225-251, https://projecteuclid.org/euclid.acta/1487102178

[6] Daniel Sion Kubert, *Universal bound on the torsion of elliptic curves*, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.873.9806&rep=rep1&type=pdf