TRZECIA LICZBA PITAGOREJSKA CIAŁ LICZBOWYCH STOPNIA 2

BARTŁOMIEJ BYCHAWSKI

Streszczenie. W pracy wyliczamy wartość 3-ciej liczby pitagorejskiej dla pewnych ciał liczbowych, głównie kwadratowych rozszerzeń $\mathbb{Q}$.

1. Wprowadzenie i oznaczenia

Niech R będzie pierścieniem przemiennym z jedynką. Definiujemy n-tą liczbą pitagorejską pierścienia R jako najmniejszą liczbę naturalną m taką, że jeśli dla $r \in R$ zachodzi

$$r = \sum_{i=1}^{M} {x_i}^n$$

dla pewnego $M \in \mathbb{Z}^+$, oraz pewnych $x_1, \ldots, x_M \in R$ to dla pewnych $y_1, \ldots, y_m \in R$ zachodzi także

$$r = \sum_{i=1}^{m} {y_i}^n.$$

Innymi słowy, jeśli element $r \in R$ jest sumą pewnej ilości n-tych potęg, to jest też sumą nie więcej niż m n-tych potęg. n-tą liczbę pitagorejską pierścienia R oznaczamy $P_n(R)$. Warto uzupełnić tę definicję o przypadek, gdy taka liczba m nie istnieje, czyli znajdziemy elementy będące sumą dowolnie dużej liczby n-tych potęg, której nie jesteśmy w stanie zmniejszyć. Zapisujemy wtedy $P_n(R) = \infty$.

Problem liczby pitagorejskiej powstał jako problem podobny oraz uogólniający problem Waringa oraz zmodyfikowany problem Waringa. Problemy te brzmią następująco.

Problem Waringa: dla danego n, wyznacz najmniejszą liczbę naturalną m, taką, że dla każdego $x \in \mathbb{Z}^+$ zachodzi

$$x = \sum_{i=1}^{m} {x_i}^n$$

przy czym $x_1, \ldots, x_m \in \mathbb{Z}_{\geqslant 0}$. Będziemy oznaczać $W_n := m$.

Zmodyfikowany problem Waringa: dla danego n, wyznacz najmniejszą liczbę naturalną m, taką, że dla każdego $x \in \mathbb{Z}^+$ zachodzi

$$x = \sum_{i=1}^{m} \epsilon_i {x_i}^n$$

przy czym $x_1, \ldots, x_m \in \mathbb{Z}_{\geqslant 0}$ oraz $\epsilon_1, \ldots, \epsilon_m \in \{-1, 1\}$. Będziemy oznaczać $w_n := m$.

Problem Waringa był rozważany także dla wielomianów czy funkcji wymiernych, co przydaje się w rozwiązaniach tego problemu dla innych pierścieni. Klasyczny problem Waringa

Praca napisana pod kierunkiem dra Tomasza Kowalczyka w IMUJ tomek.kowalczyk@uj.edu.pl.

jest prawie w całości rozwiązany, natomiast zmodyfikowany problem Waringa (zwany też "prostszym" problemem Waringa) nie jest rozwiązany prawie wcale [11].

Problem liczb pitagorejskich dla pierścienia $\mathbb{Z}$ jest problemem pomiędzy problemem Warringa a jego zmodyfikowaną wersją. Gdy n jest parzyste, to $P_n(\mathbb{Z}) = W_n$, natomiast gdy n jest nieparzyste zachodzi $P_n(\mathbb{Z}) = w_n$.

Wiadomo między innymi, że $P_n(\mathbb{R}) = 1$ dla każdego $n \in \mathbb{Z}^+$, $P_2(\mathbb{Q}) = 4$, $4 \leqslant W_3(\mathbb{Z}) \leqslant 5$ (dokładna wartość nie jest znana), $P_3(\mathbb{Q}) = 3$ (co pokażemy). W poniższej pracy znajdujemy wartości trzeciej liczby pitagorejskiej dla rozszerzeń $\mathbb{Q}$ drugiego stopnia oraz jednego rozszerzenia trzeciego stopnia. Używamy w tym celu bazy danych [7], stworzonej przez ekspertów zajmujących się krzywymi eliptycznymi, informacje o rzetelności danych można znaleźć pod linkiem (https://www.lmfdb.org/EllipticCurve/Reliability). Dodatkowo użyjemy też powszechnie używanego i sprawdzonego kalkulatora algebraicznego [8]. Pytanie o 3-cią liczbę pitagorejską ciał liczbowych pojawiło się w jeszcze nie opublikowanej pracy [2]. Pokazuje ona między innymi jak wyglądają niektóre liczby pitagorejskie dla ciał i pierścieni liczb p-adycznych.

Oznaczenia. Przypomnijmy, że ciałem liczbowym nazywamy rozszerzenie ciała $\mathbb{Q}$ skończonego stopnia. Niech F będzie ciałem liczbowym.

Krzywą zadaną równaniem

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

gdzie $a_1, a_3, a_2, a_4, a_6 \in F$, nazywamy krzywą eliptyczną (nad ciałem F), o ile jej wyróżnik zadany wzorem:

$$\Delta = -{b_2}^2b_8 - 8{b_4}^3 - 27{b_6}^2 + 9b_2b_4b_6$$

gdzie

$$\begin{aligned} b_2 &= {a_1}^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= {a_3}^2 + 4a_6 \\ b_8 &= {a_1}^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2{a_3}^2 - {a_4}^2. \end{aligned}$$

jest różny od zera. Powyższe równanie nazywamy formą Weierstrassa krzywej eliptycznej. Przez $E(F)$ oznaczamy zbiór punktów na tej krzywej eliptycznej, wraz ze zwykłym działaniem [10].

Warto zaznaczyć, że oprócz "skończonych" punktów krzywa ta zawiera jeden dodatkowy punkt - punkt w nieskończoności, będący zarazem elementem neutralnym działania zadanego na krzywej.

Zdefiniujmy j-niezmiennik krzywej $E(F)$ jako liczbę przypisaną krzywej eliptycznej, którą można wyliczyć z następującego wzoru:

$$j = \frac{{c_4}^3}{\Delta}$$

gdzie Δ to wyróżnik wybranej formy Weierstrassa, natomiast:

$$c_4 = {b_2}^2 - 24b_4.$$

Nad ciałem liczb zespolonych, dwie krzywe eliptyczne są izomorficzne wtedy i tylko wtedy gdy mają te same j-niezmienniki. Można ten fakt znaleźć w [9, Proposition 1.4]. Warto tu jednak zwrócić uwagę, że w cytowanej propozycji jest literówka w podpunkcie (i).

Poniżej podajemy jeszcze Twierdzenie Mordella-Weila, [9, Theorem 6.7], opisujące strukturę grupy na krzywej eliptycznej. Działanie w tej grupie będziemy oznaczać $+_E$.

Twierdzenie Mordella-Weila. *Dla każdego ciała liczbowego $\mathbb{K}$ zachodzi*

$$E(\mathbb{K}) \cong E(\mathbb{K})_{tor} \times \mathbb{Z}^r,$$

gdzie $E(\mathbb{K})_{tor}$ oznacza grupę elementów skończonego rzędu, natomiast liczba $r \in \mathbb{Z}_{\geqslant 0}$ jest nazywana rangą.

Będziemy mówić, że grupa torsyjna krzywej eliptycznej jest trywialna, gdy zawiera tylko jeden element, czyli punkt w nieskończoności. Powiemy, że krzywa eliptyczna jest trywialna, gdy jej grupa torsyjna jest trywialna oraz jej ranga jest równa 0.

Zbiór elementów całkowitych ciała liczbowego $\mathbb{K}$ to zbiór elementów $x \in \mathbb{K}$, takich, że istnieje wielomian unormowany (współczynnik przy najwyższej potędze równy 1) $f \in \mathbb{Z}[X]$, że x jest jego pierwiastkiem. Zbiór ten jest pierścieniem.

Dla porządku przypomnimy jeszcze definicję τ_D:

$$\tau_D = \sqrt{D},$$

gdy $D \equiv 2, 3 \pmod 4$, oraz

$$\tau_D = \frac{1+\sqrt{D}}{2},$$

gdy $D \equiv 1 \pmod 4$. Na przykład:

$$\tau_2 = \sqrt{2},\ \tau_7 = \sqrt{7},\ \tau_{-1} = \sqrt{-1} = i$$

$$\tau_5 = \frac{1+\sqrt{5}}{2},\ \tau_{13} = \frac{1+\sqrt{13}}{2},\ \tau_{-3} = \frac{1+\sqrt{-3}}{2} = \frac{1+\sqrt{3}i}{2} = e^{\frac{2\pi i}{6}}$$

Pokażmy jeszcze, że każde rozszerzenie $\mathbb{Q}$ stopnia 2 jest rozszerzeniem o pierwiastek z liczby całkowitej.

Niech $\mathbb{K} := \mathbb{Q}(\alpha)$ będzie rozszerzeniem stopnia 2. Wynika stąd, że dla pewnych $a, b \in \mathbb{Q}$ zachodzi

$$0 = \alpha^2 + a \cdot \alpha + b = (\alpha + \frac{a}{2})^2 - \frac{a^2}{4} + b$$

$$(\alpha + \frac{a}{2})^2 = \frac{a^2}{4} - b \in \mathbb{Q}.$$

Mnożąc obie strony przez odpowiednią liczbę całkowitą, otrzymujemy po prawej pewną liczbę całkowitą, po lewej element z $\mathbb{Q}(\alpha)$ nie będący elementem $\mathbb{Q}$, podniesiony do kwadratu. Definiując więc $\beta := \alpha + \frac{a}{2}$ zauważamy, że $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$ oraz oba rozszerzenia są tego samego

stopnia, zatem są sobie równe. Element o który rozszerzamy będziemy oznaczać jako $\sqrt{D}$, dla pewnej liczby całkowitej D.

Pierścień elementów całkowitych ciała $\mathbb{Q}(\sqrt{D})$ będziemy oznaczać przez

$$\mathbb{Z}[\tau_D] := \{a + b\tau_D | a, b \in \mathbb{Z}\}.$$

2. Górne ograniczenie $P_3(\mathbb{Q}(\alpha))$

Będziemy naśladować dowód Riley'a [5], pokazujący, że $P_3(\mathbb{K}) \leqslant 3$ dla każdego ciała $\mathbb{K}$, takiego, że $\mathbb{Q} \subseteq \mathbb{K}$.

Znajdujemy trójkę funkcji wymiernych F, G, i H dwóch zmiennych m, n taką, że

$$m = F(m,n)^3 + G(m,n)^3 + H(m,n)^3.$$

Na podstawie [5] te funkcje to

$$F(m,n) = \frac{27m^3 - n^9}{27m^2n^2 + 9mn^5 + 3n^8}$$

$$G(m,n) = \frac{-27m^3 + 9mn^6 + n^9}{27m^2n^2 + 9mn^5 + 3n^8}$$

$$H(m,n) = \frac{27m^2n^3 + 9mn^6}{27m^2n^2 + 9mn^5 + 3n^8}.$$

Oczywiście, są to funkcje wymierne, więc jeśli $m, n \in \mathbb{Q}(\alpha)$, to o ile mianownik się nie zeruje, to $F(m,n), G(m,n), H(m,n) \in \mathbb{Q}(\alpha)$. Dla ustalonej wartości m każdy z mianowników jest wielomianem, więc zeruje się tylko dla skończonej liczby wartości zmiennej n. Możemy dobrać dowolne n z nieskończonego zbioru $\mathbb{Q}(\alpha)$ nie zerujące mianowników, i otrzymujemy przedstawienie dowolnego $m \in \mathbb{Q}(\alpha)$ jako sumy trzech trzecich potęg elementów ciała $\mathbb{Q}(\alpha)$.

Oznacza to dodatkowo, że każdy element $\mathbb{Q}(\alpha)$ można przedstawić jako sumę trzech sześcianów, czyli szukamy ograniczenia ilości trzecich potęg, które zadziała dla wszystkich elementów ciała. Na tej obserwacji opiera się metoda znajdowania dolnych ograniczeń dla poszczególnych ciał liczbowych.

3. Dolne ograniczenie $P_3(\mathbb{Q}(\alpha))$

Podstawową i powszechną metodą wyznaczania dolnych ograniczeń n-tej liczby pitagorejskiej jest znajdowanie takiego $d \in \mathbb{Q}(\alpha)$, że równanie

$$d = \sum_{k=1}^{N} {x_k}^n,$$

nie ma rozwiązań dla $x_1, \ldots, x_N \in \mathbb{Q}(\alpha)$, gdy N jest mniejsze od naszego docelowego ograniczenia. Zatem w naszym przypadku, aby pokazać, że $P_3(\mathbb{Q}(\alpha)) \geqslant 3$ należy znaleźć takie

$d \in \mathbb{Q}(\alpha)$, że równanie

$$d = x^3 + y^3 \tag{1}$$

nie ma rozwiązań dla $x, y \in \mathbb{Q}(\alpha)$. Oczywiście wystarczy rozważyć $d \neq 0$, bo $0 = 0^3$.

Korzystając z przekształceń zawartych w pracy [1] znajdujemy krzywą eliptyczną powiązaną z tym równaniem. Jeśli powyższe równanie ma rozwiązanie, to powiązana z nim krzywa eliptyczna zawiera punkt $(x, y) \in \mathbb{Q}(\alpha)^2$.

Powyższa praca pokazuje również, że równanie $4 = x^3 + y^3$ nie ma rozwiązań w $\mathbb{Q}$ a więc $3 \leqslant P_3(\mathbb{Q})$. A stąd na podstawie wcześniejszej części $P_3(\mathbb{Q}) = 3$.

Zapiszmy więc przekształcenia, o których była mowa.

Najpierw podstawiamy

$$x = \frac{u}{v}, y = \frac{1-u}{v},$$

czyli tak naprawdę najpierw definiujemy

$$v := \frac{1}{x+y}, u := \frac{x}{x+y}.$$

Gdy $x, y \in \mathbb{Q}(\alpha)$ to oczywiście $u, v \in \mathbb{Q}(\alpha)$. Gdyby $x + y = 0$, to $y = -x$, co daje $d = x^3 + y^3 = x^3 + (-x)^3 = x^3 - x^3 = 0$, a zatem sprzeczność.

Równanie $d = x^3 + y^3$ przyjmuje więc postać

$$d = \left(\frac{u}{v}\right)^3 + \left(\frac{1-u}{v}\right)^3,$$

co po pomnożeniu przez v^3 daje

$$D \cdot v^3 = u^3 + (1-u)^3 = 3u^2 - 3u + 1 = 3 \cdot \left(u - \frac{1}{2}\right)^2 + \frac{1}{4} \tag{2}$$

Jeśli $v \neq 0$, to mając rozwiązanie (u, v) równania (2) otrzymujemy parę $(\frac{u}{v}, \frac{1-u}{v})$ będącą rozwiązaniem równania (1).

Stąd pytanie: dla jakich rozszerzeń $\mathbb{Q}(\alpha)$ istnieje rozwiązanie równania (2) takie, że $v = 0$?

Lemat 3.1. *Jeśli $\mathbb{Q}(\alpha)$ jest rozszerzeniem $\mathbb{Q}$, oraz istnieje para $(u, 0) \in \mathbb{Q}(\alpha)^2$, spełniająca równanie (2), to $\sqrt{-3} \in \mathbb{Q}(\alpha)$.*

Dowód. Gdy założenia są spełnione, zachodzą następujące równości:

$$\begin{aligned}
0 &= 3 \cdot \left(u - \frac{1}{2}\right)^2 + \frac{1}{4} \\
0 &= \left(u - \frac{1}{2}\right)^2 + \frac{1}{2}^2 \cdot \frac{1}{3} \\
-\left(\frac{1}{2}\right)^2 \cdot \frac{1}{3} &= \left(u - \frac{1}{2}\right)^2 \\
-3 &= \left(6 \cdot \left(u - \frac{1}{2}\right)\right)^2 \\
\pm\sqrt{-3} &= \left(6 \cdot \left(u - \frac{1}{2}\right)\right) \in \mathbb{Q}(\alpha)
\end{aligned}$$

Otrzymujemy więc $\sqrt{-3} \in \mathbb{Q}(\alpha)$. □

Wniosek 3.2. *Jeśli $\mathbb{Q}(\alpha)$ jest dodatkowo rozszerzeniem drugiego, lub trzeciego stopnia, to $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\alpha)$. Skoro $\mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(\alpha)$, to wymiar $\mathbb{Q}(\sqrt{-3})$ jako przestrzeni liniowej nad $\mathbb{Q}$, równy 2, dzieli wymiar $\mathbb{Q}(\alpha)$ jako przestrzeni liniowej nad $\mathbb{Q}$. Ale 2 nie dzieli 3, zatem równość wymiarów wraz z zawieraniem pociąga za sobą równość ciał.*

Innym prostym wnioskiem z Lematu 3.1 jest fakt, że dla rozszerzeń $\mathbb{Q}$ drugiego i trzeciego stopnia z wyłączeniem $\mathbb{Q}(\sqrt{-3})$ istnieje bijekcja między rozwiązaniami (1) a rozwiązaniami (2), co więcej, wzory na tą bijekcję w obie strony są zadane jawnie wyżej.

Wróćmy więc do równania (2). Podstawiając

$$\alpha := (u - \frac{1}{2}) \cdot 72d$$
$$\gamma := v \cdot 12d$$

otrzymujemy

$$\alpha^2 = \gamma^3 - 432d^2 \tag{3}$$

Przekształcenie pary (u, v) na parę (α, γ) jest bijekcją między rozwiązaniami równania (2) oraz (3) zadaną w jedną stronę powyższymi wzorami.

Twierdzenie 3.3. *Niech $0 \neq d \in \mathbb{Q}(\alpha)$ oraz niech krzywa eliptyczna $\alpha^2 + 432d^2 = \gamma^3$ będzie trywialna nad $\mathbb{Q}(\alpha)$. Wtedy równanie $d = x^3 + y^3$ nie ma rozwiązań w $\mathbb{Q}(\alpha)$.*

Dowód. Załóżmy nie wprost, że para $(x, y) \in \mathbb{Q}(\alpha)^2$ spełnia zależność $d = x^3+y^3$. Wtedy, na podstawie wyżej przeprowadzonych przekształceń wiemy, że para $(\frac{x}{x+y}, \frac{1}{x+y}) = (u, v)$ spełnia równanie (2), przez co para $((\frac{x}{x+y} - \frac{1}{2}) \cdot 72d, \frac{1}{x+y} \cdot 12d) = ((u - \frac{1}{2}) \cdot 72d, v \cdot 12d) = (\alpha, \gamma)$ spełnia równanie (3), co jest sprzeczne z założeniem, że krzywa $\alpha^2 + 432d^2 = \gamma^3$ jest trywialna nad $\mathbb{Q}(\alpha)$. □

Twierdzenie 3.4. *Niech $\mathbb{Q}(\alpha)$ będzie rozszerzeniem $\mathbb{Q}$ nie zawierającym $\sqrt{-3}$. Wtedy dla każdego $0 \neq d \in \mathbb{Q}(\alpha)$ zachodzi następująca równoważność: krzywa eliptyczna $\alpha^2 = \gamma^3 - 432d^2$ jest trywialna nad $\mathbb{Q}(\alpha)$ wtedy i tylko wtedy, gdy równanie $d = x^3 + y^3$ nie ma rozwiązań w $\mathbb{Q}(\alpha)$.*

Dowód. Twierdzenie 3.3 dostarcza implikacji ($\Rightarrow$). Pozostało udowodnić implikację w drugą stronę: jeśli równanie $d = x^3 + y^3$ nie ma rozwiązań w $\mathbb{Q}(\alpha)$, to krzywa eliptyczna $\alpha^2 = \gamma^3 - 432d^2$ jest trywialna nad $\mathbb{Q}(\alpha)$.

Ponownie przeprowadzimy dowód nie wprost. Załóżmy więc, że para $(\alpha, \gamma) \in \mathbb{Q}(\alpha)^2$ leży na krzywej $\alpha^2 = \gamma^3 - 432d^2$. Wtedy para $(\frac{\alpha}{72d} + \frac{1}{2}, \frac{\gamma}{12d}) = (u, v)$ jest rozwiązaniem równania (2), a na podstawie Lematu 3.1 $v \neq 0$, więc para $(\frac{\frac{\alpha}{72d} + \frac{1}{2}}{\frac{\gamma}{12d}}, \frac{\frac{1}{2} - \frac{\alpha}{72d}}{\frac{\gamma}{12d}}) = (\frac{u}{v}, \frac{1-u}{v}) = (x, y)$ jest rozwiązaniem równania (1). Ale założyliśmy, że (1) nie ma rozwiązań, sprzeczność. □

Otrzymujemy więc krzywą:

$$y^2 = x^3 - 3 \cdot (12d)^2.$$

Dla wygody zamieniliśmy α na y oraz γ na x.

Sprowadziliśmy więc nasz problem do znalezienia trywialnej krzywej eliptycznej (poza przypadkiem gdy $\sqrt{-3} \in \mathbb{Q}(\alpha)$).

Rozważmy teraz przypadek gdy $\sqrt{-3} \in \mathbb{Q}(\alpha)$. Zauważmy na początku, że na krzywej eliptycznej $E(\mathbb{Q}(\alpha))$:

$$y^2 = x^3 - 3A^2$$

(gdzie $A \neq 0$) oprócz punktu w nieskończoności znajdują się dodatkowo punkty $(0, \sqrt{-3}A)$, $(0, -\sqrt{-3}A)$.

Twierdzenie 3.5. *Punkty $(0, \sqrt{-3}A)$, $(0, -\sqrt{-3}A)$ wraz z punktem w nieskończoności tworzą grupę cykliczną w zbiorze punktów na krzywej $E(\mathbb{Q}(\alpha))$ z działaniem zgodnym z działaniem na krzywej.*

Dowód. Punkt w nieskończoności jest elementem neutralnym. Dodatkowo wiadomo, że

$$(0, \sqrt{-3}A) +_E (0, -\sqrt{-3}A) = e$$

Wiemy to, bo punkty te są symetryczne względem osi X, natomiast punkt w nieskończoności tej krzywej to kierunek osi Y, stąd jest współliniowy z powyższymi punktami. Wynika to z symetrii tej krzywej względem osi X.

Wystarczy więc pokazać, że zachodzi

$$(0, \sqrt{-3}A) +_E (0, \sqrt{-3}A) = (0, -\sqrt{-3}A).$$

Wzór na $P +_E P$, gdzie $P \in E(\mathbb{Q}(\alpha))$ to

$$(x_0, y_0) +_E (x_0, y_0) = (x_1, y_1)$$

przy czym zachodzą równości

$$x_1 = \left(\frac{3{x_0}^2 + a_4}{2y_0}\right)^2 - 2x_0$$
$$y_1 = -y_0 + \left(\frac{3{x_0}^2 + a_4}{2y_0}\right)^2 (x_0 - x_1)$$

W naszym przypadku $a_4 = 0$, możemy więc bezpośrednio sprawdzić, że postulowana wyżej równość zachodzi, co kończy dowód. □

Twierdzenie 3.6. *Dla rozszerzeń $\mathbb{Q}$, takich, że $\sqrt{-3} \in \mathbb{Q}(\alpha)$ dla każdego $0 \neq d \in \mathbb{Q}(\alpha)$ zachodzi: równanie $d = x^3 + y^3$ nie ma rozwiązań w ciele $\mathbb{Q}(\alpha)$ wtedy i tylko wtedy, gdy krzywa $E(\mathbb{Q}(\alpha))$ definiowana równaniem*

$$\alpha^2 = \gamma^3 - 3 \cdot (12d)^2$$

ma rangę 0 i 3 elementową grupę torsyjną.

Dowód. Na początku zauważmy, że na podstawie Twierdzenia 3.5 podstawiając $A = 12d$ widzimy, że grupa torsyjna zawiera punkt w nieskończoności oraz punkty

$$(0, \sqrt{-3} \cdot 12d),\ (0, -\sqrt{-3} \cdot 12d).$$

Współrzędne są zapisywane w kolejności: (γ_0, α_0).

Zajmijmy się implikacją ($\Rightarrow$). Zakładamy, że równanie $d = x^3 + y^3$ nie ma rozwiązań w ciele $\mathbb{Q}(\alpha)$. Załóżmy nie wprost, że krzywa $E(\mathbb{Q}(\alpha))$ posiada punkt poza trzema wyżej wymienionymi. Niech (γ_0, α_0) będzie tym punktem.

Udowodnijmy na początek, że $\gamma_0 \neq 0$. Załóżmy nie wprost, że $\gamma_0 = 0$. Wtedy

$$\alpha_0^2 = 0^3 - 3 \cdot (12d)^2 = \left(\sqrt{-3} \cdot 12d\right)^2$$
$$0 = \alpha_0^2 - (\sqrt{-3} \cdot 12d)^2 = (\alpha_0 - \sqrt{-3} \cdot 12d) \cdot (\alpha_0 + \sqrt{-3} \cdot 12d)$$

stąd $\alpha_0 \in \left\{\sqrt{-3} \cdot 12d, -\sqrt{-3} \cdot 12d\right\}$, co pociąga za sobą

$$(\gamma_0, \alpha_0) \in \left\{(0, \sqrt{-3} \cdot 12d), (0, -\sqrt{-3} \cdot 12d)\right\},$$

co jest sprzeczne z założeniami. Dowód nie wprost jest więc zakończony i mamy $\gamma_0 \neq 0$.

Para (γ_0, α_0) leżąca na krzywej (3) daje zgodnie z wcześniejszymi przekształceniami parę

$$\left(\frac{\alpha_0}{72d} + \frac{1}{2}, \frac{\gamma_0}{12d}\right) = (u_0, v_0)$$

należącą do krzywej (2). Zauważmy, że skoro $\gamma_0 \neq 0$, to $v \neq 0$. Oznacza to, że punkt

$$\left(\frac{\frac{\alpha_0}{72d} + \frac{1}{2}}{\frac{\gamma_0}{12d}}, \frac{\frac{1}{2} - \frac{\alpha_0}{72d}}{\frac{\gamma_0}{12d}}\right) = \left(\frac{u_0}{v_0}, \frac{1 - u_0}{v_0}\right) = (x_0, y_0)$$

istnieje i jest rozwiązaniem (1), co stoi w sprzeczności z założeniem, że równanie to nie ma rozwiązań w $\mathbb{Q}(\alpha)$.

Pozostało udowodnić implikację ($\Leftarrow$). Zakładamy więc, że krzywa $E(\mathbb{Q}(\alpha))$ (czyli (3)) zawiera jedynie trzy wymienione wyżej punkty.

Załóżmy niewprost, że równanie $d = x^3 + y^3$ ma rozwiązanie $(x_0, y_0) \in \mathbb{Q}(\alpha)^2$. Wtedy, na podstawie wcześnieszych wyliczeń para

$$\left(\left(\frac{x_0}{x_0 + y_0} - \frac{1}{2}\right) \cdot 72d, \frac{1}{x_0 + y_0} \cdot 12d\right) = \left(\left(u_0 - \frac{1}{2}\right) \cdot 72d, v_0 \cdot 12d\right) = (\alpha_0, \gamma_0)$$

spełnia równanie (3), a dodatkowo:

$$\frac{1}{x_0 + y_0} \cdot 12d \neq 0,$$

więc, $(\alpha_0, \gamma_0) \notin \left\{(0, \sqrt{-3} \cdot 12d), (0, -\sqrt{-3} \cdot 12d)\right\}$, co jest sprzeczne z założeniem. Dowód tej implikacji także jest zakończony, co kończy dowód całego twierdzenia. □

Na zakończenie tej części zauważmy jeszcze, że bezpośrednio z definicji j-niezmiennik krzywej $y^2 = x^3 - 3 \cdot (12d)^2$ okazuje się być równy 0.

4. Metody przeszukiwania krzywych o pożądanych właściwościach

Niech dane będzie ciało liczbowe $\mathbb{Q}(\alpha)$ oraz trywialna krzywa eliptyczna E o j-niezmienniku równym 0.

Do znalezienia takiej krzywej eliptycznej E w praktyce użyjemy bazy danych [7]. Krzywa taka może być postaci $y^2 = x^3 - 3 \cdot (12d)^2$, chcemy sprawdzić, czy tak faktycznie jest.

Oznaczmy dla ułatwienia $A := 12d$. Chcemy pokazać, że po doprowadzeniu naszej znalezionej krzywej E do formy $y^2 = x^3 - B$, gdzie $B \in \mathbb{Q}(\alpha)$ (jest to możliwe, bo $j = 0$), istnieje $A \in \mathbb{Q}(\alpha)$, takie, że:

$$B = 3A^2 \iff 3B = (3A)^2$$

Oczywiście skoro E jest krzywą eliptyczną, to $B \neq 0$, bo inaczej $\Delta = 0$, co jest niemożliwe, a więc na pewno także $A \neq 0$.

Dla ułatwienia przemnożymy jeszcze $3B$ przez takie q^2 $(0 \neq q \in \mathbb{Z})$, że $3B \cdot q^2$ jest elementem całkowitym ciała $\mathbb{Q}(\alpha)$.

Szukamy więc takiego A, że:

$$3B \cdot q^2 = (3Aq)^2$$

Poniższe twierdzenie pomoże nam w ustalaniu, czy liczba $3B \cdot q^2$ jest kwadratem jakiegoś elementu z $\mathbb{Q}(\alpha)$.

Twierdzenie 4.1. *Jeśli dla danego $x \in \mathbb{Q}(\alpha)$, x^2 jest elementem całkowitym, to x także jest elementem całkowitym.*

Dowód. Skoro x^2 jest elementem całkowitym, to istnieje wielomian unormowany $f \in \mathbb{Z}[X]$, taki, że $f(x^2) = 0$. Rozważmy teraz wielomian $f \circ X^2$. Liczba x jest jego pierwiastkiem, a wielomian ten także jest unormowany, więc x jest elementem całkowitym. □

Powyższe twierdzenie znacznie zawęża zbiór potencjalnych rozwiązań równania

$$3B \cdot q^2 = (3Aq)^2.$$

Jeśli ustalimy już, że $3B \cdot q^2 = (3Aq)^2$, to znaleziona krzywa przyjmuje postać:

$$y^2 = x^3 - 3 \cdot A^2,$$

co pozwala na zastosowanie Twierdzenia 3.4 lub 3.6. Chcemy więc znaleźć efektywną metodę sprawdzania czy $3B \cdot q^2$ jest kwadratem.

Rozważmy rozszerzenia $\mathbb{Q}$ drugiego stopnia. Niech więc zachodzi

$$X + \tau_D \cdot Y = 3B \cdot q^2,$$

gdzie $X, Y \in \mathbb{Z}$. Załóżmy, że $3B \cdot q^2$ jest kwadratem, oraz $x_0 + \tau_D \cdot y_0 = 3Aq$, gdzie $x_0, y_0 \in \mathbb{Z}$. Wiemy bowiem, że dla rozszerzeń drugiego stopnia $\mathbb{Q}(\sqrt{D})$ zbiór elementów całkowitych jest równy pierścieniowi $\mathbb{Z}[\tau_D]$. Oznacza to, że

$${x_0}^2 + 2x_0y_0 \cdot \tau_D + {y_0}^2 \cdot {\tau_D}^2 = X + \tau_D \cdot Y.$$

Wiemy stąd, że

- jeśli $D \equiv 2, 3 \pmod 4$ to punkt (x_0, y_0) leży na krzywych
$$x^2 + Dy^2 = X,$$
$$2xy = Y.$$
- jeśli $D \equiv 1 \pmod 4$ to punkt (x_0, y_0) leży na krzywych
$$x^2 + Ky^2 = X,$$
$$2xy + y^2 = Y,$$
gdzie K jest liczbą całkowitą spełniającą $D = 4K + 1$.

Aby sprawdzić czy $3B \cdot q^2$ jest kwadratem wystarczy więc sprawdzić, czy odpowiednia para krzywych ma wymierny punkt przecięcia. Na podstawie powyższego twierdzenia wiemy jednak, że jeśli punkt wymierny leży na przecięciu tych krzywych, to jest punktem kratowym.

Punkty przecięcia krzywych otrzymujemy za pomocą kalkulatora graficznego [6], który pokazuje punkty przecięcia. Zweryfikowanie, czy są to punkty całkowite jest natychmiastowe.

Punktów tych jest nie więcej niż 4 na płaszczyźnie $\mathbb{R}^2$, bo pierwsze równanie to równanie elipsy, a drugie hiperboli o tym samym środku symetrii co elipsa - mowa o punkcie $(0, 0)$, więc, chociaż formalnie nie jest to oczywiste, widać, że pojedyńcze ramię hiperboli nie może przeciąć elipsy więcej niż 2 razy za sprawą wypukłości oraz faktu że asymptoty hiperboli przecinają się w punkcie $(0, 0)$. Mała ilość punktów przecięcia pozwala efektywnie sprawdzać, czy $3B \cdot q^2$ jest kwadratem, a dzięki temu, czy znaleziona przez nas krzywa $y^2 = x^3 - B$ jest odpowiedniej postaci by zastosować Twierdzenie 3.6 lub Twierdzenie 3.4.

Dodatkowo w obliczeniach dla rozszerzeń kwadratowych pomaga fakt, że dla $D \equiv 2, 3 \pmod 4$ zachodzi
$$\tau_D^2 = D,$$
a dla $D \equiv 1 \pmod 4$ zachodzi
$${\tau_D}^2 = \tau_D + K,$$
gdzie K jest taką liczbą całkowitą, że $D = 4K + 1$.

5. Wyniki dla szczególnych rozszerzeń $\mathbb{Q}$

Korzystając z bazy danych [7] znajdujemy przykłady krzywych eliptycznych poszukiwanej postaci o żądanych własnościach, czyli o randze równej 0, trywialnej grupie torsyjnej (lub 3 elementowej gdy $\sqrt{-3} \in \mathbb{Q}(\alpha)$) oraz j-niezmienniku równym 0. Narzucając na powyższą bazę danych te ograniczenia dostajemy stosunkowo mało krzywych eliptycznych, wśród których w sensownym czasie, za pomocą opisanych wyżej metod jesteśmy w stanie znaleźć te, które są postaci
$$y^2 = x^3 - 3 \cdot (12d)^2$$
dla pewnego $0 \neq d \in \mathbb{Q}(\alpha)$, a więc pozwalają na zastosowanie Twierdzenia 3.4 (lub 3.6 gdy $\sqrt{-3} \in \mathbb{Q}(\alpha)$) i wykazanie, że $P_3(\mathbb{Q}(\alpha)) = 3$.

Uzyskane wyniki będą prezentowane w następującej postaci:

- wartość a, czyli wybranego pierwiastka wielomianu definiującego rozszerzenie;
- numer krzywej eliptycznej o trywialnej grupie, bądź grupie 3 elementowej gdy $\sqrt{-3} \in \mathbb{Q}(\alpha)$;
- przekształcenie krzywej do postaci $y^2 = x^3 - B$;
- pokazanie, że istnieje $A \in \mathbb{Q}(\alpha)$ takie, że $B = 3 \cdot A^2$;
- wyliczenie d i wskazanie równania postaci $d = x^3 + y^3$ które na mocy Twierdzenia 3.6 lub Twierdzenia 3.4 nie ma rozwiązań.

5.1. **Ciała liczbowe stopnia 2.**

Ciała rzeczywiste, czyli takie, że $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$.

5.1.1. $\mathbb{Q}(\sqrt{2})$.

- $a = \sqrt{2}$
- Numer krzywej: $2916.1 - i2$
- $y^2 = x^3 + 54a - 81$
- $B = 81 - 54a = 3 \cdot (3 \cdot (1 - a))^2$
- $d = \frac{A}{12} = \frac{3 \cdot (1-a)}{12} = \frac{1-a}{4}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{1-a}{4} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{2})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{2})) = 3$.

5.1.2. $\mathbb{Q}(\sqrt{3})$*:*

- $a = \sqrt{3}$
- Numer krzywej: $2916.1 - q1$
- $y^2 = x^3 - 4a - 7$
- $B = 7 + 4a = (2 + a)^2 = 3 \cdot (\frac{2+a}{a})^2 = 3 \cdot (\frac{2a+3}{3})^2$
- $d = \frac{\frac{2a+3}{3}}{12} = \frac{2a+3}{36}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{2a+3}{36} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{3})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{3})) = 3$.

5.1.3. $\mathbb{Q}(\sqrt{5})$*:*

- $a = \frac{1+\sqrt{5}}{2}$
- Numer krzywej: $729.1 - f2$
- $y^2 + ay = x^3 - 7a - 7$
  $(y + \frac{a}{2})^2 = y^2 + ay + \frac{a^2}{4} = x^3 - 7a - 7 + \frac{a^2}{4} = x^3 - a^2 \cdot (7 - \frac{1}{4})$
- $B = a^2 \cdot (7 - \frac{1}{4}) = a^2 \cdot \frac{27}{4} = 3 \cdot (\frac{3a}{2})^2$
- $d = \frac{A}{12} = \frac{\frac{3a}{2}}{12} = \frac{a}{8}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{a}{8} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{5})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{5})) = 3$.

5.1.4. $\mathbb{Q}(\sqrt{6})$*:*

- $a = \sqrt{6}$
- Numer krzywej: $342.1 - a1$
- $y^2 + ay = x^3 - 2$
  $(y + \frac{a}{2})^2 = y^2 + ay + \frac{a^2}{4} = x^3 - 2 + \frac{a^2}{4} = x^3 - 2 + \frac{6}{4} = x^3 - \frac{1}{2}$
- $B = \frac{1}{2} = 3 \cdot \frac{1}{6} = 3 \cdot (\frac{1}{a})^2 = 3 \cdot (\frac{a}{6})^2$
- $d = \frac{A}{12} = \frac{\frac{a}{6}}{12} = \frac{a}{72}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{a}{72} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{6})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{6})) = 3$.

5.1.5. $\mathbb{Q}(\sqrt{7})$*:*

- $a = \sqrt{7}$
- Numer krzywej: $243.2 - c2$
- $y^2 + ay = x^3 + 324a - 859$
  $(y + \frac{a}{2})^2 = y^2 + ay + \frac{a^2}{4} = x^3 + 324a - 859 + \frac{a^2}{4}$
- $B = 859 - 324a - \frac{a^2}{4} = \frac{1}{4} \cdot ((859 \cdot 4 - 7) - 324 \cdot 4a) = 3 \cdot (\frac{3 \cdot (8-3a)}{2})^2$
- $d = \frac{A}{12} = \frac{\frac{3 \cdot (8-3a)}{2}}{12} = \frac{8-3a}{8}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{8 - 3a}{8} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{7})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{7})) = 3$.

5.1.6. $\mathbb{Q}(\sqrt{10})$*:*

- $a = \sqrt{10}$
- Numer krzywej: $243.1 - d2$
- $y^2 + y = x^3 - 1539a - 4867$
  $(y + \frac{1}{2})^2 = y^2 + y + \frac{1}{4} = x^3 - 1539a - 4867 + \frac{1}{4}$
- $B = \frac{1}{4} \cdot (4867 \cdot 4 - 1 + 4 \cdot 1539a) = \frac{1}{2^2} \cdot \frac{1}{3^2} \cdot 3 \cdot (3 \cdot (4867 \cdot 4 - 1 + 4 \cdot 1539a)) =$
  $= \frac{1}{2^2} \cdot \frac{1}{3^2} \cdot 3 \cdot (171 + 54a)^2 = 3 \cdot (\frac{171+54a}{6})^2$
- $d = \frac{A}{12} = \frac{\frac{171+54a}{6}}{12} = \frac{171+54a}{72}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{171 + 54a}{72} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{10})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{10})) = 3$.

5.1.7. $\mathbb{Q}(\sqrt{13})$*:*

- $a = \frac{1+\sqrt{13}}{2}$
- Numer krzywej: $243.2 - b2$
- $y^2 + (a + 1)y = x^3 - 21a - 28$
  $(y + \frac{a+1}{2})^2 = y^2 + (a + 1)y + \frac{(a+1)^2}{4} = x^3 - 21a - 28 + \frac{(a+1)^2}{4} =$
  $= x^3 - 21a - 28 + \frac{a^2+2a+1}{4} == x^3 - 21a - 28 + \frac{3a+4}{4}$
- $B = 28 + 21a - \frac{3a+4}{4} = \frac{1}{4} \cdot ((28 \cdot 4 - 4) + (21 \cdot 4 - 3)a) =$
  $= 3 \cdot \frac{1}{2^2} \cdot ((9 \cdot 4) + (7 \cdot 4 - 1)a) = 3 \cdot \frac{1}{2^2} \cdot 3^2 \cdot (4 + 3a) = 3 \cdot \frac{1}{2^2} \cdot 3^2 \cdot (1 + a)^2$
- $d = \frac{A}{12} = \frac{\frac{3\cdot(1+a)}{2}}{12} = \frac{1+a}{8}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{1 + a}{8} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{13})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{13})) = 3$.

5.1.8. $\mathbb{Q}(\sqrt{17})$*:*

- $a = \frac{1+\sqrt{17}}{2}$
- Numer krzywej: $729.1 - g2$
- $y^2 + y = x^3 - 108a - 169$
  $(y + \frac{1}{2})^2 = y^2 + y + \frac{1}{4} = x^3 - 108a - 169 + \frac{1}{4}$
- $B = 169 - \frac{1}{4} + 108a = \frac{1}{2^2} \cdot ((169 \cdot 4 - 1) + (108 \cdot 4)a) =$
  $= \frac{1}{2^2} \cdot \frac{1}{3^2} \cdot 3 \cdot (3 \cdot ((169 \cdot 4 - 1) + (108 \cdot 4)a)) = \frac{1}{2^2} \cdot \frac{1}{3^2} \cdot 3 \cdot (27 + 18a)^2$
- $d = \frac{A}{12} = \frac{\frac{27+18a}{6}}{12} = \frac{3+2a}{8}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{3 + 2a}{8} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{17})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{17})) = 3$.

5.1.9. $\mathbb{Q}(\sqrt{21})$*:*

- $a = \frac{1+\sqrt{21}}{2}$
- Numer krzywej: $1296.1 - d1$
- $y^2 = x^3 - 96a - 172$
- $B = 172 + 96a = 3 \cdot (\frac{14+8a}{3})^2$
- $d = \frac{A}{12} = \frac{\frac{14+8a}{3}}{12} = \frac{7+4a}{18}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{7+4a}{18} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{21})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{21})) = 3$.

5.1.10. $\mathbb{Q}(\sqrt{33})$*:*

- $a = \frac{1+\sqrt{33}}{2}$
- Numer krzywej: $36.2 - a1$
- $y^2 + ay = x^3 - a - 4$
  $(y + \frac{a}{2})^2 = y^2 + ay + \frac{a^2}{4} = x^3 - a - 4 + \frac{a^2}{4}$
- $B = a + 4 - \frac{a^2}{4} = \frac{1}{2^2} \cdot (16 + 4a - a^2) = \frac{1}{2^2} \cdot (8 + 3a) =$
  $= \frac{1}{2^2} \cdot \frac{1}{3^2} \cdot 3 \cdot (3 \cdot (8 + 3a)) = \frac{1}{2^2} \cdot \frac{1}{3^2} \cdot 3 \cdot (4 + a)^2$
- $d = \frac{A}{12} = \frac{\frac{4+a}{6}}{12} = \frac{4+a}{72}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{4+a}{72} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{33})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{33})) = 3$.

5.1.11. $\mathbb{Q}(\sqrt{37})$*:*

- $a = \frac{1+\sqrt{37}}{2}$
- Numer krzywej: $243.1 - h2$
- $y^2 + y = x^3 - 162a - 412$
  $(y + \frac{1}{2})^2 = y^2 + y + \frac{1}{4} = x^3 - 162a - 412 + \frac{1}{4}$
- $B = 412 + 162a - \frac{1}{4} = \frac{1}{4} \cdot ((4 \cdot 412 - 1) + (4 \cdot 162)a) =$
  $= \frac{1}{4} \cdot \frac{1}{3^2} \cdot 3 \cdot (3 \cdot ((4 \cdot 412 - 1) + (4 \cdot 162)a)) = \frac{1}{2^2} \cdot \frac{1}{3^2} \cdot 3 \cdot (45 + 18a)^2$
- $d = \frac{A}{12} = \frac{\frac{45+18a}{6}}{12} = \frac{5+2a}{8}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{5+2a}{8} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{37})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{37})) = 3$.

5.1.12. $\mathbb{Q}(\sqrt{53})$*:*

- $a = \frac{1+\sqrt{53}}{2}$
- Numer krzywej: $729.1 - c2$
- $y^2 + ay = x^3 + 47a - 199$
  $(y + \frac{a}{2})^2 = y^2 + ay + \frac{a^2}{4} = x^3 + 47a - 199 + \frac{a^2}{4}$
- $B = 199 - 47a - \frac{a^2}{4} = \frac{1}{4} \cdot ((199 \cdot 4 - 13) - (47 \cdot 4 + 1)a) =$
  $= \frac{1}{2^2} \cdot \frac{1}{3^2} \cdot 3 \cdot (3 \cdot ((199 \cdot 4 - 13) - (47 \cdot 4 + 1)a)) = \frac{1}{2^2} \cdot \frac{1}{3^2} \cdot 3 \cdot (36 - 9a)^2$
- $d = \frac{A}{12} = \frac{\frac{36-9a}{6}}{12} = \frac{4-a}{8}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{4-a}{8} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{53})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{53})) = 3$.

5.1.13. $\mathbb{Q}(\sqrt{57})$*:*

- $a = \frac{1+\sqrt{57}}{2}$
- Numer krzywej: $36.3 - a1$
- $y^2 + ay = x^3 + 28010a - 119745$
  $(y + \frac{a}{2})^2 = y^2 + ay + \frac{a^2}{4} = x^3 + 28010a - 119745 + \frac{a^2}{4}$
- $B = 119745 - 28010a - \frac{a^2}{4} = \frac{1}{4} \cdot ((119745 \cdot 4 - 14) - (28010 \cdot 4 + 1)a) =$
  $= \frac{1}{2^2} \cdot \frac{1}{3^2} \cdot 3 \cdot (3 \cdot ((119745 \cdot 4 - 14) - (28010 \cdot 4 + 1)a)) = \frac{1}{2^2} \cdot \frac{1}{3^2} \cdot 3 \cdot (902 - 211a)^2$
- $d = \frac{A}{12} = \frac{\frac{902-211a}{6}}{12} = \frac{902-211a}{72}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{902-211a}{72} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{57})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{57})) = 3$.

Dodatkowe wyniki uzyskane za pomocą kalkulatora [8].

5.1.14. *Krzywa* $y^2 = x^3 - 3 \cdot (12 \cdot 4)^2$. Zgodnie z wyliczeniami Magmy [8] krzywa ta jest trywialna nad ciałami: $\mathbb{Q}(\sqrt{13}), \mathbb{Q}(\sqrt{21}), \mathbb{Q}(\sqrt{37}), \mathbb{Q}(\sqrt{57}), \mathbb{Q}(\sqrt{61}), \mathbb{Q}(\sqrt{73}), \mathbb{Q}(\sqrt{93}), \mathbb{Q}(\sqrt{97}),$ $\mathbb{Q}(\sqrt{107}), \mathbb{Q}(\sqrt{133}), \mathbb{Q}(\sqrt{145}), \mathbb{Q}(\sqrt{157}), \mathbb{Q}(\sqrt{165}), \mathbb{Q}(\sqrt{409})$, co na podstawie Twierdzenia 3.4 oznacza, że równanie $4 = x^3 + y^3$ nie ma rozwiązań w powyższych ciałach liczbowych, stąd trzecia liczba pitagorejska tych ciał jest równa 3.

5.1.15. *Krzywa* $y^2 = x^3 - 3 \cdot (12 \cdot 3)^2$. Zgodnie z wyliczeniami Magmy [8] krzywa ta jest trywialna nad ciałami: $\mathbb{Q}(\sqrt{21}), \mathbb{Q}(\sqrt{37}), \mathbb{Q}(\sqrt{57}), \mathbb{Q}(\sqrt{61}), \mathbb{Q}(\sqrt{73}), \mathbb{Q}(\sqrt{93})$, oraz dodatkowo nad ciałami: $\mathbb{Q}(\sqrt{85}), \mathbb{Q}(\sqrt{109})$, co na podstawie Twierdzenia 3.4 oznacza, że równanie $3 = x^3 + y^3$ nie ma rozwiązań w powyższych ciałach liczbowych, stąd trzecia liczba pitagorejska tych ciał jest równa 3.

Ciała zespolone, czyli takie, że $\mathbb{Q}(\alpha) \subseteq \mathbb{C}$ *oraz* $\mathbb{Q}(\alpha) \nsubseteq \mathbb{R}$.

5.1.16. $\mathbb{Q}(\sqrt{-1})$*:*

- $a = \sqrt{-1}$
- Numer krzywej: $59049.1 - b1$
- $y^2 + y = x^3 - 61$
  $(y + \frac{1}{2})^2 = y^2 + y + \frac{1}{4} = x^3 - 61 + \frac{1}{4}$
- $B = 61 - \frac{1}{4} = \frac{1}{4} \cdot (61 \cdot 4 - 1) = \frac{1}{2^2} \cdot 243 = \frac{1}{2^2} \cdot 9^2 \cdot 3$
- $d = \frac{A}{12} = \frac{\frac{9}{2}}{12} = \frac{3}{8}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{3}{8} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{-1})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{-1})) = 3$.

5.1.17. $\mathbb{Q}(\sqrt{-2})$*:*

- $a = \sqrt{-2}$
- Numer krzywej: $26244.6 - c1$
- $y^2 = x^3 - 6a + 3$
- $B = 6a - 3 = 3 \cdot (2a - 1) = 3 \cdot (1 + a)^2$
- $d = \frac{A}{12} = \frac{1+a}{12}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{1+a}{12} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{-2})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{-2})) = 3$.

5.1.18. $\mathbb{Q}(\sqrt{-3})$*:*

- $a = \frac{1+\sqrt{-3}}{2}$
- Numer krzywej: $1296.1 - CMa1$
- $y^2 = x^3 + 4$
- $B = (-4) = (-3) \cdot \frac{4}{3} = \sqrt{-3}^2 \cdot 3 \cdot (\frac{2}{3})^2$
- $d = \frac{A}{12} = \frac{\frac{2 \cdot \sqrt{-3}}{3}}{12} = \frac{\sqrt{-3}}{18}$

Stąd na podstawie Twierdzenia 3.6 równanie:

$$\frac{\sqrt{-3}}{18} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{-3})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{-3})) = 3$.

5.1.19. $\mathbb{Q}(\sqrt{-7})$*:*

- $a = \frac{1+\sqrt{-7}}{2}$
- Numer krzywej: $11664.3 - c1$
- $y^2 = x^3 - 108$
- $B = 108 = 3 \cdot 6^2$
- $d = \frac{A}{12} = \frac{6}{12} = \frac{1}{2}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{1}{2} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{-7})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{-7})) = 3$.

5.1.20. $\mathbb{Q}(\sqrt{-11})$*:*

- $a = \frac{1+\sqrt{-11}}{2}$
- Numer krzywej: $9801.3 - b2$
- $y^2 + y = x^3 - 817$
  $(y + \frac{1}{2})^2 = y^2 + y + \frac{1}{4} = x^3 - 817 + \frac{1}{4}$
- $B = 817 - \frac{1}{4} = \frac{1}{4} \cdot (817 \cdot 3 - 1) = \frac{1}{4} \cdot 3267 = \frac{1}{4} \cdot 3 \cdot 1089 = 3 \cdot (\frac{33}{2})^2$
- $d = \frac{A}{12} = \frac{\frac{33}{2}}{12} = \frac{11}{8}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{11}{8} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{-11})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{-11})) = 3$.

5.1.21. $\mathbb{Q}(\sqrt{-19})$*:*

- $a = \frac{1+\sqrt{-19}}{2}$
- Numer krzywej: $11664.1 - a1$
- $y^2 = x^3 - 108$
- $B = 108 = 3 \cdot 6^2$
- $d = \frac{A}{12} = \frac{6}{12} = \frac{1}{2}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{1}{2} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}(\sqrt{-19})$, co oznacza, że $P_3(\mathbb{Q}(\sqrt{-19})) = 3$.

Powyższe 6 ciał, to 6 z 9 kwadratowych zespolonych rozszerzeń $\mathbb{Q}$, takich, że pierścień elementów całkowitych tych rozszerzeń ($\mathbb{Z}[\tau_D]$) jest PID-em. Baza danych nie zawiera krzywych pozwalających na zastosowanie Twierdzenia 3.4. Za pomocą Magmy [8] jesteśmy jednak w stanie znaleźć krzywe eliptyczne o żądanych własnościach dla trzech pozostałych przypadków, $\sqrt{D} \in \{\sqrt{-43}, \sqrt{-67}, \sqrt{-163}\}$.

Dodatkowe wyniki uzyskane za pomocą kalkulatora [8].

5.1.22. $\mathbb{Q}(\sqrt{-43})$*:* Krzywa która na podstawie wyliczeń Magmy jest trywialna to $y^2 = x^3 - 3 \cdot (12 \cdot 3)^2$. Na podstawie Twierdzenia 3.4 równanie

$$3 = x^3 + y^3$$

nie ma rozwiązań. Oznacza to, że $P_3(\mathbb{Q}(\sqrt{-43})) = 3$.

5.1.23. $\mathbb{Q}(\sqrt{-67})$*:* Krzywa która na podstawie wyliczeń Magmy jest trywialna to $y^2 = x^3 - 3 \cdot (12 \cdot 4)^2$. Na podstawie Twierdzenia 3.4 równanie

$$4 = x^3 + y^3$$

nie ma rozwiązań. Oznacza to, że $P_3(\mathbb{Q}(\sqrt{-67})) = 3$.

5.1.24. $\mathbb{Q}(\sqrt{-163})$*:* Krzywa która na podstawie wyliczeń Magmy jest trywialna to $y^2 = x^3 - 3 \cdot (12 \cdot 4)^2$. Na podstawie Twierdzenia 3.4 równanie

$$4 = x^3 + y^3$$

nie ma rozwiązań. Oznacza to, że $P_3(\mathbb{Q}(\sqrt{-163})) = 3$.

Wniosek 5.1. *Dla dowolnego zespolonego ciała liczbowego stopnia* 2*, którego pierścień elementów całkowitych jest PID-em, trzecia liczba pitagorejska tego ciała wynosi* 3*.*

Jest tak, gdyż jedyne rozszerzenia o tej własności, to [12]:

$$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{-163}).$$

5.2. **Ciała liczbowe stopnia 3.**

5.2.1. $\mathbb{Q}[X] \big/ (X^3 - X^2 + 1)$*:*

- $a^3 = a^2 - 1$
- Numer krzywej: $19683.1 - f2$
- $y^2 + ay = x^3 - 7a^2$
  $(y + \frac{a}{2})^2 = y^2 + ay + \frac{a^2}{4} = x^3 - 7a^2 + \frac{a^2}{4}$
- $B = 7a^2 - \frac{a^2}{4} = a^2 \cdot (7 - \frac{1}{4}) = a^2 \cdot \frac{27}{4} = 3 \cdot (\frac{3a}{2})^2$
- $d = \frac{A}{12} = \frac{\frac{3a}{2}}{12} = \frac{a}{8}$

Stąd na podstawie Twierdzenia 3.4 równanie:

$$\frac{a}{8} = x^3 + y^3$$

nie ma rozwiązań w $\mathbb{Q}[X] \big/ (X^3 - X^2 + 1)$, co oznacza, że $P_3\left(\mathbb{Q}[X] \big/ (X^3 - X^2 + 1)\right) = 3$.

6. Nieudane próby i ślepe zaułki

6.1. **Czy możemy zmniejszyć liczbę funkcji wymiernych do dwóch?** Chcemy rozstrzygnąć, czy istnieją takie dwie funkcje wymierne $F, G \in \mathbb{Q}(\alpha)(X)$, że zachodzi:

$$X = F(X)^3 + G(X)^3$$

Problem zapisu X jako sumy jak najmniejszej liczby potęg funkcji wymiernych nosi nazwę Problemu Waringa dla wielomianów. Praca [3] zawiera dowód, że nie istnieją funkcje wymierne $F, G \in \mathbb{C}(X)$ spełniające powyższy warunek. Skoro nie istnieją takie funkcje wymierne o zespolonych współczynnikach, to w szczególności nie mogą istnieć również o współczynnikach z mniejszego ciała.

Literatura

[1] S. Chowla, J. Cowles, M. Cowles, *On $x^3 + y^3 = D$*, J. Number Theory, 14 (1982), 369-373.
[2] T. Kowalczyk, P. Miska *Sums of nth powers in henselian rings.*
[3] D. J. Newman, M. Slates, *Waring's problem for the ring of polynomials*, J. Number Theory 11 (1979), 477-487.
[4] H.W. Richmond, *On rational solution of $x^3 + y^3 + z^3 = R$*, Proc. Edinb. Math. Soc. (1930), 92-100.
[5] `https://sites.google.com/site/tpiezas/001b`
[6] `https://www.desmos.com/calculator?lang=pl`
[7] `https://www.lmfdb.org/`
[8] `http://magma.maths.usyd.edu.au`
[9] J.H. Silverman, *The arithmetic of elliptic curves,* Vol. 106, Springer, New York (2009).
[10] J.H Silverman, J.H, Tate, *Rational Points on Elliptic Curves, 2nd edn.*, Springer, Cham (2015).
[11] E.M. Wright, *An easier Waring problem*, J. London Math. Soc. 1 (1934), 267-272.
[12] A. Neugebauer, *Matematyka Olimpijska Algebra i Teoria Liczb.*, Wydawnictwo Szkolne Omega (2018).