Autoreferat

Tomasz Jędrzejak

Instytut Matematyki

Wydział Matematyczno-Fizyczny

Uniwersytet Szczeciński

Szczecin 2018

Spis treści

I. Imię i Nazwisko: Tomasz Jędrzejak

II. Dyplomy i stopnie naukowe:

- **magisterium z matematyki** (Uniwersytet Szczeciński, 31.05.2001), tytuł pracy: *Własności podzielności części algebraicznej wartości w punkcie krytycznym L-funkcji krzywych eliptycznych z mnożeniem zespolonym*, (promotor dr hab. Andrzej Dąbrowski, prof. US).
- **doktorat z matematyki** (Uniwersytet im. Adama Mickiewicza w Poznaniu, 11.04.2008; obrona 19.03), tytuł pracy: *Pewne własności rodzin krzywych typu Fermata i ich jakobianów*, (promotor dr hab. Andrzej Dąbrowski, prof. US).

III. Informacja o dotychczasowym zatrudnieniu:

- 1.10. 2001-30.09.2008, asystent, Instytut Matematyki Uniwersytetu Szczecińskiego;
- od 1.10.2008, adiunkt, Instytut Matematyki Uniwersytetu Szczecińskiego.

IV. Osiągnięcie naukowe w rozumieniu art. 16 ust 2 Ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. nr 65, poz. 595 ze zm.):

Cykl publikacji pod tytułem

Część torsyjna grupy Mordella-Weila jakobianów krzywych hiper- i supereliptycznych

składający się z następujących prac (w porządku chronologicznym):

[A1] T. Jędrzejak, M. Ulas, *Characterization of torsion of the Jacobian of* $y^2 = x^5 + Ax$ *and some applications*, Acta Arith. 144 (2010), no. 2, 183-191.

[A2] T. Jędrzejak, *Characterization of the torsion of the Jacobians of two families of hyperelliptic curves*, Acta Arith. 161 (2013), No.3, 201-218.

[A3] T. Jędrzejak, M. Ulas, *Variations on twists of tuples of hyperelliptic curves and related results*, J. Number Theory 137 (2014), 222-240.

[A4] T. Jędrzejak, *On the torsion of the Jacobians of superelliptic curves* $y^q = x^p + a$, J. Number Theory 145 (2014), 402-425.

[A5] T. Jędrzejak, *On the torsion of the Jacobians of the hyperelliptic curves* $y^2 = x^n + a$ *and* $y^2 = x(x^n + a)$, Acta Arith. 174 (2016) , 99-120.

[A6] T. Jędrzejak, *A note on the torsion of the Jacobians of superelliptic curves* $y^q = x^p + a$, Banach Center Publications 108 (2016), 143-149.

Omówienie przedstawionego cyklu prac:

1 Wprowadzenie

Niech A będzie rozmaitością abelową określoną nad ciałem liczbowym K i niech F będzie ciałem liczbowym zawierającym K. Dzięki znanemu twierdzeniu Mordella-Weila, grupa F-wymiernych punktów $A(F)$ jest skończenie generowana. W szczególności podgrupa torsyjna $A(F)_{tors}$ jest skończona. Klasyczna hipoteza o torsji (Torsion Conjecture) orzeka, że rząd $A(F)_{tors}$ jest graniczony z góry przez stałą zależną tylko od $g := \dim(A)$ i F (słaba wersja) lub tylko od g i $d := [F : \mathbb{Q}]$ (mocna wersja) odpowiednio. Mocną wersję nazywamy się czasem hipotezą o jednostajnej ograniczoności (Uniform Boundedness Conjecture). Zauważmy, że na mocy [9], hipoteza o torsji dla rozmaitości abelowych jest równoważna hipotezie o torsji dla rozmaitości Jacobiego (jakobianów).

Mazur [55] udowodnił tę hipotezę w przypadku $g = 1$ i $d = 1$. Dokładniej, pokazał, że część torsyjna krzywej eliptycznej nad $\mathbb{Q}$ jest izomorficzna z jedną z następujących 15 grup: grupą cykliczną rzędu n, gdzie $n \in \{1, ..., 10, 12\}$, produktem dwóch grup cyklicznych rzędów 2 i $2m$, gdzie $m \in \{1, 2, 3, 4\}$. Następnie Kenku-Momose [44] i Kamienny [43] udowodnili hipotezę o torsji dla $g = 1$ i $d = 2$ (również przedstawili pełną listę 26 podgrup torsyjnych krzywych eliptycznych nad kwadratowymi ciałami liczbowymi). Potem Merel [57] uzyskał dowód (silnej wersji) hipotezy o torsji dla krzywych eliptycznych nad dowolnymi ciałami liczbowymi. Najlepsze znane ograniczenie, otrzymane przez Oesterle i Parenta [60], pokazuje, że potęgi liczb pierwszych pojawiające się w wykładniku grupy $E(F)_{tors}$ (E oznacza krzywą eliptyczną) są ograniczone przez wielkości rosnące wykładniczo względem d (ściślej jeśli $E(F)$ ma punkt rzędu p^n, gdzie p jest liczbą pierwszą, to $p^n \leq 129(5^d - 1)(3d)^6)$.

Przypadek wyżej wymiarowych rozmaitości abelowych pozostaje otwarty. Nie jest znane żadne ciało liczbowe dla którego hipoteza o torsji byłaby spełniona, gdy $g > 1$. Aczkolwiek, można dać jawne ograniczenia na część torsyjną dla pewnych rodzin rozmaitości abelowych. Na przykład z rezultatów Serre'a i Tate'a wynika, że jeżeli A ma wszędzie potencjalnie dobrą redukcję (tzn. istnieje skończone rozszerzenie ciała F nad którym A ma dobrą redukcję w każdym ideale pierwszym), to $\#A(F)_{tors} < 6^{dg \times 4^{4g^2}}$.

Dla jeszcze bardziej specjalnych klas rozmaitości abelowych, mianowicie rozmaitości abelowych z mnożeniem zespolonym (w skrócie CM) lub rozmaitości abelowych typu CM, istnieje kilka interesujących wyników. Przypomnijmy definicje. Mówimy, że rozmaitość abelowa A (wymiaru g) ma *mnożenie zespolone* przez ciało liczbowe K, gdy istnieje injektywny homomorfizm $\iota : K \to End(A) \otimes \mathbb{Q}$, gdzie $[K : \mathbb{Q}] = 2g$ (K jest wówczas koniecznie CM-ciałem, tj. totalnie urojonym rozszerzeniem kwadratowym ciała totalnie rzeczywistego). Ogólniej mówimy, że A jest *typu CM*, jeśli A jest izogeniczna z produktem CM rozmaitości abelowych lub równoważnie, jeśli $End(A) \otimes \mathbb{Q}$ zawiera przemienną algebrę wymiaru $2g$. Zauważmy, że rozmaitości abelowe typu CM mają wszędzie potencjalnie dobrą redukcję. Silverberg [69, 70] udowodniła silną wersję hipotezy o torsji dla rozmaitości abelowych typu CM. Dokładniej, pokazała m.in., że jeśli A posiada punkt F-wymierny rzędu n, to

$$\varphi(n) \leq 2^{(g-1)\omega(n)+2g+\delta(n)} 3^g g! d,$$

gdzie φ oznacza funkcję Eulera, $\omega(n)$ - liczbę dzielników pierwszych n i $\delta(n) = 1$ albo 0 w zależności od tego, czy 8 dzieli n, czy nie. Pod pewnym warunkiem Aoki [1] dał lepsze ograniczenie na $\varphi(n)$. Mianowicie, $\varphi(n) \leq 2g!d$, a jeśli A jest absolutnie prosta, to $\varphi(n) \leq 2^g d$. Gdy dodatkowo CM ciało K jest abelowe, to $\varphi(n)$ dzieli $2gd$.

Dla pewnych specjalnych rodzin krzywych eliptycznych jest możliwe podanie pełnej charakteryzacji ich podgrup torsyjnych, tzn. wypisanie wszystkich punktów torsyjnych i podanie rozkładu tych grup na produkt grup cyklicznych. Na przykład rozważmy rodziny

krzywych eliptycznych (nad $\mathbb{Q}$)

$$E^a : y^2 = x^3 + a,$$
$$E_a : y^2 = x^3 + ax.$$

Te rodziny zajmują szczególne miejsce. Ich j-niezmiennik wynosi 0 i 1728 odpowiednio. Obie rodziny mają mnożenie zespolone: E^a przez $\mathbb{Q}\left(i\sqrt{3}\right)$, a E_a przez $\mathbb{Q}(i)$. Następujące wyniki są dobrze znane ([45, Theorems 5.2 i 5.3, s. 134]).

$$E^a(\mathbb{Q})_{tors} \cong \begin{cases} \{0\} & \textit{jeśli } a \textit{ nie jest kwadratem, ani sześcianem i } a \neq -432, \\ \mathbb{Z}/2\mathbb{Z} & \textit{jeśli } a \textit{ nie jest kwadratem, ale jest sześcianem} \\ \mathbb{Z}/3\mathbb{Z} & \textit{jeśli } a \textit{ jest kwadratem, ale nie jest sześcianem lub } a = -432, \\ \mathbb{Z}/6\mathbb{Z} & \textit{jeśli } a \textit{ jest kwadratem i jest sześcianem.} \end{cases} \tag{1}$$

$$E_a(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \textit{jeśli } a \neq 4 \textit{ i } -a \textit{ nie jest kwadratem,} \\ (\mathbb{Z}/2\mathbb{Z})^2 & \textit{jeśli } -a \textit{ jest kwadratem,} \\ \mathbb{Z}/4\mathbb{Z} & \textit{jeśli } a = 4. \end{cases} \tag{2}$$

(bez straty ogólności zakładamy, że a jest niezerową liczbą całkowitą wolną od szóstych lub czwartych potęg odpowiednio).

Zauważmy, że $E_a(\mathbb{Q})_{tors}$ jest 2-grupą dla dowolnego a. Niech $E(\mathbb{Q})[2]$ oznacza jądro endomorfizmu mnożenia przez 2 w $E(\mathbb{Q})$. Łatwo widać, że $E_a(\mathbb{Q})[2] = \{\infty\} \cup \{(x,0) \in \mathbb{Q} \times \mathbb{Q} : x^3 + ax = 0\}$. Zatem wobec (2), dostajemy

$$E_a(\mathbb{Q})_{tors} = E_a(\mathbb{Q})[2] \text{ dla } a \neq 4 \tag{3}$$

(mamy też $E_4(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$). Z drugiej strony, dla $a \neq -432 = -2^4 3^3$ możemy przeformułować (1) następująco

$$E^a(\mathbb{Q})_{tors} \cong \begin{cases} \{0\} & \textit{jeśli } a \textit{ nie jest kwadratem, ani sześcianem,} \\ \mathbb{Z}/2\mathbb{Z} & \textit{jeśli } a \textit{ nie jest kwadratem, ale jest sześcianem,} \\ \mathbb{Z}/3\mathbb{Z} & \textit{jeśli } a \textit{ jest kwadratem, ale nie jest sześcianem,} \\ \mathbb{Z}/6\mathbb{Z} & \textit{jeśli } a \textit{ jest kwadratem i jest sześcianem.} \end{cases} \tag{4}$$

W prezentowanej serii artykułów naszym celem jest charakteryzacja $\mathbb{Q}$-podgrupy torsyjnej grupy Mordella-Weila jakobianów krzywych hiper- i supereliptycznych, które są w pewnym sensie naturalnym uogólnieniem krzywych eliptycznych o j-niezmiennikach 0 i 1728, lub są w bliskiej relacji z nimi. Jest to zagadnienie interesujące samo w sobie, ale także można oczekiwać analogii ze wzorami (1), (2), (3), (4).

Taka charakteryzacja może mieć też ciekawe zastosowania do rang wspomnianych grup Mordella-Weila. Na przykład,w przypadku skręconych krzywych Fermata $F_m(p) : x^p + y^p = m$, jednostajna ograniczoność $\#Jac(F_m(p))(\mathbb{Q})_{tors}$ przy ustalonej nieparzystej liczbie pierwszej p została użyta do otrzymania pewnych informacji o zachowaniu rang w nieskończonej rodzinie $Jac(F_m(p))(\mathbb{Q})$ (patrz [B3] lub rozdział 4.3 w tym autoreferacie). Informacja o torsji jakobianów ilorazów krzywych Fermata (mianowicie krzywych $y^p = x^m(x+a)$) daje nam pewną wiedzę o rangach parach p-skręceń jakobianów tych krzywych (zobacz [A3] lub rozdział 3.1). Podobnie charakteryzacja $J_{4,a}(\mathbb{Q})_{tors}$ (gdzie $J_{4,a}$ jest jakobianem krzywej $y^2 = x(x^4 + a)$) ma interesujące zastosowanie do rang czwórek skręceń ósmego stopnia (octic twist) tych krzywych (zobacz [A1] lub rozdział 2.1).

2 Krzywe hipereliptyczne

Na początku przedstawimy niezbędne oznaczenia i fakty dotyczące jakobianów krzywych algebraicznych (ze szczególnym uwzględnieniem krzywych hipereliptycznych).

Dla gładkiej rzutowej krzywej C określonej nad ciałem K, niech $Div(C)$ oznacza jej grupę dywizorów, tj. wolną grupę abelową generowaną przez punkty C. Z definicji dywizor $D \in Div(C)$ jest *K-wymierny*, gdy jest niezmienniczy względem działania absolutnej grupy Galois $Gal\left(\overline{K}/K\right)$. Zauważmy, że jeśli $D = n_1P_1 + ... + n_rP_r$, gdzie $n_1, ..., n_r$ są niezerowymi liczbami całkowitymi, to fakt, że D jest K-wymierny nie oznacza, że $P_1, ..., P_r \in C(K)$. Do tego wystarczy, by $Gal\left(\overline{K}/K\right)$ permutowała punkty P_i w odpowiedni sposób. Liczbę $n_1 + ... + n_r$ nazywamy *stopniem* dywizora D. Zauważmy, że jeśli h jest elementem ciała funkcji wymiernych na C, to dywizor $div(h) := \sum_{P \in C} \mathrm{ord}_P(h) P$ (zwany *głównym*) ma stopień 0. Niech J_C oznacza rozmaitość Jacobiego (jakobian) krzywej C. Jako grupa J_C jest grupą ilorazową dywizorów stopnia zero przez dywizory główne. Odpowiadającą temu relację równoważności oznaczamy przez $\sim$, a przez $[D]$ oznaczamy klasę równoważności dywizora D. Niech $J_C(K)_{tors}$ oznacza podgrupę złożoną z K-wymiernych torsyjnych elementów w $J_C(K)$, a $J_C(K)[m]$ - jądro endomorfizmu mnożenia przez m w $J_C(K)$.

Przez *krzywą hipereliptyczną* genusu g określoną nad K ($charK \neq 2$) rozumiemy absolutnie nierozkładalną nieosobliwą krzywą C zadaną równaniem (afinicznym) postaci $y^2 = f(x)$, gdzie $f \in K[x]$ jest unormowany i ma stopień $2g+1$ lub $2g+2$. W pierwszym przypadku C nazywamy *krzywą hipereliptyczną w modelu urojonym*, a w drugim - *krzywą hipereliptyczną w modelu rzeczywistym*. W modelu urojonym istnieje dokładnie jeden punkt w nieskończoności, powiedzmy ∞, a w modelu rzeczywistym mamy dwa punkty w nieskończoności ∞^+ oraz ∞^-. Niech S oznacza zbiór punktów w nieskończoności na C. Wówczas elementy zbioru $C\left(\overline{K}\right) := \left\{(x,y) \in \overline{K}^2 : y^2 = f(x)\right\} \cup S$ nazywamy *$\overline{K}$-wymiernymi punktami* C (jeśli nie należą do S, mówimy, że są *skończone* lub *afiniczne*). Podobnie definiujemy $C(L)$ dla dowolnego ciała $K \subset L \subset \overline{K}$. Zawsze jest możliwe przekształcenie modelu urojonego na rzeczywisty, ale w drugą stronę potrzebujemy, aby C posiadała skończony K-wymierny punkt. Dla punktu $P = (x,y) \in C\left(\overline{K}\right)$ *hipereliptyczna inwolucja* dana jest przez $\tau(P) := (x, -y)$. Mamy $\tau(\infty^{\pm}) = \infty^{\mp}$ oraz $\tau(\infty) = \infty$.

Następujące dwa lematy dotyczą reprezentacji dywizorów w J_C.

Lemat 2.1. *Dowolny $\overline{K}$-wymierny dywizor stopnia 0 na krzwej hipereliptycznej C w modelu urojonym nad K genusu g jest równoważny z jedynym zredukowanym dywizorem, tzn. dywizorem D postaci*

$$D = \sum_{i=1}^{d} P_i - d\infty,$$

gdzie $P_i \in C\left(\overline{K}\right) \setminus S$, $P_i \neq \tau(P_j)$ dla $i \neq j$ oraz $0 \leq d \leq g$.

Dowód. Zobacz [56, Theorem 47]. □

Lemat 2.2. *Dowolny $\overline{K}$-wymierny dywizor stopnia 0 na krzwej hipereliptycznej C w modelu rzeczywistym nad K genusu g jest równoważny z jedynym zredukowanym dywizorem, tzn. dywizorem D postaci*

$$D = \sum_{i=1}^{d_1} P_i - d_1\infty^- + d_2\left(\infty^+ - \infty^-\right),$$

gdzie $P_i \in C\left(\overline{K}\right) \setminus S$, $P_i \neq \tau(P_j)$ dla $i \neq j$, $0 \leq d_1, d_2$ oraz $d_1 + d_2 \leq g$. W szczególności dywizory $k(\infty^+ - \infty^-)$ dla $k = 1, ..., g$ nie są główne i są parami nierównoważne.

Dowód. Pierwsze zdanie wynika z [61]. Dla dowodu drugiego położymy $d_1 = 0$ i $d_2 = k$. □

Następny lemat pomaga wyznaczyć grupę $J_C(K)[2]$.

Lemat 2.3. *Niech $f(x) = f_1(x)...f_s(x)$, gdzie $f_i \in K[x]$ są parami różnymi unormowanymi wielomiananmi stopni t_i nierozkładalnymi nad K oraz $t := t_1 + ... + t_s$. Niech r oznacza wymiar $J_C(K)[2]$ nad $\mathbb{F}_2$, tj.*

$$J_C(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^r \text{ , gdzie } C : y^2 = f(x).$$

Jeśli K jest skończonym ciałem nieparzystej charakterystyki, to

$$r = \begin{cases} s-2 & \text{jeśli } t \text{ jest parzyste i pewne } t_i \text{ jest nieparzyste,} \\ s-1 & \text{jeśli } t \text{ jest nieparzyste lub } s = 1 \text{ oraz } t \equiv 2 \pmod 4, \\ s & \text{jeśli } s > 1 \text{ i każdy } t_i \text{ jest parzysty lub } s = 1 \text{ i } t \equiv 0 \pmod 4. \end{cases}$$

Jeśli K jest rozszerzeniem $\mathbb{Q}$ oraz t jest nieparzyste lub t i g są parzyste, to

$$r = \begin{cases} s-2 & \text{jeśli } t \text{ jest parzyste i pewne } t_i \text{ jest nieparzyste,} \\ s-1 & \text{jeśli } t \text{ jest nieparzyste lub każdy } t_i \text{ jest parzysty.} \end{cases}$$

Dowód. Pierwszy przypadek wynika z [16, Theorem 1.4], a drugi z [62, Lemmata 6.1 i 12.9]. □

Teraz rozważmy krzywe algebraiczne (określone nad $\mathbb{Q}$)

$$C^{n,a} : y^2 = x^n + a,$$
$$C_{n,a} : y^2 = x(x^n + a),$$

gdzie $n \geq 3$ (odpowiednio $n \geq 2$) jest liczbą naturalną i a jest niezerową liczbą wymierną. Te krzywe i ich jakobiany ($J^{n,a}$, $J_{n,a}$ odpowiednio) są naturalnym uogólnieniem wyżej wymienionych krzywych eliptycznych E^a, E_a.

W tym rozdziale naszym celem jest charakteryzacja części torsyjnych $J^{n,a}(\mathbb{Q})_{tors}$ i $J_{n,a}(\mathbb{Q})_{tors}$ grup Mordella-Weila $J^{n,a}(\mathbb{Q})$ i $J_{n,a}(\mathbb{Q})$. Jest to ciekawy problem sam w sobie, ale również ciekawe są ewentualne analogie między $E^a(\mathbb{Q})_{tors}$ a $J^{n,a}(\mathbb{Q})_{tors}$ i między $E_a(\mathbb{Q})_{tors}$ a $J_{n,a}(\mathbb{Q})_{tors}$.

Krzywe $C_{n,a} : y^2 = x(x^n + a)$ i $C^{n,a} : y^2 = x^n + a$ są hipereliptyczne genusu $\left[\frac{n}{2}\right]$ i $\left[\frac{n-1}{2}\right]$ odpowiednio, gdzie $[x]$ oznacza część całkowitą x. Bez straty ogólności możemy założyć, że a jest liczbą całkowitą wolną od $2n$-tych potęg (w obu rodzinach krzywych). Nietrudno sprawdzić, że $|\mathrm{disc}(x(x^n + a))| = n^n a^{n+1}$ i $|\mathrm{disc}(x^n + a)| = n^n a^{n-1}$. Zatem krzywe $C_{n,a}$ i $C^{n,a}$ mają dobrą redukcję w liczbach pierwszych p nie dzielących $2na$. W konsekwencji jakobiany $J_{n,a}$ i $J^{n,a}$ także mają dobrą redukcję w tych liczbach pierwszych. Krzywa $C_{n,a}$ ma jeden punkt w nieskończoności, gdy n jest parzyste i dwa takie punkty, gdy n jest nieparzyste. Odwrotnie, $C^{n,a}$ ma dwa punkty w nieskończoności, gdy n jest parzyste i ma jeden taki punkt, gdy n jest nieparzyste. Wszystkie punkty w nieskończoności są określone nad odpowiednimi ciałami prostymi (tj. $\mathbb{Q}$ lub $\mathbb{F}_p$ po redukcji).

Aby wyznaczyć $J_{n,a}(\mathbb{Q})_{tors}$ i $J^{n,a}(\mathbb{Q})_{tors}$ pomocne jest rozważyć $J_{n,a}(\mathbb{F}_p)$ i $J^{n,a}(\mathbb{F}_p)$ odpowiednio dla liczb pierwszych $p \nmid 2na$. Tak jest ponieważ homomorfizm redukcji modulo p indukuje zanurzenia (por. [37, Theorem C.1.4, s. 263])

$$J_{n,a}(\mathbb{Q})_{tors} \hookrightarrow J_{n,a}(\mathbb{F}_p), \tag{5}$$
$$J^{n,a}(\mathbb{Q})_{tors} \hookrightarrow J^{n,a}(\mathbb{F}_p), \tag{6}$$

i stąd

$$\#J_{n,a}(\mathbb{Q})_{tors} \,|\, \#J_{n,a}(\mathbb{F}_p), \tag{7}$$
$$\#J^{n,a}(\mathbb{Q})_{tors} \,|\, \#J^{n,a}(\mathbb{F}_p). \tag{8}$$

Następujący lemat dotyczy liczby elementów w J_C nad ciałami skończonymi.

Lemat 2.4. *Niech C będzie gładką rzutową krzywą genusu $g \geq 1$ określoną nad ciałem skończonym F_q. Połóżmy $N_k := \#C\left(\mathbb{F}_{q^k}\right)$ dla $k \in \mathbb{N}$. Wówczas $\#J_C\left(\mathbb{F}_q\right)$ jest całkowicie wyznaczone przez $N_1, N_2, ..., N_g$. Ponadto,*

1. *jeśli $g = 2$, to $\#J_C\left(\mathbb{F}_q\right) = \frac{N_1^2+N_2}{2} - q$,*
2. *jeśli $g = 3$, to $\#J_C\left(\mathbb{F}_q\right) = \frac{N_1^3}{6} + \frac{N_1 N_2}{2} + \frac{N_3}{3} - qN_1$,*
3. *jeśli $N_k = 1 + q^k$ dla $k = 1, 2, ..., g$, to $\#J_C\left(\mathbb{F}_q\right) = 1 + q^g$.*

Dowód. [A2, p. 203]. □

Wobec lematu 2.4 potrzebujemy obliczyć $\#C_{n,a}\left(\mathbb{F}_{p^k}\right)$ dla $k = 1, ..., \left[\frac{n}{2}\right]$ i $\#C^{n,a}\left(\mathbb{F}_{p^k}\right)$ dla $k = 1, ..., \left[\frac{n-1}{2}\right]$. W tym celu użyjemy sum Gaussa, Jacobiego i Jacobsthala. Podamy teraz ich definicje i podstawowe własności (kładziemy poniżej $q = p^k$).

Definicja 2.5. *Niech χ oznacza charakter ciała skończonego $\mathbb{F}_q$ i niech $\beta \in \mathbb{F}_q$. Suma Gaussa $G_k(\beta, \chi)$ nad $\mathbb{F}_q$ jest zdefiniowana przez*

$$G_k(\beta, \chi) := \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha)\, e^{2\pi i \operatorname{Tr}(\alpha\beta)/p},$$

gdzie Tr *oznacza ślad z $\mathbb{F}_q$ do $\mathbb{F}_p$ (kładziemy $\chi(0) = 0$, gdy χ jest nietrywialny i $\chi(0) = 1$, gdy χ jest trywialny). Będziemy pisać krótko $G_k(\chi)$ zamiast $G_k(1, \chi)$.*

Definicja 2.6. *Niech χ i ψ oznaczają charaktery ciała $\mathbb{F}_q$ rzędów n i m odpowiednio. Sumę Jacobiego $J_k(\chi, \psi)$ nad $\mathbb{F}_q$ definiujemy przez*

$$J_k(\chi, \psi) := \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha)\, \psi(1 - \alpha).$$

Rząd $J_k(\chi, \psi)$ to z definicji $NWW(n, m)$.

Definicja 2.7. *Niech $e \in \mathbb{N}$ i $a \in \mathbb{F}_q$. Niech $\left(\frac{\cdot}{q}\right)$ oznacza kwadratowy charakter ciała $\mathbb{F}_q$. Sumy Jacobsthala $\varphi_{e,k}$, $\psi_{e,k}$ rzędu e nad $\mathbb{F}_q$ definiujemy przez*

$$\varphi_{e,k}(a) = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right)\left(\frac{x^e + a}{q}\right),$$

$$\psi_{e,k}(a) = \sum_{x \in \mathbb{F}_q} \left(\frac{x^e + a}{q}\right).$$

Dla $a \in \mathbb{Z}$ określamy $\varphi_{e,k}(a) := \varphi_{e,k}(a \bmod p)$ i $\psi_{e,k}(a) := \psi_{e,k}(a \bmod p)$.

Lemat 2.8. *Niech χ i ψ oznaczają charaktery ciała $\mathbb{F}_{p^k}$. Wtedy*

1) Suma Jacobiego rzędu m jest liczbą algebraiczną całkowitą ciała cyklotomicznego $\mathbb{Q}\left(e^{2\pi i/m}\right)$.

2) Jeśli χ i ψ są trywialne, to $J_k(\chi, \psi) = p^k$.

3) Jeśli dokładnie jeden z χ i ψ jest trywialny, to $J_k(\chi, \psi) = 0$.

4) Jeśli χ jest nietrywialny, to $J_k(\chi, \bar{\chi}) = -\chi(-1)$.

5) Jeśli χ, ψ i $\chi\psi$ są nietrywialne, to

$$J_k(\chi, \psi) = \psi(-1)\, J_k\left(\bar{\chi}\bar{\psi}, \psi\right) = \chi(-1)\, J_k\left(\bar{\chi}\bar{\psi}, \chi\right),$$

i $|J_k(\chi, \psi)| = \sqrt{p^k}$.

6) Jeśli $\chi\psi$ jest nietrywialny, to

$$J_k(\chi, \psi) = \frac{G_k(\chi)\, G_k(\psi)}{G_k(\chi\psi)}.$$

Dowód. [3, Theorems 2.1.1, 2.1.3, 2.1.5]. □

Lemat 2.9. *Niech $\beta_1, ..., \beta_l$ będą liczbami naturalnymi. Niech $\alpha_1, ..., \alpha_l, \alpha \in \mathbb{F}_q^*$. Niech χ_i będzie charakterem ciała $\mathbb{F}_q$ rzędu $d_i := \mathrm{NWD}(\beta_i, q-1)$ $(i = 1, ..., l)$. Wówczas liczba rozwiązań równania diagonalnego $\alpha_1 x_1^{\beta_1} + ... + \alpha_l x_l^{\beta_l} = \alpha$ w $\mathbb{F}_q$ wynosi*

$$q^{l-1} + \sum_{j_1=1}^{d_1-1} ... \sum_{j_l=1}^{d_l-1} \chi_1^{j_1}\left(\alpha\alpha_1^{-1}\right) ... \chi_l^{j_l}\left(\alpha\alpha_l^{-1}\right) J_k\left(\chi_1^{j_1}, ..., \chi_l^{j_l}\right).$$

Dowód. [3, Theorem 10.4.2]. □

Lemat 2.10. *1) Jeśli* $\mathrm{NWD}(e, q-1) = e_1$, *to* $\varphi_{e,k} = \varphi_{e_1,k}$.

2) Jeśli $e \mid (q-1)$, *ale* $2e \nmid (q-1)$, *to* $\varphi_{e,k} = 0$.

3) $\varphi_{e,k}(ab^e) = \left(\frac{b}{q}\right)^{e+1} \varphi_{e,k}(a)$, *dla* $b \in \mathbb{F}_q^\times$.

4) $\#C_{n,a}(\mathbb{F}_q) = q + \varphi_{n,k}(a) + \begin{cases} 1 & gdy\ 2 \mid n \\ 2 & gdy\ 2 \nmid n \end{cases}$.

5) $\#C^{n,a}(\mathbb{F}_q) = q + \psi_{n,k}(a) + \begin{cases} 2 & gdy\ 2 \mid n \\ 1 & gdy\ 2 \nmid n \end{cases}$.

6) $\psi_{2e,k} = \psi_{e,k} + \varphi_{e,k}$.

Dowód. Należy uogólnić dowód z [3, pp. 184-188] dla $\mathbb{F}_p$ na dowolne ciała skończone. Zauważmy, że nasza definicja $\psi_{e,k}$ różni się od tej z [3] wyrazem $\left(\frac{a}{q}\right)$ (ale zgadza się z [2]). □

Aby przenieść informacje o liczbie punktów w jakobianach nad ciałami skończonymi na ciało liczb wymiernych (co jest naszym celem) często używamy Twierdzenia Dirichleta o liczbach pierwszych w postępach arytmetycznych i jego uogólnienia: Twierdzenia Czebotariewa o gęstości (Chebotarev Density Theorem) w następującej wersji.

Lemat 2.11. *Niech h będzie unormowanym wielomianem o współczynnikach całkowitych. Załóżmy, że wyróżnik h nie znika. Niech K będzie ciałem rozkładu h nad $\mathbb{Q}$. Dla liczby pierwszej l niech $\sigma_l \in Gal(K/\mathbb{Q})$ oznacza automorfizm Frobeniusa dla l (tzn. $\sigma_l(x) \equiv x^l \pmod{\mathfrak{l}}$, gdzie $\mathfrak{l}$ jest ideałem pierwszym leżącym nad l w O_K). Wówczas istnieje nieskończenie wiele liczb pierwszych l takich, że wielomian h ma taki sam typ rozkładu nad $\mathbb{F}_l$ jaki σ_l, widziana jako element grupy permutacji pierwiastków wielomianu h, ma typ rozkładu na rozłączne cykle.*

Dowód. Zobacz na przykład [73, p. 35-36]. □

2.1 Artykuł [A1]

W tym artykule rozważamy krzywe $C_{4,a} : y^2 = x\left(x^4 + a\right)$ i ich jakobiany $J_{4,a}$. Podamy pełną charakteryzację $J_{4,a}(\mathbb{Q})_{tors}$.

Na początek, używając lematu 2.3, możemy określić $J_{4,a}(\mathbb{Q})[2]$.

Lemat 2.12. *Mamy*

$$J_{4,a}(\mathbb{Q})[2] \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{jeśli } \pm a \text{ nie jest kwadratem lub } a \text{ jest kwadratem i} \\ & 2\sqrt{a} \text{ nie jest kwadratem (przypadek 1),} \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{jeśli } a \text{ jest kwadratem i } 2\sqrt{a} \text{ jest kwadratem lub} \\ & -a \text{ jest kwadratem, ale } \sqrt{-a} \text{ nie jest kwadratem,} \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{jeśli } -a \text{ jest czwartą potęgą.} \end{cases}$$

Dokładniej, w przypadku 1 mamy

$$J_{4,a}(\mathbb{Q})[2] = \{0, [(0,0) - \infty]\},$$

jeśli $a = \frac{b^4}{4}$ *(tu i poniżej b jest bezkwadratową liczbą naturalną), to*

$$J_{4,a}(\mathbb{Q})[2] = \{0, [(0,0)-\infty], [\left(\frac{-b+ib}{2}, 0\right)+\left(\frac{-b-ib}{2}, 0\right)-2\infty], [\left(\frac{b+ib}{2}, 0\right)+\left(\frac{b-ib}{2}, 0\right)-2\infty]\}.$$

jeśli $a = -b^2$, *to*

$$J_{4,a}(\mathbb{Q})[2] = \left\{0, [(0,0) - \infty], [\left(\sqrt{b}, 0\right) + \left(-\sqrt{b}, 0\right) - 2\infty], [\left(i\sqrt{b}, 0\right) + \left(-i\sqrt{b}, 0\right) - 2\infty]\right\},$$

jeśli $a = -b^4$, *to*

$$J_{4,a}\left(\mathbb{Q}\right)[2] = \left\{ \begin{array}{l} 0, [(0,0) - \infty], [(b,0) - \infty], \\ [(-b,0) - \infty], [(0,0) + (b,0) - 2\infty], \\ [(0,0) + (-b,0) - 2\infty], [(b,0) + (-b,0) - 2\infty], \\ [(ib,0) + (-ib,0) - 2\infty] \end{array} \right\}.$$

Na mocy lematu 2.4, dostajemy

$$\#J_{4,a}(\mathbb{F}_p) = \frac{1}{2}(\#C_{4,a}(\mathbb{F}_p)^2 + \#C_{4,a}(\mathbb{F}_{p^2})) - p, \tag{9}$$

a zatem wystarczy obliczyć $\#C_{4,a}\left(\mathbb{F}_{p^k}\right)$ dla $k = 1, 2$. Łatwo pokazać, że

$$\#C_{4,a}(\mathbb{F}_p) = 1 + p \tag{10}$$

dla $p \not\equiv 1 (\mathrm{mod}\, 8)$. By obliczyć $\#C_{4,a}(\mathbb{F}_{p^2})$ oraz $\#C_{4,a}(\mathbb{F}_p)$ dla $p \equiv 1 (\mathrm{mod}\, 8)$ użyjemy sum Jacobsthala $\varphi_{4,2}$ i $\varphi_{4,1}$ odpowiednio. Wtedy możemy udowodnić, że $J_{4,a}(\mathbb{Q})_{tors}$ jest 2-grupą i nie posiada elementu rzędu 4 (zobacz lematy 2.7 i 2.8 w [A1]). W konsekwencji otrzymujemy główne twierdzenie.

Twierdzenie 2.13. *Dla dowolnego niezerowego wymiernego a mamy* $J_{4,a}(\mathbb{Q})_{tors} = J_{4,a}(\mathbb{Q})\,[2]$.

Jako wniosek dostajemy interesujące zastosowanie do rang. Precyzyjniej, mamy

Twierdzenie 2.14. *Niech* $a, b, c, d \in \mathbb{Z} \setminus \{0\}$ *będą parami różne. Rozważmy krzywe hipereliptyczne*

$$C_1 : y_1^2 = x_1^5 + ax_1, \quad C_2 : y_2^2 = x_2^5 + bx_2, \quad C_3 : y_3^2 = x_3^5 + cx_3, \quad C_4 : y_4^2 = x_4^5 + dx_4.$$

Wówczas istnieje wielomian $D \in \mathbb{Z}[u]$ *taki, że jakobiany skręceń ósmego stopnia krzywych* C_i *przez D mają dodatnią rangę dla* $i = 1, 2, 3, 4$.

Odnotujmy, że skręcenie ósmego stopnia krzywej $y^2 = x^5 + ax$ przez d ma postać $y^2 = x^5 + adx$. Powyższe twierdzenie daje częściową odpowiedź (że $N > 3$) na następujące

Pytanie 2.15. *Niech* $C_i : y^2 = x^5 + a_i x$, *gdzie* $a_i \in \mathbb{Z} \setminus \{0\}$ *dla* $i = 1, 2, \ldots, n$ *oraz* $C_i \neq C_j$ *dla* $i \neq j$. *Jaka jest największa liczba N, dla której istnieje wielomian* $D \in \mathbb{Z}[u]$ *taki, że jakobian skręcenia ósmego stopnia krzywej* C_i *przez D ma dodatnią rangę dla* $i = 1, 2, \ldots, N$?

2.2 Artykuł [A2]

W tym artykule rozważamy dwie rodziny krzywych hipereliptycznych $C_{6,a} : y^2 = x\left(x^6 + a\right)$ (jednoparametrowa, $a \in \mathbb{Q} \setminus \{0\}$) i $C^{p,a} : y^2 = x^p + a$ (dwuparametrowa, $a \in \mathbb{Q} \setminus \{0\}$, p jest nieparzystą liczbą pierwszą) i ich jakobiany $J_{6,a}, J^{p,a}$ odpowiednio.

Najpierw damy prawie kompletną charakteryzację grupy $J_{6,a}(\mathbb{Q})_{tors}$. Na mocy lematu 2.3, możemy wyznaczyć $J_{6,a}(\mathbb{Q})[2]$.

Lemat 2.16. *Mamy*

$$J_{6,a}\left(\mathbb{Q}\right)[2] \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{jeśli } a \text{ nie jest sześcianem i } -a \text{ nie jest kwadratem (przypadek 1),} \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{jeśli } (a \text{ jest sześcianem, ale } -a \text{ nie jest kwadratem ani } a \text{ nie jest } 27 \text{ razy szósta potęga) lub } (-a \text{ jest kwadratem, ale } a \text{ nie jest sześcianem),} \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{jeśli } a \text{ jest } 27 \text{ razy szósta potęga,} \\ (\mathbb{Z}/2\mathbb{Z})^4 & \text{jeśli } -a \text{ jest szóstą potęgą.} \end{cases}$$

Dokładniej, w przypadku 1 mamy

$$J_{6,a}\left(\mathbb{Q}\right)[2] =< [(0,0) - \infty] > .$$

Niech b oznacza bezkwadratową liczbę naturalną.
Jeśli $a = b^3$ $(b \neq 3)$, to

$$J_{6,a}\left(\mathbb{Q}\right)[2] =< [(0,0) - \infty], [\left(\sqrt{-b}, 0\right) + \left(-\sqrt{-b}, 0\right) - 2\infty] >,$$

jeśli $a = -b^2$, to

$$J_{6,a}\left(\mathbb{Q}\right)[2] =< [(0,0) - \infty],$$
$$[\left(\sqrt[3]{b}, 0\right) + \left(\frac{-1 + i\sqrt{3}}{2}\sqrt[3]{b}, 0\right) + \left(\frac{-1 - i\sqrt{3}}{2}\sqrt[3]{b}, 0\right) - 3\infty] >,$$

jeśli $a = 27b^6$, to

$$J_{6,a}\left(\mathbb{Q}\right)[2] =< [(0,0) - \infty], [\left(ib\sqrt{3}, 0\right) + \left(-ib\sqrt{3}, 0\right) - 2\infty],$$
$$\left[\left(\frac{3b + ib\sqrt{3}}{2}\right) + \left(\frac{3b - ib\sqrt{3}}{2}\right) - 2\infty\right] >,$$

jeśli $a = -b^6$, to

$$J_{6,a}\left(\mathbb{Q}\right)[2] =< [(0,0) - \infty], [(b,0) - \infty], [(-b,0) - \infty],$$
$$\left[\left(\frac{b - ib\sqrt{3}}{2}, 0\right) + \left(\frac{b + ib\sqrt{3}}{2}, 0\right) - 2\infty\right] > .$$

Dzięki lematowi 2.4 otrzymujemy

$$\#J_{6,a}\left(\mathbb{F}_p\right) = \frac{\#C_{6,a}\left(\mathbb{F}_p\right)^3}{6} + \frac{\#C_{6,a}\left(\mathbb{F}_p\right)\#C_{6,a}\left(\mathbb{F}_{p^2}\right)}{2} + \frac{\#C_{6,a}\left(\mathbb{F}_{p^3}\right)}{3} - p\#C_{6,a}\left(\mathbb{F}_p\right). \quad (11)$$

Zatem wystarczy obliczyć $\#C_{6,a}\left(\mathbb{F}_{p^k}\right)$ dla $k = 1, 2, 3$. Łatwo wykazać, że

$$\#C_{6,a}(\mathbb{F}_{p^l}) = 1 + p^l \quad (12)$$

dla $p \equiv 3 (\mathrm{mod}\, 4)$ i dla każdego nieparzystego l. Aby obliczyć $\#C_{6,a}\left(\mathbb{F}_{p^2}\right)$, a także $\#C_{6,a}\left(\mathbb{F}_p\right)$, $\#C_{6,a}\left(\mathbb{F}_{p^3}\right)$ dla $p \equiv 1 (\mathrm{mod}\, 4)$ użyjemy odpowiednich sum Jacobsthala. Następnie (używając chińskiego twierdzenia o resztach i wspomnianego twierdzenia Dirichleta) możemy udowodnić następujące.

Twierdzenie 2.17. *Dla każdego $a \in \mathbb{Q} \setminus \{0\}$ grupa $J_{6,a}(\mathbb{Q})_{tors}$ jest 2-grupą rzędu ≤ 64. Ponadto jeśli a nie jest sześcianem, to $\#J_{6,a}(\mathbb{Q})_{tors} \leq 4$.*

Stąd $J_{6,a}(\mathbb{Q})_{tors} = J_{6,a}(\mathbb{Q})[2]$ wtedy i tylko wtedy, gdy $J_{6,a}(\mathbb{Q})_{tors}$ nie posiada elementu rzędu 4. Przypomnijmy, że jeśli liczba pierwsza $p \nmid 6a$, to $J_{6,a}(\mathbb{Q})_{tors}$ jest izomorficzna z podgrupą w $J_{6,a}(\mathbb{F}_p)$. Oczywiście jeżeli $\mathrm{ord}_2(\#J_{6,a}(\mathbb{F}_p)) = \mathrm{ord}_2(\#J_{6,a}(\mathbb{F}_p)[2])$, to $J_{6,a}(\mathbb{F}_p)$ nie posiada elementu rzędu 4, więc tak samo $J_{6,a}(\mathbb{Q})_{tors}$. Opierając się na tej obserwacji, rozważając szereg przypadków i korzystając z twierdzenia Czebotariewa o gęstości dostajemy pierwszy główny wynik tego artykułu (pamiętajmy, że bez straty ogólności a jest liczbą całkowitą wolną od dwunastych potęg).

Twierdzenie 2.18. *Jeśli $a \notin 4\mathbb{N}^4 \cup \{-1728, -1259712\}$, to $J_{6,a}(\mathbb{Q})_{tors} = J_{6,a}(\mathbb{Q})[2]$.*

Mamy więc częściową analogię z twierdzeniem 2.13 (tj. z krzywą $C_{4,a}$) i z krzywą eliptyczną E_a, ale w przeciwieństwie do tamtych sytuacji mamy też poniższy wynik.

Twierdzenie 2.19. *Jeśli $a = 4b^4$ lub $a = -1259712$, to grupa $J_{6,a}(\mathbb{Q})_{tors}$ zawiera element rzędu 4. Ponadto,*

(i) jeśli $b \neq 2$, to

$$J_{6,4b^4}(\mathbb{Q})_{tors} =< [(\sqrt[3]{2b^2}, 2b^2\sqrt[3]{4b}) + (\omega\sqrt[3]{2b^2}, 2b^2\omega^2\sqrt[3]{4b}) +$$
$$(\omega^2\sqrt[3]{2b^2}, 2b^2\omega\sqrt[3]{4b}) - 3\infty] >\cong \mathbb{Z}/4\mathbb{Z},$$ *(ω oznacza pierwiastek pierwotny z 1 stopnia 3).*

(ii)

$$J_{6,-1259712}(\mathbb{Q})_{tors} \supset< [(0,0) - \infty] > \times < [(9 - 3\sqrt{21}, 29160 - 5832\sqrt{21}) +$$
$$(9 + 3\sqrt{21}, 29160 + 5832\sqrt{21}) - 2\infty] >\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Dowód opiera się na specjalnych własnościach $C_{6,a}$. Mianowicie krzywa $C_{6,a}$ posiada dwa automorfizmy: $\sigma(x,y) = \left(\sqrt[3]{a}/x, \sqrt[3]{a^2}y/x^4\right)$ określony nad $\mathbb{Q}(\sqrt[3]{a})$ i $\rho(x,y) = \left(\zeta_{12}^2 x, \zeta_{12} y\right)$ określony nad $\mathbb{Q}(\zeta_{12})$, gdzie ζ_{12} jest pierwotnym pierwiastkiem z jedynki stopnia 12. Łatwo sprawdzić, że ρ ma rząd 12, σ ma rząd 2 i $\sigma\rho = \rho^5\sigma$. Te automorfizmy indukują endomorfizmy w jakobianie $J_{6,a}$, a zatem pierścień endomorfizmów $J_{6,a}$ zawiera $\mathbb{Z}[\zeta_{12}]$.

Iloraz krzywej $C_{6,a}$ przez grupę generowaną przez σ jest krzywą eliptyczną $E_{a,1}$ o równaniu

$$E_{a,1} : y^2 = x^3 - 3\sqrt[3]{a}x,$$

a jawne odwzorowanie ilorazowe dane jest przez

$$(x,y) \mapsto \left(x + \frac{\sqrt[3]{a}}{x}, \frac{y}{x^2}\right).$$

Iloraz krzywej $C_{6,a}$ przez grupę $< \rho^4 >$ jest krzywą eliptyczną $E_{a,2}$ o równaniu

$$E_{a,2} : y^2 = x^3 + ax,$$

a jawne odwzorowanie ilorazowe dane jest przez

$$(x,y) \mapsto \left(x^3, xy\right).$$

Ponieważ krzywe eliptyczne $E_{a,1}$, $E_{a,2}$ odpowiadają liniowo niezależnym różniczkom na $C_{6,a}$, możemy wywnioskować, że jakobian $J_{6,a}$ jest izogeniczny (nad $\overline{\mathbb{Q}}$) z produktem trzech krzywych eliptycznych $E_{a,1}$, $E_{a,2}$, $E_{a,3}$. Ponadto

$$E_{a,3} = (1 - \sigma)\left(1 - \rho^4\right)\left(1 - \rho^8\right) J_{6,a}.$$

Przypadek $a=-1728=-2^6 3^3$ jest bardziej subtelny. Nie jesteśmy w stanie dać pełnej odpowiedzi (por. remarks 3.16 w [A2]), ale możemy udowodnić, że jakobian $J_{6,-1728}$ jest izogeniczny nad $\mathbb{Q}$ z produktem trzech krzywych eliptycznych $y^2=x^3+36x$, $y^2=x^3-108x$, $y^2=x^3+4x$. W konsekwencji $J_{6,-1728}(\mathbb{Q})$ ma rangę 0 oraz punkt w nieskończoności i $(0,0)$ to jedyne $\mathbb{Q}$-wymierne punkty na krzywej $C_{6,-1728}$. Ponadto dla każdej liczby pierwszej $p>3$ grupa $J_{6,-1728}(\mathbb{F}_p)$ ma punkt rzędu 4.

Teraz wróćmy do dwuparametrowej rodziny $C^{p,a}$. Zauważmy, że krzywa $C^{p,a}$ ma automorfizm $(x,y)\mapsto(\zeta_p x,y)$, gdzie ζ_p jest pierwotnym pierwiastkiem z jedynki stopnia p. Zatem jakobian $J^{p,a}$ ma mnożenie zespolone przez $\mathbb{Q}(\zeta_p)$. W przeciwieństwie do poprzedniej rodziny, dla $C_{p,a}$ nie jest możliwa redukcja do przypadku krzywych eliptycznych. Połóżmy $p^*:=(-1)^{\frac{p-1}{2}}p$. Główny wynik jest następujący (zwróćmy uwagę na piękną analogię z (1)).

Twierdzenie 2.20. *Mamy*

$$J^{p,a}(\mathbb{Q})_{tors}\cong\begin{cases}\{0\} & \text{jeśli } a \text{ nie jest kwadratem, ani kwadratem razy } p^*,\\ & \text{ani } p\text{-tą potęgą,}\\ \mathbb{Z}/2\mathbb{Z} & \text{jeśli } a \text{ nie jest kwadratem, ani kwadratem razy } p^*,\\ & \text{ale jest } p\text{-tą potęgą,}\\ \mathbb{Z}/p\mathbb{Z} & \text{jeśli } a \text{ jest kwadratem, ale nie jest } p\text{-tą potęgą,}\\ \mathbb{Z}/2p\mathbb{Z} & \text{jeśli } a \text{ jest kwadratem i jest } p\text{-tą potęgą,}\\ \{0\} \text{ lub } \mathbb{Z}/p\mathbb{Z} & \text{jeśli } a \text{ jest kwadratem razy } p^*, \text{ ale nie jest } p\text{-tą potęgą,}\\ \mathbb{Z}/2\mathbb{Z} \text{ lub } \mathbb{Z}/2p\mathbb{Z} & \text{jeśli } a \text{ jest kwadratem razy } p^* \text{ i jest } p\text{-tą potęgą.}\end{cases}$$

Ponadto można jawnie wskazać torsyjne elementy: $[(-\sqrt[p]{a},0)-\infty]$ *rzędu* 2, $[(0,\sqrt{a})-\infty]$ *rzędu* p *i* $[(0,\sqrt{a})+(-\sqrt[p]{a},0)-2\infty]$ *rzędu* $2p$.

Dwuznaczny przypadek J^{p,p^*b^2} jest bardziej skomplikowany (patrz remarks 4.5 w [A2]). Na przykład można pokazać, że $p\mid\#J^{p,\pm pb^2}(\mathbb{F}_q)$ dla dowolnej liczby pierwszej $q\nmid 2pb$. Zatem grupa $J^{p,\pm pb^2}(\mathbb{F}_q)$ zawsze ma punkt rzędu p. Jednak z drugiej strony dla $p=5$ mamy $J^{5,5b^2}(\mathbb{Q})_{tors}\cong\mathbb{Z}/5\mathbb{Z}$, tylko gdy $b=2^4 5^2$. A dla innych wartości b mamy $J^{5,5b^2}(\mathbb{Q})_{tors}=\{0\}$ z wyjątkiem $J^{5,5^5}(\mathbb{Q})_{tors}\cong\mathbb{Z}/2\mathbb{Z}$.

2.3 Artykuł [A5]

W tym artykule rozważamy krzywe $C^{n,a}:y^2=x^n+a$ i $C_{n,a}:y^2=x(x^n+a)$ oraz ich jakobiany $J^{n,a}$ i $J_{n,a}$. Naszym celem jest opisanie części torsyjnych $J^{n,a}(\mathbb{Q})$ i $J_{n,a}(\mathbb{Q})$. Dla dowolnego n ten opis nie jest zupełny, ale damy (prawie kompletne) charakteryzacje $J_{n,a}(\mathbb{Q})_{tors}$, gdzie n jest nieparzystą liczbą pierwszą lub $n=8$ oraz $J^{n,a}(\mathbb{Q})_{tors}$, gdzie n jest liczbą złożoną nie większą niż 8. Te rezultaty, razem z wynikami z artykułów [A1] and [A2], dają (prawie pełny) opis grup $J^{n,a}(\mathbb{Q})_{tors}$ i $J_{n,a}(\mathbb{Q})_{tors}$, gdzie $n\leq 8$ lub n jest nieparzystą liczbą pierwszą.

Główne składniki dowodów to wyprowadzenie jawnych wzorów na funkcje zeta krzywych $C^{n,a}$ i $C_{n,a}$ w pewnych przypadkach (które są interesujące same w sobie) oraz zastosowania twierdzenia Czebotariewa o gęstości.

Dobrze wiadomo, że funkcje zeta krzywych $C_{n,a}$ i $C^{n,a}$ nad $\mathbb{F}_p$ ($p\nmid 2na$) są postaci

$$Z(C_{n,a}/\mathbb{F}_p,T)=\frac{P_{n,a}(T)}{(1-T)(1-pT)},$$
$$Z(C^{n,a}/\mathbb{F}_p,T)=\frac{Q_{n,a}(T)}{(1-T)(1-pT)},$$

gdzie $P_{n,a}(T)$ i $Q_{n,a}(T)$ są wielomianami o całkowitych współczynnikach stopni $2\left[\frac{n}{2}\right]$ i $2\left[\frac{n-1}{2}\right]$ odpowiednio. Ponadto (zob. np. [37, exercise A.8.11]),

$$\#J_{n,a}(\mathbb{F}_p) = P_{n,a}(1), \tag{13}$$
$$\#J^{n,a}(\mathbb{F}_p) = Q_{n,a}(1). \tag{14}$$

Najpierw odnotujmy, że te krzywe są wzajemnie związane.

Stwierdzenie 2.21. *Dla dowolnych a i n mamy*

$$Q_{2n,a} = Q_{n,a} \times P_{n,a}.$$

W szczególności,

$$\#J^{2n,a}(\mathbb{F}_p) = \#J^{n,a}(\mathbb{F}_p)\,\#J_{n,a}(\mathbb{F}_p).$$

W konsekwencji na mocy znanego rezultatu Tate'a [79], rozmaitości abelowe $J^{2n,a}$ i $J^{n,a} \times J_{n,a}$ są izogeniczne nad $\mathbb{F}_p$.

Korzystając z lematów 2.9 i 2.21, wzoru Hassego-Davenporta [3, Corollary 11.5.3] oraz własności sum Jacobiegi i tzw. czystych (pure) sum Gaussa możemy udowodnić następujące.

Stwierdzenie 2.22. *Jeśli $p \equiv -1 \pmod{n}$ i $p \nmid 2a$, to*

$$Q_{n,a}(T) = \left(1 + pT^2\right)^{[(n-1)/2]}.$$

Jeśli $p \equiv -1 \pmod{2n}$ i $p \nmid a$, to

$$P_{n,a}(T) = \left(1 + pT^2\right)^{[n/2]}.$$

Teraz możemy udowodnić pierwsze dwa główne wyniki pracy [A5] (dowody wykorzystują stwierdzenie 2.22, twierdzenie Dirichleta i jawne (explicit) konstrukcje zredukowanych dywizorów danego rzędu w jakobianach).

Twierdzenie 2.23. *Dla dowolnej liczby pierwszej p mamy*

$$p \mid \#J_{n,a}(\mathbb{Q})_{tors} \Longrightarrow p = 2 \vee p \mid n,$$

i

$$\operatorname{ord}_2\left(\#J_{n,a}(\mathbb{Q})_{tors}\right) \leq \begin{cases} \frac{n}{2}\operatorname{ord}_2(2n) & gdy\ 2 \mid n \\ \frac{n-1}{2} & gdy\ 2 \nmid n \end{cases},$$

a dla $p \neq 2$

$$\operatorname{ord}_p\left(\#J_{n,a}(\mathbb{Q})_{tors}\right) \leq \begin{cases} \frac{n}{2}\operatorname{ord}_p(n) & gdy\ 2 \mid n \\ \frac{n-1}{2}\operatorname{ord}_p(n) & gdy\ 2 \nmid n \end{cases}.$$

Ponadto dla każdego $a \neq 0$,

$$\mathbb{Z}/2\mathbb{Z} \subset J_{n,a}(\mathbb{Q})_{tors},\ gdy\ 2 \mid n,$$
$$\mathbb{Z}/n\mathbb{Z} \subset J_{n,a}(\mathbb{Q})_{tors},\ gdy\ 2 \nmid n.$$

Twierdzenie 2.24. *Dla dowolnej liczby pierwszej p mamy*

$$p \mid \#J^{n,a}(\mathbb{Q})_{tors} \Longrightarrow p = 2 \vee p \mid n,$$

i

$$\operatorname{ord}_2\left(\#J^{n,a}(\mathbb{Q})_{tors}\right) \leq \begin{cases} \frac{n-2}{2}\operatorname{ord}_2(n) & if\ 2 \mid n \\ \frac{n-1}{2} & if\ 2 \nmid n \end{cases},$$

a dla $p \neq 2$

$$\operatorname{ord}_p\left(\#J^{n,a}\left(\mathbb{Q}\right)_{tors}\right) \leq \begin{cases} \frac{n-2}{2}\operatorname{ord}_p\left(n\right) & \text{if } 2 \mid n \\ \frac{n-1}{2}\operatorname{ord}_p\left(n\right) & \text{if } 2 \nmid n \end{cases}.$$

Ponadto,

$$\mathbb{Z}/m\mathbb{Z} \subset J^{2m,a}\left(\mathbb{Q}\right)_{tors},$$
$$\left(\mathbb{Z}/m\mathbb{Z}\right)^2 \subset J^{2m,c^2}\left(\mathbb{Q}\right)_{tors},$$
$$\mathbb{Z}/\left(2m+1\right)\mathbb{Z} \subset J^{2m+1,c^2}\left(\mathbb{Q}\right)_{tors},$$

dla dowolnych niezerowych a, c *i dowolnego naturalnego* m.

Natychmiast otrzymujemy

Wniosek 2.25. *Jeśli* $n = 2^k$, *to (dla dowolnego* a*)* $J_{n,a}\left(\mathbb{Q}\right)_{tors}$ *i* $J^{n,a}\left(\mathbb{Q}\right)_{tors}$ *są 2-grupami rzędów* $\leq 2^{(k+1)2^{k-1}}$ *i* $\leq 2^{k(2^{k-1}-1)}$ *odpowiednio. Z drugiej strony, jeśli* n *jest nieparzyste, to* $J_{n,a}\left(\mathbb{Q}\right)_{tors}$ *nigdy (w sensie niezależnie od* a*) nie jest 2-grupą. Podobnie, jeśli* n *jest parzyste, ale nie jest potęgą dwójki, to* $J^{n,a}\left(\mathbb{Q}\right)_{tors}$ *nigdy nie jest 2-grupą.*

Teraz przedstawimy dokładniejsze charakteryzacje części torsyjnych $J_{n,a}, J^{n,a}$ nad $\mathbb{Q}$ dla pewnych n. W dowodach korzystamy ze stwierdzenia 2.21, z obliczeń liczby elementów w jakobianach nad ciałami skończonymi i z twierdzeń o gęstości (lemat 2.11, twierdzenie Dirichleta).

Twierdzenie 2.26. *Mamy*

$$J_{8,a}\left(\mathbb{Q}\right)_{tors} = J_{8,a}\left(\mathbb{Q}\right)\left[2\right] \text{ dla dowolnego } a \in \mathbb{Q}\backslash\left\{0\right\}.$$

W jawnej postaci (bez straty ogólności a *jest liczbą całkowitą wolna od szesnastych potęg):*

$$J_{8,a}\left(\mathbb{Q}\right)_{tors} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{jeśli } a \neq 4c^4 \text{ i } a \neq -c^2, \\ \left(\mathbb{Z}/2\mathbb{Z}\right)^2 & \text{jeśli } a = 4c^4 \text{ lub } (a = -c^2 \text{ i } c \neq b^2), \\ \left(\mathbb{Z}/2\mathbb{Z}\right)^3 & \text{jeśli } a = -c^4 \text{ i } c \neq b^2 \text{ i } c \neq 2b^2, \\ \left(\mathbb{Z}/2\mathbb{Z}\right)^4 & \text{jeśli } a = -c^8 \text{ lub } a = -16c^8. \end{cases}$$

Twierdzenie 2.27. *Dla dowolnej nieparzystej liczby pierwszej* p *mamy,*

$$J_{p,a}\left(\mathbb{Q}\right)_{tors} \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{jeśli } a \text{ nie jest } p\text{-tą potęgą}, \\ \mathbb{Z}/2p\mathbb{Z} & \text{jeśli } a \text{ jest } p\text{-tą potęgą}. \end{cases}$$

Twierdzenie 2.28. *Dla dowolnego* $a \neq 0$ *mamy*

$$J^{4,a}\left(\mathbb{Q}\right)_{tors} \cong \begin{cases} \left(\mathbb{Z}/2\mathbb{Z}\right)^2 & \text{jeśli } a = c^2, \\ \mathbb{Z}/4\mathbb{Z} & \text{jeśli } a = -c^4, \\ \mathbb{Z}/2\mathbb{Z} & \text{jeśli } a \neq c^2 \text{ i } a \neq -c^4. \end{cases}$$

Twierdzenie 2.29. *Dla dowolnego* $a \neq 0$ *mamy*

$$J^{6,a}\left(\mathbb{Q}\right)_{tors} = J^{6,a}\left(\mathbb{Q}\right)\left[2\right] \times J^{6,a}\left(\mathbb{Q}\right)\left[9\right],$$

gdzie

$$J^{6,a}\left(\mathbb{Q}\right)\left[2\right] \cong \begin{cases} \left(\mathbb{Z}/2\mathbb{Z}\right)^2 & \text{jeśli } a = -c^6 \text{ lub } a = 27c^6, \\ \mathbb{Z}/2\mathbb{Z} & \text{jeśli } a = b^3 \text{ i } b \neq 3c^2 \text{ i } b \neq -c^2, \\ 0 & \text{jeśli } a \neq b^3, \end{cases}$$

i

$$J^{6,a}\left(\mathbb{Q}\right)\left[9\right] \cong \begin{cases} \left(\mathbb{Z}/3\mathbb{Z}\right)^2 & \text{jeśli } a = c^2 \text{ lub } a = -432b^6, \\ \mathbb{Z}/3\mathbb{Z} & \text{jeśli } a \neq c^2 \text{ i } a \neq -3c^2 \text{ i } a \neq 2b^3, \\ \mathbb{Z}/9\mathbb{Z} \text{ lub } \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \text{ lub } \mathbb{Z}/3\mathbb{Z} & \text{jeśli } (a = -3c^2 \text{ i } a \neq -432b^6) \text{ lub} \\ & (a = 2b^3 \text{ i } a \neq -3c^2 \text{ i } a \neq c^2). \end{cases}$$

Twierdzenie 2.30. *Dla dowolnego $a \neq 0$ mamy*

$$J^{8,a}(\mathbb{Q})_{tors} \cong \begin{cases} (\mathbb{Z}/4\mathbb{Z})^2 & \text{jeśli } a = c^2 \text{ i } a \neq 4b^4, \\ \mathbb{Z}/4\mathbb{Z} & \text{jeśli } a \neq \pm c^2, \end{cases}$$

W świetle powyższych wyników naturalnym jest postawienie następujących pytań.

Pytanie 2.31. *Dla jakich parzystych liczb naturalnych $n \neq 2^k$ grupa $J_{n,a}(\mathbb{Q})_{tors}$ jest zawsze (w sensie dla dowolnego niezerowego a) 2-grupą?*

Znamy tylko jedno takie n. Mianowicie, wiemy, że $J_{6,a}(\mathbb{Q})_{tors}$ jest 2-grupą. Dla liczb naturalnych n takich, że $J_{n,a}(\mathbb{Q})_{tors}$ jest zawsze 2-grupą możemy zadać kolejne

Pytanie 2.32. *Dla jakich liczb naturalnych n mamy zawsze $J_{n,a}(\mathbb{Q})_{tors} = J_{n,a}(\mathbb{Q})[2]$?*

Wiemy, że dla $n = 4, 8$ tak jest. Natomiast dla $n = 2, 6$ tak nie jest - dla pewnych a (nawet nieskończenie wielu, gdy $n = 6$) grupa $J_{n,a}(\mathbb{Q})$ ma element rzędu 4. Zauważmy, że analogicznie pytania dla $J^{n,a}(\mathbb{Q})_{tors}$ mają trywialne odpowiedzi. Istotnie, na mocy twierdzenia 2.24, jeśli $n \neq 2^k$, to zdanie "$J^{n,a}(\mathbb{Q})_{tors}$ jest zawsze 2-grupą" jest fałszywe. Nawet dla $n = 2^k \geq 4$ zdanie "$J_{n,a}(\mathbb{Q})_{tors} = J_{n,a}(\mathbb{Q})[2]$ dla dowolnego niezerowego a" jest fałszywe, ponieważ $J_{2^k,a}(\mathbb{Q})_{tors}$ ma element rzędu 4.

Na koniec można postawić ogólne, ciekawe (i raczej trudne).

Pytanie 2.33. *Jaka jest kompletna charakteryzacja grup $J_{n,a}(\mathbb{Q})_{tors}$ i $J^{n,a}(\mathbb{Q})_{tors}$ dla dowolnych naturalnych n i całkowitych a wolnych od $2n$-potęg?*

W szczególności można pytać o możliwe analogie między wzorami (1), (2) a wzorami na $J^{n,a}(\mathbb{Q})_{tors}, J_{n,a}(\mathbb{Q})_{tors}$ odpowiednio.

3 Krzywe supereliptyczne

Przez *krzywą supereliptyczną* będziemy rozumieć nieosobliwą rzutową krzywą C zadaną równaniem afinicznym

$$y^n = f(x) := a_m x^m + \cdots + a_0, \tag{15}$$

gdzie n, m są liczbami naturalnymi. Powiemy, że C jest *określona nad* ciałem K, gdy współczynniki a_i należą do K. Model (15) jest nieosobliwy, gdy $\mathrm{NWD}(f(x), f'(x)) = 1$ (tzn. wielomian f nie ma wielokrotnych pierwiastków) i charakterystyka ciała K nie dzieli n (co jest spełnione, gdy np. $\mathrm{char}(K) = 0$). Odnotujmy, że nie zakładamy, że afiniczny model (15) jest nieosobliwy, ale wówczas rozważamy jedyną (z dokładnością do izomorfzmu) nieosobliwą rzutową krzywą biwymiernie równoważną (birationally equivalent) z rzutowym domknięciem krzywej afinicznej (15) (por. [37, Thm. A.4.1.4]).

Jeśli $n < m$, to krzywa ta ma równanie jednorodne

$$y^n z^{m-n} = a_m x^m + a_{m-1} x^{m-1} z + \cdots + a_0 z^n. \tag{16}$$

Z postaci (16) wynika, że jedyny punkt w nieskończoności to $[x : y : z] = [0 : 1 : 0]$. Ten punkt jest osobliwy, gdy $n + 1 < m$. Jeśli $n > m$, to podobne argumenty pokazują, że punkt $[1 : 0 : 0]$ jest jedynym punktem w nieskończoności. Natomiast jeżeli $n = m$, to istnieje n różnych punktów w nieskończoności (określonych nad $\bar{K}$), mianowicie $[x : y : 0]$, gdzie $y^n = a_n x^n$. Wszystkie te punkty są nieosobliwe.

W przypadku $n \neq m$ możemy wielokrotnie rozdmuchać (blow up) osobliwe punkty w nieskończoności aż dostaniemy nieosobliwy model krzywej C. Można pokazać, że jeśli $\mathrm{NWD}(n, m) = 1$, to istnieje tylko jeden punkt w nieskończoności w modelu nieosobliwym. Innymi słowy, ideały pierwsze w nieskończoności są totalnie rozgałęzione. Ponadto warunek $\mathrm{NWD}(n, \mathrm{char}(K)) = 1$ implikuje, że rozgałęzienie jest oswojone (tame).

Ze wzoru Hurwitza genus krzywej C wynosi $\frac{1}{2}(n-1)(m-1)$, gdy $\mathrm{NWD}(n,m)=1$. Zauważmy, że jeśli $m=n+1$, to genus C jest największym możliwym genusem krzywej stopnia n. O tych i innych własnościach krzywych supereliptycznych można poczytać np. w [31].

Przypomnijmy, że J_C oznacza jakobian krzywej C. Załóżmy, że $K=\mathbb{Q}$. Podobnie jak w przypadku krzywych hipereliptycznych dla liczb pierwszych l nie dzielących n,m oraz wyróżnika wielomianu f homomorfizm redukcji modulo l indukuje zanurzenie $J_C(\mathbb{Q})_{tors} \hookrightarrow J_C(\mathbb{F}_l)$ (zob. [37, Theorem C.1.4, s. 263]) i w związku z tym

$$\#J_C(\mathbb{Q})_{tors} \,|\, \#J_C(\mathbb{F}_l)\,. \tag{17}$$

Dowód tej własności podany w [37] używa grup formalnych. Można dać bardziej geometryczne wyjaśnienie tego dla dowolnej rozmaitości abelowej A nad $\mathbb{Q}$. Dla każdej liczby pierwszej l, w której A ma dobrą redukcję, $A[n]$ jest skończonym płaskim schematem grupowym nad $\mathbb{Z}_l$ i injektywność redukcji modulo l na punktach torsyjnych wynika (przynajmniej dla $l\neq 2$) z lematu o specjalizacji (Specialization Lemma) w [54, s. 135], który z kolei wynika z klasyfikacji Oorta-Tate'a schematów grupowych [80].

Niech p będzie nieparzystą liczbą pierwszą. Rozważmy krzywą Fermata p-tego stopnia, tj. krzywą algebraiczną $F(p)$ zadaną we współrzędnych rzutowych przez równanie Fermata $X^p+Y^p=Z^p$. Zatem jej równanie afiniczne ma postać $x^p+y^p=1$. Na mocy Wielkiego twierdzenia Fermata udowodnionego przez Wilesa [86] wiadomo, że krzywe Fermata nie mają nietrywialnych punktów wymiernych. Krzywa $F(p)$ jest nieosobliwa i ma genus $\frac{1}{2}(p-1)(p-2)$. Jakobian $J(p)$ krzywej $F(p)$ był wnikliwie badany przez wielu matematyków (np. [24, 34, 15]). Faddeev [23, 24] pokazał, że jest on izogeniczny z produktem prostych rozmaitości abelowych z mnożeniem zespolonym. Przedstawimy to precyzyjniej w ogólniejszej sytuacji. Mianowicie, rozważmy (przy ustalonym p) skręcenie p-tego stopnia krzywej $F(p)$ przez liczbę całkowitą a; są to tzw. krzywe typu Fermata

$$F_a(p): x^p+y^p=a. \tag{18}$$

Oczywiście $F_a(p)$ i $F(p)=F_1(p)$ są izomorficzne nad $\mathbb{Q}(a^{1/p})$. To indukuje izomorfizm ich jakobianów $J_a(p)$ i $J(p)$ odpowiednio. Rozważmy też (dla $s=1\ldots,p-2$) krzywe genusu $(p-1)/2$

$$C_{a,s}(p): y^p=x(a-x)^s. \tag{19}$$

Krzywa $C_{a,s}(p)$ ma automorfizm $(x,y)\mapsto(x,\zeta_p y)$, jej jakobian $J_{a,s}(p)$ jest określony nad $\mathbb{Q}$ i ma mnożenie zespolone przez $\mathbb{Q}(\zeta_p)$. Można pokazać, że krzywe $C_{a,(p-1)/2}(p)$ i $C_{a,p-2}(p)$ są biwymiernie równoważne, a krzywe $C_{a,s}(p)$ są hipereliptyczne dla $s=1,(p-1)/2,p-2$ (patrz [A3, Lemma 5.7]). Przez odpowiednią zamianę zmiennych możemy otrzymać z nich krzywe hipereliptyczne postaci

$$A_{a,p}: y^2=x^p+(4a)^{p-1}\,, B_{a,p}: y^2=x^p+4^{p-1}a^2. \tag{20}$$

Dla $s=1,...,p-2$ definiujemy morfizmy

$$\varphi_{a,s}: F_a(p)\to C_{a,s}(p)$$

wzorami

$$\varphi_{a,s}(x,y)=(x^p,xy^s)\,.$$

Morfizm $\varphi_{a,s}$ indukuje dobrze określone odwzorowanie $J_a(p)\to J_{a,s}(p)$ między odpowiednimi jakobianami. Podobnie jak w [23], [24] otrzymujemy izogenię określoną nad $\mathbb{Q}$

$$\varphi:=\prod_{s=1}^{p-2}\varphi_{a,s}: J_a(p)\to\prod_{s=1}^{p-2}J_{a,s}(p)\,. \tag{21}$$

W szczególności, $J_a(5)$ jest izogeniczny z $J_{a,1}(5)J_{a,2}(5)^2$, więc problem obliczena rangi $J_a(5)(\mathbb{Q})$ sprowadza się do obliczenia rang $J_{a,s}(5)(\mathbb{Q})$ dla $s=1,2$.

3.1 Artykuł [A3]

W [B4] rozważaliśmy pewne problemy związane z istnieniem skręceń trójek i czwórek krzywych hipereliptycznych zadanych równaniami postaci $y^2 = x^n + a$, których jakobiany jednocześnie miały dodatnią rangę (twierdzenia 4.9, 4.10, 4.11 w autoreferacie). W [A1] rozważaliśmy też skręcenia ósmego stopnia krzywych $y^2 = x^5+ax$ i udowodniliśmy podobne wynik (twierdzenie 2.14). Ulas [83] badał pewne warianty tych zagadnień i pytał o istnienie skręceń (niekoniecznie tego samego stopnia) trójek krzywych eliptycznych jednocześnie dodatniej rangi. W cytowanym artykule udowodnił, że jeżeli $E_1 : y^2 = f(x)$ oraz E_2, E_3 są krzywymi eliptycznymi, przy czym E_2 i E_3 mają j-niezmiennik 0, to istnieje funkcja wymierna $D_{2,3,3} \in \mathbb{Q}(u, v, w)$ taka, że skręcenie kwadratowe E_1 oraz skręcenia sześcienne E_2, E_3 przez $D_{2,3,3}$ mają dodatnie rangi nad $\mathbb{Q}(u, v, w)$. Ponadto, udowodnił istnienie funkcji wymiernej $D_{2,6,6} \in \mathbb{Q}(u, v, w)$ takiej, że skręcenie kwadratowe E_1 oraz skręcenia szóstego stopnia E_2, E_3 przez $D_{2,6,6}$ mają dodatnie rangi nad $\mathbb{Q}(u, v, w)$.

Celem niniejszego artykułu jest uogólnienie wspomnianych wyników z [83] na przypadek trójki krzywych hipereliptycznych. Dodatkowo przedstawimy pewne rezultaty dotyczące skręceń krzywych supereliptycznych i wyznaczymy $\mathbb{Q}$-torsję ich jakobianów (co jest niezależnie interesujące).

Rozważmy krzywe hipereliptyczne

$$C_1 : y^2 = f(x), \quad C_2 : y^2 = x^m + b, \quad C_3 : y^2 = x^m + c, \tag{22}$$

gdzie $f \in \mathbb{Z}[x]$ jest bezkwadratowym wielomianem stopnia ≥ 3, $m = 2n + 1 \geq 3$ i $b, c \in \mathbb{Z} \setminus \{0\}$. Z naszych założeń na f i m wynika, że genus C_1 jest przynajmniej 1, a genus C_i jest n dla $i = 2, 3$. Przypomnijmy, że przez skręcenie k-tego stopnia (zwane też krócej k-skręceniem), gdzie $k \geq 2$, krzywej algebraicznej C określonej nad $\mathbb{Q}$ rozumiemy krzywą C' taką, że $C \simeq C'$ nad skończonym rozszerzeniem ciała $\mathbb{Q}$ stopnia k. W ogólności dla krzywej hipereliptycznej C_1 istnieją tylko skręcenia kwadratowe, tzn. dla dowolnego $d \in \mathbb{Q}^* \setminus \mathbb{Q}^{*2}$ mamy $C_1' : dy^2 = f(x)$ oraz $C_1 \simeq C_1'$ nad $\mathbb{Q}(\sqrt{d})$ (mówimy wtedy, że C_1' jest skręceniem kwadratowym krzywej C_1 przez d). Natomiast w przypadku krzywych hipereliptycznych postaci $C : y^2 = x^m + a$ z nieparzystym m istnieją skręcenia wyższego stopnia. W szczególności mamy m-skręcenia C zdefiniowane równaniem $C' : y^2 = dx^m + a$. W tym przypadku $C \simeq C'$ nad $\mathbb{Q}(\sqrt[m]{d})$ dla dowolnego $d \in \mathbb{Q}$, w którego rozkładzie na czynniki pierwsze (z dodatnimi i ujemnymi wykładnikami) występuje liczba pierwsza z wykładnikiem względnie pierwszym z m. Przy tak wybranym d będziemy mówić dalej, że krzywa C' jest m-skręceniem krzywej C przez d. Poza tym dla danego m mamy $2m$-skręcenie C zdefiniowane równaniem $C' : y^2 = x^m + ad$. W tym przypadku $C \simeq C'$ nad $\mathbb{Q}(\sqrt[2m]{d})$ dla dowolnego $d \in \mathbb{Q}$, w którego rozkładzie kanonicznym występuje liczba pierwsza z wykładnikiem względnie pierwszym z $2m$. Przy tak wybranym d będziemy mówić dalej, że krzywa C' jest $2m$-skręceniem krzywej C przez d. Wzmiankowane skręcenia są naturalnym uogólnieniem skręceń sześciennych (w przypadku m-skręceń) i skręceń szóstego stopnia (w przypadku $2m$-skręceń) krzywych eliptycznych z j-niezmiennikiem 0.

Otrzymaliśmy następujące wyniki.

Twierdzenie 3.1. *Załóżmy, że $f \in \mathbb{Q}[x]$ nie ma wielokrotnych pierwiastków. Niech $b, c \in \mathbb{Z} \setminus \{0\}$ i m będzie nieparzystą liczbą naturalną. Rozważmy krzywe hipereliptyczne dane przez (22). Wówczas istnieje funkcja wymierna $D_{2,m,m} \in \mathbb{Q}(u, v, w)$ taka, że jakobian kwadratowego skręcenia krzywej C_1 i jakobiany m-skręceń krzywych C_2, C_3 przez $D_{2,m,m}(u, v, w)$ mają dodatnią rangę nad ciałem $\mathbb{Q}(u, v, w)$.*

Wniosek 3.2. *Niech $b \in \mathbb{Z} \setminus \{0\}$, $m \in \mathbb{N}$ i niech $C_1 : y^2 = f(x)$, $C_2 : y^2 = x^m + b$. Wówczas istnieje funkcja wymierna $D_{2,m} \in \mathbb{Q}(u, v, w)$ taka, że jakobian kwadratowego skręcenia C_1 przez $D_{2,m}(u, v, w)$ ma dodatnią rangę oraz jakobian m-skręcenia C_2 przez $D_{2,m}(u, v, w)$ ma rangę ≥ 2 nad $\mathbb{Q}(u, v, w)$.*

Twierdzenie 3.3. *Załóżmy, że $f \in \mathbb{Q}[x]$ nie ma wielokrotnych pierwiastków. Niech $b, c \in \mathbb{Z} \setminus \{0\}$ i m będzie nieparzystą liczbą naturalną. Rozważmy krzywe hipereliptyczne dane przez (22). Wówczas istnieje funkcja wymierna $D_{2,2m,2m} \in \mathbb{Q}(u,v,w)$ taka, że jakobian kwadratowego skręcenia krzywej C_1 i jakobiany $2m$-skręceń krzywych C_2, C_3 przez $D_{2,2m,2m}(u,v,w)$ mają dodatnią rangę nad ciałem $\mathbb{Q}(u,v,w)$.*

Wniosek 3.4. *Niech $b \in \mathbb{Z} \setminus \{0\}$, $m \in \mathbb{N}$ i niech $C_1 : \ y^2 = f(x)$, $C_2 : \ y^2 = x^m + b$. Wówczas istnieje funkcja wymierna $D_{2,2m} \in \mathbb{Q}(u,v,w)$ taka, że jakobian kwadratowego skręcenia C_1 przez $D_{2,2m}(u,v,w)$ ma dodatnią rangę oraz jakobian $2m$-skręcenia C_2 przez $D_{2,2m}(u,v,w)$ ma rangę ≥ 2 nad $\mathbb{Q}(u,v,w)$.*

Twierdzenie 3.5. *Niech $a, b, c \in \mathbb{Z} \setminus \{0\}$ i niech m będzie nieparzystą liczbą naturalną. Rozważmy krzywe hipereliptyczne*

$$C_1 : \ y^2 = x_1^m + a, \quad C_2 : \ y^2 = x^m + b, \quad C_3 : \ y^2 = x^m + c.$$

Wówczas istnieje funkcja wymierna $D_{m,m,2m} \in \mathbb{Q}(u,v,w)$ taka, że jakobiany m-skręceń krzywych C_1, C_2 i jakobian $2m$-skręcenia krzywej C_3 przez $D_{m,m,2m}(u,v,w)$ mają dodatnią rangę nad ciałem $\mathbb{Q}(u,v,w)$.

Wniosek 3.6. *Niech $a, b \in \mathbb{Z}\setminus\{0\}$ i niech m będzie nieparzystą liczbą naturalną. Rozważmy krzywe hipereliptyczne $C_1 : \ y^2 = x^m + a$, $C_2 : \ y^2 = x^m + b$. Wówczas istnieje funkcja wymierna $D_{m,2m} \in \mathbb{Q}(u,v,w)$ taka, że jakobian m-skręcenia C_1 przez $D_{m,2m}(u,v,w)$ ma rangę ≥ 2 oraz jakobian $2m$-skręcenia C_2 przez $D_{m,2m}(u,v,w)$ ma dodatnią rangę nad $\mathbb{Q}(u,v,w)$.*

Aby udowodnić powyższe twierdzenia konstruujemy układy równań, a następnie szukamy ich parametrycznych rozwiązań. Innymi słowy konstruujemy wymierne krzywe na pewnych rozmaitościach, a potem parametryzując te krzywe znajdujemy punkty wymierne. Mając odpowiedni punkt pokazujemy, że ten punkt minus punkt w nieskończoności określa element nieskończonego rzędu w jakobianie. Aby udowodnić wnioski musimy pokazać, że tak otrzymane dywizory są liniowo niezależne. W tym celu konstruujemy automorfizmy ciał funkcyjnych, które indukują odwzorowania na naszych krzywych i ich jakobianach.

Teraz rozważmy krzywe supereliptyczne zadane równaniem afinicznym

$$C_{p,m,a} : \ y^p = x^m(x+a),$$

gdzie p jest liczbą pierwszą, $m \in \mathbb{N}$, $a \in \mathbb{Z} \setminus \{0\}$ i (bez straty ogólności) $0 < m < p-1$. Odnotujmy, że $C_{p,m,a}$ jest biwymiernie równoważna z krzywą $C_{a,s}(p)$ (daną przez (19)) dla pewnego $s \in \{1, \ldots, p-2\}$ (por. [34]). W związku z tym, na mocy (21), $C_{p,m,a}$ jest ilorazem skręconej krzywej Fermata $F_a(p)$ i ma automorfizm $(x,y) \mapsto (x, \zeta_p y)$. Jej jakobian $J_{p,m,a}$ ma mnożenie zespolone przez $\mathbb{Q}(\zeta_p)$. Zauważmy, że genus $C_{p,m,a}$ wynosi $(p-1)/2$.

Dla danego $D \in \mathbb{Z}\setminus\{0\}$, które nie jest p-tą potęgą możemy rozważać p-skręcenie $C_{p,m,a}$ zadane równaniem $C_{p,m,a}^{(D)} : \ Dy^p = x^m(x+a)$. Jesteśmy zainteresowani znalezieniem wartości $D \in \mathbb{Z}$ takich, że p-skręcenia krzywych $C_{p,m,a}$ i $C_{p,m,b}$ przez D mają punkty wymierne. To okazuje się łatwe. Trudniejszym i ciekawszym problemem jest wyznaczenie części torsyjnej jakobianu $J_{p,m,a}$ krzywej $C_{p,m,a}$. Jasne, że ta wiedza jest użyteczna w dowodzie, że pewne dywizory mają rząd nieskończony w $J_{p,m,a}$. Teraz przystępujemy do charakteryzacji $J_{p,m,a}(\mathbb{Q})_{tors}$. Po pierwsze, łatwo zobaczyć, że $\#C_{p,m,a}(\mathbb{F}_{l^n}) = l^n + 1$, gdy $p \nmid l^n - 1$. Następnie używając lematu 2.4 i technik podobnych jak w pracach dotyczących krzywych hipereliptycznych dostajemy.

Twierdzenie 3.7. *Dla powyższych p, m, a mamy $\mathbb{Z}/p\mathbb{Z} \subset J_{p,m,a}(\mathbb{Q})_{tors} \subset \mathbb{Z}/2p\mathbb{Z}$.*

Problem istnieniu elementu rzędu 2 w $J_{p,m,a}(\mathbb{Q})$ jest bardziej skomplikowany. Gross i Rohrlich [34] pokazali, że jakobian krzywej $y^p = x^m(1-x)^k$ ma $\mathbb{Q}$-wymierny punkt rzędu 2 wtedy i tylko wtedy, gdy $p = 7$ i $m^3 \equiv k^3 \equiv -(m+k)^3 \pmod 7$. Podamy warunek wystarczający na nieistnienie takiego punktu w jakobianie $J_{p,m,a,k}$ krzywej

$$C_{p,m,a,k} : y^p = x^m(a-x)^k,$$

gdzie $0 < m, k$ i $m + k < p$. Bez straty ogólności (z powodu biwymiernej równoważności) można założyć, że $m = 1$ i $0 < k < p-1$ (por. [34, p. 207]). Zauważmy, że (po oczywistych zamianach zmiennych) $C_{p,m,a,1} = C_{p,m,a}$, a $C_{p,m,1,k}$ jest krzywą badaną przez Grossa i Rohrlicha.

Niech l będzie liczbą pierwszą, w której krzywa $C_{p,m,a,k}$ ma dobrą redukcję czyli $l \neq p$ i $l \nmid a$. Wtedy, na mocy (17), $\#J_{p,m,a,k}(\mathbb{Q})_{tors} \,|\, \#J_{p,m,a,k}(\mathbb{F}_l)$. Zatem warto wyznaczyć funkcję zeta krzywej $C_{p,m,a,k}$ nad $\mathbb{F}_l$. W tym celu wprowadźmy pewne oznaczenia. Dla ideału pierwszego $\mathfrak{l}$ w $\mathbb{Z}[\zeta_p]$ leżącego nad l, niech $\chi_{\mathfrak{l}}$ będzie symbolem reszty p-tego stopnia (p-power residue symbol) modulo $\mathfrak{l}$ tj. charakterem grupy $(\mathbb{Z}[\zeta_p]/\mathfrak{l})^\times$ o wartościach w $\mu_p := <\zeta_p>$ zadanym wzorem

$$\chi_{\mathfrak{l}}(\alpha) = \zeta_p^k \Longleftrightarrow \alpha^{\frac{N\mathfrak{l}-1}{p}} \equiv \zeta_p^k \pmod{\mathfrak{l}}.$$

Rozważmy sumę Jacobiego

$$\tau_{m,k}(\mathfrak{l}) := -\sum_{\alpha \in (\mathbb{Z}[\zeta_p]/\mathfrak{l}) \setminus \{0,1\}} \chi_{\mathfrak{l}}^m(\alpha)\chi_{\mathfrak{l}}^k(1-\alpha).$$

Odnotujmy, że $\tau_{m,k}(\mathfrak{l}) \in \mathbb{Z}[\zeta_p]$ i ma wartość bezwzględną $N(\mathfrak{l})^{1/2}$ w każdym zespolonym zanurzeniu. Wówczas zachodzi następujący wzór.

Lemat 3.8. *Niech $Z(C_{p,m,a,k}, \mathbb{F}_l, T)$ będzie funkcją zeta krzywej $C_{p,m,a,k}$ nad $\mathbb{F}_l$. Mamy*

$$Z(C_{p,m,a,k}, \mathbb{F}_l, T) = \frac{P_l(T)}{(1-T)(1-lT)},$$

gdzie

$$P_l(T) = \prod_{\mathfrak{l}|l}(1 - \chi_{\mathfrak{l}}^{m+k}(a)\tau_{m,k}(\mathfrak{l})T^f),$$

a iloczyn jest brany po wszystkich ideałach pierwszych w $\mathbb{Z}[\zeta_p]$ leżących nad l i f jest rzędem l w grupie $(\mathbb{Z}/p\mathbb{Z})^*$.

Następnie używając charakteryzacji Deligne'a [21] zwyczajnych (ordinary) rozmaitości abelowych w terminach wielokątów Newtona oraz wyników Grossa i Rohrlicha [34] dostajemy.

Twierdzenie 3.9. *Jeśli a jest nieparzyste i $p \neq 7$, to $J_{p,m,a,k}(\mathbb{Q})$ nie ma elementu rzędu 2.*

Przypomnijmy, że rozmaitość abelową A wymiaru g określoną nad ciałem K charakterystyki $l > 0$ jest *zwyczajna*, gdy $A(\bar{K})_{l-torsion} \cong (\mathbb{Z}/l\mathbb{Z})^g$.

W przypadku parzystego a grupa $J_{p,m,a,k}(\mathbb{Q})$ może posiadać punkt rzędu 2. Przypomnijmy, że krzywe $C_{p,1,a,k}$ są hipereliptyczne dla $k = 1, (p-1)/2, p-2$.

Twierdzenie 3.10. *Grupa $J_{p,1,a,1}(\mathbb{Q})$ ma element rzędu 2 wtedy i tylko wtedy, gdy $a = 2$. Grupy $J_{p,1,a,(p-1)/2}(\mathbb{Q})$ i $J_{p,1,a,p-2}(\mathbb{Q})$ mają punkt rzędu 2 wtedy i tylko wtedy, gdy $a = 2^{p-2}$ (tu zakładamy bez straty ogólności, że a jest liczbą całkowitą wolną od p-tych potęg).*

Z twierdzeń 3.7, 3.9 otrzymujemy

Wniosek 3.11. *Niech a, b będą nieparzystymi liczbami całkowitymi. Rozważmy krzywe supereliptyczne*

$$C_1 : y^p = x^m(x+a), \quad C_2 : y^p = x^m(x+b),$$

gdzie p jest liczbą pierwszą różna od 2 i 7 oraz $0 < m < p-1$. Wówczas istnieje funkcja wymierna $D_{p,p} \in \mathbb{Z}(u,v,w,t)$ taka, że jakobiany p-skręceń krzywych C_1, C_2 przez $D_{p,p}(u,v,w,t)$ mają dodatnią rangę nad ciałem $\mathbb{Q}(u,v,w,t)$.

Proponujemy pewne pytania i hipotezę, które naturalnie pojawiają się w kontekście naszej pracy.

Pytanie 3.12. *Załóżmy, że $f \in \mathbb{Q}[x]$ nie ma wielokrotnych pierwiastków. Niech $b, c \in \mathbb{Z} \setminus \{0\}$ i m będzie nieparzystą liczbą naturalną. Rozważmy krzywe hipereliptyczne dane przez (22). Czy jest możliwe znalezienie funkcji wymiernej $D \in \mathbb{Q}(u_1, \ldots, u_k)$ dla pewnego k takiej, że jakobian kwadratowego skręcenia C_1, jakobian m-skręcenia C_2 i jakobian $2m$-skręcenia C_3 przez D ma jednocześnie dodatnią rangę nad $\mathbb{Q}(u_1, \ldots, u_k)$?*

Pytanie 3.13. *Dla jakich liczb naturalnych m i liczb pierwszych p układ równań*

$$\frac{x_1^m(x_1+a_1)}{y_1^p} = \frac{x_2^m(x_2+a_2)}{y_2^p} = \frac{x_3^m(x_3+a_3)}{y_3^p}$$

ma wymierne rozwiązanie x_i, y_i spełniające warunek $x_i y_i (x_i - a_i) \neq 0$ dla $i = 1,2,3$ i dla dowolnych $a_1, a_2, a_3 \in \mathbb{Z} \setminus \{0\}$?

Pytanie 3.14. *Załóżmy, że $p > 5$ jest liczbą pierwszą, a jest parzyste (i bez straty ogólności wolne od p-tych potęg) i $k \in \{2, ..., p-3\} \setminus \{\frac{p-1}{2}\}$. Dla jakich takich p, a i k grupy $J_{p,1,a,k}(\mathbb{Q})$ mają element rzędu 2?*

Odnotujmy, że dla powyższych p, a i k krzywe $C_{p,1,a,k}$ nie muszą być hipereliptyczne i mają złą redukcję w 2. Dlatego metody z dowodów twierdzeń 3.9 i 3.10 nie działają. Takie krzywe o najmniejszym genusie (równym 3) to $C_{7,1,a,2} : y^7 = x(a-x)^2$ i $C_{7,1,a,4} : y^7 = x(a-x)^4$. Obliczenia numeryczne sugerują następującą hipotezę.

Hipoteza 3.15. *Załóżmy, że p, a i k są takie jak w pytaniu 3.14. Jeśli l jest liczbą pierwszą taką, że $l \equiv 1 \pmod{p}$, $l \nmid a$ i a nie jest p-tą potęga w $\mathbb{F}_l^*$, to grupa $J_{p,1,a,k}(\mathbb{F}_l)$ ma nieparzysty rząd. W konsekwencji grupa $J_{p,1,a,k}(\mathbb{Q})$ nie ma punktu rzędu 2.*

3.2 Artykuł [A4]

W tym artykule rozważamy trójparametrową rodzinę krzywych supereliptycznych

$$C^{q,p,a} : y^q = x^p + a, \tag{23}$$

gdzie q i p są różnymi nieparzystymi liczbami pierwszymi i a jest niezerową liczbą wymierną. Te krzywe i ich jakobiany $J^{q,p,a}$ są naturalnym ogólnieniem krzywych eliptycznych E^a oraz krzywych hipereliptycznych $C^{p,a}$ i ich jakobianów $J^{p,a}$. Dokładnie mamy, $C^{2,3,a} = E^a$ i $C^{2,p,a} = C^{p,a}$. W pewnym sensie są one także uogólnieniem krzywych typu Fermata $F_p(a)$.

Naszym celem jest opisanie części torsyjnej $J^{q,p,a}(\mathbb{Q})$. Podamy częściową charakteryzację $J^{q,p,a}(\mathbb{Q})_{tors}$ i kompletną dla $J^{3,5,a}(\mathbb{Q})_{tors}$. Głównymi składnikami dowodów jest wyprowadzenie jawnych wzorów na funkcje zeta krzywych $C^{q,p,a}$ nad $\mathbb{F}_l$ (i w konsekwencji na $\#J^{q,p,a}(\mathbb{F}_l)$) dla $l \equiv -1 \pmod{qp}$ i dla $l \equiv 1, 2, 4, 8, 11 \pmod{15}$, gdy $q = 3, p = 5$, (co samo w sobie jest interesujące i może mieć inne zastosowania), stosowanie twierdzeń o gęstości (np. lematu 2.11) i wyniku Iwańca [40].

Bez straty ogólności będziemy zakładać, że $q < p$ i $a \in \mathbb{Z} \setminus \{0\}$ jest wolne od pq-tych potęg. Genus g krzywej $C^{q,p,a}$ wynosi $\frac{(q-1)(p-1)}{2}$. Zauważmy, że wyróżnik wielomianu

$x^p + a$ jest równy $(-1)^{(p-1)/2} p^p a^{p-1}$, zatem krzywa $C^{q,p,a}$ ma dobrą redukcję w liczbach pierwszych nie dzielących qpa. W konsekwencji w takich liczbach pierwszych l jakobian $J^{q,p,a}$ też ma dobrą redukcję oraz na mocy (17) mamy

$$\#J^{q,p,a}(\mathbb{Q})_{tors} \,|\, \#J^{q,p,a}(\mathbb{F}_l)\,. \tag{24}$$

Najpierw wypiszemy warunki wystarczające na istnienie elementów rzędów p i q w $J^{q,p,a}(\mathbb{Q})$ (dowody opierają się na twierdzeniu Riemanna-Rocha).

Stwierdzenie 3.16. *Jeśli a jest p-tą potęgą, to $J^{q,p,a}(\mathbb{Q})$ zawiera podgrupę rzędu q. Dokładniej, niech $a = b^p$. Wtedy $\mathbb{Q}$-wymierny dywizor $(-b, 0) - \infty$ reprezentuje element rzędu q w jakobianie $J^{q,p,a}(\mathbb{Q})$.*

Stwierdzenie 3.17. *Jeśli a jest q-tą potęgą, to $J^{q,p,a}(\mathbb{Q})$ zawiera podgrupę rzędu p. Dokładniej, niech $a = c^q$. Wtedy $\mathbb{Q}$-wymierny dywizor $(0, c) - \infty$ reprezentuje element rzędu p w jakobianie $J^{q,p,a}(\mathbb{Q})$.*

Stwierdzenie 3.18. *Jeśli a jest pq-tą potęgą, to $J^{q,p,a}(\mathbb{Q})$ zawiera podgrupę rzędu pq. Dokładniej, niech $a = d^{pq}$. Wtedy $\mathbb{Q}$-wymierny dywizor $(-d^q, 0) + (0, d^p) - 2\infty$ reprezentuje element rzędu pq w jakobianie $J^{q,p,a}(\mathbb{Q})$.*

Następnie pokażemy, że (przynajmniej dla $q = 3$ i $p = 5$) powyższe warunki są również konieczne. Ponieważ zachodzi (24), więc w celu charakteryzacji $J^{q,p,a}(\mathbb{Q})_{tors}$ wyznaczymy funkcje zeta krzywych $C^{q,p,a}$ nad ciałami $\mathbb{F}_l$ dla liczb pierwszych l dobrej redukcji. Na mocy lematu 2.9, mamy ogólny ("niejawny") wzór na liczbę punktów w $C^{q,p,a}(\mathbb{F}_{l^k})$ w terminach sum Jacobiego (lub Gaussa). W związku z tym otrzymamy takiż wzór na funkcję zeta $C^{q,p,a}$ nad $\mathbb{F}_l$, i na $\#J^{q,p,a}(\mathbb{F}_l)$. Dla pewnych klas reszt l modulo qpa możemy wyznaczyć bardziej "jawne" wzory, na przykład.

Stwierdzenie 3.19. *Jeśli liczba pierwsza $l \equiv -1 \pmod{pq}$ i $l \nmid a$, to funkcja zeta $C^{q,p,a}$ nad $\mathbb{F}_l$ ma postać*

$$Z(C^{q,p,a}/\mathbb{F}_l, X) = \frac{\left(1 + lX^2\right)^g}{(1 - X)\,(1 - lX)},$$

gdzie $g = (p-1)\,(q-1)\,/2$ jest genusem of $C^{q,p,a}$. W szczególności $\#J^{q,p,a}(\mathbb{F}_l) = (1 + l)^g$.

Dowód wykorzystuje własności charakterów i czystych sum Gaussa. Teraz możemy udowodnić nasz pierwszy główny wynik.

Twierdzenie 3.20. *Mamy $J^{q,p,a}(\mathbb{Q})_{tors} \simeq (\mathbb{Z}/2\mathbb{Z})^{e_2} \times (\mathbb{Z}/q\mathbb{Z})^{e_q} \times (\mathbb{Z}/p\mathbb{Z})^{e_p}$, gdzie $e_2, e_q, e_p \in \{0, 1, \ldots, (p-1)\,(q-1)\,/2\}$. Ponadto jeśli a jest p-tą potęgą, to $e_q > 0$, a jeśli a jest q-tą potęgą, to $e_p > 0$.*

Aby udowodnić następne główne rezultaty tej pracy musimy znaleźć "jawne" wzory na sumy Jacobiego. W tym celu używamy relacji Stickelbergera w ciałach cyklotomicznych $\mathbb{Q}(\zeta_{qp})$, gdzie $\zeta_n = \exp\left(\frac{2\pi i}{n}\right)$ (po szczegóły odsyłamy do [A4, ss. 410-411]). W konsekwencji dostajemy.

Twierdzenie 3.21. *Załóżmy, że $2^n \equiv -1 \pmod{qp}$ dla pewnego n lub rząd 2 w $(\mathbb{Z}/qp\mathbb{Z})^*$ wynosi $\frac{(q-1)(p-1)}{2}$. Wówczas $e_2 = 0$ dla dowolnego nieparzystego a.*

Odnotujmy, że wśród par liczb pierwszych (q, p), gdzie $2 < q < p < 1000$ około 37% spełnia założenia twierdzenia 3.21.

Od tej pory załóżmy, że $q = 3$. W tym przypadku możemy polepszyć Twierdzenie 3.20. Opierając się na kongruencjach modulo p współczynników licznika funkcji zeta $Z(C^{3,p,a}/\mathbb{F}_l, X)$ wnioskujemy, że $p \nmid \#J^{3,p,a}(\mathbb{F}_l)$, gdy $l \equiv 1 \pmod{3p}$ i a nie jest sześcianem modulo l. Wtedy używając lematu 2.11 otrzymamy.

Twierdzenie 3.22. *Załóżmy, że $q = 3$. Wówczas $e_p > 0$ wtedy i tylko wtedy, gdy a nie jest sześcianem (w $\mathbb{Z}$).*

Od tej pory załóżmy jeszcze, że $p = 5$. Podamy kompletny opis $J^{3,5,a}(\mathbb{Q})_{tors}$. W tym celu wyznaczymy (jawnie tzn. w terminach kwadratowych partycji liczby pierwszej l) rząd grupy $J_{3,5,a}(\mathbb{F}_l)$ dla $l \equiv 2, 4, 8, 11 \pmod{15}$. W przypadku $l \equiv 4, 11 \pmod{15}$ używamy rezultatów Friesena i innych [28] o liczbach cyklotomicznych rzędu 15. Dla $l \equiv 2, 8 \pmod{15}$ nasze wyliczenia to nowy wynik (korzystamy z relacji Stickelbergera i arytmetyki ciała $\mathbb{Q}(\zeta_{15})$). Poniżej wypisujemy przykładowy, interesujący wzór na funkcję zeta dla $C^{3,5,a}$.

Stwierdzenie 3.23. *Załóżmy, że $l \equiv 2, 8 \pmod{15}$. Wówczas $l = 3u^2 + 5v^2$ dla pewnych jedynych liczb naturalnych u, v oraz*

$$Z(C^{3,5,a}/\mathbb{F}_l, X) = \frac{1 + 2l\left(3u^2 - 5v^2\right)X^4 + l^4X^8}{(1 - X)(1 - lX)}.$$

W szczególności

$$\#J^{3,5,a}(\mathbb{F}_l) = 1 + 2l\left(3u^2 - 5v^2\right) + l^4.$$

Odnotujmy, że powyższy wzór został użyty w [18], aby otrzymać rodzinę p.f. (pairing-friendly) krzywych supereliptycznych genusu 4 z zadanym stopniem zanurzenia (embedding degree). Takie krzywe i ich jakobiany mogą być przydatne w kryptografii (zobacz np. [18], [27] oraz bibliografię tamże).

Następnie stosując parę razy twierdzenie Czebotariewa o gęstości (lemat 2.11) i rezultat Iwańca [40], dostajemy ostatni główny wynik artykułu.

Twierdzenie 3.24. *Dla $a \in \mathbb{Z} \setminus \{0\}$ mamy*

$$J^{3,5,a}(\mathbb{Q})_{tors} \cong \begin{cases} \{0\} & \text{jeśli } a \text{ nie jest sześcianem, ani piątą potęgą,} \\ \mathbb{Z}/3\mathbb{Z} & \text{jeśli } a \text{ nie jest sześcianem, ale jest piątą potęgą,} \\ \mathbb{Z}/5\mathbb{Z} & \text{jeśli } a \text{ jest sześcianem, ale nie jest piątą potęgą,} \\ \mathbb{Z}/15\mathbb{Z} & \text{jeśli } a \text{ jest sześcianem i jest piątą potęgą.} \end{cases}$$

Zauważmy piękną analogię powyższych wyników i wzoru (4) dla $E^a(\mathbb{Q})_{tors}$ oraz twierdzenia 2.20 o $J^{p,a}(\mathbb{Q})_{tors}$.

Wierzymy w prawdziwość następujących hipotez (przynajmniej obliczenia numeryczne w MAGMA to sugerują).

Hipoteza 3.25. *Mamy*

$$J^{q,p,a}(\mathbb{Q})_{tors} \simeq (\mathbb{Z}/q\mathbb{Z})^{e_q} \times (\mathbb{Z}/p\mathbb{Z})^{e_p},$$

gdzie $e_q, e_p \in \{0, 1\}$.

Hipoteza 3.26. *Ustalmy a, q i p. Jeśli a nie jest p-tą potęgą, to $e_q = 0$. Jeśli a nie jest q-tą potęgą, to $e_p = 0$.*

W konsekwencji.

Hipoteza 3.27. *Dla dowolnych liczb pierwszych $p > q > 2$ i $a \in \mathbb{Z} \setminus \{0\}$ mamy*

$$J^{q,p,a}(\mathbb{Q})_{tors} \cong \begin{cases} \{0\} & \text{jeśli } a \text{ nie jest } p\text{-tą potęgą, ani } q\text{-tą potęgą} \\ \mathbb{Z}/q\mathbb{Z} & \text{jeśli } a \text{ jest } p\text{-tą potęgą, ale nie jest } q\text{-tą potęgą,} \\ \mathbb{Z}/p\mathbb{Z} & \text{jeśli } a \text{ jest } q\text{-tą potęgą, ale nie jest } p\text{-tą potęgą,} \\ \mathbb{Z}/qp\mathbb{Z} & \text{jeśli } a \text{ jest } p\text{-tą potęgą i jest } q\text{-tą potęgą.} \end{cases}$$

3.3 Artykuł [A6]

W tym artykule badamy te same krzywe $C^{q,p,a}$ i ich jakobiany $J^{q,p,a}$ co w [A4]. Tutaj polepszymy twierdzenia 3.20, 3.21, co znacznie nas przybliża do dowodu hipotezy 3.25. Teraz przedstawimy główne rezultaty (zachowujemy oznaczenia z 3.20).

Twierdzenie 3.28. *Mamy* $e_2, e_q, e_p \in \{0, 1\}$.

Twierdzenie 3.29. *Jeśli a jest nieparzyste, to* $e_2 = 0$.

W dowodach obu twierdzeń mocno wykorzystujemy własności rozmaitości abelowych z mnożeniem zespolonym. Zauważmy, że jakobian $J^{q,p,a}$ ma mnożenie zespolone przez $\mathbb{Q}(\zeta_{qp})$. Istotnie, odwzorowanie $(x, y) \mapsto (\zeta_p x, \zeta_q y)$ określa automorfizm na $C^{q,p,a}$ i indukuje endomorfizm $\iota(\zeta_{qp}) \in End(J^{q,p,a})$. W związku z tym otrzymujemy izomorfizm $\iota : K \to End(J^{q,p,a}) \otimes \mathbb{Q}$, gdzie $K := \mathbb{Q}(\zeta_{qp})$ jest ciałem cyklotomicznym (więc też CM ciałem). Skoro $[K : \mathbb{Q}] = (q-1)(p-1) = 2\dim(J^{q,p,a})$, to jakobian $J^{q,p,a}$ jest CM rozmaitością abelową. Ponadto ta rozmaitość abelowa jest absolutnie prosta (por. [36]) i $End(J^{q,p,a}) \cong \mathbb{Z}[\zeta_{qp}]$ (= pierścień liczb algebraicznych całkowitych ciała K). Zauważmy także, że K ma dokładnie $2qp$ pierwiastków z jedynki, zatem na mocy [1, Corollary 8.8], dostajemy $J^{q,p,a}(\mathbb{Q})_{tors} \subset \mathbb{Z}/2qp\mathbb{Z}$, co dowodzi twierdzenia 3.28.

Aby udowodnić twierdzenie 3.29 potrzebujemy dwóch poniższych lematów.

Lemat 3.30. *Jeśli* $\mathbb{Z}/2\mathbb{Z} \subset J^{q,p,a}(\mathbb{Q})$, *to* $(\mathbb{Z}/2\mathbb{Z})^{(q-1)(p-1)} \subset J^{q,p,a}(K)$.

Lemat 3.31. *Jeśli a jest nieparzyste, to* $J^{q,p,a}$ *nie jest zwyczajny nad* $\mathbb{F}_2$.

Dowód lematu 3.30 przebiega analogicznie jak dowód lematu 1.3 w [34]. By udowodnić lemat 3.31 najpierw zauważmy, że skoro a jest nieparzyste, to $J^{q,p,a}$ ma dobrą redukcję w 2. Na mocy kryterium Deligne'a (patrz [21]) rozmaitość abelowa jest zwyczajna nad $\mathbb{F}_l$ wtedy i tylko wtedy, gdy nachylenia (slopes) w wielokącie Newtona wielomianu charakterystycznego endomorfizmu Frobeniusa są równe 0 lub 1. Pokazujemy (używając uogólnienia na rozmaitości abelowe kryterium redukcyjnego Deuringa udowodnionego przez Blake'a [5]), że przynajmniej jedno nachylenie dla $J^{q,p,a}$ nad $\mathbb{F}_2$ nie jest ani 0, ani 1. Teraz by zakończyć dowód twierdzenia 3.29 przypuśćmy niewprost, że $J^{q,p,a}(\mathbb{Q})$ ma element rzędu 2. Niech $\mathfrak{l}$ będzie ideałem pierwszym $\mathbb{Z}[\zeta_{qp}]$ leżącym nad 2. Na mocy lematu 3.30 dostajemy, że $(\mathbb{Z}/2\mathbb{Z})^{(q-1)(p-1)} \subset J_{q,p,a}(K_\mathfrak{l})$, gdzie $K_\mathfrak{l}$ jest uzupełnieniem ciała K względem normy odpowiadającej ideałowi $\mathfrak{l}$. Ponieważ $K_\mathfrak{l}$ jest nierozgałęzionym rozszerzeniem $\mathbb{Q}_2$, więc na mocy [34, Lemma 1.4] $J_{q,p,a}$ musi być zwyczajny nad $\mathbb{F}_2$, co przeczy lematowi 3.31.

Oczywiście ta metoda zawodzi, gdy a jest parzyste, ale wydaje się, że zawsze $e_2 = 0$.

4 Omówienie pozostałego dorobku naukowego w kolejności chronologicznej

4.1 Artykuł [B1]

W tym artykule rozważamy problem istnienia trzech punktów o całkowitych współrzędnych P_0, P_1, P_2 w globalnym minimalnym modelu krzywych eliptycznych Fermata $E_m : x^3+y^3 = m$, których pierwsze współrzędne $x_i = x(P_i)$ tworzą rosnący ciąg arytmetyczny (mówimy wtedy, że P_0, P_1, P_2 tworzą całkowity postęp arytmetyczny). Ten problem był badany przez Bremnera, Silvermana i Tzanakisa w [7] dla krzywych eliptycznych związanych z liczbami kongruentnymi (29).

Zauważmy, że całkowitość x-owych współrzędnych może zależeć od wyboru równania definiującego krzywą eliptyczną, ale nie zależy od wyboru globalnego równania minimalnego.

Używając algorytmu Tate'a [78] dostajemy

Stwierdzenie 4.1. *Globalny minimalny model Weierstrassa $E_m^{\min}$ krzywej E_m ma postać:*

(i) $y^2 = x^3 - \frac{27}{4}m^2$ *jeśli* $2 \mid m$ *i* $9 \nmid m$,
(ii) $y^2 + y = x^3 - \frac{27m^2+1}{4}$ *jeśli* $2 \nmid m$ *i* $9 \nmid m$,
(iii) $y^2 = x^3 - \frac{3m'^2}{4}$ *jeśli* $2 \mid m$ *i* $9 \mid m$,
(iv) $y^2 + y = x^3 - \frac{3m'^2+1}{4}$ *jeśli* $2 \nmid m$ *i* $9 \mid m$,

gdzie $m' = \frac{m}{9}$.

Główny wynik jest następujący.

Twierdzenie 4.2. *Załóżmy, że* $m \equiv 0, \pm 3, \pm 4 (\mathrm{mod}\, 9)$ *oraz jej każdy dzielnik pierwszy* $p > 3$ *spełnia* $p \equiv 5 (\mathrm{mod}\, 6)$. *Niech* $A \subset E_m^{\min}(\mathbb{Q})$ *będzie podgrupą rangi 1. Wówczas A nie zawiera całkowitych postępów arytmetycznych.*

Lang [50] sformułował hipotezę, która mówi, że kanoniczna wysokość nietorsyjnego punktu P krzywej eliptycznej E spełnia $\widehat{h}(P) >> \log|\Delta_E|$. Połóżmy $\beta_E := \frac{\log|\Delta_E|}{\log N_E}$ (Δ_E oznacza wyróżnik krzywej eliptycznej E, a N_E - jej przewodnik). Hindry i Silverman [38] udowodnili oszacowanie $\widehat{h}(P) \geq c(\beta_E) \log|\Delta_E|$, gdzie $c(\beta_E) = (20\beta_E)^{-8} 10^{-1.1-4\beta_E}$. W związku z tym hipoteza Langa zachodzi dla rodzin krzywych eliptycznych ze wspólnie ograniczonym β_E.

Nietrudno można policzyć, że $\beta_{E_m} \leq \beta_{E_{25}} \leq 4.2028$, stąd $\widehat{h}_{E_m}(P) \geq 4.921 \times 10^{-34} \times \log|\Delta_{E_m}|$ (w artykule [B1] jest omyłkowo inna liczba). Udowodniliśmy znacznie mocniejsze nierówności w rodzinie E_m.

Twierdzenie 4.3. *Dla* $P \in E_m(\mathbb{Q}) \setminus \{\infty\}$ *($m > 2$ wolne od sześcianów) mamy*

$$\widehat{h}_{E_m}(P) \geq \left(\frac{1}{432} - \frac{\log 2}{1404 \log 3}\right) \log\left|\Delta_{E_m^{\min}}\right| \geq 0.0018654 \log|\Delta_{E_m}|.$$

Dowody obu rezultatów odwołują się do trudnej analizy wysokości lokalnych $\widehat{h}_p : E(\mathbb{Q}_p) \to \mathbb{R}$ (ich definicje i podstawowe własności można znaleźć w [72]) w przypadkach zależnych od czynników Tamagawy krzywej E_m w liczbach pierwszych.

Odnotujmy, że nasze analizy i oszacowania wysokości lokalnych zostały mocno wykorzystane przez Everesta, Ingrama i Shauna [22] do pokazania, że dla dowolnego nietorsyjnego punktu na krzywej E_m, wszystkie wyrazy stowarzyszonych eliptycznych ciągów podzielnych (elliptic divisibility sequences), z wyjątkiem pierwszego, mają pierwotny dzielnik. Jako wniosek udowodnili oni, że jeśli m jest wolne od sześcianów i $\mathrm{rank}(E_m(\mathbb{Q})) = 1$, to E_m ma co najwyżej dwa punkty całkowite i każdy z nich generuje $E_m(\mathbb{Q})$. Ten wynik został uogólniony na przypadek $\mathrm{rank}(E_m(\mathbb{Q})) > 1$ przez Fujita i Nara [30]. Oni także polepszyli nasze oszacowanie wysokości punktów w hipotezie Langa. Z kolei Voutier i Yabuta [85] rozważali ogólniejsze krzywe, mianowicie $y^2 = x^3 + b$, gdzie $b \in \mathbb{Z}$ jest wolne od szóstych poteg (odnotujmy, że E_m mają również równania tej postaci z $b = -432m^2$). Autorzy badali hipotezę Langa w tej rodzinie i uzyskali prawie najlepsze oszacowania.

4.2 Artykuł [B2]

Mai pokazał w [53], że zbiór wolnych od sześcianów liczb naturalnych a, dla których liczba pierwiastkowa (root number) krzywej $E_a : x^3 + y^3 = a$ jest dodatnia (równa 1), ma gęstość 1/2. Hipoteza o parzystości (parity conjecture) implikuje, że w tej rodzinie (skręceń sześciennych krzywej eliptycznej Fermata $x^3+y^3 = 1$) ranga grupy $\mathbb{Q}$-wymiernych punktów E_a jest parzysta dla połowy wolnych od sześcianów liczb naturalnych a.

W tym artykule dowodzimy analogicznego rezultatu dla rodziny krzywych typu Fermata $F_a(5) : x^5 + y^5 = a$. W istocie pokazujemy coś ogólniejszego. Wprowadźmy pewne oznaczenia. Niech $\mathbb{N}^{(p)} = \{a \in \mathbb{N} : p \nmid a,\ a \text{ jest wolna od } p\text{-tych potęg}\}$. Dla $a \in \mathbb{N}^{(p)}$ połóżmy $\tau_p(a) = \#\{q \in \mathbb{P} : q > 2,\ q|a,\ \left(\frac{q}{p}\right) = -1\}$. Niech $W_{a,p}$, $W_{a,p}^A$, $W_{a,p}^B$ oznaczają

(globalne) liczby pierwiastkowe (innymi słowy, znak równania funkcyjnego odpowiednich L-funkcji) krzywych $F_a(p)$, $A_{a,p}$, $B_{a,p}$ (danych przez (18), (20)) odpowiednio. Okazuje się, że liczby $W^A_{a,p}$, $W^B_{a,p}$ zależą tylko (przy ustalonych p i a) od parzystości $\tau_p(a)$ i reszty a modulo p^2 (zob. [75]). Nasz główny wynik jest następujący.

Twierdzenie 4.4. *Zbiory* $\left\{a \in \mathbb{N}^{(p)} : W^A_{a,p} = 1\right\}$, $\left\{a \in \mathbb{N}^{(p)} : W^B_{a,p} = 1\right\}$ *mają gęstość* $\frac{1}{2}$ *w zbiorze* $\mathbb{N}^{(p)}$.

Wobec izogenii (21) mamy $W_{a,5} = \left(W^A_{a,5}\right)^2 W^B_{a,5} = W^B_{a,5}$, zatem otrzymujemy

Wniosek 4.5. *Zbiór* $\left\{a \in \mathbb{N}^{(5)} : W_{a,5} = 1\right\}$ *ma gęstość* $\frac{1}{2}$ *w* $\mathbb{N}^{(5)}$.

Głównym składnikiem dowodu jest lemat dotyczący oszacowania pewnych sum charakterów. Dokładniej, udowodniliśmy następujący.

Lemat 4.6. *Dla dowolnego charakteru Dirichleta* χ *o przewodniku* k *mamy*

$$\sum_{a \in \mathbb{N}^{(p)}_X} (-1)^{\tau_p(a)} \chi(a) = O\left(\sqrt{X} \log^{p-2} X \sqrt{k} \log k\right),$$

gdzie $\mathbb{N}^{(p)}_X = \left\{a \in \mathbb{N}^{(p)} : a \leq X\right\}$.

4.3 Artykuł [B3]

K. Rubin i A. Silverberg pokazali w [65], że nieograniczoność rang skręceń kwadratowych krzywej eliptycznej jest równoważna z rozbieżnością pewnych szeregów nieskończonych. W tym artykule udowodnimy analogiczny wynik dla rodziny jakobianów skręconych krzywych Fermata $F_a(p) : x^p + y^p = a$, gdzie p jest ustaloną nieparzystą liczbą pierwszą i a przebiega zbiór przebiega zbiór liczb naturalnych wolnych od p-tych potęg.

Ustalmy niezerową liczbę całkowitą a' taką, że $F_{a'}(p)(\mathbb{Q}) \neq \emptyset$ i wybierzmy $\alpha \in \overline{\mathbb{Q}}$ spełniająca $\alpha^p = \frac{a}{a'}$. Mamy wtedy izomorfizm (określony nad $\mathbb{Q}(\alpha)$) $\varphi : F_a(p) \to F_{a'}(p)$, $\varphi([x,y,z]) = [x,y,\alpha z]$. Indukuje on izomorfizm jakobianów $\varphi : J_a(p) \to J_{a'}(p)$.

Niech $D^p_{a'} \in Div(J_{a'}(p))$ będzie ustalonym symetrycznym, dodatnim dywizorem określonym nad $\mathbb{Q}$. Niech $\hat{h}^p_a : J_a(p)(\overline{\mathbb{Q}}) \to \mathbb{R}$ będzie kanoniczną wysokością względem dywizora $3\varphi^\star D^p_{a'}$. W szczególności $\hat{h}^p_a$ jest dodatnio określoną formą kwadratową na $J_a(p)(\mathbb{Q})$ modulo torsja. Dla nieujemnych liczb rzeczywistych i oraz j definiujemy szereg nieskończony

$$T_p(i,j) = \sum_{a \in \mathbb{N}'^{(p)}} |a|^{-i} \sum_{P \in J_a(p)(\mathbb{Q}) \setminus J_a(p)(\mathbb{Q})_{tors}} \hat{h}^p_a(P)^{-j},$$

gdzie $\mathbb{N}'^{(p)} = \{a \in \mathbb{N} : a$ jest wolna od p-tych potęg$\}$.

Główny rezultat jest następujący.

Twierdzenie 4.7. *Ustalmy liczbę rzeczywistą* $j > 0$. *Następujące warunki są równoważne: (a)* $\operatorname{rank}(J_a(p)(\mathbb{Q})) < 2j$ *dla dowolnego* $a \in \mathbb{N}'^{(p)}$, *(b)* $T_p(i,j)$ *jest zbieżny dla pewnego* $i \geq 1$, *(c)* $T_p(i,j)$ *jest zbieżny dla każdego* $i \geq 1$, *(d)* $T_p(i,j)$ *jest zbieżny dla* $i = 1$.

Dowód opiera się na trzech własnościach rodziny $J_a(p)$: rząd grup $J_a(p)(\mathbb{Q})_{tors}$ (przy ustalonym p) jest ograniczony, istnieje ograniczenie dolne na wysokość kanoniczną nietorsyjnych punktów w $J_a(p)(\mathbb{Q})$, dla dowolnej nieparzystej liczby pierwszej p istnieje liczba naturalna a_p taka, że $\operatorname{rank}(J_{a_p}(p)(\mathbb{Q})) \geq 2$.

Dla $p = 3$ (tj. dla rodziny $E_a : x^3 + y^3 = a$ skręceń sześciennych krzywej eliptycznej Fermata $E_1 : x^3 + y^3 = 1$ ($a \in \mathbb{Z} \setminus \{0\}$) można udowodnić "jawniejszy" rezultat.

Zauważmy, że E_a ma równanie Weierstrassa $y^2 = x^3 - 432a^2$ (patrz [45], p. 52). Dobrze wiadomo (zobacz [45], Thm. 5.3 lub [71], Ex. 10.19), że $E_1(\mathbb{Q}) = \{\infty, (1,0), (0,1)\}$,

$E_2(\mathbb{Q}) = \{\infty, (1,1)\}$ i $E_a(\mathbb{Q})_{tors} = \{\infty\}$ dla wolnych od sześcianów $a \geq 3$. Również $\mathrm{rank}(E_a(\mathbb{Q})) \geq 1$ wtedy i tylko wtedy, gdy istnieją $k, l, n \in \mathbb{Z} \setminus \{0\}$, $k \neq \pm n$, spełniające $n^3 + k^3 = al^3$.

Dla $q \in \mathbb{Q} \setminus \{0\}$ niech $c(q)$ oznacza wolną od sześcianów część q czyli $q = c(q)r^3$. Połóżmy

$$\Psi = \{(n,k) \in \mathbb{N} \times \mathbb{Z} : (n,k) = 1, nk \neq 0, |n| \neq |k|\}.$$

Dla nieujemnych liczb rzeczywistych i oraz j definiujemy szereg nieskończony

$$S(i,j) = \sum_{(n,k)\in\Psi} c(n^3+k^3)^{-i} \max\{\log(|nk|), \frac{2}{3}\log|\frac{n^3+k^3}{c(n^3+k^3)}|\}^{-j}.$$

Drugi główny wynik jest następujący.

Twierdzenie 4.8. *Ustalmy liczbę rzeczywistą $j > 0$. Następujące warunki są równoważne: (a) $\mathrm{rank}(E_a(\mathbb{Q})) < 2j$ dla dowolnego wolnego od sześcianów $a \in \mathbb{N}$, (b) $S(i,j)$ jest zbieżny dla pewnego $i \geq 1$, (c) $S(i,j)$ jest zbieżny dla każdego $i \geq 1$, (d) $S(i,j)$ jest zbieżny dla $i = 1$.*

Jego dowód wykorzystuje twierdzenie 4.7 oraz własności wysokości naiwnej $h_{xy}(P) = h(f(P))$ i wysokości kanonicznej $\hat{h}_a = \frac{1}{6}\lim_{N\to\infty} \frac{h_{xy}(2^N P)}{4^N}$ na $E_a(\overline{\mathbb{Q}})$ odpowiadających funkcji wymiernej $f \in \overline{\mathbb{Q}}(E_a)$ określonej wzorem $f((x,y)) = xy$.

Później Lee [51] rozważał ogólniejszą rodzinę jakobianów krzywych zadanych przez $f(x,y) = mz^n$, gdzie $f \in \mathbb{Z}[x,y]$ jest nierozkładalną formą kwadratową stonia $n \geq 3$, a m jest liczbą naturalną wolną od n-tych potęg i udowodnił podobny rezultat.

4.4 Artykuł [B4]

Kuwata i Wang w [49] udowodnili, że jeśli E_1, E_2 są krzywymi eliptycznymi nad $\mathbb{Q}$ z j-niezmiennikami $(j(E_1), j(E_2)) \notin \{(0,0), (1728, 1728)\}$, to istnieje wielomian $d(t) \in \mathbb{Q}[t]$ taki, że oba skręcenia kwadratowe E_1, E_2 przez $d(t)$ mają dodatnią rangę nad $\mathbb{Q}(t)$.

W [82] pokazano, że jeśli dopuścimy skręcenia szóstego i czwartego stopnia, to analogiczne rezultaty zachodzą dla par krzywych eliptycznych o j-niezmiennikach 0 i 1728 odpowiednio. W tym artykule rozszerzamy to do pewnych klas krzywych hipereliptycznych.

Twierdzenie 4.9. *Załóżmy $n \in \mathbb{Z}_{\geq 3}$. Dla dowolnych niezerowych $a, b \in \mathbb{Q}$ istnieje wielomian $d(t) \in \mathbb{Q}[t]$ taki, że oba jakobiany krzywych $y^2 = x^n + ad(t)$ i $y^2 = x^n + bd(t)$ mają dodatnią rangę nad $\mathbb{Q}(t)$.*

W istocie dowiedziemy czegoś więcej. Na przykład rozważamy pytanie czy jest możliwe, by wielomian $d(t) \in \mathbb{Q}[t]$ był kwadratem. Ponadto, można polepszyć powyższy wynik do przypadku więcej niż dwóch krzywych:

Twierdzenie 4.10. *Załóżmy, że $n \in \mathbb{Z}_{\geq 3}$. Dla dowolnych niezerowych $a, b, c \in \mathbb{Q}$ istnieje wielomian $d(t) \in \mathbb{Q}[t]$ taki, że jakobiany krzywych $y^2 = x^n + ad(t)$, $y^2 = x^n + bd(t)$ i $y^2 = x^n + cd(t)$ mają jednocześnie dodatnią rangę nad $\mathbb{Q}(t)$.*

Twierdzenie 4.11. *Załóżmy $n \in \mathbb{Z}_{\geq 3}$ jest nieparzyste. Dla dowolnych niezerowych a_1, a_2, $a_3, a_4 \in \mathbb{Q}$ istnieje wielomian $d(t) \in \mathbb{Q}[t]$ taki, że jakobiany krzywych $y^2 = x^n + a_j d(t)$ mają jednocześnie dodatnią rangę nad $\mathbb{Q}(t)$.*

Dowody tych twierdzeń składają się z dwóch części. Dla danego punktu $(x(t), y(t))$ na krzywej o równaniu $y^2 = x^n + ad(t)$, potrzebujemy warunku wystarczającego na to, by ten punkt minus punkt w nieskończoności dawał element rzędu nieskończonego w jakobianie. To robimy dostosowując pomysły z [74] do obecnej sytuacji. Następnie potrzebujemy

funkcji wymiernej $d(t)$ i punktów wymiernych $(x_a(t), y_a(t))$ i $(x_b(t), y_b(t))$ na krzywych $y^2 = x^n + ad(t)$ i $y^2 = x^n + bd(t)$ odpowiednio. W tym celu konstruujemy krzywą wymierną na rozmaitości trójwymiarowej (threefold) $\mathcal{X}$ o równaniu

$$\mathcal{X} \ : \ \ b(y_a^2 - x_a^n) = a(y_b^2 - x_b^n).$$

Parametryzacja tej wymiernej krzywej $t \mapsto (x_a(t), y_a(t), x_b(t), y_b(t))$ daje nam wymagane punkty przez wzięcie $d(t) := (y_a(t)^2 - x_a(t)^n)/a$. Jeśli dodatkowo żądamy, by $d(t)$ bylo kwadratem, to zamiast $\mathcal{X}$ rozważamy rozmaitość trójwymiarową $\mathcal{Y}$ daną przez dwa równania

$$\mathcal{Y} \ : \ \ z^2 = b(y_a^2 - x_a^n) = a(y_b^2 - x_b^n),$$

którą definiujemy jako podwójne nakrycie $\mathcal{X}$.

4.5 Artykuł [B5]

Ustalmy niezerowe liczby całkowite A, B i C. Dla danych liczb naturalnych p, q, r spełniających $1/p + 1/q + 1/r < 1$ uogólnione równanie Fermata

$$Ax^p + By^q = Cz^r \tag{25}$$

ma tylko skończenie wiele pierwotnych (tzn. niezerowych i względnie pierwszych) rozwiązań w liczbach całkowitych [17]. Nowoczesne techniki pochodzące z teorii reprezentacji Galois i form modularnych takie, jak metody krzywych Freya-Hellegouarcha, warianty twierdzenia Ribeta o obniżaniu poziomu (level-lowering theorem) [29], [63], [68] i oczywiście modularność krzywych eliptycznych nad ciałem liczb wymiernych udowodniona przez Wilesa i innych [86], [8], pozwalają dać częściowe (czasem kompletne) odpowiedzi na pytania dotyczące zbioru rozwiązań (25).

Wiele klasycznych równań jest jednak nadal poza zasięgiem. Rozważmy na przykład równanie diofantyczne postaci

$$x^3 + y^3 = z^p, \qquad \text{gdzie } p \text{ jest nieparzystą liczbą pierwszą.} \tag{26}$$

Oczekuje się (i wynika to z hipotezy *abc*), że nie ma ono w ogóle pierwotnych rozwiązań. Kraus [48] użył modularnego podejścia (wzmiankowanego w pierwszym akapicie) do pokazania, że powyższe równanie nie ma pierwotnych rozwiązań dla $17 \leq p \leq 10^4$. Wprowadził bardzo interesujące kryterium ([48], Théorème 3.1), które często pozwala dowieść, że (26) nie ma pierwotnych rozwiązań przy ustalonym p i z powodzeniem użył owego kryterium dla liczb pierwszym w podanym zakresie. Ten zakres łatwo można rozszerzyć. Chen i Siksek [11] zrobili to dla liczb pierwszych $p \leq 10^9$. Ponadto pokazali oni, że zbiór wykładników p, dla których (26) ma rozwiązanie pierwotne, jest gęstości 0.

Oczywiście można zastąpić lewą stronę równania (26) przez ogólniejszą formę sześcienną o całkowitych współczynnikach i spróbować znaleźć wariant kryterium Kraussa W tym artykule przedstawiamy taką metodę dla równań diofantycznych postaci

$$(x + y)(x^2 + Bxy + y^2) = Dz^p. \tag{27}$$

Zauważmy, że w przypadku $B = -1$, $D = 1$ otrzymujemy równanie badane przez Krausa. Billerey [4] udowodnił, że równanie (27) nie ma pierwotnych rozwiązań (x, y, z), gdzie $z \neq \pm 1$ dla $B = 0$ i $D \in \{2, 6, 10, 22\}$.

Nasze wyniki dotyczą równania (27) z $B \in \{0, 1, 3, 4, 5, 6\}$. Dla specjalnie wybranych B i D oraz dla liczb pierwszych p większych niż (jawnie policzalna) stała dodatnia $C_{B,D}$ dowodzimy, że (27) nie ma pierwotnych rozwiązań (x, y, z), gdzie $z \neq \pm 1$. Jednak naszym głównym celem jest uogólnienie kryterium Krausa do równania (27) z $B = 0, 1, 3, 4, 5$ lub 6 i (bardziej lub mniej) dowolnym D. Dla każdego B jak wyżej i wybranych wartości D

używamy tych kryteriów by sprawdzić, z wykorzystaniem programu MAGMA [6], że równanie (27) jest nierozwiązywalne dla liczb pierwszych $7 \leq p < 10^6$. Pokazujemy również, przy założeniu hipotez Ivorra i Krausa [41], że (27) nie ma pierwotnych rozwiązań dla nieskończenie wielu B (i $D = 1$) i dla prawie wszystkich liczb pierwszych p.

Z przyczyn technicznych (mnogość oznaczeń i terminów itp) prezentujemy tutaj tylko wybrane rezultaty dokładnie.

Twierdzenie 4.12. *Niech $p \geq 7$ będzie liczbą pierwszą, $B = 1$ i niech α, β, D będą liczbami całkowitymi spełniającymi*

$$D = 2^\alpha \cdot 3^\beta, \qquad 0 \leq \alpha, \beta \leq p.$$

Wówczas dla wszystkich $\alpha \geq 4$ równanie (27) nie ma pierwotnych rozwiązań (x, y, z).

Ponadto, jeśli istnieje pierwotne rozwiązanie (27), gdzie $z \neq \pm 1$ dla pewnego $\alpha \leq 3$, to z jest nieparzyste oraz $x \not\equiv y \pmod 3$.

Twierdzenie 4.13. *Niech p i r będą liczbami pierwszymi, $B = 1$ i niech α, β, γ, D będą liczbami całkowitymi spełniającymi*

$$D = 2^\alpha \cdot 3^\beta \cdot r^\gamma, \qquad r \neq p, \quad 0 \leq \alpha, \beta \leq p, \quad 1 \leq \gamma \leq p.$$

Załóżmy, że p i D spełniają ponadto (przynajmniej jeden) z poniższych warunków:

1. $p \geq 19$, $\alpha = 4$, $r \in \{29, 31, 41, 53, 59 (p \neq 29), 79, 101, 103, 107 (p \neq 53), 109\}$,
2. $p \geq 23$, $\alpha = 4$, $\beta \neq 1$, $r \in \{17, 37, 61 (p \neq 31), 67, 83, 89, 113\}$;
3. $p \geq 11$, $\alpha \geq 5$, $\beta \neq 1$, $r \in \{31, 109\}$;
4. $p \geq 19$, $\alpha \geq 2$, $\beta \neq 1$, $r \in \{79, 103 (p \neq 31)\}$;
5. $p \geq 23$, $\alpha \neq 1$, $\beta \neq 1$, $r \in \{53, 127\}$.

Wówczas równanie (27) nie ma pierwotnych rozwiązań (x, y, z), gdzie $z \neq \pm 1$.

Twierdzenie 4.14. *Niech $5 \leq r \leq 23$ będzie liczbą pierwszą, $B = 1$ i niech $0 \leq \alpha \leq 5$, $1 \leq \beta \leq 10$. Wtedy równanie (27) nie ma pierwotnych rozwiązań dla*

$$D = 2^\alpha \cdot r^\beta \quad i \quad 37 \leq p < 10^6,$$

chyba, że $D \in \{7,\ 7^3,\ 2 \cdot 7,\ 8 \cdot 7^2,\ 16 \cdot 7^4,\ 13,\ 4 \cdot 13,\ 8 \cdot 13^2,\ 2 \cdot 19,\ 16 \cdot 19^2\}$ lub p i D są jak niżej:

p	D	p	D	p	D
37	$2 \cdot 7^{10},\ 4 \cdot 7^6,\ 32 \cdot 11^9,$	41	$11^{10},\ 4 \cdot 11^6,\ 8 \cdot 13^5,$	47	13^6
	$4 \cdot 13^2,\ 8 \cdot 13^7,\ 32 \cdot 13,$		$2 \cdot 19^4,\ 2 \cdot 23^{10},\ 8 \cdot 23^7,$	59	13^3
	$4 \cdot 19^4,\ 2 \cdot 23^9$	43	$16 \cdot 7,\ 4 \cdot 17^6,\ 2 \cdot 23^3$	67	7^2

4.6 Artykuł [B6]

W tym artykule badamy uogólnione liczby kongruentne (generalized congruent numbers). Liczbę naturalną n nazywamy *liczbą kongruentną*, gdy jest ona polem trójkąta prostokątnego o wymiernych długościach boków, czyli gdy istnieją dodatnie liczby wymierne a, b, c takie, że

$$a^2 + b^2 = c^2 \text{ oraz } ab = 2n. \tag{28}$$

Bez straty ogólności możemy (i będziemy) zakładać, że n jest bezkwadratowa. Problem liczb kongruentnych, tzn. problem sprawdzenia, czy dana liczba naturalna jest kongruentna, czy nie, jest bardzo stary i niecałkiem rozwiązany. Istnieje efektywne przełożenie tego problemu na język teorii krzywych eliptycznych (szczegóły są zawarte w [46]). Rozważmy krzywe eliptyczne związane z liczbami kongruentnymi tj.

$$E_n : y^2 = x^3 - n^2 x. \tag{29}$$

Wiadomo, że podgrupa torsyjna w $E_n(\mathbb{Q})$ składa się tylko z punktów rzędu 2, mianowicie $(0,0), (\pm n, 0)$ oraz punktu w nieskończoności ∞. To jest kluczowa obserwacja w dowodzie poniższego kryterium.

Lemat 4.15. *Liczba naturalna n jest kongruentna wtedy i tylko wtedy, gdy grupa $E_n(\mathbb{Q})$ ma element nieskończonego rzędu.*

Z tego kryterium można wywnioskować fakt (znany już Fermatowi), że dla danej liczby kongruentnej n istnieje nieskończenie wiele trójkątów prostokatnych o wymiernych bokach a, b, c spełniających (28).

Problem liczb kongruentnych został rozwiązany prawie kompletnie przez Tunnella [81], który dał proste kryterium. Zależy ono jednak od prawdziwości słabej wersji hipotezy Birch a i Swinnertona-Dyera (BSD) dla rodziny krzywych eliptycznych $E_n : y^2 = x^3 - n^2 x$. Dokładniej Tunnell pokazał, że jeśli liczba nieparzysta n jest kongruentna, to

$$\#\left\{x, y, z \in \mathbb{Z} : 2x^2 + y^2 + 8z^2 = n\right\} = 2\#\left\{x, y, z \in \mathbb{Z} : 2x^2 + y^2 + 32z^2 = n\right\},$$

a odwrotna implikacja jest prawdziwa przy założeniu prawdziwości hipotezy BSD dla rodziny E_n (czyli, że ranga $E_n(\mathbb{Q})$ jest dodatnia wtedy i tylko wtedy, gdy odpowiadająca L-funkcja znika w punkcie centralnym 1). Podobne kryterium podał też dla liczb parzystych.

Pomysł badania problemu liczb kongruentnych nad algebraicznymi rozszerzeniami ciała liczb wymiernych pochodzi prawdopodobnie od Tady [77], który rozważał ciała kwadratowe rzeczywiste. Mówimy, że liczba naturalna n jest *liczbą kongruentną nd ciałem K* (lub krótko *liczbą K-kongruentną*), gdy istnieją $a, b, c \in K$ takie, że zachodzi (28). Zauważmy, że gdy K jest podciałem $\mathbb{R}$ nadal ma to sens geometryczny. W przeciwieństwie do przypadku liczb $\mathbb{Q}$-kongruentnych, z tego, że n jest liczbą K-kongruentną nie wynika, że istnieje nieskończenie wiele trójkatów prostokątnych o polu n (na przykład weźmy $n = 1$ i $K = \mathbb{Q}\left(\sqrt{2}\right)$). To uzasadnia następującą definicję: liczbę K-kongruentną n nazywamy *właściwie K-kongruentną*, gdy (28) ma nieskończenie wiele rozwiązań $a, b, c \in K$.

W tym artykule podajemy nieskończone rodziny rzeczywistych ciał liczbowych K, dla których każda liczba K-kongruentna jest właściwie K-kongruentna. Odnotujmy, że n jest właściwie K-kongruentna wtedy i tylko wtedy, gdy $E_n(K)$ ma element nieskończonego rzędu. W związku z tym otrzymujemy także wariant lematu 4.15.

Niech $K_{2,d} = \mathbb{Q}(\sqrt{m_1}, ..., \sqrt{m_d})$, gdzie $m_i \in \mathbb{N}$. Bez straty ogólności zakładamy, że $[K_{2,d} : \mathbb{Q}] = 2^d$, m_i są bezkwadratowe $(1 \leq i \leq d)$ i dowolne dwa różne m_i, m_j nie dzielą się nawzajem. Nasze główne wyniki są następujące.

Twierdzenie 4.16. *Załóżmy, że $\sqrt{2} \notin K_{2,d}$. Wówczas n jest liczbą kongruentną nad $K_{2,d}$ wtedy i tylko wtedy, gdy grupa $E_n(K_{2,d})$ ma element nieskończonego rzędu.*

Twierdzenie 4.17. *Niech $K \subset \mathbb{R}$ będzie ciałem liczbowym takim, że $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5} \notin K$. Załóżmy, że stopień rozszerzenia $[K : \mathbb{Q}]$ jest nieparzysty lub $[K : \mathbb{Q}] = 2p$, gdzie p jest liczbą pierwszą. Wówczas n jest liczbą kongruentną nad K wtedy i tylko wtedy, gdy grupa $E_n(K)$ ma element nieskończonego rzędu.*

Głównym wkładem w dowodach jest pokazanie, że w takich ciałach K podgrupa torsyjna $E_n(K)$ składa się tylko z czterech elementów: $(0,0), (\pm n, 0), \infty$.

Dostajemy także interesujące wnioski.

Wniosek 4.18. *Załóżmy, że $\sqrt{2} \notin K_{2,d}$. Wówczas n jest liczbą $K_{2,d}$-kongruentną wtedy i tylko wtedy, gdy przynajmniej jedna z 2^d liczb $nm_1^{e_1} \dots m_d^{e_d}$ $(e_i = 0, 1)$ jest $\mathbb{Q}$-kongruentną.*

Wniosek 4.19. *Załóżmy, że $\sqrt{2} \notin K_{2,d}$. Jeśli n jest liczbą $K_{2,d}$-kongruentną, to n jest liczbą kongruentną nad $\mathbb{Q}$ lub nad pewnym kwadratowym podciałem $\mathbb{Q}\left(\sqrt{m_1^{e_1} \dots m_d^{e_d}}\right) \subset K_{2,d}$.*

Wniosek 4.20. *Jeśli rzeczywiste ciało liczbowe K spełnia założenia twierdzeń 4.16 lub 4.17, to n jest K-kongruentna wtedy i tylko wtedy, gdy n jest właściwie K-kongruentna.*

W naturalny sposób pojawiają się następujące pytania.

Pytanie 4.21. *Czy dla każdej liczby naturalnej d istnieje ciało liczbowe K stopnia d nad $\mathbb{Q}$ takie, że $E_n(K)_{tors} = \{(0,0), (\pm n, 0), \infty\}$ dla dowolnego n?*

Pytanie 4.22. *Czy dla danej liczby naturalnej d dowolne $n \in \mathbb{N}$ jest właściwie kongruentne nad pewnym ciałem rzeczywistym stopnia d?*

Pytanie 4.23. *Jaka jest pełna charakteryzacja rzeczywistych ciał liczbowych o własności jak z wniosku 4.20?*

Zauważmy, że kryterium Tunnella (i hipoteza Bircha i Swinnertona-Dyera) implikują, że każda liczba naturalna jest kongruentna nad ciałem bikwadratowym $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. Z drugiej strony trudno oczekiwać, że równanie (28) może mieć rozwiązania wśród liczb algebraicznych całkowitych $\mathcal{O}_K$ ustalonego ciała liczbowego K dla każdego n naturalnego (nazwijmy takie liczby $\mathcal{O}_K$-kongruentnymi). Zinevicius w [88] udowodnił, że jeżeli K jest cyklicznym rozszerzeniem $\mathbb{Q}$ stopnia d, to dolna względna gęstość zbioru liczb pierwszych, które nie są $\mathcal{O}_K$-kongrunetne jest nie mniejsza niż $\varphi(d)/(2d)$. On także w [89] rozważał podobny problem z ideałami głównymi pierwszymi zamiast liczb pierwszych.

4.7 Artykuł [B7]

Ogólnie uważa się, że krzywe elityczne nad $\mathbb{Q}$ z dużą rangą stanowią niewielką część wszystkich krzywych eliptycznych (nad $\mathbb{Q}$). W szczególności, znana hipoteza Goldfelda [32] twierdzi, że średnia ranga skręceń kwadratowych dowolnej krzywej eliptycznej nad $\mathbb{Q}$ wynosi $1/2$. Natychmiastową konsekwencją tej hipotezy jest to, że dla dowolnej krzywej eliptycznej nad ciałem liczb wymiernych asymptotycznie przynajmniej połowa skręceń kwadratowych tej krzywej ma rangę zero. Tak więc stosunkowo słabsza hipoteza przypuszcza, że skręcenia kwadratowe rangi zero mają dodatnią proporcję wśród wszystkich skręceń kwadratowych. W ogólności to też jest nadal otwartym problemem.

Istnieje wiele artykułów poświęconych temu problemowi. Z powodu wyników Kolyvagina [47] większość z nich skupia się na nieznikaniu L-funkcji. Najlepszy bezwarunkowy, ale słabszy wynik w pełnej ogólności pochodzi od Ono i Skinnera [59]: $M_E(X) >> X/\log X$, gdzie $M_E(X) := \#\left\{|r| \leq X : \operatorname{rank}\left(E^{(r)}(\mathbb{Q})\right) = 0\right\}$, a $E^{(r)}$ jest skręceniem kwadratowym E przez liczbę bezkwadratową r. Bezwarunkowe rezultaty są znane tylko dla kilku specjalnych krzywych (na przykład [42], [84]).

Istnieje też inne podejście wykorzystujące metodę spadku (descent method). Na przykład Yu [87] pokazał, że dodatnia proporcja skręceń kwadratowych krzywych eliptycznych o 2-torsji $(\mathbb{Z}/2\mathbb{Z})^2$ jest rangi 0. Znaczący ogólny wynik daje Swinnerton-Dyer w [76]. Dąbrowski [19] udowodnił, że dla dowolnej liczby naturalnej k istnieje k parami nieizogenicznych krzywych $E_1, \dots, E_k$ takich, że $\operatorname{rank}(E_i^{(p)}(\mathbb{Q})) = 0$ $(1 \leq i \leq k)$ dla dodatniej proporcji liczb pierwszych p.

Poza skręceniami kwadratowymi jest możliwe rozważać dla pewnych krzywych skręcenia sześcienne. Jeden z godnych uwagi, bezwarunkowych wyników zawarty jest w artykule

Liemana [52]. Udowodnił on (używając L-funkcji i form automorficznych), że dla nieskończenie wielu liczb naturalnych r wolnych od sześcianów krzywa eliptyczna $x^3+y^3=r$ ma rangę 0 nad $\mathbb{Q}$.

Sformułujemy teraz główne wyniki z naszego artykułu. W dowodach używamy metod 2- i 3-spadku (pełny opis tych metod zawarty jest w [71, rozdz. X] i [66] odpowiednio). Dla liczby naturalnej k niech B_k oznacza zbiór bezkwadratowych liczb całkowitych względnie pierwszych z 6 posiadający dokładnie k dzielników pierwszych. Niech $E_2: x^3+y^3=2$ i niech $E_2^{(r)}$, E_{2r} oznaczają jej skręcenia kwadratowe i sześcienne przez r odpowiednio.

Twierdzenie 4.24. *Dla nieskończenie wielu liczb bezkwadratowych skręcenia kwadratowe krzywej $x^3+y^3=2$ mają rangę 0. Precyzyjniej: zbiór $\left\{r\in B_k : \operatorname{rank}\left(E_2^{(r)}(\mathbb{Q})\right)=0\right\}$ ma dodatnią gęstość w B_k dla dowolnego k.*

Twierdzenie 4.25. *Dla nieskończenie wielu liczb bezkwadratowych skręcenia sześcienne krzywej $x^3+y^3=2$ mają rangę 0. Precyzyjniej: zbiór $\{r\in B_k : \operatorname{rank}(E_{2r}(\mathbb{Q}))=0\}$ ma dodatnią gęstość w B_k dla dowolnego k.*

Odnotujmy, że powyższe wyniki nie odnoszą się do zbioru wszystkich liczb bezkwadratowych lub wolnych od sześcianów, ale do podzbiorów tych liczb, które same mają gęstość zero. W związku z tym hipotezy o gęstości pozostają otwarte (nawet dla przykładów rozważanych w tym artykule).

Pokazaliśmy również, że dla nieskończenie wielu liczb bezkwadratowych skręcenia kwadratowe i sześcienne E_2 mają jednocześnie rangę zero. Przedstawiliśmy też dokładną charakteryzację grup Selmera dla skręceń kwadratowych i sześciennych krzywej E_2 przez liczby pierwsze i iloczyny dwóch liczb pierwszych. W konsekwencji możemy porównać skręcenia kwadratowe i sześcienne E_2 przez liczby pierwsze rangi ≤ 1.

Wniosek 4.26. *Mamy*

$\operatorname{rank}\left(E_2^{(p_1)}\right)$	$\operatorname{rank}(E_{2p_1})$	$p_1 \pmod{36}$
0	0	5
0	1	29
1^*	0	23
1^*	1	11

*Tutaj * oznacza, że zakładamy hipotezę o parzystości (Parity Conjecture).*

Na koniec rozważamy skręcenia kwadratowe jakobianów $J_a(5)$ krzywych typu Fermata $F_a(5): x^5+y^5=a$ genusu 6 i rozmieszczenie ich liczb pierwiastkowych (root numbers) (por. [B2]). Przypomnijmy pewne fakty i potrzebne oznaczenia. Niech A będzie rozmaitością abelową nad $\mathbb{Q}$, a $\rho_{A,p}$ - stowarzyszoną p-adyczną reprezentacją. Wtedy skręcenie kwadratowe A przez liczbę bezkwadratową r (oznaczane przez $A^{(r)}$) ma stowarzyszoną reprezentację $\rho_{A,p}\otimes\chi_r(p)$, gdzie χ_r jest charakterem związanym z ciałem kwadratowym $\mathbb{Q}(\sqrt{r})$. Jeśli A jest jakobianem krzywej hipereliptycznej $y^2=f(x)$, to po prostu $A^{(r)}$ jest jakobianem skręconej krzywej $ry^2=f(x)$. Przypomnijmy, że $J_{a,i}(5)$ są jakobianami krzywych hipereliptycznych $C_{a,i}(5)$ $(i=1,2)$ zadanych przez (19) lub równoważnie krzywych $B_{a,5}, A_{a,5}$ (danych przez (20)) odpowiednio. Zatem skręcenie kwadratowe $J_{a,i}^{(r)}(5)$ jest jakobianem krzywej

$$B_{a,5}^{(r)}: y^2=x^5+4^4a^2r^5, \qquad A_{a,5}^{(r)}: y^2=x^5+(4a)^4r^5,$$

odpowiednio oraz $J_a^{(r)}(5)$ jest izogeniczny z $J_{a,1}^{(r)}(5)\times(J_{a,2}^{(r)}(5))^2$. Niech $W_{a,i}^{(r)}$ oznacza liczbę pierwiastkową $J_{a,i}^{(r)}(5)$ dla $i=1,2$.

Wniosek 4.27. *Położmy* $T := \{n \in \mathbb{N} : \mathrm{NWD}(10, n) = 1, n \text{ jest bezkwadratowe}\}$. *Wówczas dla* $i = 1, 2$ *zbiory* $\left\{r \in T : W_{2,i}^{(r)} = 1\right\}$ *mają gęstość* $1/2$ *w* T *(i dodatnią gęstość w* $\mathbb{N}$*).*

Przy założeniu hipotezy o parzystości otrzymujemy stąd na przykład, że dla $i = 1, 2$ gęstość zbiorów $\left\{r \in T : \mathrm{rank}\left(J_{2,i}^{(r)}(5)(\mathbb{Q})\right) \text{ jest parzysta}\right\}$ (więc też zbioru $\{r \in T : \mathrm{rank}\left(J_2^{(r)}(5)(\mathbb{Q})\right) \text{ jest parzysta}\}$) wynosi $1/2$ w T. Chciałoby się pokazać, że zbiór $\{r \in T : \mathrm{rank}\left(J_2^{(r)}(5)(\mathbb{Q})\right) = 0\}$ ma podobną własność (przynajmniej z dodatkowymi warunkami na r). Numeryczne obliczenia (wykonane w programie MAGMA [6]) potwierdzają, że wśród jakobianów $J_2^{(r)}(5)$, gdzie r jest liczbą pierwszą przystającą do $13, 17 \pmod{20}$, około 50% ma rangę zero nad $\mathbb{Q}$.

4.8 Artykuł [B8]

W tej pracy kontynuujemy badanie skręceń kwadratowych krzywych eliptycznych. Przypadek kiedy skręcenia te mają rangę zero jest szczególnie interesujący. Jest tak ponieważ uważa się, że dodatnia proporcja skręceń kwadratowych każdej krzywej eliptycznej ma rangę zero (patrz [32] i poprzednia sekcja).

Niech p będzie liczbą pierwszą różną od $2, 3$ i 17. Wtedy istnieje krzywa eliptyczna określona nad $\mathbb{Q}$ o przewodniku p z wymiernym punktem rzędu 2 wtedy i tylko wtedy, gdy $p = u^2 + 64$ dla pewnej liczby całkowitej u. Jeśli p jest postaci $u^2 + 64$, to mamy z dokładnością do izomorfizmu dwie takie krzywe (związane 2-izogenią): $E_u : y^2 = x^3 + ux^2 - 16x$ i $E'_u : y^2 = x^3 - 2ux^2 + px$, gdzie znak u jest dobrany tak, że $u \equiv 1 (\mathrm{mod}\, 4)$. Są to tzw. *krzywe eliptyczne Neumanna-Setzera* badane w [58], [67].

Dąbrowski [19] rozważał skręcenia kwadratowe przez liczby pierwsze uogólnionych krzywych Neumanna-Setzera E_u, gdzie $u^2 + 64$ jest liczbą pierwszą lub iloczynem dwóch liczb pierwszych. Ze znanego rezultatu Iwańca [39] wiadomo, że istnieje nieskończenie wiele liczb całkowitych u takich, że $u^2 + 64$ jest iloczynem co najwyżej dwóch liczb pierwszych.

W tym artykule badamy skręcenia $E_u^{(n)}$ krzywych E_u przez liczby bezkwadratowe n. Rozszerzamy pomysły Fenga i innych (zob. np. [25], [26]) wyznaczania grup Selmera krzywych $E_u^{(n)}$ używając teorii grafów. Oni rozważali krzywe $y^2 = x^3 - n^2 x$ związane z liczbami kongruentnymi i szczególnie interesowali się krzywymi rangi zero.

Wprowadźmy niezbędną terminologię i oznaczenia. Niech G będzie prostym nieskierowanym grafem o zbiorze wierzchołków $V(G) = \{v_1, \ldots, v_t\}$ i zbiorze krawędzi $E(G)$. *Partycją* zbioru wierzchołków V (lub grafu G) nazywamy parę $\{V_1, V_2\}$ taką, że $V_1 \cup V_2 = V$ i $V_1 \cap V_2 = \emptyset$. Partycję $\{\emptyset, V\}$ nazywamy *trywialną*. Dla $v \in V_1$ oznaczmy przez $\#\{v \to V_2\}$ liczbę wierzchołków w V_2 przylegających do (adjacent to) v. Partycję $\{V_1, V_2\}$ zbioru V nazywamy *nieparzystą*, gdy istnieje $v \in V_1$ taki, że $\#\{v \to V_2\}$ jest nieparzysta lub istnieje $v \in V_2$ taki, że $\#\{v \to V_1\}$ jest nieparzysta. W przeciwnym razie partycję $\{V_1, V_2\}$ nazywamy *parzystą* (zauważmy, że trywialne partycje są parzyste). Mówimy, że graf G jest *nieparzysty*, gdy każda jego nietrywialna partycja jest nieparzysta. W przeciwnym razie graf G nazywamy *parzystym*. Mówimy, że graf G jest *półnieparzysty (semi-odd)*, gdy ma tylko jedną nietrywialną parzystą partycję. Liczbę $rs(E_u^{(n)}(\mathbb{Q})) := \dim_{\mathbb{F}_2} S_n^{\varphi} + \dim_{\mathbb{F}_2} S_n^{\varphi'} - 2$ nazywamy *rangą Selmera* grupy $E_u^{(n)}(\mathbb{Q})$ (tutaj $S_n^{\varphi}, S_n^{\varphi'}$ oznaczają grupy Selmera odpowiadające odpowiednio izogenii φ stopnia 2 z $E_u^{(n)}$ do $E_u'^{(n)}$ i izogenii dualnej (szczegóły w [B8, s. 77]). Odnotujmy, że $\mathrm{rank}\left(E_u^{(n)}(\mathbb{Q})\right) \leq rs(E_u^{(n)}(\mathbb{Q}))$.

Podamy pełny opis rozmiarów grup Selmera krzywych $E_u^{(n)}$ w terminach liczby parzystych partycji pewnych grafów, gdy $u^2 + 64 = p$ lub $p_1 p_2$ oraz $n = \pm q_1 \cdot \ldots \cdot q_k \equiv 1 (\mathrm{mod}\, 4)$, gdzie wszystkie dzielniki pierwsze $q_i \equiv 3 (\mathrm{mod}\, 4)$. Podamy też warunki (w terminach symboli Legendre'a) na to, by $\mathrm{rank}(E_n^u(\mathbb{Q}))$ wynosiła 0 lub (hipotetycznie) 1. W konsekwencji

wnioskujemy, że krzywa E_n^u ma rangę zero dla dodatniej proporcji bezkwadratowych n z ustaloną liczbą dzielników pierwszych.

Najpierw załóżmy, że $u^2+64=p$ i $\mathrm{NWD}\,(q_i, up)=1$. Definiujemy nieskierowany graf $G_1(n)$ następująco: zbiór wierzchołków $V(G_1(n)) := \{p, q_1, ..., q_k\}$ i zbiór krawędzi $E(G_1(n)) := \{\overline{pq_i} : (\frac{p}{q_i}) = -1,\ i = 1, ..., k\}$.

Twierdzenie 4.28. *Przy powyższych założeniach* $2^{rs\left(E_u^{(n)}(\mathbb{Q})\right)}$ *jest równa liczbie parzystych partycji grafu* $G_1(n)$. *W szczególności* $\mathrm{rank}\left(E_u^{(n)}(\mathbb{Q})\right) = rs(E_u^{(n)}(\mathbb{Q})) = 0$ *wtedy i tylko wtedy, gdy graf* $G_1(n)$ *jest nieparzysty. Ponadto,* $rs(E_u^{(n)}(\mathbb{Q}))$ *jest największa (równa* k*) wtedy i tylko wtedy, gdy* $E(G_1(n)) = \emptyset$.

Wniosek 4.29. *Załóżmy, że* $n = \pm q_1...q_k \equiv 1 \pmod 4$, $q_i \equiv 3 \pmod 4$, $(\frac{q_i}{p}) = -1$ *i* $q_i \nmid u$ *dla* $1 \leq i \leq k$. *Wtedy* $\mathrm{rank}\left(E_u^{(n)}(\mathbb{Q})\right) = 0$.

Wniosek 4.30. *Załóżmy, że* $n = \pm q_1...q_k \equiv 1 \pmod 4$, $q_i \equiv 3 \pmod 4$, $q_i \nmid u$ *dla* $1 \leq i \leq k$ *oraz* $\exists_{i_0}(\frac{q_{i_0}}{p}) = 1$, $\forall_{i\neq i_0}(\frac{q_i}{p}) = -1$. *Wtedy* $rs\left(E_u^{(n)}(\mathbb{Q})\right) = 1$. *Ponadto ponieważ globalna liczba pierwiastkowa L-funkcji stowarzyszonej z* $E_u^{(n)}$ *wynosi* -1*, więc przy założeniu hipotezy o parzystości* $\mathrm{rank}\left(E_u^{(n)}(\mathbb{Q})\right) = 1$.

Wniosek 4.31. *Zbiór* $\left\{n \in A_k^1 : \mathrm{rank}\left(E_u^{(n)}(\mathbb{Q})\right) = 0\right\}$ *ma dodatnią gęstość w* A_k^1 *dla dowolnego* k*, gdzie* A_k^1 *oznacza zbiór nieparzystych liczb bezkwadratowych (dodatnich, gdy* k *jest parzyste, a ujemnych, gdy* k *jest nieparzyste)* n *takich, że* $\mathrm{NWD}\,(n, u) = \mathrm{NWD}\left(n, u^2+64\right) = 1$ *o dokładnie* k *dzielnikach pierwszych. W szczególności dla nieskończenie wielu nieparzystych liczb bezkwadratowych skręcenia kwadratowe krzywej* $y^2 = x^3 + ux^2 - 16x$ *(gdzie* u^2+64 *jest liczbą pierwszą) mają rangę 0.*

Teraz załóżmy, że $u^2+64 = p_1p_2$ i zdefiniujmy nieskierowany graf $G_2(n)$ następująco: zbiór wierzchołków $V(G_2(n)) := \{p_1, p_2, q_1, ..., q_k\}$ i zbiór krawędzi $E(G_2(n)) := \{\overline{p_jq_i} : (\frac{p_j}{q_i}) = -1,\ i = 1, ..., k,\ j = 1, 2\}$.

Twierdzenie 4.32. *Przy powyższych założeniach* $2^{rs\left(E_u^{(n)}(\mathbb{Q})\right)}$ *jest równa liczbie parzystych partycji grafu* $G_2(n)$. *W szczególności* $\mathrm{rank}\left(E_u^{(n)}(\mathbb{Q})\right) = rs(E_u^{(n)}(\mathbb{Q})) = 0$ *wtedy i tylko wtedy, gdy graf* $G_2(n)$ *jest nieparzysty. Ponadto,* $rs(E_u^{(n)}(\mathbb{Q}))$ *jest największa (równa* $k+1$*) wtedy i tylko wtedy, gdy* $E(G_2(n)) = \emptyset$.

Wniosek 4.33. *Załóżmy, że* $n = \pm q_1...q_k \equiv 1 \pmod 4$, $q_i \equiv 3 \pmod 4$, $(\frac{q_i}{p_1}) = -1$ *i* $q_i \nmid u$ *dla* $1 \leq i \leq k$. *Ponadto załóżmy, że* $\exists_{i_0}(\frac{q_{i_0}}{p_2}) = -1$ *i* $\forall_{i\neq i_0}(\frac{q_i}{p_2}) = 1$. *Wówczas* $\mathrm{rank}\,(E_n^u(\mathbb{Q})) = 0$.

Wniosek 4.34. *Załóżmy, że* $n = \pm q_1...q_k \equiv 1 \pmod 4$, $q_i \equiv 3 \pmod 4$, $q_i \nmid u$ *dla* $1 \leq i \leq k$ *oraz* $\forall_i(\frac{q_i}{p_2}) = -(\frac{q_i}{p_1}) = 1$ *(lub odwrotnie). Wówczas* $rs\,(E_n^u(\mathbb{Q})) = 1$. *Ponadto ponieważ globalna liczba pierwiastkowa L-funkcji stowarzyszonej z* $E_u^{(n)}$ *wynosi* -1*, więc przy założeniu hipotezy o parzystości* $\mathrm{rank}\left(E_u^{(n)}(\mathbb{Q})\right) = 1$.

Wniosek 4.35. *Zbiór* $\left\{n \in A_k^1 : \mathrm{rank}\left(E_u^{(n)}(\mathbb{Q})\right) = 0\right\}$ *ma dodatnią gęstość w* A_k^1 *dla dowolnego* k*. W szczególności dla nieskończenie wielu nieparzystych liczb bezkwadratowych skręcenia kwadratowe krzywej* $y^2 = x^3+ux^2-16x$ *(gdzie* u^2+64 *jest iloczynem dwóch liczb pierwszych) mają rangę 0.*

Gdy n jest parzyste skupiamy się tylko na skręceniach rangi zero i dostajemy podobne wyniki dotyczące gęstości (nie używamy tu teorii grafów). Także w przypadku $u^2+64 = p_1 \cdot \ldots \cdot p_l$, gdzie $l > 2$ podajemy warunki by skręcenia kwadratowe były rangi zero nie używając grafów. Napiszemy tutaj tylko dwa wybrane rezultaty.

Wniosek 4.36. *Zbiór* $\left\{n \in A_k^2 : \operatorname{rank}\left(E_u^{(n)}(\mathbb{Q})\right) = 0\right\}$ *ma dodatnią gęstość w* A_k^2 *dla dowolnego k, gdzie* A_k^2 *oznacza zbiór parzystych liczb bezkwadratowych (dodatnich, gdy k jest parzyste, a ujemnych, gdy k jest nieparzyste) n takich, że* $\operatorname{NWD}(n,u) = \operatorname{NWD}\left(n, u^2+64\right) = 1$ *o dokładnie k dzielnikach pierwszych. W szczególności dla nieskończenie wielu parzystych liczb bezkwadratowych skręcenia kwadratowe krzywej* $y^2 = x^3 + ux^2 - 16x$ *(gdzie* u^2+64 *jest liczbą pierwszą lub iloczynem dwóch liczb pierwszych) mają rangę 0.*

Stwierdzenie 4.37. *Załóżmy, że* $u^2+64 = p_1 \cdot \ldots \cdot p_l$, $l \geq 2$ *i* $n = \pm q_1 \ldots q_k \equiv 1 \pmod 4$, $k \geq l-1$, *gdzie (dla* $1 \leq i \leq k$*)* $q_i \equiv 3 \pmod 4$ *i* $q_i \nmid u$. *Załóżmy ponadto, że* $\forall_{1\leq i\leq k}(\frac{p_1}{q_i}) = -1$, $\exists_{1\leq i_1\leq k}(\frac{p_2}{q_{i_1}}) = -1$, $\forall_{i\neq i_1, 1\leq i\leq k}(\frac{p_2}{q_i}) = 1$, $\exists_{i_2\neq i_1, 1\leq i_2\leq k}(\frac{p_3}{q_{i_2}}) = -1$, $\forall_{i\neq i_2, 1\leq i\leq k}(\frac{p_3}{q_i}) = 1, \ldots$, $\exists_{i_{l-1}\neq i_1, i_2, \ldots, i_{l-2}, 1\leq i_{l-1}\leq k}(\frac{p_l}{q_{i_{l-1}}}) = -1$, $\forall_{i\neq i_{l-1}, 1\leq i\leq k}(\frac{p_l}{q_i}) = 1$. *Wówczas* $S_n^{\varphi} =< p_1 \cdot \ldots \cdot p_l >$, $S_n^{\varphi'} =< -1 >$. *W szczególności* $\operatorname{rank}(E_u^{(n)}(\mathbb{Q})) = 0$.

4.9 Artykuł [B9]

Niech E będzie krzywą eliptyczną nad $\mathbb{Q}$ o przewodniku N_E i niech $L(E,s)$ oznacza odpowiadający jej L-szereg. Niech $Ш(E)$ będzie grupą Tate'a-Shafarevicha krzywej E (hipotetycznie skończoną), a $R(E)$ jej regulatorem. W końcu niech Ω będzie rzeczywistym okresem (real period), $C_\infty = \Omega$ lub 2Ω (zależnie od tego czy $E(\mathbb{R})$ jest spójne czy nie) i C_{fin} oznacza iloczyn czynników Tamagawy w liczbach pierwszych, gdzie E ma złą redukcję. L-szereg $L(E,s)$ jest zbieżny dla $\operatorname{Re} s > 3/2$. Hipoteza o modularności (kompletnie rozwiązana przez Wilesa,Taylora, Diamonda, Breuila i Conrada) implikuje, że $L(E,s)$ ma przedłużenie analityczne do funkcji całkowitej. Słynna hipoteza Bircha i Swinnertona-Dyera (BSD) wiąże arytmetyczne niezmienniki krzywej E z zachowaniem $L(E,s)$ w $s=1$.

Hipoteza 4.38. *(Birch i Swinnerton-Dyer) (i) L-funkcja* $L(E,s)$ *ma zero rzędu* $r := \operatorname{rank} E(\mathbb{Q})$ *w* $s=1$,

(ii)

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{C_\infty(E) C_{fin}(E)\, R(E)\, |Ш(E)|}{|E(\mathbb{Q})_{tors}|^2}.$$

Pierwszy ogólny rezultat dotyczący BSD został udowodniony przez Coatesa i Wilesa [12] w 1976 dla krzywych eliptycznych E z mnożeniem zespolonym (CM): jeśli $L(E,1) \neq 0$, to grupa $E(\mathbb{Q})$ jest skończona. Gross i Zagier [35] pokazali, że jeśli $L(E,s)$ ma zero pierwszego rzędu w $s=1$, to E ma wymierny punkt nieskończonego rzędu. Rubin [64] udowodnił, że jeżeli E ma CM i $L(E,1) \neq 0$, to $Ш(E)$ jest skończona. Kolyvagin [47] pokazał, że jeśli $L(E,1) \neq 0$, to $r=0$, a jeśli $L(E,1)=0$, ale $L'(E,1) \neq 0$, to $r=1$. W istocie wyniki Rubina i Kolyvagina są bardziej precyzyjne. Praca [33] dokańcza częściową weryfikację Rubina hipotezy BSD dla skręceń kwadratowych $X_0(49)$. Coates i inni [13] [14] pokazali, że istnieje duża klasa jawnych skręceń kwadratowych $X_0(49)$, których L-szereg nie znika w $s=1$ i dla których zachodzi mocna wersja hipotezy BSD.

Wiadomo od dawna, że $|Ш(E)|$ (pod warunkiem, że jest skończona) może być dowolnie duży (Cassels). Podkreślmy, że w 1987 w końcu ustalono, że istnieją krzywe eliptyczne nad $\mathbb{Q}$ o skończonych grupach Tate'a-Shafarevicha (Rubin, Kolyvagin). Przypuszcza się, że $Ш(E)$ jest zawsze skończona; wiadomo, że jeśli $Ш(E)$ jest skończona, to $|Ш(E)|$ jest kwadratem.

Rozważmy $E = X_0(49)$. Przypomnijmy, że E ma równanie minimalne Weierstrassa postaci $y^2 + xy = x^3 - x^2 - 2x - 1$. W tym artykule przedstawiamy wyniki naszych

poszukiwań rzędów grup Tate'a-Shafarevicha skręceń kwadratowych $E^{(d)}$ krzywej E. Nasze obliczenia i hipotezy mogą służyć jako dodatek do pięknych wyników Gonzaleza-Aviléza ([33], Theorem B) oraz Coatesa, Li, Tian i Zhai ([14], Theorems 1.2 i 1.4). Z drugiej strony, otwierają nowe perspektywy dla lepszego zrozumienia rzędów grup Tate'a-Shafarevicha w rodzinach krzywych eliptycznych.

Nasze dane liczbowe zawierają rząd $|Ш(E^{(d)}|$ dla wszystkich 5 598 893 691 dodatnich nieparzystych wyróżników d (ciał kwadratowych), względnie pierwszych z 7, przy czym $d < 32 \times 10^9$ i $L(E^{(d)}, 1) \neq 0$. Obliczenia sugerują, że dla dowolnej liczby naturalnej k istnieje liczba bezkwadratowa d, gdzie $\mathrm{NWD}(d, 7) = 1$ (lub nawet nieskończenie wiele takich d) dla których $E^{(d)}$ ma rangę zero i $|Ш(E^{(d)}| = k^2$. Proponujemy także asymptotyczne wzory na liczbę takich d. Dane liczbowe dostarczają również silnych informacji o zachowaniu się sum rzędów $|Ш(E^{(d)}|$ dla dodatnich nieparzystych d względnie pierwszych z 7 dla których $L(E^{(d)}, 1) \neq 0$ względem wszystkich d takich, że $d \leq X$ gdy $X \to \infty$. Okazuje się, że oba rozkłady$L(E^{(d)}, 1)$ i $\log(|Ш(E^{(d)}|/\sqrt{d})$ są w przybliżeniu zgodne z rozkładem normalnym. Także numerycznie potwierdzamy, że $|Ш(E^{(d)}| = 1$ jest tak częste jak $L(E^{(d)}, 1) = 0$. Tablice dołączone do naszego artykułu zawierają dla każdej liczby naturalnej $k \leq 1793$ (i dla wybranych liczb do 2941) krzywą eliptyczną $E^{(d_k)}$ dla której $|Ш(E^{(d)}| = k^2$.

Główna część obliczeń została przeprowadzona na stacjonarnych komputerach osobistych. Dla niektórych obliczeń wykorzystaliśmy także HPC klaster HAL9000. Użyliśmy skryptu PARI / GP (z funkcją `qfrep`) do obliczeń $|Ш(E^{(d)}|$ dla $d \leq B := 5 \times 10^7$ (na standardowym PC). Poczyniliśmy dalsze postępy implementując funkcję `qfrep` w języku `C++`. Nasz algorytm można zsynchronizować. Wydaje się, że równoległe wykonywanie obliczeń umożliwi znaczne zwiększenie B w porównaniu z naszymi osiągnięciami.

Warianty powyższych obliczeń i hipotez zostały rozszerzone przez Dąbrowskiegi i Szymaszkiewicza na rodziny skręceń kwadratowych innych krzywych eliptycznych, na rodziny skręceń sześciennych krzywej $X_0(27)$ i na rodzinę krzywych elitycznych Neumanna-Setzera [20].

Bibliografia

[1] N. Aoki, *Torsion points on CM abelian varieties*, Comment. Math. Univ. St. Pauli **55** (2006), no. 2, 207-229.

[2] B. C. Berndt, R. J. Evans, *Sums of Gauss, Jacobi and Jacobsthal*, J. Number Theory **11** (1979), 349-498.

[3] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts **21**, A Wiley-Interscience Publication 1998.

[4] N. Billerey, *Formes homogènes de degré 3 et puissances p-ièmes*, Journal of Number Theory **128** (2008), 1272-1294.

[5] C. Blake, *A Deuring criterion for abelian varieties*, Bull. Lond. Math. Soc. **46** (2014), no. 6, 1256-1263.

[6] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235-265.

[7] A. Bremner, J.H. Silverman, N. Tzanakis, *Intergral points in arithmetic progression on* $y^2 = x\left(x^2 - n^2\right)$, J. Number Theory **80** (2000), 187-208.

[8] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843-939.

[9] A. Cadoret, A. Tamagawa, *Note on torsion conjecture. Geometric and differential Galois theories*, Sémin. Congr., **27**, Soc. Math. France, Paris (2013), 57-68.

[10] J. W. S. Cassels, E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge University Press, 1996.

[11] I. Chen, S. Siksek, *Perfect powers expressible as sums of two cubes*, J. Algebra **322** (2009), 638-656.

[12] J. Coates, A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223-251.

[13] J. Coates, *Lectures on the Birch-Swinnerton-Dyer Conjecture*, Notices of the ICCM **1** (2013), 29-46.

[14] J. Coates, Y. Li, Y. Tian, S. Zhai, *Quadratic twists of elliptic curves*, Proc. London Math. Soc. **110** (2015), 357-394.

[15] R. Coleman, *Torsion points on Fermat curves*, Compos. Math. **58** (1986), 191-208.

[16] G. Cornelissen, *Two-torsion in the Jacobian of hyperelliptic curves over finite fields*, Arch. Math. **77** (2001), 241-246.

[17] H. Darmon, A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), 513-543.

[18] A. Dąbrowski, *A family of pairing-friendly superelliptic curves of genus 4*, Studia Bezpieczeństwa Narodowego, **6** (2014), 133-137.

[19] A. Dąbrowski, *On the proportion of rank 0 twists of elliptic curves*, C. R. Acad. Sci. Paris, **346** (2008), 483-486.

[20] A. Dąbrowski, L. Szymaszkiewicz, *Orders of Tate-Shafarevich groups for the Neumann-Setzer type elliptic curves*, Math. Comp. **87** (2018), no. 311, 1509-1522.

[21] P. Deligne, *Varietes Abeliennes Ordinaires sur un Corps Fini*, Inven. Math **8** (1969), 238-243.

[22] G. Everest, P. Ingram, S. Shaun, *Primitive divisors on twists of Fermat's cubic*, LMS J. Comput. Math. **12** (2009), 54-81.

[23] D.K. Faddeev, *On the Divisor Class Groups of some Algebraic Curves*, Sov. Math. Dokl. **2** (1961), 67-69 (in Russian)

[24] D.K. Faddeev, *Invariants of Divisor Classes for the Curves $x^k(1-x) = y^l$ in l-adic Cyclotomic Field*, Trudy Mat. Inst. Steklov **64** (1961), 284-293 (in Russian)

[25] K. Feng, *Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arith. **75** (1996), 71-83.

[26] K. Feng and M. Xiong, *On elliptic curves $y^2 = x^3 - n^2x$ with rank zero*, J. Number Theory **109** (2004), 1-26.

[27] D. Freeman,*Constructing pairing-friendly genus 2 curves over prime fields with ordinary Jacobians*, Lecture Notes in Computer Science **4575** (2007), 152-176.

[28] C. Friesen, J. B. Muskat, B. K. Spearman, K. S. Williams, *Cyclotomy of order 15 over $GF(p^2), p \equiv 4, 11 (\mathrm{mod}\, 15)$*, Internat. J. Math. and Math. Sci. **9**, no. 4 (1986), 665-704.

[29] G. Frey, *Links between solutions of $A - B = C$ and elliptic curves*, Number theory (Ulm, 1987), Lecture Notes in Math. **1380** (1989), 31-62.

[30] Y. Fujita, T. Nara, *Generators and integral points on twists of the Fermat cubic*, Acta Arith. **168** (2015), no. 1, 1-16.

[31] S. D. Galbraith, S. Paulus, N. P. Smart, *Arithmetic on Superelliptic Curves*, Math. Comp. **237** (2000), 393-405.

[32] D. Goldfeld, Conjectures on Elliptic Curves over Quadratic Fields, *Springer Lecture Notes*, **751**, Springer, Berlin 1979, 108-118.

[33] C.D. Gonzalez-Avilés, *On the conjecture of Birch and Swinnerton-Dyer*, Trans. Amer. Math. Soc. **349** (1997), 4181-4200.

[34] B. H. Gross, D. E. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*, Invent. Math. **44** (1978), 201-224.

[35] B. Gross, D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225-320.

[36] F. Hamaza, *Hodge cycles on the jacobian variety of the Catalan curve*, Compositio Math. **107** (1997), 339-353.

[37] M. Hindry, J. H. Silverman, *Diophantine Geometry*, Graduate Texts in Math **201**, Springer-Verlag 2000.

[38] M. Hindry, J.H. Silverman, *The cannonical heights and integral points on elliptic curves*, Invent. Math **93** (1998), 419-450.

[39] H. Iwaniec, *Almost-primes represented by quadratic polynomials*, Invent. Math. **47** (1978), 171-188.

[40] H. Iwaniec, *Primes represented by quadratic polynomials in two variables*, Acta Arith. **24** (1973/74), 435-459.

[41] W. Ivorra, A. Kraus, *Quelques résultats sur les équations* $ax^p + by^p = cz^2$, Canad. J. Math. **58** (2006), 115-153.

[42] K. James, *L-series with non-zero central critical value*, J. Amer. Math. Soc. **11** (1998), 635-641.

[43] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221-229.

[44] M.A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125-149.

[45] A. Knapp, *Elliptic Curves*, Princeton University Press, New Jersey 1992.

[46] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Grad. Texts in Math. **97**, Springer, New York, 1984.

[47] V. A. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and the Tate-Shafarevich* $E(\mathbb{Q})$ *for a subclass of Weil curves*,Izv. Akad. Nauk SSSR **52** (1988), 522-540.

[48] A. Kraus, *Sur l'équation* $a^3 + b^3 = c^p$, Experimental Math. **7** (1998), 1-13.

[49] M. Kuwata, L. Wang, *Topology of rational points on isotrivial elliptic surfaces*, Int. Math. Research Notices, **4** (1993), 113-123.

[50] S. Lang, *Elliptic Curves: Diophantine Analysis*, Springer-Verlag 1978, Grund-lehren der Math. Wiss.

[51] J.-J. Lee *Ranks of Jacobians of curves related to binary forms*, J. Ramanujan Math. Soc. **27** (2012), no. 2, 119-126.

[52] D. Lieman, *Non-vanishing of L-series associated to cubic twists of elliptic curves*, Ann. of Math. (2) **140**(1994), no. 1, 81-108.

[53] L. Mai, *The analytic rank of a family of elliptic curves*, Can. J. Math. **45(4)** (1993), 847-862.

[54] B. Mazur, *Rational isogenies of prime order*, Invent. Math. **44** (1978), 129-162.

[55] B. Mazur , *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1978), 33-186.

[56] A. Menezes, Y. Wu, R. Zuccherato, *An elementary introduction to hyperelliptic curves*, appendix in *Algebraic Aspects of Cryptography* by Neal Koblitz, Springer-Verlag, 1998, 155-178.

[57] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437-449.

[58] O. Neumann, *Elliptische Kurven mit vorgeschriebenen Reduktionsverhalten. I*, Math. Nachr. **49** (1971), 107-123.

[59] K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. **34.3** (1998), 651-660.

[60] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. **506** (1999), 85-116.

[61] S. Paulus, H.-G. Rück, *Real and imaginary quadratic representations of hyperelliptic function fields*, Mathematics of Computation **68** (1999), 1233-1241.

[62] B. Poonen, E. F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141-188.

[63] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431-476.

[64] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527-560.

[65] K. Rubin and A. Silverberg, *Ranks of elliptic curves in families of quadratic twists*, Experiment. Math. **9** (2000), 583-590.

[66] P. Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory **23** (1986), 294-317.

[67] B. Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. **10** (1975), 367-378.

[68] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), 179-230.

[69] A. Silverberg, *Torsion points on abelian varieties of CM-type*, Compositio Math. **68** (1988), no. 3, 241-249.

[70] A. Silverberg, *Points of finite order on abelian varieties*, Contemp. Math., **133** (1992), 175-193.

[71] J.H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Math. **106**, Springer - New York 1986.

[72] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Math. **151**, Springer-New York 1994.

[73] P. Stevenhagen, H. W. Lenstra, *Chebotarev and his Density Theorem,* Math. Intelligencer **18**, no. 2 (1996), 26-37.

[74] C.L. Stewart, J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc., **8** (1995), 943-973.

[75] M. Stoll, *On the Arithmetic of the Curves* $y^2 = x^l + A$, *II*, J. Number Theory **93** (2002), 183-206.

[76] P. Swinnerton-Dyer, *The effect of twisting on the 2-Selmer group*, Math. Proc. Camb. Phil. Soc. **145** (2008), no. 3, 513-526.

[77] M. Tada, *Congruent numbers over real quadratic fields*, Hiroshima Math. J. **31**(2001), 331-343

[78] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, In: Modular Functions of One Variable IV, Notes in Math. **476**, Springer-Verlag 1975.

[79] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1996), 134-144.

[80] J. Tate, F. Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3**, no. 1 (1970), 1-21.

[81] J. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983), 323-334.

[82] M. Ulas, *A note on higher twists of elliptic curves*, Glasg. Math. J., **52** (2010), 371-381.

[83] M. Ulas, *Variations on twists on elliptic curves*, Rocky Mountain J. Math, **43** (2) (2013), 645-660.

[84] V. Vatsal, *Rank-one twists of a certain elliptic curve*, Math. Ann. **311** (1998), 791-794.

[85] P. Voutier, M. Yabuta, *Lang's conjecture and sharp height estimates for the elliptic curves* $y^2 = x^3 + b$, Acta Arith. **173** (2016), no. 3, 197-224.

[86] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), 443-551.

[87] G. Yu, *On the quadratic twists of a family of elliptic curves*, Mathematika **52** (2005), no. 1-2, 139-154.

[88] A. Zinevicius, *On the congruent number problem over integers of cyclic number fields*, Math. Slovaca **66** (2016), no. 3, 561-564.

[89] A. Zinevicius, *On the congruent number problem over integers of real number fields*, Albanian J. Math. **8** (2014), no. 1, 49-53.

Prace wchodzące w skład osiągnięcia naukowego:

[A1] T. Jędrzejak, M. Ulas, *Characterization of torsion of the Jacobian of* $y^2 = x^5 + Ax$ *and some applications*, Acta Arith. **144** (2010), no. 2, 183-191.

[A2] T. Jędrzejak, *Characterization of the torsion of the Jacobians of two families of hyperelliptic curves*, Acta Arith. **161** (2013), No.3, 201-218.

[A3] T. Jędrzejak, M. Ulas, *Variations on twists of tuples of hyperelliptic curves and related results*, J. Number Theory **137** (2014), 222-240.

[A4] T. Jędrzejak, *On the torsion of the Jacobians of superelliptic curves* $y^q = x^p + a$, J. Number Theory **145** (2014), 402-425.

[A5] T. Jędrzejak, *On the torsion of the Jacobians of the hyperelliptic curves* $y^2 = x^n + a$ *and* $y^2 = x(x^n + a)$, Acta Arith. **174** (2016) , 99-120.

[A6] T. Jędrzejak, *A note on the torsion of the Jacobians of superelliptic curves* $y^q = x^p + a$, Banach Center Publications **108** (2016), 143-149.

Pozostałe prace naukowe mojego autorstwa w kolejności chronologicznej:

[B1] T. Jędrzejak, *Height estimates on cubic twists of the Fermat elliptic curve*, Bull. Austral. Math. Soc. **72** (2005), 177-186.

[B2] T. Jędrzejak, *The analytic rank of a family of jacobians of Fermat curves*, Bull. Polish Acad. Sci. Math. **56** (2008), 199-206.

[B3] A. Dąbrowski, T. Jędrzejak, *Ranks in families of Jacobian varieties of twisted Fermat curves*, Canad. Math. Bull. **53** (2010), 58-63.

[B4] T. Jędrzejak, J. Top, M. Ulas, *Tuples of hyperelliptic curves* $y^2 = x^n + a$, Acta Arith. **150** (2011), no. 2, 105-113.

[B5] A. Dąbrowski, T. Jędrzejak, K. Krawciów, *Cubic forms, power of primes and the Kraus method*, Colloq. Math. **128** (2012), no. 1, 35-48.

[B6] T. Jędrzejak, *Congruent numbers over real number fields*, Colloq. Math. **128** (2012), no. 2, 179-186.

[B7] T. Jędrzejak, *On twists of the Fermat cubic* $x^3 + y^3 = 2$, Int. J. Number Theory **10** (2014), 55-72.

[B8] T. Jędrzejak, M. Wieczorek, *Partitions of graphs and Selmer groups of elliptic curves of Neumann-Setzer type*, J. Ramanujan Math. Soc. **29**, no.1 (2014) 75-92.

[B9] A. Dąbrowski, T. Jędrzejak, L. Szymaszkiewicz, *Behaviour of the Order of Tate-Shafarevich Groups for the Quadratic Twists of* $X_0(49)$, in: Springer Proceedings in Mathematics & Statistics **188** (2016) *Elliptic Curves, Modular Forms and Iwasawa Theory*, 125-159.

[B3] A. Dąbrowski, T. Jędrzejak, *Ranks in families of Jacobian varieties of twisted Fermat curves*, Canad. Math. Bull. **53** (2010), 58-63.

[B4] T. Jędrzejak, J. Top, M. Ulas, *Tuples of hyperelliptic curves* $y^2 = x^n + a$, Acta Arith. **150** (2011), no. 2, 105-113.

[B5] A. Dąbrowski, T. Jędrzejak, K. Krawciów, *Cubic forms, power of primes and the Kraus method*, Colloq. Math. **128** (2012), no. 1, 35-48.

[B6] T. Jędrzejak, *Congruent numbers over real number fields*, Colloq. Math. **128** (2012), no. 2, 179-186.

[B7] T. Jędrzejak, *On twists of the Fermat cubic* $x^3 + y^3 = 2$, Int. J. Number Theory **10** (2014), 55-72.

[B8] T. Jędrzejak, M. Wieczorek, *Partitions of graphs and Selmer groups of elliptic curves of Neumann-Setzer type*, J. Ramanujan Math. Soc. **29**, no.1 (2014) 75-92.

[B9] A. Dąbrowski, T. Jędrzejak, L. Szymaszkiewicz, *Behaviour of the Order of Tate-Shafarevich Groups for the Quadratic Twists of* $X_0(49)$, in: Springer Proceedings in Mathematics & Statistics **188** (2016) *Elliptic Curves, Modular Forms and Iwasawa Theory*, 125-159.

Tomasz Jędrzejak