Zadania o krzywych eliptycznych prof. W.Gajda
wykład **DAKE 410**
Zima 2012

Zadanie 1. Niech E będzie krzywą zadaną równaniem $y^2 = f(x)$, gdzie $f \in \mathbf{Z}[x]$ jest wielomianem unormowanym stopnia 3, który ma różne pierwiastki w $\mathbf{C}$. Dowieść, że:

(a) $P = (x, y)$ jest punktem torsyjnym rzędu 2 wtedy i tylko wtedy, gdy $y = 0$ oraz $f(x) = 0$.

(b) $E(\mathbf{Q})[2]$ jest grupą skończoną, która ma 1, 2 lub 4 elementy. Podać przykłady krzywych E, które realizują te przypadki.

Zadanie 2. Niech E będzie krzywą zadaną równaniem $y^2 = f(x)$, gdzie $f \in K[x]$ jest wielomianem unormowanym stopnia 3 takim, że

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma),$$

gdzie α, β, $\gamma \in \bar{K}$. Definiujemy wyróżnik $D := [(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)]^2$. Dowieść, że E jest krzywą gładką wtedy i tylko wtedy, gdy $D \neq 0$.

Wskazówki.

(a) Na początek wykazać, że jeśli $f(x) \in K[x]$ jest wielomanem, a $f'(x)$ jest jego pochodną oraz $f(\delta) = f'(\delta) = 0$, to $f(x)$ ma pierwiastek podwójny w δ.

(b) Wykazać, że jeśli $y^2 = f(x)$ jest krzywą osobliwą, gdzie $f(x) \in K$ jest unormowanym wielomianem stopnia 3, to osobliwość jest w punkcie $(\delta, 0)$ i $f(\delta) = 0$.

(c) Dowieść, że $(\delta, 0)$ jest punktem osobliwym krzywej z (b) wtedy i tylko wtedy, gdy δ jest pierwastkiem podwójnym wielomianu $f(x)$. Wyprowadzić z tego równoważnośc: $D = 0$ *wtedy i tylko wtedy, gdy* E *jest krzywą osobliwą.*

Zadanie 3.

(a) Zastosuj metodę parametryzacji do okręgu C: $x^2 + y^2 = 1$ i punktu $P = (-1, 0)$, aby dowieść, że:

$$x = \frac{1 - t^2}{1 + t^2} \qquad y = \frac{2t}{1 + t^2}$$

jest parametryzacją krzywej C.

(b) Załóżmy, że x, y, i z są liczbami całkowitymi takimi, że $x^2 + y^2 = z^2$, $NWD(x, y, z) = 1$ i x jest parzyste. Korzystając z (a) pokazać, że istnieją liczby całkowite m, n takie, że $NWD(m, n) = 1$, $m - n$ jest nieparzyste oraz:

$$x = 2mn \qquad y = m^2 - n^2 \qquad z = m^2 + n^2.$$

Zadanie 4. Niech $p \neq 2$ będzie liczbą pierwszą, $a, b, c, d \in \mathbf{F}_p^\times$ i niech $C : ax^2 + bxy + cy^2 = dz^2$ będzie stożkową w $\mathbf{P}^2_{\mathbf{F}_p}$.

(a) Pokazać, że jeśli $b^2 \neq 4ac$, to $\#C(\mathbf{F}_p) = p + 1$.

(b) Pokazać, że jeśli $b^2 = 4ac$, to $\#C(\mathbf{F}_p) = 2$ lub $\#C(\mathbf{F}_p) = 2p + 1$.

Zadanie 5.

(a) Obliczyć grupę Mordella-Weila $E(\mathbf{F}_5)$ dla krzywej $E : y^2 = x^3 + x + 1$.

(b) Dowieść, że $E(\mathbf{F}_4) = \mathbf{Z}/8$, dla krzywej eliptycznej $E: y^2+xy = x^3+1$ zdefiniowanej nad ciałem $\mathbf{F}_2$, gdzie $\mathbf{F}_4 = \mathbf{F}_2(\omega) = \mathbf{F}_2[x]/(x^2+x+1)$ oraz $\omega^2 + \omega + 1 = 0$.

Zadanie 6. Niech $E/\mathbf{Q}$ $y^2 = X^3 + Ax + B$ będzie krzywą eliptyczną, która ma złą redukcję w $p > 2$. Wykazać, że wtedy $E(\mathbf{F}_p)$ ma dokładnie jeden punkt osobliwy.

Zadanie 7. Niech $E_t:\ y^2 + (1-t)xy - ty = x^3 - tx^2$ dla takich t, że

$$\Delta_t = t^5(t^2 - 11t - 1) \neq 0.$$

Z tabeli Kuberta wiemy, że $E_t(\mathbf{Q}) \supset \mathbf{Z}/5$. Wykorzystaj SAGE do znalezienia takich t, że $E_t(\mathbf{Q}) = \mathbf{Z}/5$ oraz $r_{E_t} = 0, 1, 2$. Spróbuj znaleźć takie t, dla których $r_{E_t} > 2$. W 2009 roku Dujella i Lecauchaux podali t, dla którego $E_t(\mathbf{Q}) = \mathbf{Z}/5$ oraz $r_{E_t} = 6$.

Zadanie 8. Niech p będzie liczbą pierwszą i niech $E_p:\ y^2 = x^3 + p^2$. Dowieśc, że:

(a) W grupie $E_p(\mathbf{Q})$ nie ma punktu torsyjnego $P = (x_P, y_P)$, dla którego

$$y_P \in \{\pm 1,\ \pm p^2,\ \pm 3p,\ \pm 3p^2,\ \pm 3\}.$$

(b) Punkt $Q = (0, p)$ należy do $E_p(\mathbf{Q})[3]$ oraz $E(\mathbf{Q})_{tors} \cong \mathbf{Z}/3$.

(c) Punkt $R = (-2, 1) \in E_3(\mathbf{Q})$ jest punktem nieskończonego rzędu.

Zadanie 9. Niech E będzie krzywą eliptyczną, która jest zdefiniowana nad ciałem $\mathbf{F}_q$, gdzie $q = p^{2m}$ oraz $p \neq 2, 3$. Załóżmy, że $\#E(\mathbf{F}_q) = q+1-2\sqrt{q}$.

(a) Niech ϕ_q oznacza endomorfim Frobeniusa. Dowieść, że $(\phi_q - p^m)^2 = 0$.

(b) Dowieść, że $\phi_q - p^m = 0$.

Wskazówka Należy skorzystać z faktu, który omawialiśmy na wykładzie: każdy niezerowy endomorfizm $\alpha\colon E(\bar{K}) \longrightarrow E(\bar{K})$ jest epimorfizmem.

(c) Sprawdzić, że Frobenius ϕ_q działa trywialnie na $E[p^m-1]$ i dlatego $E[p^m-1] \subset E(\mathbf{F}_q)$.

(d) Dowieść, że $E(\mathbf{F}_q) = \mathbf{Z}/(p^m-1) \oplus \mathbf{Z}/(p^m-1)$.

Zadanie 10. Obliczyć współrzędne zespolone punktów 2-torsyjnych i punktów 3-torsyjnych krzywej E: $y^2 = x^3 + 1$.

Zadanie 11. Niech E: $y^2 = x^3+Ax+B$ będzie krzywą eliptyczną określoną nad ciałem K charakterystyki różnej od 2, 3. Niech $j(E) := 1728\frac{4A^3}{4A^3+27B^2}$ oznacza $j-$inwariant krzywej E. Dla $d \in K^\times$ definiujemy nową krzywą eliptyczną $E^{(d)}$: $y^2 = x^3 + Ad^2x + Bd^3$.

(a) Dowieść, że $j(E) = j(E^{(d)})$

(b) Dowieść, że krzywe E i $E^{(d)}$ są izomorficzne nad ciałem $K(\sqrt{d})$.

(c) Podać przykład pary krzywych eliptycznych E_1 i E_2 określonych nad $\mathbf{Q}$, które są izomorficzne nad $\mathbf{Q}(\sqrt{d})$ dla pewnego $d \in \mathbf{Z}$, ale nie są izomorficzne nad ciałem $\mathbf{Q}$.

(d)* Niech E będzie krzywą eliptyczną zadaną nad ciałem skończonym $\mathbf{F}_q$, gdzie $q \neq 2$. Niech $a = q+1-\#E(\mathbf{F}_q)$ i niech $d \in \mathbf{F}_q^\times$. Korzystając z formuły Langa-Trottera dowieść, że $\#E^{(d)}(\mathbf{F}_q) = q+1-(\frac{d}{\mathbf{F}_q})a$.

Zadanie 12. Niech E: $y^2 = x(x-1)(x-\lambda)$ dla $\lambda \in K^\times$ i $\lambda \neq 1$.

(a) Sprowadzić E do równania Weierstrassa za pomocą podstawienia $x = x_1 + \frac{\lambda+1}{3}$ oraz obliczyć j-inwariant krzywej E :

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

(b) Pokazać, że jeśli $j \neq 0, 1728$, to istnieje sześć różnych wartości λ, które dają to samo j oraz, że jeśli λ jest jedną z nich, to

$$\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\}$$

stanowią zbiór tych sześciu wartości.

(c) Jeśli $j = 0$, to $\lambda = -1, 2, \frac{1}{2}$, a jeśli $j = 1728$, to $\lambda^2 - \lambda + 1 = 0$.

Zadanie 13. Obliczyć $E(\mathbf{Q})_{tors}$ dla krzywych eliptycznych E :

(a) E: $y^2 = x^3 + 8$

(b) E: $y^2 = x^3 + 4x$

(c) E: $y^2 = x^3 + 1$

(d) E: $y^2 = x^3 - px$, gdzie p jest liczbą pierwszą.

Zadanie 14. Niech $A \in M_{m,m}(K)$ będzie macierzą kwadratową o współczynnikach w ciele K. Dowieść, że w pierścieniu szeregów formalnych $K[[T]]$ zachodzi równość

$$exp(\sum_{n=1}^{\infty} tr(A^n)\frac{T^n}{n}) = \frac{1}{\det(I_m - AT)},$$

gdzie $tr(B) = \sum b_{ii}$ dla $B = [b_{ij}] \in M_{m,m}(K)$ oznacza ślad macierzy B.

Zadanie 15. Załóżmy, że E: $y^2 = x^3 + Ax + B$ gdzie $A, B \in \mathbf{Z}$ oraz $\Delta_E = -4A^3 - 27B^2 \neq 0$. Dla liczby pierwszej p, która nie dzieli Δ_E przyjmijmy oznaczenie $a_p = p+1-\#E(\mathbf{F}_p)$. Na wykładzie zdefiniowaliśmy L-szereg Hasse-Weila krzywej E za pomocą iloczynu nieskończonego:

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{(p,\Delta_E)=1} \frac{1}{p^{1-2s} - a_p p^{-s} + 1}$$

zmiennej zespolonej s. Pokazać, że dla $Re(s) > 3/2$ szereg $L(E,s)$ jest zbieżny bezwzględnie. Przypomnijmy, że Wiles dowiódł w 1994 roku, że $L(E,s)$ posiada przedłużenie analityczne na całą płaszczyznę zespoloną.

Wskazówka. Skorzystać z faktu, który dowiedliśmy na wykładzie: Jeśli

$$X^2 - a_p X + p = (X - \alpha)(X - \beta),$$

dla $\alpha, \beta \in \mathbf{C}$, to $|\alpha| = |\beta| = \sqrt{p}$.

Zadanie 16. Dowieść, że $E(\mathbf{Q}) = \mathbf{Z}/2 \oplus \mathbf{Z}/2$, gdzie E: $y^2 = x^3 - x$.

Zadanie 17. Jeśli $x = \frac{m}{n} \in \mathbf{Q}^\times$, gdzie $NWD(m,n) = 1$, to tak jak na wykładzie, określamy wysokość $H(x) = \max(|m|, |n|)$.

(a) Niech $P = (x,y)$ będzie punktem wymiernym na krzywej eliptycznej E : $y^2 = x^3 - 4$. Sprawdzić, że jeśli $x = \frac{m}{n}$, gdzie $NWD(m,n) = 1$, to

$$x(2P) = \frac{(m^3 + 32n^3)m}{4(m^3 - 4n^3)n}.$$

(b) Pokazać, że

$$144H(x(2P)) \geqslant H(x)^4.$$

(c) Korzystając z (b) dowieść, że na krzywej E istnieje nieskończenie wiele punktów wymiernych, to znaczy ranga grupy Mordella-Weila $E(\mathbf{Q})$ jest większa od zera.

Zadanie 18. Niech $E: y^2 = x^3 + Ax + B$ będzie krzywą eliptyczną zdefiniowaną nad ciałem K taką, że $j(E) = j$. Zakładamy, że $\operatorname{char} K \neq 2, 3$. Pokazać, że:

(i) jeśli $j \neq 0$, 1728, to przyporządkowanie $dK^{\times 2} \mapsto [E'_d]$, gdzie

$$E'_d: y^2 = x^3 + Ad^2x + Bd^3,$$

ustala bijekcję grupy $K^\times/K^{\times 2}$ ze zbiorem klas K-izomorfizmów krzywych eliptycznych $[E']$ takich, że $j(E') = j$

(ii) jeśli $j = 0$, to przyporządkowanie $dK^{\times 6} \mapsto [E'_d]$, gdzie

$$E'_d: y^2 = x^3 + Bd,$$

ustala bijekcję grupy $K^\times/K^{\times 6}$ ze zbiorem klas K-izomorfizmów krzywych eliptycznych $[E']$ takich, że $j(E') = 0$

(iii) jeśli $j = 1728$, to przyporządkowanie $dK^{\times 4} \mapsto [E'_d]$, gdzie

$$E'_d: y^2 = x^3 + Adx,$$

ustala bijekcję grupy $K^\times/K^{\times 4}$ ze zbiorem klas K-izomorfizmów krzywych eliptycznych $[E']$ takich, że $j(E') = 1728$.

Zadanie 19. Niech $E: y^2 = x^3 + Ax + B$ będzie krzywą eliptyczną zdefiniowaną nad ciałem K. Dowieść, że forma różniczkowa $\frac{dx}{y}$ jest niemiennicza ze względu na translacje, to znaczy: dla $(u, v) \in E(L)$, gdzie L/K jest rozserzeniem ciał jeżeli

$$(x, y) + (u, v) = (f(x, y), g(x, y)),$$

gdzie $f(x, y)$, $g(x, y) \in L(x, y)$, to

$$\frac{\frac{\partial f}{\partial x}}{g(x, y)} = \frac{1}{y}.$$

Zadanie 20. Dowieść, że dla każdej liczby pierwszej $p \geqslant 3$ liczba punktów $\mathbf{F}_p-$wymiernych na krzywej $E: y^2{=}x^3{+}x$ jest podzielna przez 4.

Zadanie 21. Niech $P \in E(\mathbf{Q})$ będzie punktem $\mathbf{Q}-$wymiernym na $E: y^2{=}x^3{+}Ax{+}B$, gdzie $A, B \in \mathbf{Z}$. Dowieść, że istnieją liczby całkowite a, b i $d \neq 0$ takie, że $NWD(d, ab){=}1$ oraz $P{=}(\frac{a}{d^2}, \frac{b}{d^3})$.

Zadanie 22. Niech E_1 i E_2 będą krzywymi eliptycznymi nad ciałem skończonym $\mathbf{F}_p$ i niech $\phi: E_1 \longrightarrow E_2$ będzie izogenią nad $\mathbf{F}_p$ (tzn. ϕ jest homomorfizmem grup algebraicznych nad $\mathbf{F}_p$, który ma skończone jądro). Dowieść, że wtedy grupy $E_1(\mathbf{F}_p)$ i $E_2(\mathbf{F}_p)$ są równoliczne. **Uwaga.** Tate dowiódł, ze odwrotne twierdzenie jest również prawdziwe.

Zadanie 23. Korzystając z twierdzenia Lutz-Nagella i twierdzenia o redukcji oblicz $E(\mathbf{Q})_{tors}$ dla krzywych E: $y^2 = x^3 \pm px$, gdzie p jest liczbą pierwszą. Za pomocą SAGE lub innego pakietu numerycznego oblicz rangę grup Mordella-Weila $E(\mathbf{Q})$ powyższych krzywych dla wielu wartości p. Postaw odpowiednią hipotezę o randze tych grup i przeprowadź jej dowód.[1]

Zadanie 24. Niech $E/\mathbf{Q}$ będzie krzywą eliptyczną zadaną krotkim równaniem Weierstrassa i taką, że $j(E) = 0$.

[1] Ta część zadania wymaga umiejętności posługiwania się programem mwrank lub innym, który oblicza rangę grupy Mordella-Weila

(a) Dowieść, że istnieje dokładnie jedna, wolna od sześcianów liczba całkowita D taka, że krzywa E zadana jest równaniem $y^2=x^3+D$.

(b) Niech $p \equiv 2 \bmod 3$ będzie liczbą pierwszą, która nie dzieli $6D$. Dowieść, że $\#\bar{E}_p(\mathbf{F}_p)=p+1$.

(c) Dowieść, że $\#E(\mathbf{Q})_{tors}$ dzieli 6.

(d)* Dokładniej - pokazać, że grupa $E(\mathbf{Q})_{tors}$ równa jest:

$\mathbf{Z}/6$, gdy $D = 1$;

$\mathbf{Z}/3$, gdy $D \neq 1$ i D jest sześcianem, lub $D=-432$;

$\mathbf{Z}/2$, gdy $D \neq 1$ i D jest kwadratem; oraz jest grupą trywialną w pozostałych przypadkach.

Zadanie 25. Sprowadzić następujące równania do skróconej postaci Weierstrassa. Zakładamy, że *char* $K \neq 2, 3$.

(i) $X^3 + Y^3 + dZ^3 = 0$ (ii) $X^3 + Y^3 + Z^3 - mXYZ = 0$

(iii) $Y^2 - kT^2 = X^2$, $Y^2 + kT^2 = Z^2$ (iv) $X_1^2X_2 - X_1X_2^2 + X_1X_3^2 + X_2X_3 = 0$.

Zadanie 26.

(i) Znaleźć wszystkie punkty $\mathbf{F}_5$-wymierne na krzywych:

$$Y^2Z = X^3 + XZ^2, \quad Y^2Z = X^3 + 2XZ^2, \quad Y^2Z = X^3 + Z^3.$$

W każdym przypadku sprawdź, że zbiór punktów $\mathbf{F}_5$-wymiernych razem z punktem $[0, 1, 0]$ stanowi grupę.

(ii) Podobnie jak w (i), ale dla innych $\mathbf{F}_p$ i krzywych: $Y^2Z = X^3 + AXZ^2 + BZ^3$. Znaleźć p, A i B dla których grupa punktów $\mathbf{F}_p$-wymiernych nie jest grupą cykliczną. Czy istnieje taki przykład grupy, która ma więcej niż dwa generatory ?

Zadanie 27.

(i) Niech $E : y^2 + y = x^3 - x^2 - 10x - 20$ oraz $E' : y^2 + y = x^3 - 93x + 625$. Sprowadzić E i E' do skróconej postaci Weierstrassa. Czy krzywe E i E' są izomorficzne nad ciałem $\mathbf{Q}$? nad domknięciem algebraicznym ciała $\mathbf{Q}$?

(ii) Ile istnieje klas izomorfizmów krzywych eliptycznych nad ciałem $\mathbf{F}_5$? nad ciałem $\mathbf{F}_{13}$?

Zadanie 28. Niec $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$, gdzie $e_i \in \mathbf{Q}$ są różnymi liczbami wymiernymi takimi, że $e_1 + e_2 + e_3 = 0$. Ponadto, załóżmy, że $e_1 - e_2 = n^2$ i $e_2 - e_3 = m^2$ są kwadratami. W tym zadaniu dowodzimy, że przy tych założeniach istnieje punkt $P = (x_0, y_0) \in E(\mathbf{Q})$ taki, że $2P = (e_1, 0)$ czyli P jest rzędu 4.

(a) Wykazać, że $e_1 = \frac{n^2+m^2}{3}$, $e_2 = \frac{m^2-2n^2}{3}$ oraz $e_3 = \frac{n^2-2m^2}{3}$.

(b) Wyznaczyć A i B (w terminach m i n) takie, że $x^3 + AX + B = (x - e_1)(x - e_2)(x - e_3)$. SAGE może okazać się przy tym pomocne.

(c) Niech $p(x) = x^4 - 2Ax^2 - 8Bx + A^2 - 4(x^3 + Ax + B)e_1$. Wykazać, że $p(x_0) = 0$ wtedy i tylko wtedy, gdy $x(2P) = e_1$, czyli, gdy $2P = (e_1, 0)$.

(d) Wyrazić wsółczynniki wielomianu $p(x)$ za pomocą m i n (Wykorzystaj SAGE).

(e) Znaleźć rozkład wielomianu $p(x)$ na czynniki dla $(n, m) = (3, 6)$, $(3, 12)$, $(9, 12)$, ...

(f) Zapisać $p(x) = (x-a)^2(x-b)^2$ dla pewnych a i b. Wyrazić współczyniki wielomianu $p(x)$ za pomocą a i b.

(g) W końcu, porównując wpółczynniki $p(x)$ wyrażone przez a, b oraz przez n, m obliczyć pierwiastki wielomianu $p(x)$ za pomocą n i m.

(h) Zapisać $P = (x_0, y_0)$ za pomocą n i m.

Zadanie 29. Niech $E : y^2 = x^3 - 10081x$. Za pomocą programu SAGE wyznaczyć minimalny zbiór generatorów podgrupy w $E(\mathbf{Q})$, którą generują punkty:

$$(0,0), \quad (-100,90), \quad (\frac{10081}{100}, \frac{90729}{1000}), \quad (-17,408),$$

$$(\frac{907137}{6889}, \frac{-559000596}{571787}), \quad (\frac{1681}{16}, \frac{20295}{64}),$$

$$(\frac{833}{4}, \frac{21063}{8}), \quad (\frac{-161296}{1681}, \frac{19960380}{68921}), \quad (\frac{-6790208}{168921}, \frac{-40498852616}{69426531}).$$

Wykorzystać Twierdzenie 8.8.

Zadanie 30. Krzywa $E : y^2 = x^3 - (157)^2x$ ma punkt wymierny Q, którego wspołrzędną odciętą jest liczba

$$x(Q) = (\frac{224403517704336969924557513090674863160948472041}{1782466453785771917605107035793432714003296166 0})^2.$$

Wykazać, że istnieje punkt $P \in E(\mathbf{Q})$ taki, że $2P = Q$. Znaleźć $x(P)$.

Zadanie 31. Wykazać, że przestrzeń jednorodna: $C : \ 2Y^2 - X^2 = 34, \quad Y^2 - Z^2 = 34$ nie posiada punktów wymiernych $(X, Y, Z) \in \mathbf{Q}^3$. **Wskazówka:** Zmodyfikować układ równań zadający C w ten sposó, aby w mianownikach nie występowały potęgi liczby 2, a następnie rozważyć kongruencje modulo 8.

Zadanie 32. Dla następujących krzywych wyznaczyć rangę $E(\mathbf{Q})$ i generatory $E(\mathbf{Q})/2E(\mathbf{Q})$ za pomocą metody 2−spadku z wykładów 10 i 11. **Nie korzystać** przy tym z SAGE'a.

(a) $E : y^2 = x^3 - 14931x + 220590$

(b) $E : y^2 = x^3 - x^2 - 6x$

(c) $E : y^2 = x^3 - 37636x$

(d) $E : y^2 = x^3 - 962x^2 + 148417x$ (W tym przypadku rozpocząć od oszacowania rangi za pomocą Twierdzenia 8.8.)

$E : y^2 = x^3 - 14931x + 220590$

Zadanie 33. (*Krzywe wysokiej rangi*) Celem tego zadania jest znajdowanie bez użycia tablic krzywych eliptycznych określonej rangi Mordella-Weila.

(**Łatwe**) Znaleźć trzy nieizomorficzne krzywe eliptyczne nad $\mathbf{Q}$, których rangi Mordella-Weila są nie mniejsze od 2 (Wykorzystać SAGE do obliczenia macierzy wysokości).

(**Średnio trudne**) Znaleźć trzy nieizomorficzne krzywe eliptyczne nad $\mathbf{Q}$, których rangi Mordella-Weila są nie mniejsze od 3.

(**Trudniejsze**) Znaleźć trzy nieizomorficzne krzywe eliptyczne nad $\mathbf{Q}$, których rangi Mordella-Weila są nie mniejsze od 6. Jeśli to się już udało, to można teraz wyznaczyć trzy nieizomorficzne krzywe eliptyczne nad $\mathbf{Q}$, których rangi Mordella-Weila są nie mniejsze od 8.

(**Istotnie trudniejsze**) Znaleźć trzy nieizomorficzne krzywe eliptyczne nad $\mathbf{Q}$, których rangi Mordella-Weila są nie mniejsze od 10.

(**Droga do sławy**) Znaleźć krzywą eliptyczną nad $\mathbf{Q}$, której ranga Mordella-Weila jest nie mniejsza od 29.

Zadanie 34. Niech E będzie krzywą eliptyczną na ciałem liczb wymiernych i niech $P_1, P_2, \ldots, P_n \in E(\mathbf{Q})$ będą punktami których obrazy generują grupę $E(\mathbf{Q})/2E(\mathbf{Q})$. Niech G będzie podgrupą w $E(\mathbf{Q})$ generowaną przez $P_1, P_2, \ldots, P_n$.

(1) Wykazać, że indeks G w $E(\mathbf{Q})$ jest skończony.

(2) Dowieść, że w zależności od wyboru generatorów $\{P_i\}$ grupy $E(\mathbf{Q})/2E(\mathbf{Q})$ liczba elementów grupy ilorazowej $E(\mathbf{Q})/G$ może być dowolnie duża.

Zadanie 35. Zgodnie z pewnym twierdzeniem Fermata równanie $x^3 + y^3 = z^3$ nie ma rozwiązań całkowitych, dla których $xyz \neq 0$. Znaleźć najmniejszą liczbę naturalną d, dla której równanie $x^3 + y^3 = dz^3$ ma nieskończenie wiele rozwiązań. Wyznaczyć generator i obliczyć kilka przykładowych rozwiązań.

Zadanie 36. Niech $E/\mathbf{Q}$ będzie krzywą eliptyczną i niech p będzie liczbą pierwszą. Symbolem $E^{ns}(\mathbf{F}_p)$ oznaczamy zbiór punktów nieosobliwych krzywej nad ciałem skończonym $\mathbf{F}_p$ oraz $N_p^{ns} := \#E^{ns}(\mathbf{F}_p)$. W szczególności jeśli w p krzywa E ma dobrą redukcję, to $N_p^{ns} := \#E(\mathbf{F}_p) = p + 1 - a_p$.

(a) Załóżmy, że E ma złą redukcję w p. Wykazać, że:

- $N_p^{ns} = p$, jeśli E ma złą addytywną redukcję w p
- $N_p^{ns} = p-1$, jeśli E ma złą multyplikatywną rozłożoną redukcję (split multiplicative reduction) w p
- $N_p^{ns} = p + 1$, jeśli E ma złą multyplikatywną nierozłożoną redukcję (non-split multiplicative reduction) w p.

(b) Wyprowadzić z tego równość na lokalny L-czynnik funkcji Hasse-Weila: $L_p(p^{-1}) = \frac{N_p^{ns}}{p}$ dla wszystkich $p \geqslant 2$ takich, że E ma dobrą lub złą redukcję w p. **Wskazówka.** Porównaj zadania 2 i 6.

Zadanie 37. Niech $E/\mathbf{Q}$ będzie krzywą eliptyczną i niech $L(E, s)$ oznacza jej L-szereg Hasse-Weila. Definiujemy ciąg liczb $(a_n)_{n=1}^{\infty}$ w następujący sposób: $a_1 = 1$ i dla liczby pierwszej p

- $a_p = p + 1 - \#E(\mathbf{F}_p)$, jeśli E ma dobrą redukcję w p
- $a_p = 0$, jeśli E ma złą addytywną redukcję w p
- $a_p = 1$, jeśli E ma złą multyplikatywną rozłożoną redukcję (split multiplicative reduction) w p
- $a_p = -1$, jeśli E ma złą multyplikatywną nierozłożoną redukcję (non-split multiplicative reduction) w p.

Jeśli $n = p^r$ dla liczby pierwszej p i $r \geqslant 1$, to a_{p^r} definiujemy za pomocą rekurencji $a_p a_{p^r} := a_{p^{r+1}} + p a_{p^{r-1}}$, jeśli E ma dobrą redukcję w p, oraz $a_{p^r} := (a_p)^r$, jeśli E ma złą redukcję w p. W końcu $a_{nm} := a_n a_m$, jeśli n i m są względnie pierwsze. Wykazać, że $L(E, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$. **Wskazówka.** Wykorzystać podstawowe twierdzenie arytmetyki i wzór na sumę szeregu geometrycznego.

Zadanie 38. Wyprowadzić hipotezę o parzystości z hipotezy Bircha i Swinnertona-Dyera oraz z równania funkcyjnego dla L-funkcji Hasse-Weila. **Wskazówka.** Wykorzystać rozwinięcie Taylora L-szeregu $L(E, s)$ w $s = 1$. Wyprowadzić z tego, że jeśli liczba $w(E) = -1$, to $E(\mathbf{Q})$ jest nieskończonym zbiorem.

Zadanie 39. (krzywe Freya) Niech $p > 3$ będzie liczbą pierwszą i niech $a, b, c \in \mathbf{Z}$ będą parami względnie pierwsze, $a^p + b^p = c^p$ i $abc \neq 0$. Definiujemy krzywą eliptyczną $E/\mathbf{Q}$:

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

W tym zadaniu wykażemy, że E jest *semistabilną* krzywą o przewodniku $N_E = \prod_{\ell | abc} \ell$.

(a) Wykazać, że po ewentualnej zamianie liczb możemy założyć, że $a \equiv 0 \bmod 2$ oraz $b \equiv c \equiv 1 \bmod 4$.

(b) Obliczyć wyróżnik Δ_E.

(c) Wykazać, że E ma dobrą redukcję we wszystkich liczbach pierwszych ℓ, które nie dzielą abc.

(d) Wykazać, że jeśli $\ell \geqslant 3$ jest liczbą pierwszą, która dzieli abc, to $E/\mathbf{Q}$ ma złą multyplikatywną redukcję w ℓ.

(e) Dowieść, że $E/\mathbf{Q}$ ma złą multyplikatywna redukcję w $\ell = 2$. **Wskazówka.** Zastosować zamianę zmiennych:

$$x = \frac{X}{4}, \qquad y = \frac{Y}{8} + \frac{3X}{8}$$

do znalezienia innego, izomorficznego modelu dla $E/\mathbf{Q}$. Wykazać, że ten model ma współczynniki w $\mathbf{Z}$ i przeanalizować jego redukcję na $\ell = 2$.

(f) Wyprowadzić z tego, że przewodnik krzywej E wynosi $N_E = \prod_{\ell | abc} \ell$.