Teoria liczb
mix, 1-5 czerwca

Zadanie 1 (krzywa, która jest eliptyczna, choć nie wygląda)**.** Rozważmy zbiór rozwiązań

$$S := \left\{(t,u) \in \mathbb{C}^2 \mid u^2 = t^4 - 1\right\}$$

oraz przekształcenie $\pi\colon S \setminus \{(1,0)\} \to \mathbb{C}^2$ zadane wzorem

$$\pi\,(t,u) = \left(\frac{1}{t-1}, \frac{u}{(t-1)^2}\right).$$

(a) Pokaż, że przekształcenie π jest injektywne.

(b) Pokaż, że jego obraz zawiera się w zbiorze $y^2 = f(x)$ dla pewnego wielomianu f *stopnia trzy*, który nie ma pierwiastków wielokrotnych w $\mathbb{C}$. Znajdź f.

(c) Pokaż odwrotnie, że jeśli $(x,y) \in \mathbb{C}^2$ są takie, że $y^2 = f(x)$ oraz $x \neq 0$, to $(x,y) = \pi(t,u)$ dla pewnych $(t,u) \in S$.

Zadanie 2. Niech f będzie wielomianem unormowanym stopnia 3 o współczynnikach w ciele $\Bbbk$, który posiada w $\Bbbk$ pierwiastek wielokrotny.

(a) Pokaż, że jest dokładnie jeden taki pierwiastek, niech będzie to $x_0 \in \Bbbk$.

(b) Pokaż, że zbiór $E(\Bbbk) \setminus \{(x_0,0)\}$ tworzy grupę z działaniem jak na wykładzie. *Wskazówka: dowód łączności jest ten sam i nie potrzeba go powtarzać.*

(c) $\star$ Niech $\Bbbk$ będzie ciałem dowolnej charakterystyki, zaś $f(x) = x^3$. Pokaż, że grupa powyżej jest izomorficzna z grupą $\mathbb{G}_{\mathrm{a}}(\Bbbk) := (\Bbbk, +)$.

(d) $\star$ Niech $\Bbbk$ będzie ciałem charakterystyki dwa, zaś $f(x) = x^3 - x$, zatem krzywa ma równanie Weierstrassa $y^2 = x^3 - x$. Pokaż, że grupa powyżej jest izomorficzna z grupą $\mathbb{G}_{\mathrm{m}}(\Bbbk) := (\Bbbk \setminus \{0\}, \cdot)$.

(e) $\star$ Pokaż, że powyższe dwie możliwości są jedyne, tzn. dla dowolnego f z pierwiastkiem wielokrotnym, grupa $E(\Bbbk) \setminus \{(x_0,0)\}$ powyżej jest izomorficzna z $\mathbb{G}_{\mathrm{m}}(\Bbbk)$ lub $\mathbb{G}_{\mathrm{a}}(\Bbbk)$.

Zadanie 3. Niech E będzie krzywą eliptyczną zadaną równaniem $y^2 = f(x)$, gdzie f ma współczynniki w ciele $\mathbb{Z}_p$. Zadajmy endomorfizm Frobeniusa dla ciała $K \supseteq \mathbb{Z}_p$ jako $F\colon K^2 \to K^2$, $F(x,y) = (x^p, y^p)$.

(a) Pokaż, że F obcina się do endomorfizmu zbioru $\{(x,y) \in K^2 \mid y^2 = f(x)\} \subseteq E(K)$. Uznajmy, że $F(0_E) = 0_E$.

(b) Pokaż, że $E(\mathbb{Z}_p) = \ker(F - \mathrm{id})$ jako podzbiory $E(\overline{\mathbb{Z}_p})$, gdzie po prawej stronie dodajemy endomorfizmy krzywej eliptycznej.