Teoria liczb
równania stopnia trzy, 18-22 maja

We wszystkich poniższych zadaniach krzywa E jest zdefiniowana nad ciałem $\Bbbk$. Bez większych problemów możesz założyć, że $\Bbbk = \mathbb{Q}$ lub $\Bbbk = \mathbb{Z}_p$.

Zadanie 1. Niech E będzie krzywą eliptyczną zadaną równaniem $y^2 = x^3 - x$. Dla $p = 3, 5, 7$ ustal liczbę punktów $E(\mathbb{Z}_p)$, nie zapomnij o punkcie w nieskończoności, oraz zbadaj, jaka jest grupa $E(\mathbb{Z}_p)$. A co otrzymujemy dla $p = 2$?

Zadanie 2. Zakładamy, że charakterystyka ciała bazowego jest różna od $2, 3$.

(a) Sprawdź, że równanie $y^2 = x^3 - x^2$ nie definiuje krzywej eliptycznej oraz, że równanie $y^2 = x^3 - 1$ definiuje krzywą eliptyczną.

(b) Sprawdź ogólnie, że gdy $f(x) \in \Bbbk[x]_{\leq 3}$ jest wielomianem stopnia trzy, to następujące warunki są równoważne

  (a) równanie $y^2 = f(x)$ definiuje krzywą eliptyczną,

  (b) wielomiany $f, \partial_x f$ są względnie pierwsze.

(c) $\star$ Pokaż, że wielomian $f(x) = x^3 + ax + b$ ma pierwiastek wielokrotny wtedy i tylko wtedy, gdy f i f' nie są względnie pierwsze, wtedy i tylko wtedy, gdy $4a^3 + 27b^2 = 0$.

Zadanie 3. Niech E będzie krzywą eliptyczną o współczynnikach w ciele charakterystyki różnej od dwa. Punkt $p \in E$ nazywamy 2-*torsyjnym* jeśli $2p = 0$.

(a) Pokaż, że nieneutralny punkt $p = (x, y)$ jest 2-torsyjny wtedy i tylko wtedy, gdy $y = 0$.

(b) Jakie są możliwe liczby punktów 2-torsyjnych w $E(\Bbbk)$?

Uwaga: dodawanie wykonujemy tu na E, tzn. $2p = p +_E p$ oraz 0 jest elementem neutralnym w E.

Zadanie 4. Niech p będzie liczbą pierwszą taką, że $p \equiv 2 \pmod 3$ i niech $a \in \mathbb{Z}$. Pokaż, że jest dokładnie p rozwiązań równania $y^2 = x^3 + a$ w liczbach $(x, y) \in \mathbb{Z}_p^2$.