Teoria liczb
mix, 25-29 maja

Zadanie 1. Niech E będzie krzywą eliptyczną zadaną równaniem $y^2 = x^3 - Dx$, gdzie D jest ustaloną liczbą całkowitą. Pokaż, że E indukuje krzywą eliptyczną nad $\mathbb{Z}_p$ wtedy i tylko wtedy, gdy p nie dzieli $2D$.

Zadanie 2 (krzywa eliptyczna z zespolonym mnożeniem)**.** Pokaż, że dla każdej liczby pierwszej $p \equiv 1 \pmod 4$, krzywa eliptyczna zadana równaniem $y^2 = x^3 + x$ ma liczbę punktów $E(\mathbb{Z}_p)$ podzielną przez 4. *Wskazówka: znajdź symetrie.*

Zadanie 3. Niech $p > 2$ będzie liczbą pierwszą.

(a) Uzasadnij, że E zadana równaniem $y^2 = x^3 - x$ jest krzywą eliptyczną, gdy współczynniki zredukujemy modulo p.

(b) Załóżmy, że $E(\mathbb{Z}_p)$ ma b rozwiązań. Oblicz liczbę rozwiązań $E(\mathbb{Z}/p^k)$ dla każdego k. *Wskazówka: rozważ na początku konkretne p i $k = 2$ i zobacz, jak zmienia się liczba rozwiązań.*