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 $2D$.

Rozwiązanie.

Wiemy z wykładu, że równanie $y^2 = x^3 - Dx$ potraktowane modulo p definiuje krzywą eliptyczną wtedy i tylko wtedy, gdy modulo p układ

$$\begin{cases} y^2 = x^3 - Dx \\ 2y = 0 \\ 0 = 3x^2 - D \end{cases}$$

nie ma rozwiązań w algebraicznym domknięciu $\mathbb{Z}_p$. (Szczęśliwie, w tym przypadku nie potrzebujemy wiedzieć, czym jest to domknięcie.) Załóżmy najpierw, że p nie dzieli $2D$ i że (x_0, y_0) jest rozwiązaniem. Wtedy z drugiego równania wynika $y_0 = 0$. Z pozostałych równań wynika wtedy $0 = 3(x_0^3 - x_0 D) - x_0(3x_0^2 - D) = 2Dx_0$. Zatem $x_0 = 0$. Z ostatniego równania wynika wtedy $D = 0$, sprzeczność.

Załóżmy teraz, że p dzieli $2D$. Jeśli p dzieli 2, to $p = 2$, więc $(x_0, y_0) = (D, 0)$ jest rozwiązaniem bowiem $D^2 \equiv D \pmod 2$. Jeśli zaś p dzieli D, to $(x_0, y_0) = (0, 0)$ jest rozwiązaniem.

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.*

Rozwiązanie.

Grupa $\mathbb{Z}_p^*$ jest cykliczna rzędu $p-1$. Z założenia, 4 dzieli $p-1$, więc w grupie tej istnieje element rzędu 4, na przykład $g^{\frac{p-1}{4}}$, gdzie g jest generatorem (dowolnie wziętym). Oznaczmy ten element jako $i \in \mathbb{Z}_p$. Wtedy $i^2 \equiv -1 \pmod p$.

Przejdźmy do rozwiązania zadania. Niech

$$\mathcal{S} := \left\{(x_0, y_0) \in \mathbb{Z}_p^2 \mid y_0^2 \equiv x_0^3 + x_0\right\}.$$

Rozważmy odwzorowanie liniowe $\alpha\colon \mathbb{Z}_p^2 \to \mathbb{Z}_p^2$ zadane przez $(x_0, y_0) \mapsto (-x_0, iy_0)$, gdzie i jest zdefiniowane jak wyżej. Zauważmy, że $\alpha(\alpha(x_0, y_0)) = (x_0, -y_0)$, więc czterokrotne złożenie α jest identycznością. Ponadto jeśli $y_0^2 \equiv x_0^3 + x_0 \pmod p$, to również

$$(iy_0)^2 \equiv -y_0^2 = (-x_0)^3 + (-x_0) \pmod p.$$

Zatem $\alpha(\mathcal{S}) \subseteq \mathcal{S}$.

Dokończenie rozwiązania korzysta z języka działań grup na zbiorze. Odwzorowanie α zadaje działanie grupy C_4 na $\mathcal{S}$. Orbity tej grupy mogą być czteroelementowe, dwuelementowe lub jednoelementowe. Jeśli element (x_0, y_0) ma orbitę złożoną z mniej niż 4 elementów, to jego stabilizator jest nietrywialną podgrupą C_4, więc zawiera element α^2. To znaczy, że $(x_0, y_0) = \alpha^2(x_0, y_0) =$

$(x_0, i^2 y_0) = (x_0, -y_0)$, czyli $y_0 = 0$. Zatem są trzy punkty, które mają orbitę mniejszą niż czteroelementową: $(0,0)$, $(i,0)$, $(-i,0)$. To pokazuje, że zbiór $\mathcal{S}$ ma $4k+3$ elementów, gdzie k jest liczbą orbit czteroelementowych. Doliczając punkt $0_E \in E(\mathbb{Z}_p) \setminus \mathcal{S}$ otrzymujemy liczbę $4k+4$ podzielną przez 4.

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.*

Rozwiązanie.
(a) Wynika to z zadania pierwszego dla $D = 1$.
(b) Pokażemy, że liczba rozwiązań wynosi $p^{k-1}(b-1)+1$. (Dziwaczne -1 i $+1$ wynikają z dodatku punktu w nieskończoności.) Niech

$$\mathcal{S}_k := \left\{(x_0, y_0) \in (\mathbb{Z}/p^k)^2 \mid y_0^2 = x_0^3 - x_0\right\}.$$

Twierdzimy zatem, że $|\mathcal{S}_k| = p^{k-1}(b-1)$. Dla $k = 1$ wynika to z określenia b. Mamy odwzorowanie $\pi_k \colon \mathcal{S}_{k+1} \to \mathcal{S}_k$ pochodzące od $\mathbb{Z}/p^{k+1} \twoheadrightarrow \mathbb{Z}/p^k$. Pokażemy, że dla każdego elementu $(x_0, y_0) \in \mathcal{S}_k$, zbiór $\pi_k^{-1}((x_0, y_0))$ ma p elementów. Przez indukcję, pokaże to, że $|\mathcal{S}_k| = p^{k-1}(b-1)$ dla każdego k, czyli tezę.

Dokładniej, pokażemy, że jeśli $(x_0, y_0) \in \mathcal{S}_k$ oraz $y_1 \in \mathbb{Z}/p^{k+1}$ jest takie, że $y_1 \mod p^k = y_0$, to istnieje dokładnie jeden element $x_1 \in \mathbb{Z}/p^{k+1}$ taki, że $x_1 \mod p^k = x_0$ oraz $(x_1, y_1) \in \mathcal{S}_{k+1}$. Weźmy zatem rozwiązanie $(x_0, y_0) \in \mathcal{S}_k$, element $y_1 \in \mathbb{Z}/p^{k+1}$ i dowolne liczby całkowite (x', y') takie, że $x_0 = x' \mod p^k$ oraz $y_1 = y' \mod p^{k+1}$. Skoro $(x_0, y_0) \in \mathcal{S}_k$ oraz $y' \mod p^k = y_0$, to

$$(y')^2 - ((x')^3 - x') = p^k r$$

dla pewnego $r \in \mathbb{Z}$. Niech $x' = x'' + ap^k$. Podstawiając to do równania powyżej, otrzymujemy

$$(y')^2 - ((x'')^3 - x'') \equiv (y')^2 - ((x')^3 - x') - 3(x')^2 ap^k - ap^k \equiv p^k\left(r - 3(x')^2 a - a\right) \pmod{p^{k+1}}. \quad (1.1)$$

Zauważmy, że $3(x')^2 + 1 \not\equiv 0 \mod p$, bowiem inaczej $(x' \mod p, y' \mod p)$ byłoby punktem osobliwym E, co przeczy (a). Zatem w sytuacji (1.1) równanie $r - (3(x')^2 + 1)a \equiv 0 \pmod{p}$ ma jednoznaczne rozwiązanie $a \mod p$. To znaczy, że element x'' powyżej jest wyznaczony jednoznacznie modulo p^{k+1}, więc mamy jednoznaczne rozwiązanie $(x'' \mod p^{k+1}, y' \mod p^{k+1}) \in \mathcal{S}_{k+1}$ takie, że $x'' \mod p^k = x_0$.