Teoria liczb
równania stopnia trzy, 18-22 maja

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

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 $p = 2$?

Rozwiązanie.

Niech $p = 3$. Kwadraty w $\mathbb{Z}_3$ to $0 \mod 3$, $1 \mod 3$. Z małego twierdzenia Fermata mamy $x^3 - x \equiv 0 \mod 3$. Zatem rozwiązania to $\{(0,0), (1,0), (2,0)\}$. Wobec tego

$$E(\mathbb{Z}_3) = \{(0,0), (1,0), (2,0)\} \cup \{0_E\}.$$

Z wykładu wiemy, że $2(x_0, 0) = 0_E$ dla każdego x_0. Zatem każdy niezerowy punkt grupy ma rząd dwa (i grupa jest przemienna), co pokazuje, że $E(\mathbb{Z}_3)$ jest izomorficzna z $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Niech $p = 5$. Kwadraty w $\mathbb{Z}_5$ to $0 \mod 5, 1 \mod 5, 4 \mod 5$. Obliczamy, że

x	0	1	2	3	4
$x^3 - x \mod 5$	0	0	1	4	0

Zatem $E(\mathbb{Z}_5) = \{(0,0), (1,0), (2,1), (2,4), (3,2), (3,3), (4,0), 0_E\}$. Jest to grupa 8-elementowa. Z wykładu wiemy, że $2(0,0) = 0_E$. Rozważmy prostą $y = 2x$. Przecięcie $E \cap (y = 2x)$ jest zadane wielomianem $(x^3 - x) - (2x)^2 = x \cdot (x-2)^2$. To pokazuje, że $(0,0) +_E 2(2,4) = 0_E$. Zatem $2(2,4) = -(0,0) = (0,0)$. Podobnie, rozważając prostą $y = x$ dowiadujemy się, że $2(3,3) = (0,0)$.

Powyższe obliczenia wystarczają, by stwierdzić, że grupa jest abstrakcyjnie izomorficzna z grupą $\mathbb{Z}_2 \times \mathbb{Z}_4$. Zaiste, wiemy, że $4(2,4) = 2(0,0) = 0_E$. Skoro $(2,1) = -(2,4)$, to $4(2,1) = 0_E$. Analogicznie, $4(3,3) = 0_E$ i $4(3,2) = 0_E$. Wreszcie, $2(4,0) = 0_E$ jak na wykładzie. Zatem każdy element $p \in E(\mathbb{Z}_5)$ spełnia $4p = 0$. Ponadto $(2,4)$ nie spełnia $2(2,4) = 0_E$. Z klasyfikacji skończonych grup przemiennych, jedyna możliwość to $\mathbb{Z}_2 \times \mathbb{Z}_4$.
Można też wypisać izomorfizm bezpośrednio (aczkolwiek nie jest to wymagane!). Niech $p = (2,4)$. Wtedy $2p = (0,0)$, $3p = -p = (2,1)$, $4p = 0_E$. Niech $q = (3,3)$. Wtedy $2(q+p) = (0,0) + (0,0) = 0_E$, ale $q + p \neq 2p = (0,0)$, więc $q + p = (4,0)$. Wobec tego odwzorowanie $\mathbb{Z}_2 \times \mathbb{Z}_4$ zadane przez $(a,b) \mapsto a(q+p) + bp$ jest dobrze określoną surjekcją, zatem izomorfizmem.

Weźmy wreszcie $p = 7$. Obliczamy jak poprzednio kwadraty w $\mathbb{Z}_7$ to $0 \mod 7, 1 \mod 5, 4 \mod 7, 2 \mod 7$. Obliczamy, że

x	0	1	2	3	4	5	6
$x^3 - x \mod 5$	0	0	6	3	4	1	0

Zatem $E(\mathbb{Z}_5) = \{(0,0), (1,0), (4,2), (4,5), (5,1), (5,6), (6,0), 0_E\}$. Jest to znowu grupa 8-elementowa. Ma ona co najmniej (a nawet dokładnie, patrz zadanie 3) cztery elementy p takie, że $2p = 0$, a mianowicie $(0,0)$, $(1,0)$, $(6,0)$, 0_E. Rozważając prostą $y = -2(x-1)$ stwierdzamy, że przecina ona $E(\mathbb{Z}_7)$ w punkcie $(1,0)$ oraz *dwukrotnie* w punkcie $(5,6)$. Zatem $2(5,6) = -(1,0) \neq 0_E$. To pokazuje, że grupa $E(\mathbb{Z}_7)$ nie jest izomorficzna z $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, więc z klasyfikacji grup skończonych, jest ona izomorficzna z $\mathbb{Z}_2 \times \mathbb{Z}_4$.

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 $4a^3 + 27b^2 = 0$.

Rozwiązanie.
(a) Punkt $(0, 0)$ jest osobliwy w krzywej $y^2 = x^3 - x^2$, zatem z definicji nie jest ona eliptyczna. Jeśli chodzi o krzywą $y^2 = x^3 - 1$, to jej ewentualne punkty osobliwe są rozwiązaniem układu równań

$$\begin{cases} y^2 = x^3 - 1 \\ 3x^2 = 0 \\ 2y = 0 \end{cases}$$

Na mocy założenia o charakterystyce, układ ten redukuje się do $x = y = 0$, $y^2 = x^3 - 1$, zatem do układu sprzecznego. To pokazuje, że $y^2 = x^3 - 1$ jest nieosobliwa, a więc definiuje krzywą eliptyczną.
(b) Układ równań z poprzedniego podpunktu wygląda następująco

$$\begin{cases} y^2 = f(x) \\ f'(x) = 0 \\ 2y = 0 \end{cases}$$

Sprowadza się on do $y = 0$, $f(x) = 0$, $f'(x) = 0$. Ten układ ma rozwiązanie (w algebraicznym domknięciu ciała) wtedy i tylko wtedy, gdy $f(x)$, $f'(x)$ nie są względnie pierwsze. To dowodzi równoważności z podpunktu.
(c) Dla dowolnego α, ze wzoru Taylora otrzymujemy $f(x) = f(\alpha) + (x - \alpha)f'(\alpha) \pmod{(x-\alpha)^2}$. Wobec tego α jest pierwiastkiem dwukrotnym f wtedy i tylko wtedy, gdy $f(\alpha) = 0$ oraz $(x - \alpha)f'(\alpha) = 0$, czyli gdy α jest wspólnym pierwiastkiem f i f'. Pozostaje policzyć, kiedy f i f' mają nietrywialny wspólny pierwiastek, czyli nietrywialny wspólny dzielnik. Załóżmy najpierw, że $a \neq 0$. Obliczamy

$$\begin{aligned} \mathrm{NWD}\left(x^3 + ax + b,\ 3x^2 + a\right) &= \mathrm{NWD}\left(3x^3 + 3ax + 3b,\ 3x^2 + a\right) = \mathrm{NWD}\left(2ax + 3b,\ 3x^2 + a\right) \\ &= \mathrm{NWD}(2ax + 3b,\ 6ax^2 + 2a^2) = \mathrm{NWD}(2ax + 3b,\ -9bx + 2a^2) \\ &= \mathrm{NWD}(2ax + 3b, -18abx + 4a^3) = \mathrm{NWD}(2ax + 3b,\ 27b^2 + 4a^3) \end{aligned}$$

Z założenia $2a \neq 0$, więc ostatni największy wspólny dzielnik jest nietrywialny dokładny 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 $E(\mathbb{k})$?

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

Rozwiązanie.
(a) Jeśli $p = (x_0, 0)$, to prosta $x = x_0$ przecina krzywą dwukrotnie w p i nie przecina jej w żadnym innym punkcie, zatem $2p = 0$. Jeśli zaś $p = (x_0, y_0)$, gdzie $y_0 \neq 0$. Rozważmy styczną do E w punkcie p. Jeśli styczna ta jest postaci $x = x_0$, to prosta $x = x_0$ przecina E dwukrotnie w p oraz dwukrotnie w $-p$, czyli łącznie czterokrotnie; sprzeczność, bo z wykładu wiemy, że każda prosta przecina krzywą co najwyżej trzykrotnie, licząc z krotnościami. Zatem styczna jest postaci $y = \alpha x + \beta$. Ale wtedy równanie E po obcięciu do stycznej jest nadal równaniem stopnia *dokładnie* trzy. Ma ono pierwiastek co najmniej dwukrotny w p. Niech r będzie punktem odpowiadającym trzeciemu pierwiastkowi (potencjalnie r może być równe p, to nic nie zmienia). To pokazuje, że $2p + r = 0_E$ dla pewnego punktu r. Jeśli $2p = 0$, to $r = 0$, sprzeczność!
(b) Liczba punktów 2-torsyjnych to liczba rozwiązań układu $E \cap (y = 0)$ plus jeden (za punkt neutralny), zatem jest ona równa co najwyżej $3 + 1 = 4$, a co najmniej 1. Jeśli E jest zadana równaniem $y^2 = f(x)$, to liczba punktów to $1 + \#\{\alpha \in \mathbb{k} \mid f(\alpha) = 0\}$. Wielomian f może mieć zero, jeden lub trzy pierwiastki w $\mathbb{k}$. Zatem liczby punktów 2-torsyjnych to 1, 2 lub 4.

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 $(x, y) \in \mathbb{Z}_p^2$.

Rozwiązanie.

Z założenia wynika, że 3 nie dzieli rzędu grupy $\mathbb{Z}_p^*$, więc odwzorowanie $z \mapsto z^3$ jest bijekcją nad $\mathbb{Z}_p$. Zatem dla dowolnego y istnieje dokładnie jeden element $x \in \mathbb{Z}_p$ taki, że $x^3 = y^2 + a$. To pokazuje, że jest p rozwiązań.