Krzywe eliptyczne

Lev KOURLIANDTCHIK, Boris LURJE

Lev Kourliandtchik pracuje na Uniwersytecie Mikołaja Kopernika w Toruniu, a Boris Lurje – w Instytucie Matematyki w Sankt-Petersburgu.

O krzywych eliptycznych można też przeczytać np. w *Delcie* 1/2001.

Krzywa nazywa się *eliptyczna*, jeżeli za pomocą pewnych przekształceń (z których część będzie zademonstrowana dalej) może być przedstawiona w postaci $y^2 = f(x)$, gdzie f jest wielomianem stopnia trzeciego bez pierwiastków wielokrotnych. Jest oczywiste, że taka krzywa jest symetryczna względem osi odciętych.

Szczególną własnością krzywych eliptycznych jest fakt, że punkty na tych krzywych można „dodawać".

Niech P_1 i P_2 będą dwoma różnymi punktami krzywej eliptycznej, niesymetrycznymi względem osi odciętych. Poprowadźmy prostą przez te punkty. Gdy prosta ta przecina krzywą w punkcie P_3, punkt P_4, symetryczny do punktu P_3 względem osi odciętych, nazywa się *sumą* punktów P_1 i P_2. Oznaczmy ją przez $P_1 \oplus P_2$. Jeżeli prosta P_1P_2 jest styczna do krzywej w jednym z tych dwóch punktów, to ten punkt styczności przyjmujemy jako P_3. Dalej, gdy $P_1 = P_2$, zamiast siecznej bierzemy styczną. Gdy wreszcie prosta P_1P_2 jest równoległa do osi rzędnych, za sumę uważamy oddalony w nieskończoność punkt O, który odgrywa rolę zera względem definiowanego dodawania, to znaczy

$$O \oplus A = A \oplus O = A.$$

Okazuje się, że tak zdefiniowane dodawanie punktów ma „zwykłe" własności dodawania, mianowicie

$$A \oplus B = B \oplus A,$$
$$(A \oplus B) \oplus C = A \oplus (B \oplus C),$$

a równanie $A \oplus X = B$ ma tylko jedno rozwiązanie.

Zinterpretujemy teraz to dodawanie analitycznie.

Niech sieczna (styczna) ma równanie $y = kx + b$. Podstawiając y do równania krzywej $y^2 = f(x)$, otrzymujemy równanie trzeciego stopnia $f(x) - (kx + b)^2 = 0$. Znane są nam dwa pierwiastki x_1 i x_2 tego równania (odpowiadające punktom P_1 i P_2). Trzeci pierwiastek x_3 wyraża się przez x_1 i x_2, na mocy wzorów Viète'a, w sposób wymierny. Ponadto

$$P_1 \oplus P_2 = \big(x_3,\ -(kx_3 + b)\big).$$

Jeśli współczynniki wielomianu f są liczbami wymiernymi, a dodawane punkty krzywej mają współrzędne wymierne (punkt O też uważamy za wymierny), to ich suma jest punktem o współrzędnych wymiernych.

Rzeczywiście, współczynnik kierunkowy prostej łączącej punkty wymierne jest liczbą wymierną (współczynnik kierunkowy stycznej też jest wymierny). Zatem na mocy twierdzenia Viète'a odcięta sumy (a więc i rzędna) jest liczbą wymierną. Na przykład na krzywej $y^2 = x^3 + x + 6$ łatwo znaleźć dwa punkty o współrzędnych wymiernych, mianowicie $(2, 4)$ i $(3, -6)$, które w sumie dają punkt zupełnie nieoczywisty, mianowicie $(95, 926)$.

Idea dodawania punktów krzywej eliptycznej okazała się wyjątkowo owocna i pozwoliła uzyskać dość głębokie wyniki. Na przykład jeden z najbardziej znaczących wyników końca dwudziestego wieku, mianowicie dowód Wielkiego Twierdzenia Fermata, przeprowadzony przez Andrew Wilesa, opiera się na głębokim badaniu pewnej krzywej eliptycznej.

Tu zajmiemy się sprawą liczby punktów wymiernych na krzywej

$$y^2 = x(x+1)(x+9). \tag{1}$$

O krzywej tej pisaliśmy już w *Delcie* 7/2002, gdzie wykazaliśmy, iż fakt istnienia na niej tylko siedmiu punktów o obu współrzędnych wymiernych pociąga za sobą nieistnienie trójkąta równoramiennego o bokach i środkowych długości całkowitej. Niemniej jednak zliczenie punktów wymiernych na tej krzywej jest interesujące samo w sobie.

Punkty wymierne rozpatrywanej krzywej to, jak łatwo sprawdzić

$$A_1 = (-9, 0),\quad A_2 = (-3, 6),\quad A_3 = (-3, -6),$$
$$A_4 = (-1, 0),\quad A_5 = (0, 0),\quad A_6 = (3, 12),\quad A_7 = (3, -12).$$

Prosimy też sprawdzić, że poniższa tabelka opisuje ich dodawanie.

$\oplus$	O	A_1	A_2	A_3	A_4	A_5	A_6	A_7
O	O	A_1	A_2	A_3	A_4	A_5	A_6	A_7
A_1	A_1	O	A_7	A_6	A_5	A_4	A_3	A_2
A_2	A_2	A_7	A_5	O	A_6	A_3	A_1	A_4
A_3	A_3	A_6	O	A_5	A_7	A_2	A_4	A_1
A_4	A_4	A_5	A_6	A_7	O	A_1	A_2	A_3
A_5	A_5	A_4	A_3	A_2	A_1	O	A_7	A_6
A_6	A_6	A_3	A_1	A_4	A_2	A_7	A_5	O
A_7	A_7	A_2	A_4	A_1	A_3	A_6	O	A_5

Wykażemy, że nie ma ich więcej.

Sposób będzie taki, że zamiast badać tę krzywą, będziemy badać inną, na której punktów wymiernych jest jeszcze mniej. Skorzystamy z dość często stosowanej metody.

Poprowadźmy prostą $y = kx$ przez początek układu współrzędnych i dowolny inny punkt (x, y) badanej krzywej. Jeśli wybrany punkt jest wymierny, to liczba k oczywiście też będzie wymierna. Otrzymujemy

$$(kx)^2 = x(x+1)(x+9),\quad \text{stąd}\quad x^2 + (10 - k^2)x + 9 = 0.$$

A więc wyróżnik tej funkcji kwadratowej

$$(10 - k^2)^2 - 36 = (k^2 - 4)(k^2 - 16)$$

jest kwadratem liczby wymiernej.

Niech $k = 2p$. Wtedy

$$(k^2 - 4)(k^2 - 16) = 16(p^2 - 1)(p^2 - 4),$$

i liczba $p^2(p^2 - 1)(p^2 - 4)$ jest kwadratem. Oznaczmy $t = p^2$.

Mamy $z^2 = t(t-1)(t-4)$, gdzie z jest liczbą wymierną.

A więc każdy punkt wymierny krzywej (1) generuje punkt wymierny krzywej

$$y^2 = x(x-1)(x-4). \tag{2}$$

Stosując takie samo rozumowanie, dojdziemy do wniosku, że każdy punkt wymierny krzywej (2) generuje punkt wymierny krzywej (1). Takie krzywe nazywamy *biwymiernie równoważnymi*.

Dalej wykażemy, że na krzywej (2) są tylko trzy punkty o obu współrzędnych wymiernych, mianowicie $(0, 0)$, $(1, 0)$ i $(4, 0)$. Punkty te tworzą siedem wymiernych punktów krzywej (1) w następujący sposób:

- dla punktu $(0, 0)$ krzywej (2) mamy $t = p = k = 0$, co prowadzi do punktów A_1, A_4 i A_5 krzywej (1);
- punkt $(1, 0)$ krzywej (2) odpowiada liczbie $t = 1$, co oznacza, że $p = -1$ lub $p = 1$, a więc $k = -2$ lub $k = 2$, co daje punkty A_2 i A_3 krzywej (1);
- wreszcie punkt $(4, 0)$ generuje punkty A_6 i A_7.

Aby więc wykazać, że na krzywej (1) jest dokładnie siedem punktów wymiernych wystarczy wykazać, że na krzywej (2) jest ich dokładnie trzy.

W tym celu warto udowodnić najpierw dwa lematy.

$\star\star\star$

Lemat 1. Niech $C = (x_0, y_0)$ będzie punktem wymiernym krzywej (2), przy czym $y_0 \neq 0$. Wtedy odcięta punktu $C \oplus C$ jest liczbą wymierną.

Dowód. Równanie stycznej do krzywej (2) w punkcie C ma postać

$$y = y'(x_0)(x - x_0) + y_0.$$

Otrzymujemy

$$(y'(x_0)(x - x_0) + y_0)^2 = x^3 - 5x^2 + 4x.$$

Stąd

$$x^3 - (5 + (y'(x_0))^2)x^2 + px + q = 0.$$

Niech x_1 będzie odciętą punktu $C \oplus C$. Wtedy liczby x_0 i x_1 będą pierwiastkami tego równania. Co więcej, x_0 jest pierwiastkiem podwójnym.

Zatem na mocy twierdzenia Viète'a uzyskujemy

$$2x_0 + x_1 = 5 + (y'(x_0))^2.$$

Ponieważ

$$y^2 = f(x) = x^3 - 5x^2 + 4x,$$

więc

$$2y \cdot y' = f' = 3x^2 - 10x + 4.$$

Wobec tego

$$y' = \frac{f'}{2y} \quad \text{i} \quad (y')^2 = \frac{(f')^2}{4y^2} = \frac{(f')^2}{4f}.$$

A więc

$$x_1 = 5 + \frac{(f'(x_0))^2}{4f(x_0)} - 2x_0 = 5 + \frac{(3x_0^2 - 10x_0 + 4)^2}{4(x_0^3 - 5x_0^2 + 4x_0)} - 2x_0 =$$

$$= \frac{x_0^4 - 8x_0^2 + 16}{4f(x_0)} = \left(\frac{x_0^2 - 4}{2y_0}\right)^2,$$

co kończy dowód lematu 1.

$\star\star\star$

Lemat 2. Jeśli na krzywej (2) istnieją punkty wymierne różne od trzech oczywistych, to na tej krzywej istnieje punkt wymierny $C_1 = (x_1, y_1)$, taki że
1) $x_1 > 4$,
2) x_1 jest kwadratem liczby wymiernej,
3) licznik liczby x_1 w postaci nieskracalnej jest liczbą parzystą.

Dowód. Niech $C_0 = (x_0, y_0)$ będzie dowolnym punktem wymiernym na krzywej (2) różnym od trzech oczywistych. Oznaczmy $B_1 = (0, 0)$, $B_2 = (1, 0)$, $B_3 = (4, 0)$. Znajdziemy odcięte punktów $C_0 \oplus B_1$, $C_0 \oplus B_2$, $C_0 \oplus B_3$.

Dość prosty rachunek wykazuje, że odcięta $C_0 \oplus B_1$ wynosi $\frac{4}{x_0}$.
Odcięta punktu $C_0 \oplus B_2$ jest równa

$$\frac{y_0^2}{(x_0-1)^2 x_0} = \frac{x_0(x_0-1)(x_0-4)}{(x_0-1)^2 x_0} = \frac{x_0-4}{x_0-1}.$$

Wreszcie, odcięta punktu $C_0 \oplus B_3$ wynosi

$$\frac{(4y_0)^2}{(x_0-4)^2 4x_0} = \frac{4(x_0-1)}{x_0-4}.$$

Na mocy lematu 1 można przyjąć, że x_0 jest kwadratem liczby wymiernej. Wtedy odcięte czterech rozważanych punktów C_0, $C_0 \oplus B_1$, $C_0 \oplus B_2$, $C_0 \oplus B_3$ będą kwadratami liczb wymiernych.

Te odcięte wynoszą odpowiednio

$$x_0, \quad \frac{4}{x_0}, \quad \frac{x_0-4}{x_0-1}, \quad \frac{4(x_0-1)}{x_0-4}.$$

Wszystkie te liczby należą do zbioru $(0, 1) \cup (4, \infty)$.

Zatem dokładnie dwie liczby należą do przedziału $(0, 1)$, dwie pozostałe zaś są większe od czterech.

Zaznaczmy, iż w parze x_0 i $\frac{4}{x_0}$ przynajmniej jeden z liczników jest liczbą parzystą. To samo jest prawdziwe dla drugiej pary liczb. Łatwo sprawdzić, że jedna spośród czterech liczb spełnia warunki 1) i 3). Na przykład jeżeli liczba $0 < x_0 < 1$ ma parzysty licznik, to żądaną liczbą będzie $\frac{x_0-4}{x_0-1}$.

A to kończy dowód lematu 2.

$\star\star\star$

Powróćmy do dowodu, że na krzywej (2) istnieją tylko trzy, podane wyżej, punkty o obu współrzędnych wymiernych.

Przypuśćmy zatem, że na krzywej (2) istnieje czwarty punkt wymierny. Niech $C_1 = (x_1, y_1)$ będzie punktem, którego istnienie gwarantuje lemat 2, czyli niech dla pewnych liczb naturalnych a i b będzie $x_1 = \frac{4a^2}{b^2}$, gdzie b jest liczbą nieparzystą, $a > b$ i $(a, b) = 1$.

Ponieważ $x_1(x_1-1)(x_1-4)$ jest kwadratem, więc $(4a^2 - b^2)(a^2 - b^2)$ jest kwadratem liczby naturalnej. Ponieważ liczby a i b są względnie pierwsze, więc liczby naturalne $4a^2 - b^2$ i $a^2 - b^2$ mają największy wspólny dzielnik równy 1 lub 3. Ponieważ liczba $4a^2 - b^2$ przy dzieleniu przez 4 daje resztę 3, więc nie może być kwadratem.

Zatem

$$a^2 - b^2 = 3c^2, \quad 4a^2 - b^2 = 3d^2,$$

gdzie liczby c i d są względnie pierwszymi liczbami naturalnymi.

Stąd

$$a^2 = d^2 - c^2, \quad b^2 = d^2 - 4c^2.$$

Z równości $b^2 + (2c)^2 = d^2$ wynika, że

$$c = uv, \quad b = u^2 - v^2, \quad d = u^2 + v^2,$$

gdzie u i v są względnie pierwszymi liczbami całkowitymi o różnej parzystości. Wobec tego

$$a^2 = d^2 - c^2 = (u^2+v^2)^2 - u^2v^2 = u^4 + u^2v^2 + v^4.$$

Zauważmy, że wynika stąd, iż liczba a jest nieparzysta.

Jeżeli u jest liczbą nieparzystą, połóżmy $z = a - u^2$, w przeciwnym razie $z = a - v^2$. Dla ustalenia uwagi przyjmijmy, że ma miejsce ta pierwsza sytuacja. Wtedy

$$(u^2+z)^2 = u^4 + u^2v^2 + v^4,$$

zatem

$$z^2 - v^4 = u^2(v^2 - 2z).$$

Oznaczając $z_1 = -2z$, otrzymujemy

$$z_1^2 - 4v^4 = 4u^2(v^2 + z_1).$$

Stąd

$$(z_1 - 2v^2)(z_1 + 2v^2)(z_1 + v^2) = 4u^2(z_1 + v^2)^2 = \\ = \big(2u(z_1 + v^2)\big)^2.$$

Połóżmy $x_2' = \dfrac{2v^2 + z_1}{v^2}$. Wtedy biorąc y_2', takie że

$$x_2'(x_2' - 1)(x_2' - 4) = (y_2')^2,$$

stwierdzamy, iż punkt (x_2', y_2') jest punktem wymiernym krzywej (2). A więc znajduje się na tej krzywej punkt wymierny o odciętej $x_2 = \dfrac{4}{x_2'}$.

⋆ ⋆ ⋆

Lemat 3. Liczba x_2 jest kwadratem liczby wymiernej.

Dowód. Mamy

$$x_2 = \frac{4v^2}{2v^2 - 2z} = \frac{2v^2}{v^2 - z} = \frac{2v^2}{v^2 + u^2 - a} = \frac{2v^2(u^2+v^2+a)}{(u^2+v^2)^2 - a^2} = \\ = \frac{2v^2(u^2+v^2+a)}{u^2v^2} = \frac{2(u^2+v^2+a)}{u^2},$$

a także $x_2 = \dfrac{v^2}{\frac{v^2+u^2-a}{2}}$.

Wykażemy, że liczby $\dfrac{v^2+u^2-a}{2}$ i $2(u^2+v^2+a)$ nie mają wspólnych nieparzystych dzielników pierwszych.

Przypuśćmy, że p jest takim dzielnikiem. Ponieważ iloczyn tych liczb jest równy u^2v^2, więc p jest dzielnikiem uv.

Jeżeli p jest dzielnikiem u, to jest też dzielnikiem $v^2 + a$ i $v^2 - a$, a co za tym idzie dzielnikiem v, co jest sprzeczne z założeniem, że liczby u i v są względnie pierwsze. Analogicznie p nie może być dzielnikiem v.

A więc wspólnym dzielnikiem liczb $\dfrac{v^2+u^2-a}{2}$ i $2(u^2+v^2+a)$ może być tylko potęga dwójki, a ich iloczyn $(uv)^2$ jest kwadratem. Oznacza to, że liczby te są kwadratami albo podwojonymi kwadratami. Zatem liczba x_2 jest albo kwadratem liczby wymiernej, albo podwojonym kwadratem liczby wymiernej.

Wykażemy, że druga z tych ewentualności jest niemożliwa. Rzeczywiście, jeżeli $x_2 = 2t^2$, to $2t^2(2t^2-1)(2t^2-4)$ jest kwadratem, skąd wynika, iż $(2t^2-1)(t^2-2)$ jest kwadratem.

Dalej, jeśli licznik lub mianownik liczby t jest parzysty, to licznik liczby $(2t^2-1)(t^2-2)$ dzieli się przez 2, nie dzieli się zaś przez 4.

Jeśli natomiast i licznik, i mianownik liczby t są nieparzyste, to licznik liczby $(2t^2-1)(t^2-2)$ daje resztę 3 przy dzieleniu przez 4. W obu przypadkach licznik nie będzie kwadratem, mianownik zaś kwadratem będzie.

A więc x_2 jest kwadratem i lemat został udowodniony.

⋆ ⋆ ⋆

Ponieważ

$$x_2 = 2 + \frac{2(v^2+a)}{u^2} > 2 \quad \text{i} \quad x_2 \in (0;\,1) \cup (4;\,\infty),$$

więc liczba x_2 jest większa od 4.

Jeżeli liczba u jest nieparzysta, to mianownik x_2 jest nieparzysty, a więc licznik x_2 jest parzysty.

Jeżeli liczba v jest nieparzysta, to – wobec równości

$$z = a - v^2 \quad \text{i} \quad x_2 = \frac{2(u^2+v^2+a)}{v^2}$$

– mianownik x_2 jest nieparzysty, a więc licznik x_2 jest parzysty.

Podsumowując, okazało się, że uzyskaliśmy punkt $C_2 = (x_2,\, y_2)$ również spełniający warunki lematu 2.

Teraz zastosujemy metodę regresji. W tym celu weźmy pod uwagę funkcję $\phi(A)$, która punktowi $A = (x,\, y)$ o współrzędnych wymiernych przyporządkowuje sumę licznika i mianownika liczby x w postaci nieskracalnej.

Wykażemy, że $\phi(C_2) < \phi(C_1)$.

Przypomnijmy, że

$$x_1 = \frac{4a^2}{b^2}, \quad x_2 = \frac{v^2}{\frac{v^2+u^2-a}{2}} = \frac{2(u^2+v^2+a)}{u^2}.$$

Wobec tego licznik x_2 jest dzielnikiem v^2, mianownik x_2 jest dzielnikiem u^2, a więc $\phi(C_2) \le u^2 + v^2$.

Zatem istotnie

$$\phi(C_1) = 4a^2 + b^2 = 4\big((u^2+v^2)^2 - u^2v^2\big) + (u^2 - v^2)^2 = \\ = 5u^4 + 5v^4 + 2u^2v^2 > u^2 + v^2 \ge \phi(C_2).$$

Wobec tego dowód nieistnienia na krzywej (2) innych punktów wymiernych od trzech podanych na początku można zakończyć.

Gdyby bowiem istniał taki punkt C_1, za jego pomocą uzyskalibyśmy punkt C_2, potem C_3 itd. Ale wtedy byłoby $\phi(C_1) > \phi(C_2) > \phi(C_3) > \ldots$, a przecież malejący ciąg liczb naturalnych nie może być nieskończony.

Każdemu z Czytelników, który doczytał do tego miejsca, proponujemy sprawdzenie, że na krzywej

$$y^2 = x(x+1)(x+4)$$

jest tylko siedem, łatwych do odgadnięcia, punktów o obu współrzędnych wymiernych. Przypominamy, że dowodzi to faktu, iż nie istnieje trójkąt prostokątny, którego boki i środkowe mają długości wymierne.

Droga jest podobna do przedstawionej wyżej. Dla zachęty podamy, że pomocniczą krzywą jest tu

$$y^2 = x(x-1)(x-9);$$

na niej są tylko trzy oczywiste punkty o współrzędnych wymiernych. Aby to wykazać, trzeba skorzystać z faktu (poprzednio lemat 2), że gdyby był jeszcze jeden taki punkt, to byłby też punkt $D_1 = (x_1,\, y_1)$, taki że $x_1 > 9$, liczba x_1 byłaby kwadratem liczby wymiernej i miałaby licznik podzielny przez 3. Potem…, ale zostawmy coś inwencji Czytelnika.