Krzywe eliptyczne w kryptografii

Tomasz KAZANA

1. Bestiariusz algebraika

Wybierzmy i ustalmy sobie jakąś liczbę pierwszą p, na przykład 13. Na początku będziemy zajmować się zbiorem:

$$\mathbb{F}_{13} = \{0, 1, 2, \ldots, 12\} \text{ (ogólniej: } \mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}).$$

W tym zbiorze wykonywać będziemy działania dodawania i mnożenia, ale nie klasycznie, lecz zgodnie z arytmetyką *modulo*, czyli po prostu reszt z dzielenia. To znaczy, w naszym świecie będziemy mieli:

$$5 + 10 = 2 \text{ czy } 4 \cdot 7 = 2.$$

Struktury o własnościach takich jak $\mathbb{F}_p$ – dla matematyków niezwykle ważne – nazywane są ciałami. Ciało stanowią chociażby liczby rzeczywiste, liczby zespolone czy właśnie $\mathbb{F}_p$. Oczywiście, istnieją inne przykłady – zarówno skończone, jak i nieskończone.

Co ciekawe, w tak dziwacznej strukturze zaskakująco wiele własności zwykłych liczb rzeczywistych jest zachowanych. Znane jeszcze ze szkoły podstawowej prawa łączności, przemienności czy rozdzielności mnożenia względem dodawania są prawdziwe także w $\mathbb{F}_{13}$ z działaniami *modulo*. Możemy nawet sensownie określić odejmowanie i dzielenie jako operacje odwrotne do (odpowiednio) dodawania i mnożenia. Przykładowo określmy:

$$a : b = x \text{ wtedy i tylko wtedy, gdy } b \cdot x = a.$$

Możemy łatwo sprawdzić, że – przy powyższej definicji – zachodzi $8 : 3 = 7$ czy $7 : 5 = 4$. Więcej, okazuje się, że jeśli tylko nie próbujemy dzielić przez 0, to wynik zawsze istnieje i to jednoznaczny.

Pójdźmy krok dalej i zacznijmy badać równania w świecie $\mathbb{F}_{13}$. Zapytajmy chociażby o rozwiązania następującego równania kwadratowego:

$$x^2 + 3x + 8 = 0.$$

$\Delta = 3^2 - 4 \cdot 1 \cdot 8 = 3,$
$\sqrt{\Delta} = 4$ lub $9,$
$x_1 = (-3 + 4) : 2 = 7$
$x_2 = (-3 + 9) : 2 = 3.$

Możemy sprawdzić, że rozwiązania są dokładnie dwa: 3 oraz 7. Ba, działają nawet klasyczne wzory z *deltą*, o ile tylko określimy sensownie *pierwiastkowanie modulo*.

Oczywiście, ma sens pytanie o zbiory, których definicja kojarzy nam się z obiektami klasycznej geometrii. Chociażby popatrzmy na zbiór:

$$O = \{(x, y) \in \mathbb{F}_{13} \times \mathbb{F}_{13} \mid x^2 + y^2 = 9\}.$$

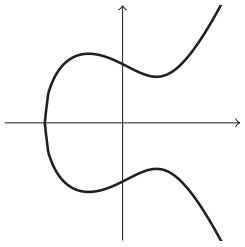
Możemy po prostu obliczyć, że

$$O = \{(0,3), (0,10), (3,0), (5,6), (5,7), (6,5), (6,8), (7,5), (7,8), (8,6), (8,7), (10,0)\},$$

a otrzymany zbiór O nazwać *okręgiem nad* $\mathbb{F}_{13}$, choć to przecież żaden prawdziwy okrąg, a tylko 12 punktów iloczynu kartezjańskiego $\mathbb{F}_{13} \times \mathbb{F}_{13}$. Niemniej tego typu obiekty są bardzo użyteczne i intensywnie badane przez dziedzinę matematyki zwaną *geometrią algebraiczną*. W tym artykule chcemy przybliżyć przykład takiego obiektu – tak zwane krzywe eliptyczne, czyli punkty spełniające równanie:

$$K_{\mathbb{F}_{13}} = \{(x, y) \in \mathbb{F}_{13} \times \mathbb{F}_{13} \mid y^2 = x^3 + ax + b\},$$

dla pewnych ustalonych $a, b \in \mathbb{F}_{13}$.

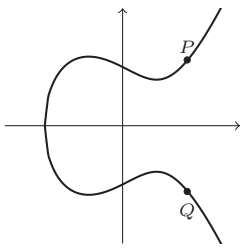


Rys. 1. $y^2 = x^3 - x + 1$

Zanim powrócimy do właśnie przedstawionych krzywych eliptycznych nad ciałem $\mathbb{F}_{13}$, przyjrzyjmy się jeszcze ich rzeczywistym odpowiednikom, tzn. krzywym typu

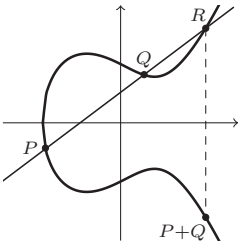
$$K = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y^2 = x^3 + ax + b\},$$

$(a, b \in \mathbb{R})$, których przykład możemy obejrzeć na rysunku 1. Udziwnijmy świat punktów tej krzywej. Dorzućmy do K jeden nowy punkt specjalny: ∞ (nieskończoność), a w powstałym zbiorze $\overline{K} = K \cup \{\infty\}$ zdefiniujmy następujące dodawanie punktów (tzn. pewną operację $+ : \overline{K} \times \overline{K} \to \overline{K}$):

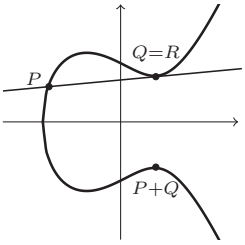


Rys. 2. $P + Q = \infty$

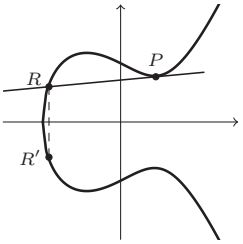
- dla dowolnego $P \in \overline{K}$ mamy $P + \infty = \infty + P = P$;
- Jeśli dwa różne punkty $P, Q \in K$ mają tę samą pierwszą współrzędną (jak na rysunku 2), to $P + Q = \infty$;



Rys. 3



Rys. 4



Rys. 5. $P + P = R'$

Przykładowo rozważmy krzywą
$\{(x, y) \in \mathbb{F}_{13} \times \mathbb{F}_{13} \mid y^2 = x^3 - x + 1\} \cup \{\infty\}$.
Jej punkty to:
$(0, 1), (0, 12), (1, 1), (1, 12), (3, 5), (3, 8), (4, 3), (4, 10), (5, 2), (5, 11), (6, 4), (6, 9), (7, 5), (7, 8), (10, 4), (10, 9), (12, 1), (12, 12), \infty$.
Przykładowe działania (sprawdź!):
$(6, 9) + \infty = (6, 9)$,
$(6, 9) + (3, 8) = (7, 8)$,
$(3, 5) + (3, 5) = (7, 8)$.

- Jeśli dwa różne punkty $P, Q \in K$ mają różną pierwszą współrzędną, to rysujemy prostą przechodzącą przez P i Q, zaznaczamy trzeci punkt przecięcia z krzywą (R), a ostatecznym wynikiem dodawania P i Q jest odbicie symetryczne R względem osi OX (rys. 3). Może się zdarzyć, że dorysowana prosta nie przetnie się w żadnym dodatkowym punkcie (jak na rysunku 4). Wówczas dorysowana prosta na pewno będzie styczna do naszej krzywej i jako punkt R należy przyjąć punkt styczności.
- Jeśli liczymy $P + P$, to rysujemy styczną do K w punkcie P. Jeśli ta styczna nie przecina się z K w żadnym innym punkcie, to $P + P = \infty$, w przeciwnym razie (prosta przecina się jeszcze w punkcie R) $P + P = R'$, gdzie R' jest odbiciem symetrycznym R względem osi OX (zob. rys. 5).

Jak widać, dodawanie punktów jest zdefiniowane w pełni geometrycznie. Jednakże możemy to samo działanie (sprawdź! – jest to żmudne, ale proste) opisać analitycznie. Gdy $P = (x_1, y_1)$, $Q = (x_2, y_2)$ i $P + Q = W = (x_3, y_3)$, dla $x_1 \neq x_2$, mamy

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2,$$
$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3),$$

a gdy $x_1 = x_2$ oraz $y_1 = y_2$, wzory są następujące:

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1,$$
$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3).$$

Forma analityczna dodawania punktów jest wygodniejsza, ponieważ pozwala na zdefiniowanie dodawania punktów również w zbiorze $\overline{K_{\mathbb{F}_{13}}} = K_{\mathbb{F}_{13}} \cup \{\infty\}$, poprzez zwykłą analogię. To znaczy umawiamy się, że powyższe wzory analityczne (mające sens również w arytmetyce modulo 13) na x_3 i y_3 określają dodawanie punktów również w $\overline{K_{\mathbb{F}_{13}}}$.

Dodawanie punktów na krzywej (zarówno w $\overline{K}$, jak i w $\overline{K_{\mathbb{F}_{13}}}$) jest działaniem o ładnych własnościach: jest łączne, ma element neutralny (tutaj ∞) oraz własność, że każdy element P ma element odwrotny P' (czyli taki, że $P + P' = \infty$). Struktury o takich własnościach zwyczajowo nazywamy *grupą*. Przykładem grupy innej niż te dwie opisane wyżej może być też $\mathbb{F}_p \setminus \{0\}$ z działaniem mnożenia modulo p (warto samemu sprawdzić). Dla nas te grupy będą mieć jednak jeszcze jedną bardzo ważną własność, związaną z trudnością obliczeniową. O tym już za chwilkę.

2. Bestia na usługach kryptografii

Wiele protokołów szyfrowania w kryptografii opiera się na trudności obliczeniowej różnych problemów. Pewnie najsłynniejsze jest szyfrowanie RSA, którego bezpieczeństwo gwarantowane jest przez trudność faktoryzacji dużych liczb. Są jednak i inne protokoły (np. szyfr El-Gamal), których bezpieczeństwo opiera się na innym założeniu, mianowicie na trudności obliczania logarytmu dyskretnego. Na czym to polega? Chodzi o problem znalezienia w danej grupie G z mnożeniem dla danych $a, b \in G$ takiego k, że

$$a^k = b$$

bądź w wersji z grupą z dodawaniem takiego k, że: $\underbrace{a + a + \cdots + a}_{k \text{ razy}} = b$.

Przykładowe instancje problemu logarytmu dyskretnego:
1. ($\mathbb{F}_{13}$ z mnożeniem)
znajdź taki x, że $3^x = 7 \mod 13$
2. ($K_{\mathbb{F}_{13}}$ z dodawaniem punktów)
znajdź takie k, że:
$\underbrace{(6, 9) + \cdots + (6, 9)}_{k \text{ razy}} = (5, 11)$

Oczywiście, nie dla każdej grupy problem logarytmu dyskretnego jest trudny. Dla grupy $\mathbb{F}_p$ z dodawaniem jest on banalny (dlaczego?), ale dla tego samego $\mathbb{F}_p$, tylko z mnożeniem – już uchodzi za trudny. Konkretnie, najszybszy znany algorytm dla tego problemu działa w czasie

$$2^{O(\sqrt[3]{\ln p \ln \ln^2 p})},$$

co dla p rozsądnie dużych rozmiarów jest już poza zasięgiem współczesnych komputerów.

Po co więc te całe krzywe eliptyczne? Po prostu najszybsze algorytmy rozwiązujące logarytm dyskretny dla losowej krzywej postaci $K_{\mathbb{F}_p}$ są jeszcze wolniejsze niż algorytmy dla grupy $\mathbb{F}_p$ podobnego rozmiaru. Konkretnie dla krzywych eliptycznych wszystkie znane ogólne algorytmy rozwiązujące problem logarytmu dyskretnego działają w czasie

$$2^{O(\ln p)} \gg 2^{O(\sqrt[3]{\ln p \ln\ln^2 p})}.$$

Z takimi deklaracjami należy uważać. Uczciwiej byłoby napisać *na dzień dzisiejszy bezpieczniejszy*, gdyż nie znamy żadnych ścisłych dolnych oszacowań na czas rozwiązywania tych problemów. W każdej chwili może ktoś znaleźć jakiś efektywniejszy algorytm i sytuacja może się odwrócić.

Oznacza to, że każdy protokół kryptograficzny, oparty o problem logarytmu dyskretnego, staje się *bezpieczniejszy* bez zwiększenia p (a więc bez zwiększenia rozmiaru kluczy), jeśli tylko zmienimy grupę, z którą pracujemy, z $\mathbb{F}_p$ z mnożeniem na $K_{\mathbb{F}_p}$ z dodawaniem punktów. Dokładnie z tego powodu już nie jest popularne używanie podpisu cyfrowego DSA (z roku 1991), a powszechnie używa się podpisu ECDSA (z roku 1999) – czyli jego odpowiednika, ale opartego o krzywe eliptyczne.

A jednak ta geometria algebraiczna gdzieś się przydaje!

Wyniki XXXV Ogólnopolskiego Sejmiku Matematyków, Szczyrk, 14–17 VI 2018

Konkurs polega na przedstawieniu opracowania jednego z tematów zaproponowanych (wraz z bibliografią) przez Jury lub tematu własnego oraz – w przypadku zakwalifikowania się do finału – krótkim, publicznym zreferowaniu tego opracowania.

Jury w składzie: prof. dr hab. Maciej Sablik – przewodniczący, dr Paweł Błaszczyk, dr Anna Brzeska, dr Dawid Czapla, mgr Żywilla Fechner, dr hab. Mieczysław Kula, dr Agnieszka Kulawik, dr Marian Podhorodyński, dr Anna Szczerba-Zubek, dr Hanna Wojewódka postanowiło przyznać następujące wyróżnienia:

I miejsce: **Bartosz Bartoszek** – I LO w Zduńskiej Woli
za pracę *Funkcje potęgowo* (j, k) *symetryczne*, opiekun: dr inż. Renata Długosz;
II miejsce: **Filip Rękawek** – Katolickie LO w Garwolinie
za pracę *O trójkątach kappa i ich własnościach*, opiekun: mgr Zofia Burno;
III miejsce: **Krzysztof Witkowski** – I LO w Gliwicach
za pracę *O własnościach sum Freya*, opiekun: mgr Joanna Olesińska;
IV miejsce **Gabriela Pietras** – Publiczna Szkoła Podst. w Leszczynie,
za pracę *Wokół twierdzenia Morse'a–Hedlunda*, opiekun mgr Martha Łącka;
V miejsce **Jakub Michalec**– LO Zakonu Pijarów w Krakowie
za pracę *Paradoksy nieskończoności*, opiekun: Jolanta Przybylska.

Sejmiki organizuje Pracownia Matematyki i Informatyki Pałacu Młodzieży w Katowicach we współpracy z Uniwersytetem Śląskim;
`www.spinor.edu.pl`

W głosowaniu publiczności na najlepszą prezentację
nauczyciele nagrodzili **Rafała Loskę** – VIII LO w Katowicach,
praca *Jak obliczyć pole figury płaskiej?*,
a uczniowie **Pawła Tyrnę** – LO Towarzystwa Szkolnego w Bielsku–Białej,
praca *Matematyczne podstawy projektowania origami*.

Problemy sztucznej grawitacji

Szymon CHARZYŃSKI

Podróże w kosmos to marzenie większości dzieci i licznej grupy dorosłych (wliczając autora). Niestety, okazję do zrealizowania tych marzeń miała, jak na razie, bardzo nieliczna grupa ludzi, a najdalsze loty załogowe odbyte do tej pory to te z przełomu lat sześćdziesiątych i siedemdziesiątych dwudziestego wieku w ramach programu Apollo, dzięki któremu ludzie kilkukrotnie lądowali na Księżycu. Z kolei najdłuższe pobyty w przestrzeni kosmicznej były udziałem załóg stacji kosmicznych krążących na niskiej orbicie okołoziemskiej (kilkaset km nad jej powierzchnią) i trwały kilka miesięcy. Pomimo tego, że podbój kosmosu przez gatunek ludzki jest ciągle jeszcze w powijakach, to wizjonerzy snują ambitne plany kolonizacji innych planet, zakładania na stałe zamieszkałych baz w przestrzeni i wysyłania załogowych statków nawet poza Układ Słoneczny.

Te kilkadziesiąt lat doświadczeń z lotami kosmicznymi nauczyły nas, z jakimi problemami przyjdzie się mierzyć konstruktorom pojazdów przyszłości i ich załogom. Jednym z nich jest problem ciążenia, a raczej jego braku. Długie pozostawanie w stanie nieważkości ma dla organizmu ludzkiego różne, bardzo negatywne skutki zdrowotne. Dlatego wizjonerzy planujący długie podróże