УДК 511.3

Г. М. Барабаш, Я. М. Холявка (Львівський національний університет імені Івана Франка)

ПРО АРИФМЕТИЧНІ ВЛАСТИВОСТІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ НА КРИВИХ ЛЕЖАНДРА

Properties of divisibility of points of elliptic Legendre curves over finite field are learned. Arithmetic progressions on such curves are examined. Criterion of divisibility by 2 of the points of elliptic Legendre curves is proved.

Вивчаються властивості подільності точок еліптичних кривих Лежандра над скінченним полем. Розглянуто арифметичні прогресії на таких кривих. Доведено критерій подільності на 2 точок еліптичних кривих Лежандра.

1. Вступ

Вивчення послідовностей, пов'язаних з точками на еліптичних кривих, викликане їх застосуванням в криптографії [1], [2] та теорії кодування [3]. Такі послідовності також використовують при побудові послідовностей псевдовипадкових чисел, тому вивчення їх властивостей буде корисним для створення і коректного застосування генераторів псевдовипадкових чисел, побудованих на цій основі. Зазвичай використовують еліптичні криві, задані в канонічній формі Вейєрштрасса [4], [5]. В роботі [6] розглянуто арифметичну прогресію, елементами якої є точки еліптичної кривої Вейєрштрасса, та досліджуються арифметичні властивості координат цих точок. Крім еліптичних кривих Вейєрштрасса, відомо декілька інших видів еліптичних кривих [7], кожен з яких має певні переваги. Розглянемо подібні до [6] побудови та властивості елементів послідовностей, обчислених на еліптичній кривій Лежандра.

2. Еліптичні криві Лежандра

Нехай E – еліптична крива над полем $\mathbb{F}_q$, $\operatorname{char}\mathbb{F}_q \neq 2$, яка задана у формі Лежандра

$$E: \quad y^2 = x(x-1)(x-\lambda), \quad \lambda \in \mathbb{F}_q, \quad \lambda \neq 0,\ 1. \tag{1}$$

Точками еліптичної кривої E над довільним полем $\mathcal{F}$ називають пари елементів $(x,\ y)$, які належать будь-якому розширенню поля $\mathcal{F}$ і задовольняють (1); крім того, точкою еліптичної кривої E вважають нескінченно віддалену точку O. Якщо при цьому $x,\ y \in \mathcal{F}$, то точку $(x,\ y)$ називають раціональною або $\mathcal{F}$- точкою. Точку O вважають раціональною для довільної еліптичної кривої. В цій роботі, говорячи про точки E, будемо розглядати тільки раціональні точки цієї кривої.

Для довільної точки $P = (x,\ y)$ кривої E позначимо $\ominus P = (x,\ -y)$. Координати $\ominus P$ задовольняють (1), тому $\ominus P \in E$.

Якщо $P_1 = (x_1, y_1)$ і $P_2 = (x_2, y_2)$ – різні точки еліптичної кривої E, заданої рівнянням (1), і $P_2 \neq \ominus P_1$, то $P_1 \oplus P_2$ визначимо як точку $P_3 = (x_3, y_3)$, де (x_3, y_3)

обчислюють так:

$$\begin{cases} x_3 = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 + \lambda + 1, \\ y_3 = \dfrac{y_1 - y_2}{x_2 - x_1} x_3 - \dfrac{y_1 x_2 - x_1 y_2}{x_2 - x_1}. \end{cases}$$

Якщо $P_1 = P_2$, то $P_1 \oplus P_1 = P_3$ і

$$\begin{cases} x_3 = \left(\dfrac{3x_1^2 - 2(\lambda+1)x_1 + \lambda}{2y_1}\right)^2 - 2x_1 + \lambda + 1, \\ y_3 = -\left(\dfrac{3x_1^2 - 2(\lambda+1)x_1 + \lambda}{2y_1}\right) x_3 + \dfrac{x_1^3 - \lambda x_1}{2y_1}. \end{cases} \tag{2}$$

Як відомо [5], точки $P = (x,\ y)$ еліптичної кривої E (1), $x,\ y \in \mathbb{F}_q$, разом з O утворюють абелеву групу відносно операції $\oplus$. Нейтральним елементом цієї групи є точка O, оберненим до елементу $P = (x,\ y)$ є елемент $\ominus P = (x,\ -y)$, тобто для довільної точки $P \in E$ справджуються співвідношення $P \oplus (\ominus P) = O$, $P \oplus O = P$.

Надалі позначимо $P_1 \oplus P_2$ через $P_1 + P_2$ і назвемо сумою точок еліптичної кривої E. Також позначимо $nP = P + \cdots + P$, де сума складається з n доданків.

3. Арифметичні прогресії на кривій Лежандра

Для цілого r точку $Q \in E$ називають r-подільною, якщо на кривій E існує точка R, для якої $rR = Q$. Наприклад, для еліптичної кривої E (1) точка O є 2-подільною, так як точками порядку 2 є точки $(0,\ 0)$, $(1,\ 0)$, $(\lambda,\ 0)$.

Нехай E – еліптична крива (1), P_1 і P_2 – деякі фіксовані точки E, відмінні від точки O. Послідовність відмінних від O точок M_l еліптичної кривої E з першим членом $M_1 = P_1 + P_2$ і кожен наступний член якої визначають рівністю

$$M_{l+1} = M_l + P_2,\ l = 1, 2, \ldots, \tag{3}$$

називають арифметичною прогресією на E з початковим членом $P_1 + P_2$ і різницею P_2. Кількість різних елементів послідовності (3) відповідає порядку точки P_2, тому на практиці цю точку вибирають високого порядку. Позначимо координати $M_l,\ l = 1, 2, \ldots$, через $x_l = x(M_l),\ y_l = y(M_l)$. З послідовністю (3) пов'яжемо послідовність x-координат її точок:

$$x_1,\quad x_2,\quad \ldots\ . \tag{4}$$

Теорема 1. *Над полем $\mathbb{F}_q$, $\operatorname{char}\mathbb{F}_q \neq 2$, для елементів послідовності (4) справджуються такі твердження:*

якщо P_1 є 2-подільна точка на E, то x_{2l} є квадрати елементів $\mathbb{F}_q$;

якщо $P_1 + P_2$ є 2-подільна точка, то x_{2l-1} є квадрати елементів $\mathbb{F}_q$;

якщо P_1 і P_2 є 2-подільні точки, то x_l є квадрати елементів $\mathbb{F}_q$ для усіх l.

Доведення. Нехай E – еліптична крива над скінченим полем $\mathbb{F}_q$, $\operatorname{char}\mathbb{F}_q \neq 2$, яка задана рівнянням (1). Знайдемо необхідні і достатні умови 2-подільності її

точок. Будемо вважати, що точка $Q = (u,\ v) \in E$, $Q \neq O$, 2-подільна, тобто на E існує точка $R = (u_1,\ v_1)$, для якої $2R = Q$. Так як $Q \neq O$, то $v_1 \neq 0$.

Згідно формул (2) маємо

$$u = t^2 - 2u_1 + \lambda + 1, \tag{5}$$

$$v = -tu + \frac{u_1^3 - \lambda u_1}{2v_1}, \tag{6}$$

де

$$t = \frac{3u_1^2 - 2(\lambda+1)u_1 + \lambda}{2v_1}. \tag{7}$$

З (5) та (7) одержимо

$$u = \frac{1}{4}\,\frac{\left(3\,{u_1}^2 - 2\,(\lambda+1)\,u_1 + \lambda\right)^2}{{v_1}^2} - 2\,u_1 + \lambda + 1. \tag{8}$$

Перетворивши (8), отримаємо

$$\begin{gathered} 4\,\lambda^2{u_1}^2 - 12\,\lambda{u_1}^3 + 9\,{u_1}^4 - 4\,\lambda^2 u_1 + 14\,\lambda{u_1}^2 + 4\,\lambda{v_1}^2 - 12\,{u_1}^3 - 8\,u_1\,{v_1}^2 - \\ -4\,u\,{v_1}^2 + \lambda^2 - 4\,\lambda u_1 + 4\,{u_1}^2 + 4\,{v_1}^2 = 0. \end{gathered} \tag{9}$$

Так як $R \in E$, то $v_1^2 = u_1(u_1 - 1)(u_1 - \lambda)$, тому з (9)

$$\begin{gathered} 4\lambda^2{u_1}^2 - 12\lambda{u_1}^3 + 9{u_1}^4 - 4\lambda^2 u_1 + 14\lambda{u_1}^2 - 8{u_1}^3 + \lambda^2 + 4{u_1}^2 + \\ +4\lambda\left({u_1}^3 - (\lambda+1)\,{u_1}^2 + \lambda u_1\right) - 8u_1\left({u_1}^3 - (\lambda+1)\,{u_1}^2 + \lambda u_1\right) - \\ -4u\left({u_1}^3 - (\lambda+1)\,{u_1}^2 + \lambda u_1\right) - 4\,(\lambda+1)\,{u_1}^2 = 0. \end{gathered} \tag{10}$$

Спростивши (6) та (10), де t визначається формулою (7), отримаємо, що координати $(u_1,\ v_1)$ точки R задовольняють такі рівняння

$${u_1}^4 - 4\,{u_1}^3 u + (4\,\lambda u + 4\,u - 2\,\lambda)\,{u_1}^2 - 4\,\lambda u_1\,u + \lambda^2 = 0, \tag{11}$$

$$u_1^3 - 3uu_1^2 - \lambda u_1 + 2\lambda u u_1 + 2uu_1 - \lambda u - 2vv_1 = 0 \tag{12}$$

Навпаки, нехай $Q = (u,\ v) \in E$ та рівняння (11) має розв'язок $\widetilde{u}_1$, а рівняння (12) має розв'язок $\widetilde{v}_1$. Тоді $\widetilde{R} = (\widetilde{u}_1,\ \widetilde{v}_1) \in E$ та справджуються (5), (6), тобто $Q = 2\widetilde{R}$ для точки $\widetilde{R} = (\widetilde{u}_1,\ \widetilde{v}_1)$ на E.

Якщо $Q = (u,\ v) = 2R$, де $R = (u_1,\ v_1)$, тоді з (11) отримаємо, що

$$u = -\frac{1}{4}\frac{(u_1^4 - 2\lambda u_1^2 + \lambda^2)}{(u_1(\lambda u_1 - u_1^2 - \lambda + u_1))}. \tag{13}$$

Так як ${v_1}^2 = u_1(u_1 - 1)(u_1 - \lambda) \neq 0$, то з (13) ми одержимо рівність

$$u = \frac{1}{4}\,\frac{\left({u_1}^2 - \lambda\right)^2}{v_1^2}.$$

Отже, для довільної 2-подільної точки $Q = (u,\ v),\ Q \neq O$, еліптичної кривої E над полем $\mathbb{F}_q$, заданої рівнянням (1), перша координата є повним квадратом.

Якщо P_1 є 2-подільна точка на кривій E, то 2-подільною буде будь-яка точка $M_l = P_1 + lP_2$ послідовності (3) з парним l; якщо ж 2-подільною точкою є точка $P_1 + P_2$, то 2-подільною точкою буде будь-яка точка M_l в послідовності (3), що має непарне l; якщо ж обидві точки P_1 і P_2 є 2-подільні, то 2-подільною точкою буде будь-яка точка в послідовності (3). Звідси випливає, що відповідні елементи x_l послідовності (4) у всіх вказаних випадках є точними квадратами.

1. *Болотов А. А., Гашков С. Б., Фролов А. Б.* Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. – М.: КомКнига, 2006. – 280 с.
2. *Василенко О. В.* Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, – 2006. – 334 с.
3. *Kaliski B. S., Jr.* A pseudo-random bit generator based on elliptic logarithms. – Lect. Notes Comput.Sci., – 1987, V. 263, – P. 84–103.
4. ДСТУ4145-2002. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К.: Держстандарт України, – 2003. – 94 с.
5. *Silverman J. H.* The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, – 106, Springer-Verlag, New York. – 1986.
6. *Тараканов В. Е.* Несколько замечаний об арифметических свойствах рекуррентных последовательностей на эллиптических кривых над конечным полем// Матем. заметки – 2007. – Т.82, Вып. 6. – С. 926–933.
7. *Muhammad Ashraf.* On the Alternate Models of Elliptic Curves / Muhammad Ashraf, Baris Bulent Kirlar // International Journal of Information Security Science.. – 2012.. – Vol 1., No 2. – P. 49–66.

Одержано 28.04.2014