УДК 681.3.06

О. Ю. Беспалов, аспірант
Національний технічний університет України «КПІ», м. Київ

УЗАГАЛЬНЕННЯ ЛЕМИ ГАУССА ПРО ХАРАКТЕРИ ПАР ЕЛЕМЕНТІВ ПРОСТОГО СКІНЧЕННОГО ПОЛЯ

У роботі доведено узагальнення леми Гаусса про характери пар елементів простого скінченного поля та наслідки з неї. Ці результати мають суттєве застосування при дослідженні властивостей еліптичних кривих.

Ключові слова: *характери скінченного поля, еліптичні криві.*

Вступ. Сучасну криптологію неможливо уявити без стійких та швидких алгоритмів цифрового підпису на еліптичних кривих. Зокрема, за останні роки з'явився новий клас еліптичних кривих, так звані криві Едвардса [1], що є рекордсменами у швидкодії операцій у групі точок кривої. Цей напрямок почав розвиватися приблизно десять років тому, але кількість робіт, йому присвячена, налічує не одну тисячу. З основними результатами цього напрямку можна ознайомитись у [2–7].

Звичайно, при дослідженні властивостей кривих Едвардса активно використовуються результати теорії чисел. Це є природнім і зрозумілим. Наприклад, одна з найголовніших для криптографії на еліптичних кривих теорем — теорема Хассе про кількість точок кривої [8, с. 196–197] теж є результатом теорії чисел.

У роботах вітчизняних авторів [5, 7] при дослідженні еліптичних кривих Едвардса неодноразово використовувався інший, менш поширений, але досить цікавий результат з теорії чисел — так звана лема Гаусса про характери пар елементів скінченного поля [9, с. 75–79]. Також певні міркування показують, що при подальших дослідженнях може виявитись необхідним більш загальне твердження, яке ми у цій роботі назвемо узагальненою лемою Гаусса про характери пар елементів скінченного поля. Зазначимо, що з узагальнення цієї леми, яке буде доведено далі у роботі, зразу випливає і сама лема, і деякі її наслідки, які використовувались, наприклад, у [5] при обчисленні кількості кривих Едвардса над простим полем, які мають певні властивості.

1. Основні позначення та терміни. Для довільного простого p позначимо $Q_p = \left\{ x \in Z_p^* \mid \exists y \in Z:\ x \equiv y^2 \pmod p \right\}$ — множину зведених квадратичних лишків за модулем p. Також позначимо

$$\left(\frac{x}{p} \right) = \begin{cases} 1, & if \quad x \bmod p \in Q_p; \\ 0, & if \quad x \vdots p; \\ -1, & if \quad x \bmod p \in Z_p^* \setminus Q_p, \end{cases} \tag{1}$$

символ Лежандра елемента x за модулем p.

Безпосередньо з означення випливає, що символ Лежандра (1) є характером мультиплікативної групи простого скінченного поля Z_p.

Для довільного $l \in N$, $1 \le l \le p-1$, введемо наступні множини:

$$RR_l = \left\{ (i, i+l) \bmod p \mid \left(i \in Z_p^* \setminus \{p-l\} \right) \Lambda \left(\left(\frac{i}{p} \right) = \left(\frac{i+l}{p} \right) = 1 \right) \right\},$$

$$RN_l = \left\{ (i, i+l) \bmod p \mid \left(i \in Z_p^* \setminus \{p-l\} \right) \Lambda \left(\left(\frac{i}{p} \right) = 1, \left(\frac{i+l}{p} \right) = -1 \right) \right\},$$

$$NR_l = \left\{ (i, i+l) \bmod p \mid \left(i \in Z_p^* \setminus \{p-l\} \right) \Lambda \left(\left(\frac{i}{p} \right) = -1, \left(\frac{i+l}{p} \right) = 1 \right) \right\},$$

$$NN_l = \left\{ (i, i+l) \bmod p \mid \left(i \in Z_p^* \setminus \{p-l\} \right) \Lambda \left(\left(\frac{i}{p} \right) = \left(\frac{i+l}{p} \right) = -1 \right) \right\}. \quad (2)$$

Також через

$$rr_l, rn_l, nr_l, nn_l \quad (3)$$

позначимо потужності відповідних множин з (2).

Зазначимо, що у частковому випадку, коли $l = 1$, величини (3) збігаються з величинами

$$(\text{BB}), (\text{BH}), (\text{HB}) \text{ та } (\text{HH}), \quad (4)$$

введеними в [9]. Величини (4) використовувались потім у роботі [5] (леми 2 та 3) при обчисленні точної кількості кривих Едвардса над простим скінченним полем, що мають певні властивості.

Для обчислення величин (4) в книзі [9] наведений результат Гаусса, який дозволяє обчислити ці величини. Тут і далі цей результат ми будемо називати лемою Гаусса, або лемою про характери пар елементів скінченного поля.

Лема 1 (лема Гаусса [9]): у наших позначеннях справедливі рівності:

$$(\text{BB}) + (\text{BH}) = \frac{1}{2}\left(p - 2 - \varepsilon\right); (\text{HB}) + (\text{HH}) = \frac{1}{2}\left(p - 2 + \varepsilon\right);$$

$$(\text{BB}) + (\text{HB}) = \frac{1}{2}\left(p - 1\right) - 1; \quad (5)$$

$$(\text{BH}) + (\text{HH}) = \frac{1}{2}\left(p - 1\right); (\text{BB}) + (\text{BH}) - (\text{HB}) - (\text{HH}) = -1.$$

На основі результатів (5) у роботі [5, с. 168–169] доведені дві допоміжні леми, які в певному сенсі можна вважати частковими узагальненнями леми Гаусса. Потім, з використанням цих лем, у роботі було отримано основний результат щодо кількості кривих Едвардса.

У цій роботі буде доведено більш глобальне узагальнення леми Гаусса. Зазначимо, що з нашого результату одразу випливає як сама лема Гаусса (5), так і леми 2 та 3 з роботи [5], а також деякі інші корисні наслідки.

2. Узагальнення леми про характери пар елементів скінченного поля.

Лема 2 (про характери пар елементів скінченного поля).

Нехай p — просте, $l \in Z_p^*$. Тоді для величин (3) справедливі наступні рівності:

$$rn_l + nn_l = \frac{p-2+\left(\frac{l}{p}\right)}{2};\ rr_l + nr_l = \frac{p-2-\left(\frac{l}{p}\right)}{2};$$

$$nr_l + nn_l = \frac{p-2+\left(\frac{-l}{p}\right)}{2}; \qquad (6)$$

$$rr_l + rn_l = \frac{p-2-\left(\frac{-l}{p}\right)}{2};\ rr_l + nn_l - rn_l - nr_l = -1.$$

Доведення. Доводимо перше твердження з (6). Доведення інших рівностей виконуються аналогічно з певними модифікаціями. Всього кількість пар $(i, i+l)$, де $i \in Z_p^* \setminus \{p-l\}$, дорівнює $p-2$. При цьому перший елемент пари пробігає всі значення з Z_p^*, крім $p-l$, а другий — всі значення з Z_p^*, крім l (оскільки $i \neq 0$). Потрібно визначити, скільки разів другий елемент у цих парах є квадратичним нелишком, тобто скільки існує таких елементів $a \in Z_p^* \setminus \{l\}$, що $a \in Z_p^* \setminus Q_p$.

Зрозуміло, що ця кількість залежить від квадратичності елемента l. Оскільки кількість квадратичних нелишків у Z_p^* дорівнює $\frac{p-1}{2}$, то кількість квадратичних нелишків у $a \in Z_p^* \setminus \{l\}$ є $\frac{p-1}{2}$, якщо $l \in Q_p$, та $\frac{p-1}{2} - 1 = \frac{p-3}{2}$, у протилежному випадку. Звідси

$$rn_l + nn_l = \begin{cases} \frac{p-3}{2}, & if \quad \left(\frac{l}{p}\right) = -1 \\ \frac{p-1}{2}, & if \quad \left(\frac{l}{p}\right) = 1 \end{cases} = \frac{p-2+\left(\frac{l}{p}\right)}{2}.$$

Перша рівність доведена.

Для доведення рівностей з другої по четверту, зазначимо, що:

- у парах $(i, i+l) \in RR_l \cup NR_l$ перший елемент приймає значення з $Z_p^* \setminus \{p-l\}$, а другий — з $\left(Z_p^* \setminus \{l\}\right) \cap Q_p$;
- у парах $(i, i+l) \in NR_l \cup NN_l$ перший елемент приймає значення з $\left(Z_p^* \setminus \{p-l\}\right) \cap \left(Z_p^* \setminus Q_p\right)$, а другий — з $Z_p^* \setminus \{l\}$;
- у парах $(i, i+1) \in RR_l \cup RN_l$ перший елемент приймає значення з $\left(Z_p^* \setminus \{p-l\}\right) \cap Q_p$, а другий — з $Z_p^* \setminus \{l\}$.

Далі ці твердження доводяться з використанням міркувань, аналогічних до тих, що наведені при доведенні першої рівності.

Остання, п'ята рівність, доводиться інакше. Для її доведення зазначимо, що

$$rr_l + nn_l - rn_l - nr_l = \sum_{\substack{i=1 \\ i \neq p-l}}^{p-1} \left(\frac{i(i+l)}{p} \right).$$

Позначимо $m = i^{-1} \bmod p$ перетворимо вираз $\left(\frac{i(i+l)}{p} \right)$ наступним чином, використовуючи властивості символа Лежандра:

$$\left(\frac{i(i+l)}{p} \right) = \left(\frac{i(i+l)i^{-2}}{p} \right) = \left(\frac{i^{-1}(i+l)}{p} \right) = \left(\frac{(1+lm)}{p} \right).$$

Оскільки $i \neq p-l$, то $m \neq (p-l)^{-1}$, або $m \neq -l^{-1}$, тому $1+lm \neq 1+l \cdot \left(-l^{-1}\right)$, тобто $1+lm \neq 0$. Крім того, оскільки $l \neq 0$, $m \neq 0$, то $1+lm \neq 1$. Покажемо, що вираз $1+lm$ приймає всі значення з $Z_p^* \setminus \{1\}$. Дійсно, нехай $a \in Z_p^* \setminus \{1\}$. Тоді

$$1+lm = a \Leftrightarrow lm = a-1 \Leftrightarrow m = l^{-1}(a-1).$$

Отже,

$$rr_l + nn_l - rn_l - nr_l = \sum_{\substack{i=1 \\ i \neq p-l}}^{p-1} \left(\frac{i(i+l)}{p} \right) = \sum_{i=2}^{p-1} \left(\frac{i}{p} \right) = \sum_{i=1}^{p-1} \left(\frac{i}{p} \right) - \left(\frac{1}{p} \right) =$$

$$= \left|Q_p\right| - \left|Z_p^* \setminus Q_p\right| - 1 = 0 - 1 = -1.$$

Лему доведено.

3. Наслідки з узагальненої леми Гаусса. Тепер наведемо ряд тверджень, що випливають з доведеної леми. Ці твердження є цікавими не тільки з математичної точки зору, але й з точки зору вирішення практичних задач криптології. Наведені далі твердження можна використовувати для обчислення кількості кривих або точок кривої, що має певні властивості або задана певними параметрами. Оскільки задача обчислення кількості точок є фактично задачею обчислення кількості розв'язків певного рівняння.

Зазначимо, що класичну лему Гаусса також можна вважати наслідком узагальненої леми при $l = 1$.

Наслідок 1. Позначимо $\varepsilon_1 = \left(\frac{l}{p}\right)$ та $\varepsilon_2 = \left(\frac{-l}{p}\right)$. Тоді величини (3) приймають такі значення:

$$rn_l = \frac{p-1+\varepsilon_1-\varepsilon_2}{4};\ nn_l = \frac{p-3+\varepsilon_1+\varepsilon_2}{4};$$

$$rr_l = \frac{p-3-\varepsilon_1-\varepsilon_2}{4};\ nr_l = \frac{p-1-\varepsilon_1+\varepsilon_2}{4}.$$

Доведення наслідку 1 полягає у безпосередньому обчисленні значень цих величин з системи (6).

Наслідок 2. Якщо $l \in Q_p$, то

$$rn_l = \frac{p-\left(\frac{-1}{p}\right)}{4};\ nn_l = \frac{p-2+\left(\frac{-1}{p}\right)}{4};$$

$$rr_l = \frac{p-4-\left(\frac{-1}{p}\right)}{4};\ nr_l = \frac{p-2+\left(\frac{-1}{p}\right)}{4}.$$

В протилежному випадку (тобто коли $l \notin Q_p$)

$$rn_l = \frac{p-2+\left(\frac{-1}{p}\right)}{4};\ nn_l = \frac{p-4-\left(\frac{-1}{p}\right)}{4};$$

$$rr_l = \frac{p-2+\left(\frac{-1}{p}\right)}{4};\ nr_l = \frac{p-\left(\frac{-1}{p}\right)}{4}.$$

Для доведення цього наслідку скористаємось тим, що за умови $l \in Q_p$ виконується $\varepsilon_1 = \left(\frac{l}{p}\right) = 1$ та $\varepsilon_2 = \left(\frac{-l}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{l}{p}\right) = \left(\frac{-1}{p}\right)$.

Аналогічно, за умови $l \notin Q_p$ виконується $\varepsilon_1 = \left(\frac{l}{p}\right) = -1$ та $\varepsilon_2 = \left(\frac{-l}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{l}{p}\right) = -\left(\frac{-1}{p}\right)$.

Зауважимо, що з наслідку 2 відразу випливають леми 2 та 3 з роботи [7].

Висновки. У роботі доведено узагальнення відомого результату з теорії чисел — леми Гаусса про характери пар елементів скінченного простого поля. Також отримано наслідки цієї леми. Ці результати мають практичне значення при аналізі властивостей еліптичних кривих над простим скінченним полем.

Список використаних джерел:

1. Edwards H. M. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*. 2007. Vol. 44, N. 3. P. 393–422.
2. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. *IST Programme under Contract IST–2002–507932 ECRYPT,* 2007, P. 1–20.
3. Bernstein Daniel J., Birkner Peter, Joye Marc, Lange Tanja, Peters Christiane. Twisted Edwards Curves. *IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498.* 2008. P. 1–17.
4. Бессалов А. В., Дихтенко А. А., Третьяков Д. Б. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем. *Сучасний захист інформації*. 2011. №4. С. 33–36.
5. Kovalchuk L., Bessalov A. Exact Number of Elliptic Curves in the Canonical Form, Which are Isomorphic to EdvardsEdwards Curves Over Prime Field. *Cybernetics and Systems Analysis*. 2015. Vol. 51, issue 2. P. 165–172.
6. Ковальчук Л. В., Бессалов А. В., Беспалов А. Ю. Алгоритмы генерации базовой точки кривой Едвардса с использованием критериев делимости точки. *Кибернетика и системный анализ*. 2016. Т. 52, № 5. С. 14–24.
7. Бессалов А. В., Цыганкова О.В.. Новые свойства кривой Эдвардса над простым полем. *Радиотехника*. 2015. №180. С. 137–143.
8. Коблиц Н. Курс теории чисел и криптографии. М.: Научное изд-во ТВП, 2001. 254 с.
9. Дэвенпорт Г. Высшая арифметика: введение в теорию чисел: Пер. с англ. под редакцией Ю. В. Линника. М.: Наука, 1965. 176 с.

Generalized Gauss Lemma about characters of pair of elements of finite prime field is proved and, some corollaries are obtained. These results are useful in investigations of different properties of elliptic curves.

Key words: *characters of finite prime field, elliptic curves.*

Одержано 27.02.2017