УДК 512.772:512.624

Р. В. Скуратовський
Міжрегіональна академія управління персоналом
Інститут комп'ютерно-інформаційних технологій

СУПЕРСИНГУЛЯРНІСТЬ ЕЛІПТИЧНИХ КРИВИХ І КРИВИХ ЕДВАРДСА НАД F_{P^N}

Ми розглядаємо алгебраїчні криві у формі Едвардса і еліптичні криві Монтгомері над скінченним полем F_{p^n}, які на даний час є одним з найбільш швидких і перспективиих носіїв груп, що на даний час мають багато застосувань. В роботі знайдено умови суперсингулярності кривих Едвардса і великого класу скручених кривих Едвардса над полем F_{p^n} характеристики $p \equiv 3 \mod 4$. Показано, що проективна крива Едвардса не є еліптичною. Досліджено деякі цікаві властивості групи точок цих кривих. Побудовано криві заданого порядку з мінімальним кофактором. Підраховано род скрученої кривої Едвардса. Знайдено умови мінімальності кофактора скрученої кривої Едвардса та її род.

MSC: 11G20, 11G07.

Ключові слова: суперсингулярні криві, скінченне поле, еліптична криптографія, крива Едвардса, еліптичні криві з малим степенем занурення в поле .
DOI: 10.18524/2519–206x.2018.1.134622.

Вступ. Крива Едвардса E_d вперше була представлена Едвардсом в роботі [6] і потім детальніше досліджена в роботі Бернштейна і Ланге [7]. Відомо, що суперсингулярні криві, на відміну від несуперсингулярних, над алгебраїчно замкненим полем, зокрема над $\mathbb{C}$, мають не комутативне кільце ендоморфізмів $End\,(\mathbb{C})$. Внаслідок чого суперсингулярні криві, окрім n-мультиплікативного множення, наділені ще і комплексним множенням. Ще більш складні властивості суперсингулярні криві мають над скінченними полями. Ці властивості ще далеко не повністю вивчено, а класи суперсинулярних кривих над $\mathbb{F}_{p^n}$ ще не знайдено. Ці властивості викликають інтерес як з точки зору теорії кілець едоморфізмів, так і з точки зору алгебраїчної геометрії. Їх дослідження є одною з цілей даної роботи.

Перевагою E_d є простота групової операції, універсальність закона додавання, симетричність точок і представлення нейтрального елемента групи точкою в афінних координатах. Ці властивості помічені і обґрунтовані вже в першій роботі [10] відомих фахівців з алгебраїчної геометрії.

З точки зору алгебраїчної геометрії, крива Едвардса не є еліптичною, бо є сингулярною. Криві Едвардса, також як і скручені криві Едвардса, мають афінне представлення, ізоморфне деякій афінній частині еліптичної кривої, що має в порядку групи кривої множник 4. Актуаліність даного питання полягає в тому, що в еліптичній криптографії дуже важливо знати ті криві, які є суперсингулярними, бо вони є крипографічно слабкими. Суперсингулярність кривих Едвардса раніше досліджувалася лише в [18] і лише для простих полів $\mathbb{F}_p$, при цьому автори обмежилися доведенням суперсингулярності лише для кривої з коефіцієнтами $d = 2,\ d = 2^{-1}$, де пізніше при підрахунках у полі характеристики $p = 8k + 7$ у

Надійшла 29.11.2017

них виявлена неточність, тому задача дослідження її над скінченим алгебраїчним розширенням, тобто $\mathbb{F}_{p^n}$, є новою.

Одною з головних задач даного дослідження є узагальнення результата про суперсингулярність кривої отриманого в [18] для коефіцієнтів $d = 2,\ \ d = 2^{-1}$ над $\mathbb{F}_p$ на випадок довільного не простого поля $\mathbb{F}_{p^n}$ та виправлення неточності у кількості точок афінної кривої Едвардса над полем характеристики $p \equiv 7(mod 8)$, яка була в теоремі 3 з [18]. Окрім цього метою нашого дослідження є пошук всієї множини параметрів, при яких крива E_d стає суперсингулярною. Не менш важливою метою цієї роботи є проведення аналогічного дослідження для еліптичних кривих у формах Монтгомері і Веєрштрасса.

Дуже часто виникає задача про знаходження кривих, які мають нульовий $j(E)$-інваріант над полем характеристики $p = 2$, тобто є суперсингулярними, бо вони допускають побудову гомоморфізму у мультиплікативну групу скінченного поля з невеликим степенем розширення.

Метою работи є не тільки аналіз умов суперсингулярності кривої Едвардса і кривої Монтгомері, а ще й знаходження умов мінімальності кофактора скрученої кривої Едвардса [21].

Цікавою є можливість побудови скрученої кривої Едвардса порядку $N_E = 4p, p \in \mathbf{P}$, тобто такої, яка має мінімальний кофактор 4 [10, 15]. Зараз в алгоритмах доведення без розголошення активно використовуються криві з малим степенем занурення k [30] їх групи в поле F_{p^k}, а суперсингулярні криві володіють цією властивістю завдяки спарюванню Тейта. Тому ми досліджуємо їх серед кривих Едвардса. Частково викладені результати представлено в тезах [23,27,28].

Основні результати

1. Обґрунтування основних результатів

1.1. Аналіз особливостей скрученої кривої Едвардса. Скручена крива Едвадрса [7] $E_{\mathrm{a,d}}$ має вигляд:

$$ax^2 + y^2 = 1 + dx^2y^2, a, d \in F_p{}^*, ad(a\text{-}d) \neq 0,\ \ d \neq 1,\ p \neq 2. \tag{1}$$

При $a = d$ перетворимо криву $ax^2+y^2 = 1+ax^2y^2$ до вигляду $ax^2-ax^2y^2-1+y^2 = 0$ або $ax^2(1-y^2)-(1-y^2) = 0$, отже, крива розкладається у добуток двох пар прямих $(ax^2-1)(y^2-1) = 0$. З умови гладкості знаходимо особливі точки афінної кривої

$$\begin{cases} \frac{F(x,y)}{\partial x} = 0, \\ \frac{F(x,y)}{\partial y} = 0, \end{cases} \quad \left[\begin{array}{l} (0,0), \\ \left(\pm\sqrt{\frac{1}{d}}, \pm\sqrt{\frac{a}{d}}\right). \end{array} \right.$$

Але точка $(0,0)$ кривій $E_{\mathrm{a,d}}$ не належить не залежно від поля і від d. При $a \neq d$ точка $\left(\pm\sqrt{\frac{1}{d}}, \pm\sqrt{\frac{a}{d}}\right)$ не належить кривій (1), при $(\frac{d}{p}) = -1$ її не існує. Тому в афінному представленні особливих точок не має, залишилося перевірити їх існування в проективному представленні.

Як відомо, [11] проективна крива дала можливість отримати більш швидкі операції над точками кривої. Тому дослідимо цю криву у проективній формі.

Проаналізуємо особливі точки в проективному замиканні кривої (1). Для цього зробимо проективізацію кривої (1). Нехай $x = \frac{X}{Z},\ y = \frac{X}{Z}$, тоді $a\frac{x^2}{z^2} + \frac{y^2}{z^2} =$

$1 + d\frac{x^2y^2}{z^4}$, звідси $F(x, y, z) = ax^2z^2 + y^2z^2 - z^4 - dx^2y^2$. Перевіримо умови гладкості (для алгебраїчних кривих поняття гладкості і нормальності збігаються [9]):

$$\begin{cases} \frac{\partial F(x,y,z)}{\partial x} = 2axz^2 - 2dxy^2 = 0, \\ \frac{\partial F(x,y,z)}{\partial y} = 2yz^2 + 2dx^2y = 0, \\ \frac{\partial F(x,y,z)}{\partial y} = 2azx^2 + 2zy^2 - 4z^3 = 0. \end{cases}$$

Тут розв'язком очевидно є $(0, 0, 0)$, але ця точка не належить $\mathbb{P}^2$. А при $z = 0$ розв'язками є точки $(x_0, 0, 0) = (1, 0, 0)$ і $(0, y_0, 0) = (0, 1, 0)$. Тобто маємо 2 особливі точки $p = (1, 0, 0)$ і $p' = (0, 1, 0)$. Це прості особливості. Отже, розв'язками є лише особливі точки (нескінченно віддалені точки) $(1, 0, 0)$ і $(0, 1, 0)$, тому маємо особливості на нескінченності у відповідних афінних компонентах $A^1 : \ az^2 + y^2z^2 = z^4 + dy^2$ і $A^2 : \ ax^2z^2 + z^2 = z^4 + dx^2$.

Проаналізуємо будову локального кільця $\mathcal{O}_p$ в точках p і p'. Позначимо $\delta_p = \dim {}^{\widetilde{\mathcal{O}}_p}/_{\mathcal{O}_p}$ розмірність фактора як векторного простору або кратність особливої точки. Оскільки базис розширення – $\widetilde{\mathcal{O}}_p$ над локальним кільцем точки $\mathcal{O}_p$ складається з одного елемента, то $\delta_p = 1$. Тут $\widetilde{\mathcal{O}}_p$ – цілозамкнене кільце. Оскільки додали два нові елементи, кожен з яких відповідає своєму локальному кільцю особливої точки, яких теж дві, тому $\delta_p = 1$ і $\delta_{p'} = 1$. Підрахуємо геометричний род (взагалі род кривої — це кількість ЛНЗ регулярних диференціалів) кривої $F(x, y, z) = ax^2z^2 + y^2z^2 - z^4 - dx^2y^2$. При $a \neq d$ ми маємо нерозкладну проективну криву степеня 4, тоді згідно з [9,12], геометричний род алгебраїчної незвідної проективної кривої:

$$\rho^*(C) = \rho_\alpha(C) - \sum_{p \in E} \delta_p = \ \frac{(n-1)(n-2)}{2} - \sum_{p \in E} \delta_p = 3 - 2 = 1,$$

де $\rho_\alpha(C)$ — арифметичний род кривої C, параметр $n = degC = 4$. Оскільки вона роду 1, то вона ізоморфна плоскій кубічній кривій але не є еліптичною, бо має особливості в проективній частині. Крива Едварса, як і скручена крива Едаварса, ізоморфна деякій афінній частині еліптичної кривої. Нормалізація кривої Едвардса — еліптична крива $E_M : Bu^2 = v^3 + Av^2 + v$, що запропонована Монтгомері [7]. З наявності особливих точок p і p' одразу слідує наступна властивість.

Проективні криві $E_{\mathrm{a,d}}$ і E_M не є ізоморфними як алгебраїчні множини [13].

2. Суперсингулярність кривої Едвардса, криві з малим кофактором

2.1. Класи суперсингулярності кривих Едвардса і їх порядки. Нагадаємо, що саме Кобліц [15] запропонував суперсингулярні криві зі скінченою кількістю $|\#E(GF(q))| = q + 1$ точок на кривій над скінченним полем F_q. Саме криві з таким порядком ми і виявляємо в сімействі кривих Едвардса. Суперсингулярні криві, запропоновані Кобліцем, у силу наявності на них комплексного множення допускали побудову гомоморфізму в скінченне поле [16].

Виявлення суперсингулярних кривих рівносильне пошуку параметрів, при яких крива і відповідна їй крива зі скрутом мають однакові кількості розв'язків. Як показано в [7], крива $E_{1,d}$ є кривою кручення для $E_{1,d^{-1}}$. Також в більш загальному випадку для кривої $E_{a,d}$ перехід до кривої кручення задається відображенням $(\bar{x}, \bar{y}) \mapsto (x, y) = \left(\bar{x}, \frac{1}{\bar{y}}\right)$ [7]. Тому скористаємося цим відображенням для

пошуку суперсингулярних кривих. Ми виявили неточність в роботі [18], в умові суперсингулярності для кривої Едвардса E_d. Більш точно, якщо $p \equiv -3(\mathrm{mod}8)$, то не маємо виродженої (суперсингулярної) пари кривих, незважаючи на те, що це стверджується в теоремі 3 з [18]. Крім того, якщо $p \equiv 7(\mathrm{mod}8)$, то порядки пари скручених кривих є наступними $N_{E_2} = N_{E_{2^{-1}}} = p - 3$, що не збігається з $p + 1$, як це стверджується в теоремі 3 з [18]. Наприклад, якщо $p = 31$, то $N_{E_2} = N_{E_{2^{-1}}} = 28 = 31 - 3$, що не дорівнює $p + 1$. Також для випадку $p \equiv 7(\mathrm{mod}8)$ при $p = 7, d = 2^{-1} \equiv 4(\mathrm{mod}\,7)$ крива має наступні 4 точки: $(0,1); (0,6); (1,0); (6,0)$, якщо $p = 7, d = 2(\mathrm{mod}\,7)$, то крива теж має 4 точки: $(0,1); (0,6); (1,0); (6,0)$. Отже, ці порядки відповідають числу $p - 3$, а не числу $p + 1$, як це стверджується у вище згаданій теоремі з [18]. Обчислимо порядки пари кривих для $p \equiv -3(\mathrm{mod}8)$ і коефіцієнтів $d = 2$, $d = 2^{-1} \equiv 7(\mathrm{mod}8)$, згідно з теоремою 3 з [18] це вироджена пара кривих, але обчислення свідчять, що порядок кривої для $p = 13$, $d = 2$ це $N_{E_{(2)}} = 8$ і для $p = 13$, $d = 7$ це $N_{E_{(7)}} = 20$, отже насправді не маємо виродженої пари кривих. Множина точок над полем F_{13} при $d = 2$ є наступною $(0,1); (0,12); (1,0); (4,4); (4,9); (9,4); (9,9); (12,0)$, а для $d = 7$ це $\{(0,1); (0,12); (1,0); (2,4); (2,9); (4,2); (4,11); (5,6); (5,7); (6,5); (6,8);$
$(7,5); (7,8); (8,6); (8,7); (9,2); (9,11); (11,4); (11,9); (12,0)\}$.

Аналогічно для $p = 29 \equiv -3(\mathrm{mod}\,8)$ і $d = 2$ маємо $N_{E_{(15)}} = 20$ але $p = 29 \equiv -3(\mathrm{mod}\,8)$ і $d = 15$ маємо $N_{E_{(15)}} = 20$, що знову підтверджує наші зауваження до теореми 3 з [18]. Наведемо обчислення для випадку $p = 23 \equiv 7(\mathrm{mod}\,8)$ $d = 12$ на кривій будуть точки $\{(0,1); (0,22); (1,0); (5,10); (5,13); (6,11); (6,12); (10,5);$
$(10,18); (11,6); (11,17); (12,6); (12,17); (13,5); (13,18); (17,11); (17,12); (18,10);$
$(18,13); (22,0)\}$ тому $N_{E_{(12)}} = 20$. Також $N_{E_{(2)}} = 20$ це точки $\{(0,1); (0,22); (1,0);$
$(2,7); (2,16); (4,9); (4,14); (7,2); (7,21); (9,4); (9,19); (14,4); (14,19); (16,2); (16,21);$
$(19,9); (19,14); (21,7); (21,16); (22,0)\}$.

Сформулюємо теорему про умови суперсингулярності кривої Едвардса, попередньо навівши допоміжні твердження.

Зауваження 1. *Має місце симетрія квадратів лишків:*
$(\frac{p-1}{2} - k)^2 \equiv (\frac{p-1}{2} + 1 + k)^2 (\underline{m}odp), 0 \leqslant k \leqslant \frac{p-1}{2}$.

Справді, виконується конгруенція $(\frac{p-1}{2}) - k = p - ((\frac{p-1}{2}) + 1 + k) \equiv -((\frac{p-1}{2}) + 1 + k)(\mathrm{mod}p)$. Отже, $(\frac{p-1}{2} - 2)^2 \equiv (\frac{p-1}{2} + 3)^2, \ldots, (\frac{p-1}{2} - k)^2 \equiv (\frac{p-1}{2} + k + 1)^2 (\mathrm{mod}\ p)$. Без квадратів маємо антисиметричну конгруенцію $(\frac{p-1}{2} - k) \equiv -(\frac{p-1}{2} + 1 + k)(modp)$.

Нагадаємо лему про суму степенів [19].

Лема 1. *Якщо $p \in \mathbb{P}$ і $n \in \mathbb{N}_0$, то*

$$\sum_{k=1}^{p-1} k^n \equiv \begin{cases} 0\ (modp), & (p-1) \nmid n, \\ -1\ (modp), & (p-1) \mid n. \end{cases}$$

Теорема 1. *Якщо $p \equiv 3\ (mod\ 4)$ і p — просте, то для $d = 2$ і $d = 2^{-1}$ кількості точок кривої $x^2 + y^2 = 1 + dx^2y^2$ та кривої $x^2 + y^2 = 1 + d^{-1}x^2y^2$ над F_p збігаються і дорівнюють $N_E = p + 1$, якщо $p \equiv 3(\mathrm{mod}8)$ та $N_E = p - 3$, якщо $p \equiv 7(\mathrm{mod}8)$.*

Над полем F_{p^n}, де $n \equiv 1(mod 2)$, порядки вищевказаних кривих $N_E = p^n + 1$, якщо $p \equiv 3(\mathrm{mod} 8)$ і $N_E = p^n - 3$, якщо $p \equiv 7(\mathrm{mod} 8)$.

Доведення. Розглянемо криву

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

Перетворимо рівняння (2) на $y^2 = \frac{x^2-1}{2x^2-1}$. Множина розв'язків цього рівняння збігається з множиною розв'язків рівняння (2), бо значення $x_0 = (\sqrt{2})^{-1}$, яке перетворює на 0 вираз $2x^2-1$, не є коренем (2), оскільки чисельник x^2-1 не набуває при цьому значення 0. У випадку $p \equiv 3(\mathrm{\ mod\ } 8)$ вираз $2x^2-1$ зі знаменника $\frac{x^2-1}{2x^2-1}$, який отримано біраціональним перетворенням з еквівалентного рівняння до рівняння початкової кривої $y^2(2x^2-1) = x^2-1$, не може бути нулем, бо $(\frac{2}{p}) \equiv -1$. Тому за умови $p \equiv 3(\mathrm{\ mod\ } 8)$ крива $y^2 = (x^2-1)(2x^2-1)$ має стільки ж точок N_2, що і крива (2), тобто $N_2 = N_E$, бо для кожного x з F_p символ Лежандра елементів $(x^2-1)/(2x^2-1)$ та $(x^2-1)(2x^2-1)$ є однаковим, але множини цих розв'язків можуть не збігатися. У випадку $p \equiv 7(\mathrm{mod}\, 8)$ крива $y^2 = (x^2-1)(2x^2-1)$ буде мати на 2 точки більше, ніж (2), оскільки з'являться точки $(\frac{1}{\sqrt{2}}, 0)$ і $(-\frac{1}{\sqrt{2}}, 0)$, бо $(\frac{2}{p}) \equiv 1$. Отже, потрібно показати, що число N_2, рівне кількості точок на кривій

$$y^2 = (x^2-1)(2x^2-1), \tag{3}$$

задовільняє умову $N_2 \equiv 1(\mathrm{mod}\, p)$ для $p \equiv 3(\mathrm{mod}\, 8)$ і $N_2 \equiv -1(\mathrm{mod}\, p)$ для $p \equiv 7(\mathrm{mod}\, 8)$. Тоді матимемо $N_2 = p+1$ для $p \equiv 3\ (\mathrm{mod}\, 8)$ та $N_2 = p-1$ для $p \equiv 7(\mathrm{mod}\, 8)$. (Випадки $N_2 = 1$ або $N_2 = 2p-1$ неможливі, бо $N_2 \geqslant 2$ і $N_2 \leqslant 2p-2$). Звідси випливає твердження про кількість точок на початковій кривій (2).

Покажемо, що кількість розв'язків рівняння $y^2 = (x^2-1)(2x^2-1)$, тобто N_2, порівняна з $(-a_{2p-2} - a_{p-1})(\mathrm{mod}\, p)$, де a_{2p-2}, a_{p-1} — коефіцієнти многочлена $(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} = a_0 + a_1x + ... + a_{2p-2}x^{2p-2}$ після розкриття дужок і застосування леми 1 про суму степенів [19] зі зведенням за модулем p.

Для фіксованого значення x кількість розв'язків рівняння (3) дорівнює $1 + \left(\frac{(x^2-1)(2x^2-1)}{p}\right)$, де $\left(\frac{a}{p}\right)$ — символ Лежандра. Як відомо, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}(\mathrm{mod} p)$, тому для фіксованого x кількість розв'язків рівняння (3) порівнянна за модулем p з $1 + ((x^2-1)(2x^2-1))^{\frac{p-1}{2}}$. Отже, підсумовуючи за всіма x, маємо $N_2 \equiv \sum\limits_{x=0}^{p-1} 1 + ((x^2-1)(2x^2-1))^{\frac{p-1}{2}} \equiv p + \sum\limits_{x=0}^{p-1} (x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} (\mathrm{mod}\, p)$. Розкривши дужки в $(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}}$, отримуємо, що $a_{2p-2} = 1^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}} \equiv (\frac{2}{p})(\mathrm{mod}\ p)$. Отже, використавши лему 1, маємо

$$N_2 \equiv -(\frac{2}{p}) - a_{p-1}(\mathrm{mod}\, p). \tag{4}$$

Нам потрібно було довести, що $N_2 \equiv 1(\mathrm{\ mod}\, p)$ при $p \equiv 3(\mathrm{mod}\, 8)$ і $N_2 \equiv -1(\mathrm{\ mod}\ p)$ при $p \equiv 7(\mathrm{\ mod}\, 8)$. Тобто треба було показати, що $N_2 \equiv -(\frac{2}{p}) - a_{p-1}(\mathrm{\ mod}\, p)$ для $p \equiv 3\,(\mathrm{\ mod}\, 4)$. Це випливатиме з (3), якщо ми покажемо, що $a_{p-1} \equiv 0(\mathrm{\ mod}\ p)$. Визначимо згідно з формулою бінома Ньютона коефіцієнт a_{p-1} при x^{p-1}

многочлена утвореного з добутку $(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}}$. Він дорівнює $a_{p-1} = (-1)^{\frac{p-1}{2}}\sum\limits_{j=0}^{\frac{p-1}{2}} 2^j(C^j_{\frac{p-1}{2}})^2$. Справді,

$$\sum_{j=0}^{\frac{p-1}{2}} 2^j(C^{\frac{p-1}{2}-j}_{\frac{p-1}{2}})(-1)^{\frac{p-1}{2}-(\frac{p-1}{2}-j)}\cdot 2^j(C^j_{\frac{p-1}{2}})^2(-1)^{\frac{p-1}{2}-j} =$$

$$= (-1)^{\frac{p-1}{2}}\sum_{j=0}^{\frac{p-1}{2}} 2^j C^{\frac{p-1}{2}-j}_{\frac{p-1}{2}}\cdot C^j_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}\sum_{j=0}^{\frac{p-1}{2}} 2^j(C^j_{\frac{p-1}{2}})^2.$$

Покажемо, що за умови $p\equiv 3(\mathrm{mod}4)$ виконуватиметься

$$\sum_{j=0}^{\frac{p-1}{2}} 2^j(C^j_{\frac{p-1}{2}})^2 \equiv 0\,(\mathrm{mod}\,p).$$

Домножимо кожен біноміальний коефіцієнт у попередній сумі на $(\frac{p-1}{2})!$. Отримуємо

$$(\frac{p-1}{2})!C^j_{\frac{p-1}{2}} = \frac{(\frac{p-1}{2})(\frac{p-1}{2}-1)...(\frac{p-1}{2}-j+1)(\frac{p-1}{2})!}{1\cdot 2\cdot ...\cdot j} =$$

$$= (\frac{p-1}{2})(\frac{p-1}{2}-1)...(\frac{p-1}{2}-j+1)[(\frac{p-1}{2})(\frac{p-1}{2}-1)...(j+1)].$$

Застосовуємо рівності з зауваження $1: (\frac{p-1}{2}-k)^2 \equiv (\frac{p-1}{2}+1+k)^2(modp), 0\leqslant k\leqslant \frac{p-1}{2}$ до множників у квадратних дужках $[(\frac{p-1}{2})(\frac{p-1}{2}-1)...(j+1)]$, отримаємо: $(\frac{p-1}{2})(\frac{p-1}{2}-1)...(\frac{p-1}{2}-j+1)[(\frac{p-1}{2}+1)...(\frac{p-1}{2}+\frac{p-1}{2}-j)](-1)^{\frac{p-1}{2}-j}$.

Переставивши множники бачимо, що з зауваження 1 випливає: $(\frac{p-1}{2})!C^j_{\frac{p-1}{2}} = (\frac{p-1}{2}-j+1)(\frac{p-1}{2}-j+2)...(\frac{p-1}{2})(\frac{p-1}{2}+1)...(p-j-1)(-1)^{\frac{p-1}{2}-j}$.

Піднісши дві частини до квадрату, отримаємо:

$$\left(\left(\frac{p-1}{2}\right)!C^j_{\frac{p-1}{2}}\right)^2 \equiv \left(\frac{p-1}{2}-j+1\right)^2\left(\frac{p-1}{2}-j+2\right)^2\ldots(p-j-1)^2(\mathrm{mod}p). \tag{5}$$

Покажемо, як обчислити $N_2(\mathrm{mod}\,p)$. Помітимо, що для заданого x кількість розв'язків рівняння $y^2 = (x^2-1)(2x^2-1)(\mathrm{\ mod\ }p)$ конгруентна значенню суми виразів $1+((x^2-1)(2x^2-1))^{\frac{p-1}{2}}(\mathrm{mod}\,p)$ по x від 0 до $p-1$. Отже,

$$N_2 \equiv \sum\nolimits_{x=0}^{p-1} 1+(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} \equiv p+\sum\nolimits_{x=0}^{p-1}(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}}$$

$$\equiv \sum\nolimits_{x=0}^{p-1}(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}}(\mathrm{mod}p).$$

Вираз $(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}}$ — це деякий многочлен $a_{2p-2}x^{p-1}+a_{2p-3}x^{p-2}+ ... + a_1x+a_0$. Для всіх $i=0,1...,2p-2$, окрім $i=2p-2$ і $i=p-1$, сума $\sum\limits_{x=0}^{p-1} x^i$ рівна 0 за модулем p.

Для $i = 2p-2$ і $i = p-1$ ця сума порівняна з -1, що слідує з леми про суму степенів. Тому $\sum_{x=0}^{p-1}(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} \equiv -a_{2p-2} - a_{p-1}(\mathrm{mod}p)$.

Має місце конгруенція суми коефіцієнтів з індексами, кратними $p-1$,

$$-a_{2p-2} - a_{p-1}(\mathrm{mod}p) \equiv \begin{cases} 1, & p \equiv 3(\mathrm{mod}8) \\ -1, & p \equiv 7(\mathrm{mod}8). \end{cases}$$

Для доведення цього залишилося обчислити a_{2p-2} і a_{p-1}. Очевидно, a_{2p-2} рівний $2^{\frac{p-1}{2}} \equiv (\frac{2}{p})(\mathrm{mod}p)$. А коефіцієнт a_{p-1} виражається як

$$a_{p-1} = \sum\nolimits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 2^j (-1)^{\frac{p-1}{2}},$$

тому що це коофіцієнт у многочлені

$$\left(\sum_{j=0}^{\frac{p-1}{2}} C^j_{\frac{p-1}{2}} (x^2)^j (-1)^{\frac{p-1}{2}-j}\right)\left(\sum_{j=0}^{\frac{p-1}{2}} C^j_{\frac{p-1}{2}} 2^j (x^2)^j (-1)^{\frac{p-1}{2}-j}\right)$$

при x^{p-1}. Оскільки $p \equiv 3(\mod 4)$, то $(-1)^{\frac{p-1}{2}} = -1$ і $a_{p-1} = -\sum\limits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 2^j$. Тому

$$N_2 \equiv -a_{2p-2} - a_{p-1} \equiv -(\frac{2}{p}) + \sum_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 2^j (\mathrm{mod}p).$$

Нагадуємо, що

$$\left(\frac{2}{p}\right) \equiv \begin{cases} -1, & p \equiv 3(\mathrm{mod}\,8) \\ 1, & p \equiv 7(\mathrm{mod}\,8). \end{cases}$$

Отже, в обох випадках треба довести співвідношення $P(2) = \sum\limits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 2^j \equiv 0(\mathrm{mod}p)$, з якого слідувало б $N_2 \equiv -1(\mathrm{mod}p)$ при $p \equiv 7(\mathrm{mod}8)$ і $N_2 \equiv 1(\mathrm{mod}p)$ при $p \equiv 3(\mathrm{mod}8)$.

Залишилося довести, що

$$\sum_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 2^j \equiv 0(\mathrm{mod}\,p)$$

при $p \equiv 3(\mod 4)$. Взагалі, для випадку довільного $d \in F_p^*$, міркуючи аналогічно, отримали б, що при $p \equiv 3(\mathrm{mod}\,4)$ E_d є суперсингулярною, якщо і тільки якщо виконано співвідношення

$$\sum_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j \equiv 0(\mathrm{mod}\,p). \tag{6}$$

Розглянемо допоміжний поліном $P(t) = (\frac{p-1}{2}!)^2 \sum_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 t^j$. Використовуючи (5), можна показати

$$a_{p-1} = P(t) = (\frac{p-1}{2}!)^2 \sum\nolimits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 t^j = \sum\nolimits_{j=0}^{\frac{p-1}{2}} (k+1)^2(k+2)^2 \dots (\frac{p-1}{2}+k)^2 t^k$$

над F_p. Тут у суму (6), яка визначає a_{p-1}, замість d підставили t для дослідження узагальненої задачі.

Помітимо, що $P(t) = \partial^{\frac{p-1}{2}}(\partial^{\frac{p-1}{2}}(Q(t)t^{\frac{p-1}{2}})t^{\frac{p-1}{2}})$ над F_p, де $Q(t) = t^{p-1} + \dots + t + 1$, а $\partial^{\frac{p-1}{2}}$ позначають $\frac{p-1}{2}$-шу похідну по змінній, t — це нова змінна, а не координата кривої. Помітимо, що $Q(t) = \frac{t^p-1}{t-1} \equiv \frac{(t-1)^p}{t-1} = (t-1)^{p-1}(mod p)$, тому в F_p виконується $P(t) = (((t-1)^{p-1}t^{(\frac{p-1}{2})})t^{\frac{p-1}{2}})^{(\frac{p-1}{2})}$. Нехай $\theta = t-1$. Позначимо $R(\theta) = P(t)$. Для випадку $t+1 = 2$ отримаємо $\theta = 1$, бо $\theta = t-1$. Ця заміна зводить многочлен $P(t)$ від 2 до многочлена $R(t-1)$ від 1, тобто $P(t+1) = R(t)$, що зручно зокрема і для дифернціювання, можна вважати, що $R(t)$ — це многочлен $P(\theta-1)$ від нової змінної θ, $\theta = t-1$. Зауважимо, що в силу лінійності заміни, диференціювання за θ і за t збігаються. Диференціювання потрібне для перетворення многочлена $R(\theta)$ до такого вигляду, де явно видно потрібний коефіцієнт a_{p-1}. Тоді $R(\theta) = P(t) = ((\theta^{p-1}(\theta+1)^{\frac{p-1}{2}})^{(\frac{p-1}{2})}(\theta+1)^{\frac{p-1}{2}})^{(\frac{p-1}{2})}$. Для доведення співвідношення $a_{p-1} \equiv 0(mod p)$ достатньо показати, що $R(\theta) = 0$ при $\theta = 1$ над F_p. Помітимо, що $(\theta^{p-1}(\theta+1)^{\frac{p-1}{2}})^{(\frac{p-1}{2})} =$

$= (\theta^{p-1} + C^1_{\frac{p-1}{2}}\theta^p + C^2_{\frac{p-1}{2}}\theta^{p+1} + ... + C^{\frac{p-1}{2}}_{\frac{p-1}{2}}\theta^{p-1+\frac{p-1}{2}})^{(\frac{p-1}{2})} = (\theta^{p-2})^{(\frac{p-1}{2})} = (p-1)(p-2)...(\frac{p-1}{2}+1)\theta^{\frac{p-1}{2}}$. Всі доданки, окрім першого, стали рівними 0. Тому

$$R(\theta) = \frac{(p-1)!}{(\frac{p-1}{2})!}(\theta^{\frac{p-1}{2}}(\theta+1)^{\frac{p-1}{2}})^{(\frac{p-1}{2})} = \frac{(p-1)!}{(\frac{p-1}{2})!}\sum_{j=0}^{\frac{p-1}{2}}(j+1)...(j+\frac{p-1}{2})\theta^j C^j_{\frac{p-1}{2}}.$$

Потрібно показати, що $P(1+1) = R(1) \equiv 0(\mathrm{mod}\, p)$ а тому і $a_{p-1} \equiv 0(\mathrm{mod}\, p)$. Маємо

$$R(1) = \frac{(p-1)!}{(\frac{p-1}{2})!}\sum\nolimits_{j=0}^{\frac{p-1}{2}} C^j_{\frac{p-1}{2}}(j+1)...(j+\tfrac{p-1}{2}). \tag{7}$$

Помічаємо, що $(\frac{p-1}{2}-j+2)...(\frac{p-1}{2}-j+\frac{p-1}{2}) = (-1)^{\frac{p-1}{2}}(j+1)...(j+\frac{p-1}{2}) = -1(j+1)...(j+\frac{p-1}{2})$, Через те симетричні доданки в (7) скорочуються. Тут ми використовуємо те, що $(-1)^{\frac{p-1}{2}} = -1$, так як $p = Mk+3$ і $\frac{p-1}{2} = 2k+1$. Значить, $P(2) = R(1) = 0$, тобто $a_{p-1} \equiv 0(\mathrm{mod} p)$, що і потрібно було довести. Отже, $\sum_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 \equiv 0(\mathrm{mod} p)$, що завершує доведення основної частини теореми.

Аналогічний результат матиме місце для кривої $x^2+y^2 = 1+2^{-1}x^2y^2$. Дійсно, для доведення аналогічного твердження щодо кривої $x^2+y^2 = 1+2^{-1}x^2y^2$ потрібно показати, що $\sum\limits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 2^{-j} \equiv 0(\mathrm{mod}\, p)$. Для отримання останньої формули

враховуємо, що $(\frac{2}{p}) = (\frac{2^{-1}}{p})$ слідує з вже доведеного $\sum\limits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 2^j \equiv 0(\mathrm{mod}\, p)$ якщо домножити останнє на $2^{-\frac{p-1}{2}}$. Тобто $\sum_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 2^{-j} \equiv 0$ так як

$$2^{\frac{p-1}{2}} \sum\nolimits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 2^{-j} = \sum\nolimits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 2^{\frac{p-1}{2}-j} = \sum\nolimits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 2^j.$$

наприклад, для параметрів $p = 8k + 7 = 23$ і $d = 12 = 2^{-1}$ маємо $N_E(12) = 20 = p - 3$, а для $d = 2$ маємо $N_E(2) = 20 = p - 3$, отже, обидва рази 20 пар точок, що підтверджує нашу теорему.

Розглянемо розширення базового поля до $\mathbb{F}_{p^n}$, тоді отримуємо кількість точок вищевказаної кривої $x^2 + y^2 = 1 + dx^2y^2$ з врахуванням того, що кількість розв'язків рівняння $y^2 = P(x)$, де $P(x)$ – многочлен степеня $m > 2$ з коефіцієнтами з $\mathbb{F}_p$, над $\mathbb{F}_{p^n}$. Цей многочлен має вигляд $p^n + \omega_1^n + ... + \omega_{m-1}^n$, де $\omega_1, ..., \omega_{m-1} \in \mathbb{C}$ залежать лише від x (і не залежать від n) [20]. Оскільки суперсингулярність кривої $x^2 + y^2 = 1 + dx^2y^2$ рівносильна, тому що еліптична крива $v^2 = (d-1)u^3 + 2(d+1)u^2 + (d-1)u$ має рівно p звичайних (не нескінченно віддалених) точок, ми можемо застосувати даний результат для $m = 3$. Згідно з цим кількість розв'язків рівняння $v^2 = (d-1)u^3 + 2(d+1)u^2 + (d-1)u$ над $\mathbb{F}_{p^n}$ задається виразом $p^n + \omega_1^n + \omega_2^n$. Оскільки для $n = 1$ виходить рівно p розв'язків, то маємо $\omega_1 + \omega_2 = 0$, тому $p^n + \omega_1^n + \omega_2^n = p^n$, при $n \equiv 1(mod 2)$.

Нагадаємо, що еліптична крива у формі Монтгомері $E_M : v^2 = u^3 + 6u^2 + u$ є біраціонально еквівалентною до кривої $x^2 + y^2 = 1 + 2x^2y^2$ над F_{p^k}.

Покажемо, що для непарних степенів k розширень поля F_p до F_{p^k} порядок групи кривої Монтгомері E_M є наступним: $N_M = p^k$.

Позначимо кількість точок на кривій Монтгомері над $\mathbb{F}_{p^k}$ як $N_{M,k}$, а на кривій Едвардса як $N_{E,k}$. Порядок $N_{M,k}$ групи кривої Монтгомері $v^2 = u^3 + 6u^2 + u$ над F_{p^k}, яка є біраціонально еквівалентною до кривої $x^2+y^2 = 1+2x^2y^2$, обчислюється за допомогою теорем Степанова [20] і Деліня [15]: $N_M = p^k + \omega_1^k + \omega_2^k$, де $\omega_i^k \in \mathbb{C}$ і $\omega_1^k = -\omega_2^k$, $|\omega_i| = \sqrt{p}$, $i \in 1, 2$. Згідно з теоремою Деліня: $|\omega_i| = \sqrt{p}$. А для еліптичної кривої виконується $\omega_1 = \bar{\omega}_2$ [15], тому, враховуючи, що виведене вище $\omega_1 + \omega_2 = 0$, яке слідувало з $N_{M,1} = p$, маємо $\omega_1 = i\sqrt{p}$, $\omega_2 = -i\sqrt{p}$. Звідси для парних k маємо, що $N_{M,k} = p^k + 2(-p)^{\frac{k}{2}}$. Для непарних k маємо $\omega_1^k + \omega_2^k = 0$, тому $N_{M,k} = p^k$.

В силу того, що при $k \equiv 1(\mathrm{mod}\ 2)$ кількість афінних точок $N_{M,1} = p$ рівна p^k маємо, що кількість афінних точок у образі при відображенні з E_M на (3) рівна $N_{E,k} = p^k - 2$ для $p \equiv 3(\mathrm{mod}\, 4)$ і $k \equiv 1(\mathrm{mod}\, 2)$. Це так, бо відображення $y = (u-1)/(u+1)$ відображає 2 точки 4-го порядку, кривої Монтгомері, з координатою $u = -1$ на нескінченність, тобто не у точку з афінної площини. Звідси маємо $N_E = p^k - 3$ при $p \equiv 7(\mathrm{mod}\, 8)$, $N_E = p$ при $p \equiv 3(\mathrm{mod}\, 8)$ і $k \equiv 1(\mathrm{mod}\, 2)$.

Крива Едвардса в афінній формі над $\mathbb{F}_p, p \equiv 7(\mathrm{mod}\, 8)$ має тільки $N_E = p - 3$ точок замість очікуваних $p + 1$. Це так, оскільки наявні на проективній кривій Едвардса 2 особливі точки $p = (1, 0, 0)$ і $p' = (0, 1, 0)$ після її нормалізації шляхом біраціонального відображення $u = (1 + y)/(1 - y)$, $v = \sqrt{A}u/x$ [7, 10], мають по 2 образи. Властивостями, вказаними в означенні біраціонального ізоморфізму в [13], володіють і відображення $x = \frac{u}{v}$, $y = \frac{u-1}{u+1}$ з [7] та оберненим $(u, v) =$

$((y+1)/(y-1),\ x(y+1)/(y-1))$ зі спеціальними точками цього раціонального відображення, де $v=0$ або $u=-1$. В них відображення не визначено. Особливі точки скрученої кривої Едвардса при відображенні нормалізації переходять в саме ці спеціальні точки відображення бірaціональної еквівалентності $x=\frac{u}{v},\ y=\frac{u-1}{u+1}$ заданого в [7]. Точки, де $v=0$, це $((-A\pm\sqrt{(A+2)(A-2)})/2,\ 0)$, що мають порядок 2 на кривій Монтгомері, і точки, де $u=-1$ — це точки порядку 4 з координатами $(-1,\pm(A-2)/B)$ на кривій Монтгомері. При цьому ці особливі точки переходять в не особливі точки нормалізованої кривої E_M. Тому нормалізована крива Едвардса містить вже на 4 точки більше, а саме $(p-3)+4=p+1$ точок. Зауважимо, що за умови $(\frac{a}{p})=1$ крива E_d ізоморфна кривій (1), цей ізоморфізм задається відображенням $X=\frac{x}{\sqrt{a}}, Y=y$, тому в цьому випадку результати теореми поширюються на криву (1).

Наслідок 1. *Якщо коефіцієнт d кривої E_d задовольняє рівняння суперсингулярності $\sum\limits_{j=0}^{\frac{p-1}{2}}\left(C^j_{\frac{p-1}{2}}\right)^2 d^j\equiv 0(\mathrm{mod}\,p)$, наведене в доведені теоремі 1, то E_d має $p-1-2(\frac{d}{p})$ точок над F_p, а бірaціонально еквівалентна [12,13] їй крива E_M має $p+1$ точку над F_p.*

Доведення. З доведення теореми 1 слідує, що конгруенція (6) а саме

$$\sum_{j=0}^{\frac{p-1}{2}}\left(C^j_{\frac{p-1}{2}}\right)^2 d^j\equiv 0(\mathrm{mod}\,p)$$

є визначальною для виконання умови суперсингулярності. З вище сказаного слідує, що суперсингулярність кривої Едвардса рівносильна тому, що рівняння (1) або рівносильне йому $y^2\left(dx^2-1\right)=x^2-1$ має в $\mathbb{F}_p$ рівно $p-1-2\left(\frac{d}{p}\right)$ розв'язків. Це випливає з формули кількості точок (4), виведеної у теоремі 1, і умови $a_{p-1}\equiv 0(modp)$, що забезпечує виконання умови суперсингулярності (6), при цьому враховано наявність 2 особливих точок у проективної кривої $F(x;y;z)$, що знайдені у розділі 1. А це рівносильно тому, що узагальнене рівняння (3), яке має вигляд

$$y^2=(dx^2-1)(x^2-1), \tag{8}$$

має рівно $p-\left(\frac{d}{p}\right)$ розв'язків. Справді, кожний розв'язок рівняння (1) відповідає розв'язку рівняння (8), але (8) має ще розв'язки, при яких $dx^2-1\equiv 0$. Їх стільки, скільки є квадратних коренів з d в $\mathbb{F}_p$, тобто їх $1+\left(\frac{d}{p}\right)$. Отже суперсингулярність кривої Едвардса рівносильна тому, що рівняння (8) має $p-1-2\left(\frac{d}{p}\right)+1+\left(\frac{d}{p}\right)=p-\left(\frac{d}{p}\right)$ розв'язків.

Як показано вище, кількість розв'язків (2) конгруентна $-(a_{2p-2}-a_{p-1})modp$, де коефіцієнти многочлена $\left(dx^2-1\right)^{\frac{p-1}{2}}\left(x^2-1\right)^{\frac{p-1}{2}}=a_{2p-2}x^{2p-2}+...+a_0$. Тому якщо $-a_{2p}-a_{p-1}\equiv p-\left(\frac{d}{p}\right)\mathrm{mod}\,p$ тобто $a_{p-1}\equiv 0(modp)$, то крива Едвардса є суперсингулярною. Випадки $N_{E_d}=-\left(\frac{d}{p}\right)$ і $N_{E_d}=2p-\left(\frac{d}{p}\right)$ є неможливими, в

силу нерівності $2 \leqslant N_{E_d} \leqslant 2p-2$. Дійсно, вона має хоч 2 розв'язки $y=0$, $x=\pm 1$, а більше ніж $2p-2$ розв'язків вона мати не може, бо для $x=\pm 1$ є існує один можливий $y=0$, а для інших значень x не більше ніж 2 можливих y.

Отже, результат теореми 1 можна розповсюдити на всі $d \in F_p^*$, що його задовольняють (6). Суперсингулярній кривій E_d відповідає суперсингулярна крива E_M, що має $p+1$ точок, серед яких 1 нескінченно віддалена.

2.2. Суперсингулярність еліптичних кривих

Наслідок 2. *Якщо виконується умова* $\sum\limits_{j=0}^{\frac{p-1}{2}} \left(C_{\frac{p-1}{2}}^{j}\right)^2 d^j \equiv 0(\bmod p)$, *то крива Монтгомері* $u^2 = (d-1)\,v^3 + 2(d+1)v^2 + (d-1)\,v$ *для непарних* k *має рівно* p^k *афінних точок над* $\mathbb{F}_{p^k}$.

Доведення. Як доведено в теоремі 3.4 [2], кожна крива Монтгомері над скінченим полем k, $char(k) \equiv 3(\bmod 4)$ є біраціонально еквівалентною кривій Едвардса. З формули біраціонального відображення над k, $char(k) \neq 2$ кривої $E_{a,d}$ в E_M були отримані коефіцієнти кривої E_M: $A = 2\frac{(a+d)}{(a-d)}$ і $B = \frac{4}{a-d}$ [2]. Отже, образом знайденої нами суперсингулярної кривої E_d, де коефіцієнт d задовольняє вказану в умові конгруенцію, є крива E_M: $\frac{4}{a-d}u^2 = v^3 + 2\frac{a+d}{a-d}v^2 + v$. Враховуючи, що $a=1$, отримуємо еліптичну криву у формі Монтгомері $\frac{4}{1-d}u^2 = v^3 + 2\frac{1+d}{1-d}v^2 + v$, з відповідними коефіцієнтами $B = \frac{4}{1-d}$, $A = 2\frac{1+d}{1-d}$. Оскільки $d \neq 1$, маємо рівняння еквівалентної еліптичної кривої $4u^2 = (1-d)v^3 + 2(1+d)v^2 + (1-d)v$.

З умови наслідку 1 і теореми 1 легко отримується, що властивістю суперсингулярності володіють і криві E_d з коефіцієнтами $d = 17 + 12\sqrt{2}$ і $d = 17 - 12\sqrt{2}$ при $p \equiv 7(\bmod 8)$. Випадок $p \equiv 3(\bmod 8)$ неможливий в силу неіснування $\sqrt{2}$.

Наслідок 3. *Якщо коефіцієнт кривої Едвардса* $d=2$ *і* $p^k \equiv 3(mod 4)$, *то в полі* F_{p^k} *кількість розв'язків* $y^2 = u^3 + 6u^2 + u$ *рівна* p^k. *Відповідно крива (1) має* $p^k + 1$ *при* $p^k \equiv 3(\bmod 4)$ *і* $p^k - 3$ *при* $p^k \equiv 7(\bmod 8)$.

Доведення цього наслідку слідує безпосередньо з наслідків 1 і 2 та дослідженої в теоремі 1 кількості розв'язків рівняння $y^2 = (x^2-1)(2x^2-1)$, яка рівна p^k+1 при $p^k \equiv 3(\mod 8)$ і $p^k - 1$ при $p^k \equiv 7(\bmod 8)$. Тобто має рівно $p^k - \left(\frac{d}{p}\right)$ розв'язків над F_{p^k}, що випливає з наслідку 1, бо $-a_{2p} - a_{p-1} \equiv p^k - \left(\frac{d}{p}\right)(\bmod p^k)$, де $a_{p-1} \equiv 0(\bmod p^k)$.

Сформулюємо спосіб знаходження суперсингулярної еліптичної кривої у формі Веєрштрасса.

Зауваження 2. *Суперсингулярній еліптичній кривій у канонічній формі Веєрштрасса* $y^2 = x^3 + ax + b$ *ізоморфна суперсингулярна еліптична крива Монтгомері* E_M.

Для зведення кривої E_M до канонічної форми Веєрштрасса поділимо рівняння кривої $4u^2 = (1-d)v^3 + 2(1+d)v^2 + (1-d)v$ на 4 і до отриманної кривої $u^2 = 4^{-1}((1-d)v^3 + 2(1+d)v^2 + (1-d)v) = av^3 + bv^2 + ax$ застосуємо заміну $t = v - \frac{b}{3a}$, де $a = (d-1)4^{-1}$, $b = 2^{-1}(1+d)$. Ця крива буде суперсингулярною еліптичною кривою у формі Веєрштрасса.

Зауваження 3. *Скручена крива Едварса допускає кофактор 4.*

Доведення. Менше ніж 4 кофактор бути не може, бо точки 4-го порядку існують на кожній кривій Едвардса. Доведення їх існування дає прикдад такої кривої. Так якщо $p = 2192 - 264 - 1$, то скручена крива Едвардса $E_{102,47} : 102x^2 + y^2 = 1 + 47x^2y^2$ має кофактор 4 [7].

Наслідок 4. *Умова неіснування точки 8-го порядку є необхідною умовою мінімальності кофактора [14] кривої Едвардса.*

Доведення. Справді, відомо, що порядок групи точок кривих E_d з мінімальним кофактором рівний $4p$ [7], тобто не ділиться на 8. Тому необхідна і достатня умова подільності на 8, яка досліджена у властивості 4, виключає максимальність порядку в разі її виконання і забезпечує мінімальність кофактора кривої в разі її невиконання, інакше в силу циклічності групи точок даної кривої в ній би існувала мультиплікативна підгрупа C_8, яка породжувалась би елементом 8-го порядку, необхідна і достатня умова існування якого досліджена автором в [28], внаслідок чого порядок кривої був би $8p$.

Наступна властивість дає спосіб побудови кривої з заданою циклічною підгрупою простого порядка q і мінімальним кофактором — 4.

Зауваження 4. *Якщо $p = 8k + 7$, де p, $q \in P$ і $p - 3 = 4q$, а коефіцієнт d задовольняє умову суперсингулярності (6) кривої $E_{1,d}$ над F_p, то $E_{1,d}$ має мінімальний кофактор 4 і містить просту циклічну підгрупу порядка q. Якщо $p = 8k + 3$, де p, $q \in P$ і $p + 1 = 4q$, а коефіцієнт d задовольняє умову суперсингулярності (6) кривої $E_{1,d}$ над F_p, то $E_{1,d}$ має мінімальний кофактор 4 і містить циклічну підгрупу простого порядка q.*

Доведення. Доведення слідує з теореми 1 про порядок суперсингулярної кривої над відповідним F_p і того факту, що точка порядку 4 [7] завжди існує на $E_{1,d}$. Окрім того простота підгрупи C_q слідує з того, що циклічна група порядку q не містить не тривіальних підгруп.

Висновки. Отже, знайдено необхідні і достатні умови суперсингулярності кривих $E_{a,d}$ і еліптичних кривих для полів F_{p^n} характеристики $p = 4k+3$. Запропоновано теоретичне підґрунтя для нового методу перевірки еліптичних кривих у формі Монтгомері і у нормальній формі Веєрштрасса на суперсингулярність, що ґрунтується на біраціональному ізоморфізмі еліптичної кривої і дослідженної нами кривої (1). Зроблено аналіз особливостей і роду скрученої кривої Едвардса.

1. **Edwards H.** A normal form for elliptic curves // American Mathematical Society. – 2007. – Vol. 44, No. 3, July – pp. 393–422.

2. **Bernstein D. J., Birkner P., Joye M., Lange T., Peters Ch.** Twisted Edwards Curves // IST Programme ECRYPT, and in part by grant ITR-0716498, 2008. – pp. 1–17.

3. **Дрозд Ю. А.** Вступ до алгебраїчної геометрії. – Л.: Внтл-Класика. 2004. – 251 с.

4. **Шафаревич Ю. А.** Основы алгебраической геометрии. – М.: Наука, 1969. – Т. 1. – 184 с.

5. **Bernstein D. J., Lange T.** Faster addition and doubling on elliptic curves // IST Programme Contract 2002-507932 ECRYPT. – 2007. – pp. 1–20.

6. **Hisil H., Koon-Ho Wong Kenneth, Carter G.** Twisted Edwards Curves Revisited // ASIACRYPT LNCS 5350. – 2008. – pp. 326–343.

7. **Fulton W.** Algebraic curves. An Introduction to Algebraic Geometry. – Third Preface – January, 2008. – 121 P.

8. **Рид М.** Алгебраическая геометрия для всех. Москва: Мир, 1991, 143 с.

9. **Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.** Элементарное введение в эллиптическую криптографию. – М.: КомКника, 2006. – Т. 2. – 328 с.

10. **Koblitz N.** Eliptic Curve Cryptosystems // Mathematics of Computation. – 1987. – Vol. 48, № 177. – P. 203–209.

11. **Menezes A. J., Okamoto T., Vanstone S. A.** Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field // IEEE Transactions On Information Theory. – 1993. – Vol. 39, No. 5, September. – pp. 1603–1646.

12. **Алексеев Е. К., Ошкин И. Б., Попов В. О., Смышляев С. В., Сонина Л. А.** О перспективах использования скрученных эллиптических кривых Эдвардса со стандартом ГОСТ Р 34.10-2012 и алгоритмом ключевого обмена на его основе: Материалы XVI международной конференции «РусКрипто 2014».

13. **Бессалов А. В., Цыганкова О. В.** Взаимосвязь семейства точек больших порядков кривой Эдвардса над простым полем // Захист інформації. – 2015. – Т. 17, № 1. – С. 73–80.

14. **Виноградов И. М.** Основы теории чисел: учебное пособие, 12-е изд. – СПб.: «Лань», 2009. – 271 с.

15. **Степанов С.** Арифметика алгебраических кривых. – М.: Наука, 1991. – 368 с.

16. **Gupta R., Murty M. R.** Primitive points on elliptic curves // Compos. Math. – 1986. – 58. – P. 13-–44.

17. **Montgomery P. L.**, Speeding the Pollard and Elliptic Curve Methods of Factorizations, Math. Comp. 48, (1987), PP. 243–264.

18. **Скуратовський Р.** Дослідження властивостей скрученої кривої Едвардса: Конференція державної служби спеціального звязку та захисту інформації. http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?showHidden=1arti &id=252312&cat&id=240232&ctime=1464080781894.

19. **Skuratovskii R. V.** Twisted Edwards curve and its group of points over finite field F_p // XI Літня школа «Алгебра, Топологія, Аналіз» Одеса, 2016. – pp. 122–124.

20. **Скуратовский Р. В., Осадчий Е. О., Квашук Д. М.** Деление точки скрученной кривой Эдвардса на два и ее применение в криптографии // Вісник національного технічного університету «ХПІ». – №44. – С. 90-96.

21. **Skuratovskii R. V., Skruncovich U. V.** Twisted Edwards curve and its group of points over finite field F_p // Conference «Graphs and Groups, Spectra and Symmetries», Novosibirsk, Russia. http://math.nsc.ru/conference/g2/g2s2/exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf.

22. **Скуратовський Р., Мовчан П.** Нормалізація скрученої кривої Едвардса та дослідження її властивостей над F_p // Збірник праць 14-ї Всеукраїнської науково-практичної конференції. ФТІ НТУУ «КПІ» 2016. – Т. 2. – С. 102–104.

23. **Skuratovskii R. V.** Constructing of finite field normal basis in deterministic polynomial time // Bulletin of Taras Shevchenko Kiev National University. – 2011. – P. 49–54.

24. **Paulo S., Barreto L. M., Naehrig M.** Pairing-Friendly Elliptic Curves of Prime Order // International Workshop on Selected Areas in Cryptography SAC, 2005. – pp. 319–331.

Скуратовский Р. В.
Суперсингулярность эллиптических кривых и кривых Эдвардса над F_{p^n}

Резюме

Мы рассматриваем алгебраические кривые в форме Эдвардса и эллиптические кривые Монтгомери над конечным полем F_{p^n}, которые в настоящее время являются одним из самых быстрых и перспективиих носителей групп, на настоящее время имеют много применений. В работе найдены условия суперсингулярности кривых Эдвардса и большого класса скрученных кривых Эдвардса над полем F_{p^n} характеристики p $equiv 3$ mod 4. Показано, что проективная кривая Эдвардса не является эллиптической. Исследованы некоторые интересные свойства группы точек этих кривых. Построение кривой заданного порядка с минимальным кофактором. Подсчитан род скрученной кривой Эдвардса. Сделан анализ ее классов суперсингулярних кривых. Найдены условия минимальности кофактора скрученной кривой Эдвардса и его род.
Ключевые слова: суперсингулярные кривые, конечное поле, эллиптическая криптография, кривая Эдвардса, эллиптические кривые с малой степенью погружения в поле .

Skuratovskii R. V.
Supersingularity of elliptic and Edwards curves over F_{p^n}

Summary

We consider the algebraic curves which have form of Edwards and elliptic curves with coordinates in F_{p^n}. These curves are most effective support for a cyclic group of points which have many applications now. In this paper it was found conditions of supersingularity for Edwards curve and same case of twisted Edwards and Montgomery curves over F_{p^n} where $p \equiv 3 mod 4$. There was proved that projective twisted Edwards curve is not elliptic. Some properties of this curve were investigated. Conditions of minimal cofactor of twisted Edwards curve were founded. Construction of a curve with given order and minimal cofactor was made.
Key words: supersingularity, finite field, elliptic cryptography, Edwards curve, pairing-friendly elliptic curves.

References

1. Samko, S. G., Kilbas, A. A. & Marichev, O. I. (1987). *Integraly i proizvodnye drobnoho poryadka i nekotorye ih prilozheniya [Fractional integrals and derivatives with some applications].* Minsk: Nauka i tekhnika, 688 p.

2. Arestov, V. V. (1981). Ob integralnykh neravenstvakh dlya trigonometricheskikh polinomov i ikh proizvodnykh [About integral inequalities for trigonometrical polynomials and theirs derivatives]. *Izv. AN USSR. Ser. matem.*, Vol. 45, P. 3–22.

3. Fikhtengolz, G. M. (2001). *Kurs differentsialnogo i integralnogo ischisleniya [A Course of Differential and Integral Calculus], Vol. II.* Moscow: Fizmatlit, 810 p.

4. Gradshtein, I. S. & Ryzhyk, I. M. (1963). *Tablitsy sntegralov, sum i proizvedeniy [Tables of integrals, sums and derivatives].* Moscow: GITTL, 1100 p.

5. Storozhenko, E. A. (1996). K odnoi zadache Malera o nulyakh polinoma i ego proizvodnoy [For one Mahler's prooblem about zeros of polinomial and its derivative]. *Matem. sbornik*, Vol. 187, №5, P. 111–120.

6. Edwards, H. (2007). *A normal form for elliptic curves. American Mathematical Society, Vol. 44, No. 3, July – pp. 393-422.*

7. *Bernstein, D. J., Birkner, P., Joye, M., Lange, T. & Peters, Ch. Twisted Edwards Curves. IST Programme ECRYPT, and in part by grant ITR-0716498, 2008. PP. 1-17.*

8. *Drozd, Yu. A. Vstup do alhebrayichnoyi heometriyi – L.: Vntl-Klasyka. 2004. – 251 p.*

9. *Shafarevych, Yu. A. Osnovy alhebraycheskoy heometryy – M.: Nauka, T.1, 1969. – 184 p.*

10. *Bernstein, D. J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme Contract 2002-507932 ECRYPT, – 2007. – pp. 1-20.*

11. *Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary. Twisted Edwards Curves Revisited. ASIACRYPT LNCS 5350 – 2008. – pp. 326-343.*

12. *W. Fulton Algebraic curves. An Introduction to Algebraic Geometry – Third Preface – January, 2008. – 121 P.*

13. *Rid M. Algebraicheskaya geometriya dlya vsekh. Moskva: Mir, 1991, 143 p.*

14. *Bolotov, A. A., Gashkov, S. B., Frolov, A. B. & Chasovskikh, A. A. Elementarnoye vvedeniye v ellipticheskuyu kriptografiyu – M.: KomKnika. Tom 2., 2006. – 328 s.*

15. *Koblitz, N. [Eliptic Curve Cryptosystems] // Mathematics of Computation. - 1987. - V. 48, № 177. - P. 203-209.*

16. *Menezes, A. J., Okamoto, T. & Vanstone, S. A. [Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field]. IEEE Transactions On Information Theory. – 1993. – Vol. 39, No. 5, September. pp. 1603-1646.*

17. *Alekseyev, Ye. K., Oshkin, I. B., Popov, V. O., Smyshlyayev, S. V. & Sonina, L. A. O perspektivakh ispol'zovaniya skruchennykh ellipticheskikh krivykh Edvardsa so standartom GOST R 34.10-2012 i algoritmom klyuchevogo obmena na yego osnove Conference RusCrypto 2014. pp. 75-79.*

18. *Bessalov, A. V. & Tsygankova, O. B. Vzaimosvyaz' semeystva tochek bol'shikh poryadkov krivoy Edvardsa nad prostym polem. Zakhist informatsii. 2015. – T. 17, № 1. – pp. 73-80.*

19. *Vinogradov, I. M. Osnovy teorii chisel: Uchebnoye posobiye. 12-ye izd. - SPb.: Izdatel'stvo "Lan' 2009. 271 p.*

20. *Stepanov, S. Arifmetika algebraicheskikh krivykh. M.: Nauka., 1991g., 368 p.*

21. *Gupta, R., & Murty, M. R. Primitive points on elliptic curves. Compos. Math.58, (1986) P. 13–44.*

22. *Montgomery, P. L., Speeding the Pollard and Elliptic Curve Methods of Factorizations, Math. Comp. 48, (1987), pp. 243–264.*

23. *Skuratovskii, R. Doslidzhennya vlastyvostey skruchenoyi kryvoyi Edvardsa. Konferentsiya derzhavnoyi sluzhby spetsial?noho zvyazku ta zakhystu informatsiyi. http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?showHidden=1art id=252312 cat id=240232 ctime=1464080781894*

24. *Skuratovskii, R. V. Twisted Edwards curve and its group of points over finite field F_p. XI Letnia shkola "Algebra, Topoloia, Analys "Odessa. (2016), PP. 122-124.*

25. *Skuratovskyy, R. V., Osadchyy,E. O. & Kvashuk, D. M. Delenye tochky skruchennoy kryvoy Edvardsa na dva y ee prymenenye v kryptohrafyy. Visnyk natsional?noho tekhnichnoho universytetu «KHPI», №44, st. 90-96.*

26. *Skuratovskyy, R. V., Osadchyy,E. O. & Kvashuk, D. M. Delenye tochky skruchennoy kryvoy ?dvardsa na dva y ee prymenenye v kryptohrafyy. Visnyk natsionalnoho tekhnichnoho universytetu «KHPI», №44, st. 90-96.*

27. *Skuratovskii, R. V. & Skruncovich, U. V. Twisted Edwards curve and its group of points over finite field F_p. Akademgorodok, Novosibirsk, Russia. Conference. Graphs and Groups, Spectra and Symmetries. http://math.nsc.ru/conference/g2/g2s2/exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf*

28. *Skuratovskii, R. V. & Movchan P. Normalizacia skruchennoi krivoi Edwardsa i doslidgennia yy vlastuvostei nad F_p. Zbirnuk prac 14 naukovo praktichoy conferencii FTI NRUU "KPI"2016, Tom 2, p. 102-104.*

29. *Skuratovskii, R. V. Constructing of finite field normal basis in deterministic polynomial time(in ukraine). Bulletin of Kiev national university of Tarasa Shevchenka. 2011, P. 49-54.*

30. *Paul, S., Barreto, L. M. & Naehrig M. Pairing-Friendly Elliptic Curves of Prime Order. International Workshop on Selected Areas in Cryptography SAC, 2005, pp. 319–331.*