УДК 619.12
DOI https://doi.org/10.32689/maup.it.2021.1.7

Руслан СКУРАТОВСЬКИЙ
викладач кафедри обчислювальної математики і компютерного моделювання, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Фрометівська, 2, м. Київ, Україна, індекс 03039

ORCID: https://orcid.org/0000-0002-5692-6123

Ruslan SKURATOVSKYI
Lecturer at the Department of Computational Mathematics and Computer Modeling, Interregional Academy of personnel management, 2 Frometivska Street, Kyiv, Ukraine, postal code 03039

Бібліографічний опис статті: Скуратовський Р. Підхід до перевірки суперсингулярності еліптичних кривих і обчислення їх порядку. *Інформаційні технології та суспільство*. 2021. Вип. 1. С. 59–69. DOI: https://doi.org/10.32689/maup.it.2021.1.7

Bibliographic description of the article: Skuratovskyi, R. (2021). Pidkhid do perevirky supersynhuliarnosti eliptychnykh kryvykh i obchyslennia yikh poriadku [Approach to checking the supersingularity of elliptic curves and calculating their order]. *Informatsiini tekhnolohii ta suspilstvo – Informati on technology and society*, 1, 59–69. DOI: https://doi.org/10.32689/maup.it.2021.1.7

ПІДХІД ДО ПЕРЕВІРКИ СУПЕРСИНГУЛЯРНОСТІ ЕЛІПТИЧНИХ КРИВИХ І ОБЧИСЛЕННЯ ЇХ ПОРЯДКУ

Анотація. *Більшість криптосистем сучасної криптографії природним чином можна «перекласти» на еліптичні криві. Ми розглядаємо алгебраїчні криві Едвардса над скінчнним полем, які на даний час є одним з найбільш перспективних носіїв множин точок, що використовують для швидких групових операцій [1; 2; 14], які наявні в асиметричних криптосистемах, зокрема для побудови випадкових криптостійких послідовностей.*

Показано, що проективна крива $E_{a,d}$ не є еліптичною. Метою роботи є пошук критерію і достатніх умов суперсингулярності кривої Едвардса і еліптичної кривої у формі Монтгомері над простим полем $\mathbb{F}_p$, а потім узагальнення цього критерія для скінченного алгебраїчного розширення цього поля до F_{p^n}. Отриманий результат дозволяє побудувати всі суперсингулярні криві Едварса і Монтгомері не розкладаючи на множники многочлен від x який наявний у записі кривої.

В роботі [10] було представлене доведення суперсингулярності кривої E_d лише для коефіцієнтів $d=2,\ d=2^{-1}$ над $\mathbb{F}_p$, нашою ж метою є дослідження всіх коефіцієнтів при яких ця крива є суперсингулярною. В нашій роботі знайдено критерії і достатні умови суперсингулярності кривої Едвардса і еліптичної кривої у формі Монтгомері над полем F_{p^n}, тобто досліджено при яких коефіцієнтах отримується пара кривих зі слідом Фробеніуса рівним 0. При цьому криві Монтгомері над полем характристики 2 мають нульовий j-інваріант. Знайдено не тільки конкретну множину коефіцієнтів з відповідними характеристиками полів при яких ці криві є суперсингулярними а й загальну формулу за якою можна визначити чи є крива суперсингуярною над даним полем чи ні. В роботі узагальнено результат про суперсингулярність кривої над $\mathbb{F}_p$ отриманий в [10] для коефіцієнтів $d=2,\ d=2^{-1}$ на випадок довільного розширення простого поля $\mathbb{F}_{p^n}$ та уточнено формулювання теореми 3 з [10]. Зроблено аналогічне дослідження і для еліптичних кривих у формі Монтгомері.

Ключові слова: *скінченне поле, еліптична крива, крива Едвардса, порядок кривої, квадратичний лишок, символ Лежандра, алгебраїчна крива, група точок еліптичної кривої, порядок точки, криві кручення.*

APPROACH TO CHECKING THE SUPERSINGULARITY OF ELLIPTIC CURVES AND CALCULATING THEIR ORDER

Abstract. *Most cryptosystems in modern cryptography can naturally be "translated" into elliptical curves. We consider algebraic Edwards curves over a finite field, which are currently one of the most promising carriers of sets of points used for fast group operations [1; 2; 14], which are available in asymmetric cryptosystems, in particular for the construction of random cryptocurrency sequences.*

It is shown that the projective curve $E_{a,d}$ is not elliptical. The aim of this work is to find a criterion and sufficient conditions for the supersingularity of the Edwards curve $\mathbb{F}_p$ and an elliptic curve in the form of Montgomery over a simple field and then generalize this criterion for a finite algebraic extension of this field to F_{p^n}. The obtained result allows us to construct all supersingular curves of Edwards and Montgomery without factorizing the polynomial from which the curve is present in the record.

In [10], the proof of the supersingularity of a curve E_d was presented only for the coefficients $d=2,\ d=2^{-1}$ over $\mathbb{F}_p$, and our goal is to study all the coefficients at which this curve is supersingular. In our work we found the criteria and sufficient conditions for the supersingularity of the Edwards curve and the elliptic curve in the form of Montgomery over the field F_{p^n},

ie we investigated at what coefficients a pair of curves with a Frobenius trace equal to 0. The Montgomery curves over the field of characteristic 2 have zero j-invariant. Not only a specific set of coefficients with the corresponding characteristics of the fields at which these curves are supersingular is found, but also a general formula by which it is possible to determine whether the curve is supersingular over a given field or not. The paper summarizes the result on the supersingularity of the curve over $\mathbb{F}_p$ *obtained in [10] for the coefficients* $d=2,\ d=2^{-1}$ *in the case of arbitrary expansion of a simple field* $\mathbb{F}_{p^n}$ *and clarifies the formulation of Theorem 3 from [10]. A similar study was performed for elliptic curves in the form of Montgomery.*

Key words: *finite field, elliptic curve, Edwards curve, curve order, quadratic excess, Legendre symbol, algebraic curve, group of elliptic curve points, point order, torsion curves.*

Вступ. Вперше криві Едвардса E_d представлено Едвардсом в роботі [1] і розвинуті в роботі Бернштейна і Ланге [2]. 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 ендоморфізмів, так і з точки зору алгебраїчної геометрії. Їх дослідження є одною з цілей даної роботи.

Одною з головних задач даного дослідження є узагальнення результата про суперсингулярність кривої отриманого в [10] 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 $p\equiv 7(\mathrm{mod}8)$, яка була в теоремі 3 з [10]. 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. Суперсингулярність кривих Едвардса досліджувалася в [10] лише для простих полів $\mathbb{F}_p$, тому *наша мета дослідити її* над скінченим алгебраїчним розширенням тобто над полем – $\mathbb{F}_{p^n}$.

Актуаліність даного питання полягає в тому, що в еліптичній криптографії дуже важливо знати ті криві, які є суперсингулярними (ті, що мають нульовий *j*-інварівант при $p=2$), бо вони є крипографічно слабкими. Корисною є відсутність ділення точки на 2 при виконанні подвоєння точки на суперсингулярних кривих. Водночас одними з найбільш придатних для швидких обчислень є криві Едвардса [14], що потребують найменших обчислювальних затрат для проведення групової операції додавання точок а також подвоєння точок.

Суперсингулярність кривих Едвардса раніше досліджувалася лише в [10] і лише для простих полів $\mathbb{F}_p$ і автори обмежилися доведенням суперсингулярності лише для кривої з коефіцієнтами $d=2,\ d=2^{-1}$, *тому* ***задача дослідження*** *її над скінченим алгебраїчним розширенням тобто над полем –* $\mathbb{F}_{p^n}$ ***є новою***.

Авторами статті [10] було знайдено суперсингулярність кривої E_d лише для коефіцієнтів $d=2,\ d=2^{-1}$ і $d=(\sqrt{3}\pm 2)/(\sqrt{3}-(\pm 2))$ над $\mathbb{F}_p$ при відповідних p, **метою** нашої статті є пошук множини всіх коефіцієнтів при яких ця крива є суперсингулярною.

Метою роботи є пошук критерію і достатніх умов суперсингулярності кривої Едвардса і еліптичної кривої у формі Монтгомері над полем F_{p^n}, тобто досліджено при яких коефіцієнтах над полями відповідної характристики ці криві мають нульовий *j*-інварівант.

Властивості скрученої кривої Едвардса.

З точки зору алгебраїчної геометрії, крива Едвардса не є еліптичною, бо є сингулярною.

Криві Едвардса також як і скручені криві Едвардса мають афінне представленя ізоморфне деякій афінній частині еліптичної кривої, що містить в порядку групи кривої множник 4, що доведено автором в [8] у твердженні про необхідні і достатні умови існування точок 8-го порядку.

Згідно теореми Хассе порядок групи алгебраїчної кривої $N_E=p+1\pm t$. Якщо слід Фробеніуса $t=0$, то маємо вироджену пару кривих (крива *E* і крива зі скрутом), тому порядки обох кривих співпадають і рівні $N_E=p+1$. Такі криві є суперсингулярними кривими. Таким чином, порядок групи точок для суперсингулярних кривих над простим полем рівний $N_E=p+1$, тому період генератора криптостійкої послідовності [7] є мінімальним серед еліптичних кривих над заданим полем.

Дані криві задовольняють самим сильним вимогам по стійкості до MOV-атаки, про що неодноразово зазначалось у працях вітчизняних [7; 9; 11; 12; 20] та закордонних вчених [3; 4; 21]: неможливість застосувати цей метод забезпечується через відсутність можливості вкласти групу точок кривої в мультипликативну групу поля достатньо малого порядку. Для цього достатньо, щоб мінімальне натуральне t, $p^t\equiv 1 mod|N_E|$ було достатньо великим. Для скручених кривих Едвардса $t=|N_E|-1$, що є максимально можливим. Великою перевагою є можливість побудови скрученої кривої Едвардса порядку $4p$, $p\in\mathbf{P}$, тому не може бути використана атака підміни точки, що належить рекомендованій кривій на точку

зі скрученої кривої тобто так званої кривої кручення. Також це не дає противнику використовувати китайську теорему про лишки для визначення секретного ключа [4], бо маємо великий множник p в $|N_E|$. З точки зору алгебраїчної геометрії, крива не є еліптичною, бо є сингулярною.

Також важливість визначення не суперсингулярності еліптичної кривої для побудови генераторів випадкових чисел є показано в роботі [5] для побудови "elliptic curve power generator" генератора "Naor–Reingold" використовують не суперсингулярну еліптичну криву і її точку P великого простого порядку, якщо ж порядок l точки P не простий, то вибирають початкове заповнення e таке, що $(e,l)=1$. У випадку побудови такого генератора ще важливо і те, що для суперсингулярних кривих відсутня операція ділення при подвоєнні точки.

Особливі точки скрученої кривої Едвардса.

Розглянемо скручену криву Едвадрса $E_{a,\mathrm{d}}$

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

При $a=d$ крива перетворюється до вигляду $ax^2+y^2=1+ax^2y^2$ звідки $ax^2-ax^2y^2-1+y^2=0$ або $ax^2(1-y^2)-(1-y^2)=0$. Отже, крива розкладається у добуток двох пар прямих $(ax^2-1)(y^2-1)=0$. Якщо $a=1$, то $E_{a,\mathrm{d}}$ перетворюється у криву E_{d}. З умови гладкості знаходимо особливі точки афінної кривої.

Для цього зробимо проективізацію кривої. 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 співпадають.

Пошукаємо інші корені в припущенні $z=0$ коренем є також точка $(0,y_0,0)=(0,1,0)$. Тобто маємо 2 особливі точки $p_1=(1,0,0)$ і $p_2=(0,1,0)$. Це прості особливості.

Особливими точками є (нескінченно віддаленні точки) $(1,0,0)$ і $(0,1,0)$, тому маємо особливості на нескінченності у відповідних афінних компонентах

$$A^1: az^2+y^2z^2=z^4+dy^2 \text{ і } A^2:\ ax^2z^2+z^2=z^4+dx^2.$$

Опишемо будову локального кільця в точці p_1, його елементами є дроби з функцій виду $F(x,y,z)=\frac{f(x,y,z)}{g(x,y,z)}$, знаменники яких не обертаються в 0 у точці p_1. Локальне кільце, що має особливості в 2-ух точках має функції у яких знаменники не діляться на $(x-1)(y-1)$.

Знайдемо $\delta_{\mathrm{p}}=\dim\overline{\mathcal{O}_{\mathrm{p}}}/\mathcal{O}_p$, де $\mathcal{O}_{\mathrm{p}}$ – локальне кільця в особливій точці p, це кільце породжується відношеннями регулярних функцій $\mathcal{O}_{\mathrm{p}}=\left\{\frac{f}{g}:(g,(x-1)(y-1))=1\right\}$, $\overline{\mathcal{O}}_{\mathrm{p}}$ – ціле замикання локального кільця в особливій точці p. Позначимо $\delta_p=\dim\overline{\mathcal{O}_p}/\mathcal{O}_p=1$ розмірність фактора як векторного простору. Оскільки, базис розширення $\overline{\mathcal{O}}_p$ над $\mathcal{O}_p$ складається з одного елемента в кожній з двох особливих точок, то $\delta_p=1$.

Отже, підрахуємо род кривої за Рідом [13] $\rho^*(C)=\rho_\alpha(\mathrm{C})-\sum_{p\in E}\delta_p=\ =\frac{(n-1)(n-2)}{2}-\sum_{p\in E}\delta_p=3-2=1$ бо $n=4$. де $\rho_\alpha(C)$ – арифметичний рід 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 Едвардса ізоморфна деякій афінній частині еліптичної кривої. Нормалізація кривої Едвардса – крива в формі Веєрштраса, що запропонована Монтгомері E_M [2].

Суперсингулярні криві Едвардса і еліптичні криві в формі Монтгомері.

Для виявлення суперсингулярних кривих, згідно дослідженням Кобліца [16], можна скористатися пошуком таких параметрів при яких крива і відповідна їй крива зі скрутом мають однакові кількості розв'язків.

Як показано в [2] 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 $(\overline{x},\overline{y})\mapsto(x,y)=\left(\overline{x},\frac{1}{\overline{y}}\right)$ [2]. Тому скористаємося цим відображенням для пошуку суперсингулярних кривих. Ми виявили суттєву неточність в роботі [10], в умові суперсингулярності для кривої Едвардса $E_{1,d}$. Більш точно, якщо $p\equiv -3(mod 8)$, то не маємо виродженої (суперсингулярної) пари кривих, не дивлячись на те, що це стверджують-

ся в теоремі 3 з [10]. Крім того якщо $p \equiv 7(mod 8)$, то порядки пари скручених кривих є наступними $N_{E_2} = N_{E_2^{-1}} = p-3$, що не співпадає з p + 1, як це стверджується в теоремі 3 з [10]. Це підтверджують приклади, так якщо $p=31$, то $N_{E_2} = N_{E_2^{-1}} = p-3=28$ над $\mathbb{F}_p$, що не дорівнює $p+1$. Також ми узагальнили теорему 3 з [10], отримавши умови суперсингулярності цих кривих не тільки для простого поля а й для його алгебраїчного розширення $\mathbb{F}_{p^n}$ довільної скінченної степені n.

Зауваження 1. Має місце симетрія квадратів лишків:

$$(\frac{p-1}{2}-k)^2 \equiv (\frac{p-1}{2}+1+k)^2 (\mathrm{mod}\, p), 0 \le k \le \frac{p-1}{2}.$$

Доведення. 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,

$$(\frac{p-1}{2}-1)^2 \equiv (\frac{p-1}{2}+2)^2, (\frac{p-1}{2}-2)^2 \equiv (\frac{p-1}{2}+3)^2, \ \ldots, (\frac{p-1}{2}-k)^2 \equiv (\frac{p-1}{2}+k+1)^2 (\mathrm{mod}\, p).$$

Без квадратів маємо антисиметричну конгруенцію

$$(\frac{p-1}{2}-k) \equiv -(\frac{p-1}{2}+1+k)(mod p).$$

Нагадаємо лему про суму степенів [6].

Лема 1. Нехай $k \in \mathbb{N}$, $p \in \mathbb{P}$. Тоді

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

Теорема. Якщо $p \equiv 3(mod\, 4)$ і p – просте число, 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 співпадають 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 вище вказаних 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 (1) на $y^2 = \frac{x^2-1}{2x^2-1}$. У випадку $p \equiv 3 \pmod 8$ вираз $2x^2-1$ зі знаменника не може бути нулем, бо $(\frac{2}{p}) \equiv -1$. Тому за умови $p \equiv 3(mod 8)$ крива $y^2 = (x^2-1)(2x^2-1)$ має стільки ж точок, що і (1), бо для кожного x з F_p символ Лежандра від елементів $(x^2-1)/(2x^2-1)$ та $(x^2-1)(2x^2-1)$ буде однаковим. У випадку $p \equiv 7(\mathrm{mod}\, 8)$ крива $y^2 = (x^2-1)(2x^2-1)$ буде мати на 2 точки більше, ніж (1), 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, що 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 $p \equiv 3(mod 8)$ та $N_2 = p-1$ для $p \equiv 7 \pmod 8$. (Випадки $N_2 = 1$ або $N_2 = 2p-1$ неможливі, бо $N_2 \ge 2$ і $N_2 \le 2p-2$, бо випадки $(x^2-1)=0$ і $(2x^2-1)=0$ дають лише один розв'язок рівняння (2), де $y=0$ на відміну від 2-ох розв'язків коли ліва частина (2) є лишком.) Звідси слідуватиме твердження про кількість точок на вихідній кривій (1).

Покажемо, що кількість розв'язків рівняння $y^2 = (x^2-1)(2x^2-1)$ тобто N_2, порівнянна з $(-a_{2p-2} - a_{p-1}) \mathrm{mod}\, p$, де a_{2p-2}, a_{p-1} – коефіцієнти многочлена, бо коефіцієнти при інших степенях згідно з Лемою 1 конгруентні 0 за modp. Тому, порівняння $N_2 \equiv -a_{2p-2} - a_{p-1} (\mathrm{mod}\, p)$ слідує з леми 1. Обчислимо значення символу Лежандра [17,18,19] від лівої частини рівняння $y^2 = (x^2-1)(2x^2-1)$ за допомогою формули Ейлера $(x^2-1)^{\frac{p-1}{2}} (2x^2-1)^{\frac{p-1}{2}} = a_0 + a_1 x + \ldots + a_{2p-2} x^{2p-2}$.

Для фіксованого значення x кількість розв'язків рівняння (2) дорівнює $1+(\frac{(x^2-1)(2x^2-1)}{p})$, 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 (2) порівняння за модулем p з $1+((x^2-1)(2x^2-1))^{\frac{p-1}{2}}$. Отже, підсумовуючи за всіма x, маємо $N_2 \equiv \sum_{x=0}^{p-1} 1+((x^2-1)(2x^2-1))^{\frac{p-1}{2}} \equiv p+\sum_{x=0}^{p-1}(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} \bmod p$. Перетворимо вираз $(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}}$, за допомогою бінома Ньютона маємо $(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} = N_2 \equiv (\sum_{x=0}^{p-1} C_{\frac{p-1}{2}}^{k} x^{2k}(-1)^{\frac{p-1}{2}-k})(\sum_{x=0}^{p-1} C_{\frac{p-1}{2}}^{j} 2^j x^{2j}(-1)^{\frac{p-1}{2}-j})$. З цих дужок виберемо степені, що рівні $p-1$ і додавши їх отримаємо коефіцієнт при x^{p-1}.

Звідси отримуємо, що $a_{2p-2} = 1^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}} \equiv (\frac{2}{p}) (\bmod p)$.

Отже,

$$N_2 \equiv -(\frac{2}{p}) - a_{p-1} (\bmod p) \tag{4}$$

Для випадку $8k+3$ маємо

Нам потрібно було довести, що $N_2 \equiv 1(\bmod p)$ при $p \equiv 3(\bmod 8)$, $N_2 \equiv -1(\bmod p)$, $p \equiv 7(\bmod 8)$. Тобто треба буде показати, що $N_2 \equiv -(\frac{2}{p}) - a_{p-1}(\bmod p)$ для $p \equiv 3(\bmod 4)$. Це буде слідувати з (3), якщо ми покажемо, що $a_{p-1} \equiv 0(\bmod p)$. Тоді розв'язків буде або $p-1$ або $p+1$. Знайдемо a_{p-1}. Згідно з формулою бінома Ньютона a_{p-1} рівний коефіцієнту при x^{p-1} в добутку двох дужок і при підстановці у нього 2 замість x є таким $(-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} 2^j (C_{\frac{p-1}{2}}^{j})^2$, тобто має форму зворотнього полінома. Справді

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

Покажемо що за умови $p \equiv 3(\bmod 4)$ виконуватиметься $\sum_{j=0}^{\frac{p-1}{2}} 2^j (C_{\frac{p-1}{2}}^{j})^2 \equiv 0(\bmod p)$.

Домножимо кожен біноміальний коефіцієнт у попередній сумі на $\frac{p-1}{2}!$:

$$(\frac{p-1}{2})! C_{\frac{p-1}{2}}^{j} = \frac{(\frac{p-1}{2})(\frac{p-1}{2}-1)\ldots(\frac{p-1}{2}-j+1)(\frac{p-1}{2})!}{1 \cdot 2 \cdot \ldots \cdot j} =$$

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

Помітимо, що має місце симетрія квадратів лишків:

$$(\frac{p-1}{2}-j)^2 \equiv (\frac{p-1}{2}+j+1)^2, \ 0 \le j \le \frac{p-1}{2},$$

Справді квадрати мають місце наступні конгруенції $(\frac{p-1}{2}-1)^2 \equiv (\frac{p-1}{2}+2)^2$, $(\frac{p-1}{2}-2)^2 \equiv (\frac{p-1}{2}+3)^2$, …, $(\frac{p-1}{2}-k)^2 \equiv (\frac{p-1}{2}+k+1)^2 (\bmod p)$. Без квадратів маємо антисиметричну конгруенцію $(\frac{p-1}{2}-k) \equiv -(\frac{p-1}{2}+1+k)(\bmod p)$.

Використаємо конгруенції описані у зауваженні 1, тобто $(\frac{p-1}{2}-k) \equiv -(\frac{p-1}{2}+1+k)(modp)$ запишемо добутки які конгруентні

$$(\frac{p-1}{2})(\frac{p-1}{2}-1)\ldots(\frac{p-1}{2}-j+1) \equiv [(\frac{p-1}{2}+1)\ldots(\frac{p-1}{2}+\frac{p-1}{2}-j)](-1)^{\frac{p-1}{2}-j} (\bmod p).$$

Переставивши множники бачимо, що з властивості 1 слідує:

$$(\frac{p-1}{2})! C_{\frac{p-1}{2}}^{j} = (\frac{p-1}{2}-j+1)(\frac{p-1}{2}-j+2)\ldots(\frac{p-1}{2})(\frac{p-1}{2}+1)\ldots(p-j-1)(-1)^{\frac{p-1}{2}-j}.$$

Піднісши дві частини до квадрату, отримаємо:

$$((\frac{p-1}{2})! C_{\frac{p-1}{2}}^{j})^2 \equiv (\frac{p-1}{2}-j+1)^2 (\frac{p-1}{2}-j+2)^2 \ldots (p-j-1)^2 (\bmod p) \tag{5}$$

Покажемо, як обчислити $N_2 (\mathrm{mod}\, p)$.

Помітимо, що для заданого x кількість розв'язків рівняння $y^2 = (x^2-1)(2x^2-1) mod$ p конгруентно значенню суми виразів $1+((x^2-1)(2x^2-1))^{\frac{p-1}{2}} \bmod p$ по x від 0 до $p-1$ всіх значень виразу.

Отже,

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

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

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 $\sum_{x=0}^{p-1} x^i$ рівна 0 за модулем *p.*

Для $i = 2p-2$ і $i = p-1$ ця сума порівняна з -1, що слідує з Леми 1.

Тому $\sum_{x=0}^{p-1}(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} \equiv -a_{2p-2}-a_{p-1} (\mathrm{mod}\, p)$.

Дослідимо величину $-a_{2p-2}-a_{p-1} (\mathrm{mod}\, p)$ окремо а саме, покажемо, що

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

Для цього потрібно обчислити a_{2p-2} і a_{p-1}.

a_{2p-2}, очевидно, рівне $2^{\frac{p-1}{2}} \equiv (\frac{2}{p}) (\mathrm{mod}\, p)$.

$a_{p-1} = \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 2^j (-1)^{\frac{p-1}{2}}$, тому, що це коофіцієнт в многочлені $(\sum_{j=0}^{\frac{p-1}{2}} C_{\frac{p-1}{2}}^j (x^2)^j (-1)^{\frac{p-1}{2}-j})(\sum_{j=0}^{\frac{p-1}{2}} C_{\frac{p-1}{2}}^j 2^j (x^2)^j (-1)^{\frac{p-1}{2}-j})$ при x^{p-1}. Оскільки $p \equiv 3 (\mathrm{mod}\, 4)$, то $(-1)^{\frac{p-1}{2}} = -1$ і $a_{p-1} = -\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 2^j$. Тому $N_2 \equiv -a_{p-1}-a_{2p-2} \equiv -(\frac{2}{p}) + \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 2^j (\mathrm{mod}\, p)$.

Нагадаємо, що $(\frac{2}{p}) = \begin{cases} -1, p \equiv 3 (\mathrm{mod}\, 8) \\ 1, p \equiv 7 (\mathrm{mod}\, 8) \end{cases}$.

Отже, в обох випадках потрібно довести співвідношення $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 2^j \equiv 0 (\mathrm{mod}\, p)$, 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

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

при $p \equiv 3 (\mathrm{mod}\, 4)$.

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

$$\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j \equiv 0 (\mathrm{mod}\, p) \quad (6)$$

Розглянемо многочлен $P(x) = \sum_{j=0}^{\frac{p-1}{2}} (j+1)^2 ... (j+\frac{p-1}{2})^2 x^j$. Тому достатньо показати, що: $P(2) \equiv 0 (\mathrm{mod}\, p)$ або в більш загальному випадку $P(d) \equiv 0 (\mathrm{mod}\, p)$.

Використовуючи конгруенцію (4) отримуємо, що $\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 x^j = P(x)\frac{1}{(\frac{p-1}{2}!)^2}$ або $P(x)=\left(\frac{p-1}{2}!\right)^2\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 x^j=\sum_{j=0}^{\frac{p-1}{2}}(k+1)^2(k+2)^2...\left(\left(\frac{p-1}{2}\right)+k\right)^2 x^j$. Тобто в суму (5) замість d підставлено x.

Помітимо, що $P(x)=\partial^{\frac{p-1}{2}}(\partial^{\frac{p-1}{2}}(Q(x)x^{\frac{p-1}{2}})x^{\frac{p-1}{2}})$, де $Q(x)=x^{p-1}+...+x+1$, де $\partial^{\frac{p-1}{2}}$ позначають $\frac{p-1}{2}$ похідну а не степінь. Але тоді $Q(x)=\frac{x^p-1}{x-1}=\frac{(x-1)^p}{x-1}=(x-1)^{p-1}$, тому $P(x)=(((x-1)^{p-1}x^{(\frac{p-1}{2})})x^{\frac{p-1}{2}})^{(\frac{p-1}{2})}$. Нехай $y=x-1$. Позначимо $R(y)=P(x)$ це буде для випадку $y+1=2$ це зведе випадок $x+1=2$ до $y=1$. Ця заміна зводить многочлен $P(x)$, при $x=2$ до многочлена $R(x-1)$ від $x-1=1$, тобто $P(x)=R(x-1)$, що зручно зокрема і для диференціювання, можна вважати, що $R(y)$ це многочлен $P(y)$ від нової змінної $y=x-1$. Зауважимо, що в силу лінійності заміни, диференціювання за y і за x співпадають. Застосуємо диференціювання для перетворення многочлена P(x) до такого вигляду, де явно видно потрібний коефіцієнт a_{p-1}.

Тоді $R(y)=P(y+1)=((y^{p-1}(y+1)^{(\frac{p-1}{2})})^{(\frac{p-1}{2})}(y+1)^{(\frac{p-1}{2})})^{(\frac{p-1}{2})}$. Шукаємо коефіцієнт a_{p-1} від P(y+1) в точці $y=1$. Помітимо, що $(y^{p-1}(y+1)^{(\frac{p-1}{2})})^{(\frac{p-1}{2})}=(y^{p-2})^{\frac{p-1}{2}}=|=(p-1)(p-2)...(\frac{p-1}{2}+1)y^{\frac{p-1}{2}}$. Всі доданки, окрім першого, стануть рівними 0. Тому $R(y)=\frac{(p-1)!}{(\frac{p-1}{2})!}(y^{\frac{p-1}{2}}(y+1)^{\frac{p-1}{2}})^{\frac{p-1}{2}}=\frac{(p-1)!}{(\frac{p-1}{2})!}\sum_{j=0}^{\frac{p-1}{2}}(j+1)...(j+\frac{p-1}{2})y^j C_{\frac{p-1}{2}}^{j}$.

Нам потрібно показати, що $a_{p-1}=P(1+1)=R(1)\equiv 0(\mathrm{mod}\,p)$. Маємо

$$R(1)=\frac{(p-1)!}{(\frac{p-1}{2})!}\sum_{j=0}^{\frac{p-1}{2}}C_{\frac{p-1}{2}}^{j}(j+1)...(j+\frac{p-1}{2}). \qquad (7)$$

Помітимо, що

$$(\frac{p-1}{2}-j+2)...(\frac{p-1}{2}-j+\frac{p-1}{2})=-1^{\frac{p-1}{2}}(j+1)...(j+\frac{p-1}{2})=-1(j+1)...(j+\frac{p-1}{2}),$$

Саме тому, симетричні доданки в (7) скорочуються.

Тут ми використано те, що $(-1)^{\frac{p-1}{2}}=-1$, так, як $p=Mk+3$ і $\frac{p-1}{2}=2k+1$.

Значить, $P(2)=R(1)=0$, що і потрібно було.

Отже, $\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2\equiv 0(\mathrm{mod}\,p)$, 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 $\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{-j}\equiv 0(\mathrm{mod}\,p)$. Для отримання останньої формули враховуємо, що має місце $(\frac{2}{p})=(\frac{2^{-1}}{p})$ тоді рівність $\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{-j}\equiv 0(\mathrm{mod}\,p)$ слідує з вже доведеної формули $\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{j}\equiv 0(\mathrm{mod}\,p)$, якщо її домножити на $2^{-\frac{p-1}{2}}$. Тобто

$$\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{-j}\equiv 0,\ \text{так, як}\ 2^{\frac{p-1}{2}}\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{-j}=\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{\frac{p-1}{2}-j}=\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{j}.$$

Як наслідок маємо, що криві $x^2+y^2=1+2x^2y^2$ і $x^2+y^2=1+2^{-1}x^2y^2$ мають однакове число точок для $p=4k+3$ (тобто для $p=8k+3$ і $p=8k+7$). На цьому твердження про доведення.

Доведемо твердження про порядок групи над розширенним полем.

Використовуючи теорему Степанова [15] результат можна узагальнити для довільного p^n, де $n \equiv 1(\mathrm{mod}\,2)$. Відомо, що якщо $y^2 = P(x)$, де $P(x)$ многочлен степені d, над полем F_{p^n} має кількість розв'язків рівну $p^n + w_1^n + ... + w_{d-1}^n$, де $w_1, ..., w_{d-1}$ – деякі комплексні числа.

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 і Деліня [15; 16]: $N_M = p^k + \omega_1^k + \omega_2^k$, де $\omega_i^k \in \mathbb{C}$ і $\omega_1^k = -\omega_2^k, |\omega_i| = \sqrt{p}, i \in 1,2$. Тобто знайдуться такі $\omega_1, \omega_2 \in \mathbb{C}$, що для всіх $k \in \mathbb{N}$ вірна рівність $N_M = p^k + \omega_1^k + \omega_2^k$. Оскільки $N_M = p$ для $k = 1$, то звідси маємо $\omega_1 + \omega_2 = 0$ або $\omega_1 = -\omega_2$. Згідно з теоремою Деліня: $|\omega_i| = \sqrt{p}$. А для еліптичної кривої виконується $\omega_1 = \overline{\omega}_2$ [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 $k \equiv 1(mod 2)$ порядок відповідної кривої Монтгомері $N_{M,k} = p^k$, то кількість точок у образі при переході від E_M до (2) є $N_{E,k} = p^k - 1 - 2(\frac{d}{p})$ для випадку $p \equiv 3(\mathrm{mod}\,4)$ і $k \equiv 1(mod 2)$, бо заміна $y = (u-1)/(u+1)$ відображає 2 точки 4-го порядку, кривої Монтгомері, з координатою $u = -1$ на нескінченність, тобто не у точку з афінної площини.

Цілком зрозуміло, що значеннями $d = -1, 2, 2^{-1}$ не вичерпується множина параметрів при яких крива Едвардса суперсингулярна.

Наслідок 1. Якщо коефіцієнт d кривої E_d задовольняє рівняння суперсингулярності $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j \equiv 0(\mathrm{mod}\,p)$ досліджене в теоремі 1, то E_d має $p - 1 - 2(\frac{d}{p})$ точок над F_p а біраціонально еквівалентна [2, 12, 13, 14] їй крива E_M має р +1 точок над F_p.

Доведення. З доведення теореми 1 слідує, що конгруенція (6) тобто $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j \equiv 0(\mathrm{mod}\,p)$ 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 F_p рівно $p - 1 - 2\left(\frac{d}{p}\right)$ розв'язків. Це випливає з формули кількості точок (4) виведеній у теоремі 1 і умови $a_{p-1} \equiv 0(modp)$, що забезпечує виконання умови суперсингулярності (6), при цьому враховано наявність 2 особливих точок 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 $p - 1 - 2\left(\frac{d}{p}\right) + \left(1 + (\frac{d}{p})\right) = p - \left(\frac{d}{p}\right)$ розв'язків. Справді кожний розвязок рівняння (1) відповідає розв'язку рівняння (8), але (8) має ще розвязки, при яких $dx^2 - 1 \equiv 0$ їх стільки скільки є квадратних коренів з d в F_p, тобто $1 + \left(\frac{d}{p}\right)$. Тому твердження, що $x^2 + y^2 = 1 + dx^2y^2$ має $p - 1 - 2\left(\frac{d}{p}\right)$ розвязків рівносильна тому, що рівняння $y^2 = (dx^2 - 1)(x^2 - 1)$ має $p - 1 - 2\left(\frac{d}{p}\right) + \left(1 + (\frac{d}{p})\right) = p - \left(\frac{d}{p}\right)$.

Отже, суперсингулярність кривої Едвардса рівносильно тому, що рівняння (8) має $p - 1 - 2\left(\frac{d}{p}\right) + 1 + \left(\frac{d}{p}\right) = p - \left(\frac{d}{p}\right)$. Як показано вище кількість розв'язків (2) конгруентна $-(a_{2p-2} - a_{p-1}) mod p$, 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 $2 \le N_{E_d} \le 2p - 2$. Дійс-

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

Наслідок 2. Якщо виконується умова $\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 d^j \equiv 0(\bmod p)$, 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 скінченним 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: $A=2\dfrac{(a+d)}{(a-d)}$ і $B=\dfrac{4}{a-d}$ [2].

Отже, образом знайденої нами суперсингулярної кривої E_d, де коефіцієнт d задовольняє вказану в умові конгруенцію є крива E_M: $\dfrac{4}{a-d}u^2=v^3+2\dfrac{a+d}{a-d}v^2+v$ враховуючи, що $a=1$ отримуємо еліптичну криву у формі Монтгомері $\dfrac{4}{1-d}u^2=v^3+2\dfrac{1+d}{1-d}v^2+v$, з відповідними коефіцієнтами $B=\dfrac{4}{1-d}$, $A=2\dfrac{1+d}{1-d}$. Оскільки $d\neq 1$, маємо рівняння еквівалентної еліптичної кривої $4u^2=(1-d)v^3+2(1+d)v^2+(1-d)v$.

Кінець доведення Наслідку 2. З умови наслідку 2 і з її біраціональної еквівалентності кривій E_d 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 $p\equiv 3(\bmod 8)$ не можливий в силу не існування $\sqrt{2}$.

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

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 Монгомері 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 $t=v-\dfrac{b}{3a}$, де $a=(d-1)4^{-1}$, $b=2^{-1}(1+d)$. Ця крива буде суперсингулярною еліптичною кривою у формі Веєрштрасса.

Висновки. Було знайдено умову, у вигляді конгруенції з наслідку 1, на коефіцієнти кривої Едвардса, яка є необхідною і достатньою для суперсингулярності цієї кривої це дозволило описати всю множину параметрів при яких є суперсингулярною. Узагальнено результата про суперсингулярність кривої отриманого в [10] для коефіцієнтів над на випадок довільного не простого поля та виправлено неточності у кількості точок афінної кривої Едвардса над полем характеристики, яка була в теоремі 3 з [10]. Дослідження дозволило знайти критерій суперсингулярності еліптичних кривих у формі Монтгомері, що дає можливість перевіряти криві на придатність до використання в якості носія групи точок для побудови крипто систем та електронно-цифрового підпису на еліптичній кривій.

Список використаних джерел:

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

2. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters. Twisted Edwards Curves. *IST Programme ECRYPT, and in part by grant ITR-071649.* 2008. P. 1–17.

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

4. *Алексеев Е., Ошкин И., Попов В., Смышляев С., Сонина Л.* 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». 2014. С. 24–26.

5. Hallgren S. Linear congruential generators over elliptic curves. *Preprint CS-94-143, Dept. Of Comp. Sci., CornegieMellon Univ.* 1994. P. 1–10.

6. Виноградов И. Основы теории чисел: Учебное пособие. 12-е изд. СПб. : Издательство «Лань», 2009. 271 с.

7. Белецкий А.Я., Белецкий А.А. Симметричный блочный криптоалгоритм. *Захист інформації*. 2006. № 2 (29). С. 42–51.

8. Скуратовський Р., Мовчан П. В., Нормалізація скрученої кривої Едвардса та дослідження її властивостей над Fp. *Збірник праць 14 Всеукраїнської науково-практичної конференції. ФТІ НТУУ «КПІ»*. 2016. Том 2. С. 102–104.

9. Скуратовський Р. Дослідження властивостей скрученої кривої Едвардса. *Конференція державної служби спеціального зв'язку та захисту інформації*. URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?showHidden=1artid=252312catid=240232 ctime=1464080781894

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

11. Skuratovskii R. V. Twisted Edwards curve and its group of points over finite field Fp. *Літня школа «Алгебра, Топологія, Аналіз»*. Одеса, 2016. С. 122–124.

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

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

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

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

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

17. Сергієнко І., Задірака В., Литвин О. Елементи загальної теорії оптимальних алгоритмів та суміжні питання. К. : Наук. думка, 2012. 400 с.

18. Рибак О. Розкладність рядків та звідність многочленів. *У світі математики*. 2006. № 12(4). С. 18–29.

19. Скуратовский Р. Метод быстрого таймерного кодирования текстов. *Кибернетика и системный анализ*. 2013. Т. 49. № 1. С. 154–160.

20. Долгов В. Эллиптические кривые в криптографии. *Системи обробки інформації*. 2008. Вип. 6 (73). С. 3–10.

21. Болотов С. Б., Гашков А. Б., Фролов А. А. Часовских Элементарное введение в эллиптическую криптографию М. : КомКника, 2006. Том 2. 328 с.

References:

1. Edwards, H. (2007). A normal form for elliptic curves. *American Mathematical Society*, vol. 44, no. 3, pp. 393–422. [in English].

2. Daniel, J. Bernstein, Peter, Birkner, Marc, Joye, Tanja, Lange, Christiane, Peters. (2008). Twisted Edwards Curves. *IST Programme ECRYPT, and in part by grant ITR-071649*, pp. 1–17. [in English].

3. Menezes, A., Okamoto, T., Vanstone, S. (1993). Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Transactions On Information Theory*, vol. 39, no. 5, pp. 1603–1646. [in English].

4. Alekseev, E., Oshkin, I., Popov, V., Smyshlyaev, S., Sonina, L. (2014). O perspektivah ispolzovaniya skruchennyh ellipticheskih krivyh Edvardsa so standartom GOST R 34.10-2012 i algoritmom klyuchevogo obmena na ego osnove. *Materialy XVI mezhdunarodnoj konferencii «RusKripto 2014»*, pp. 24–26. [in Russian].

5. Hallgren, S. (1994). Linear congruential generators over elliptic curves. *Preprint CS-94-143, Dept. Of Comp. Sci., CornegieMellon Univ*, pp. 1–10. [in English].

6. Vinogradov, I. (2009). Osnovy teorii chisel: Uchebnoe posobie. 12-e izd. SPb.: Izdatelstvo «Lan», 271 p. [in Russian].

7. Beleckij, A.Ya., Beleckij, A.A. (2006). Simmetrichnyj blochnyj kriptoalgoritm. *Zahist informaciyi*, no. 2 (29), pp. 42–51. [in Russian].

8. Skuratovskyi, R., Movchan, P. V. (2016). Normalizatsiia skruchenoi kryvoi Edvardsa ta doslidzhennia yii vlastyvostei nad Fp. *Zbirnyk prats 14 Vseukrainskoi naukovo-praktychnoi konferentsii. FTI NTUU «KPI»*, vol. 2, pp. 102–104. [in Ukrainian].

9. Skuratovskyi, R. Doslidzhennia vlastyvostei skruchenoi kryvoi Edvardsa. *Konferentsiia derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii*. URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?showHidden=1artid=252312catid=240232 ctime=1464080781894 [in Ukrainian].

10. Bessalov, A., Cygankova, O. (2015). Vzaimosvyaz semejstva tochek bolshih poryadkov krivoj Edvardsa nad prostym pole. *Zahist informaciyi*, vol. 17, no. 1, pp. 73–80. [in Russian].

11. Skuratovskii, R. V. (2016). Twisted Edwards curve and its group of points over finite field Fp. *Litnia shkola «Alhebra, Topolohiia, Analiz»*, Odesa, pp. 122–124. [in English].

12. Skuratovskii, R., Skruncovich, U. Twisted Edwards curve and its group of points over finite field Fp. Akademgorodok, Novosibirsk, Russia. *Conference. Graphs and Groups, Spectra and Symmetries*. URL: http://math.nsc.ru/conference/g2/g2s2/exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf [in English].

13. Rid, M. (1991). Algebraicheskaya geometriya dlya vseh. Moskva: Mir, 143 p. [in Russian].

14. Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary. (2008). Twisted Edwards Curves Revisited. *ASIACRYPT LNCS 5350*, pp. 326–343. [in English].

15. Stepanov, S. (1991). Arifmetika algebraicheskih krivyh. M.: Nauka, 368 p. [in Russian].

16. Koblitz, N. (1987). Eliptic Curve Cryptosystems. *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209. [in English].

17. Serhiienko, I., Zadiraka, V., Lytvyn, O. (2012). Elementy zahalnoi teorii optymalnykh alhorytmiv ta sumizhni pytannia. K.: Nauk. dumka, 400 p. [in Ukrainian].

18. Rybak, O. (2006). Rozkladnist riadkiv ta zvidnist mnohochleniv. *U sviti matematyky*, no. 12(4), pp. 18–29. [in Ukrainian].
19. Skuratovskij, R. (2013) Metod bystrogo tajmernogo kodirovaniya tekstov. *Kibernetika i sistemnyj analiz*, vol. 49, no. 1, pp. 154–160. [in Russian].
20. Dolgov, V. (2008). Ellipticheskie krivye v kriptografii. *Sistemi obrobki informaciyi*, vol. 6 (73), pp. 3–10. [in Russian].
21. Bolotov, S. B., Gashkov, A. B., Frolov, A. A. (2006). Chasovskih Elementarnoe vvedenie v ellipticheskuyu kriptografiyu M.: KomKnika, vol. 2, 328 p. [in Russian].