НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“___”_____2020 р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки : 113 «Прикладна математика»
(код і назва)

на тему: Удосконалення методу факторизації Лєнстра з використанням кривих Едвардса

Виконав: студент __4__ курсу, групи ____ФІ-62_____
(шифр групи)

_____Бурлука Максим Володимирович_____ _____
(прізвище, ім’я, по батькові) (підпис)

Керівник _____к.т.н., доцент Кучинська Н.В._____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2020року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Фізико-технічний інститут

Кафедра математичних методів захисту інформації

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки - 113 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедрою

М.М.Савчук

_____
(підпис) (ініціали, прізвище)

«___»_____2020 р.

ЗАВДАННЯ
на дипломну роботу студенту

Бурлуці Максиму Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Удосконалення методу факторизації Лєнстра з використанням кривих Едвардса,

керівник роботи к.т.н., доцент Кучинська Н. В.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від _____ р. № _____

2. Термін подання студентом роботи

3. Вихідні дані до роботи

4. Зміст роботи У роботі був зроблений аналіз опублікованих результатів використання методу Лєнстра на кривих Едвардса. Досліджено властивості кривих Едвардса в залежності від параметрів кривих, в тому числі наявність особливих точок. Отримано оцінки кількості таких точок для всіх класів кривих Едвардса. Було встановлено який клас кривих має найбільшу кількість особливих точок та на основі отриманих результатів було запропоновано модифікований алгоритм Лєнстра з використанням таких кривих.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) презентація_____

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1.	Огляд опублікованих матеріалів за темою дослідження		
2.	Дослідження методу Лєнстра на кривих Вейєрштрасса та Едвардса		
3.	Дослідження параметрів кривих у формі Едвардса		
4.	Побудова оцінок особливих точок кривих Едвардса над кільцем n=pq		
5.	Запропонувати модифікований алгоритм Лєнстра з використанням кривих Едвардса		

Студент _____ Бурлука М.В.
(підпис) (ініціали, прізвище)

Керівник роботи _____ Кучинська Н.В.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Кваліфікаційна робота містить: 54 сторінки, 6 рисунків, 7 таблиць, 13 джерел.

У роботі зроблений аналіз літературних джерел, що стосуються теорії еліптичних кривих. Були розглянуті опубліковані результати використання методу Лєнстра на кривих Вейєрштрасса та кривих Едвардса. А також виконано аналіз параметрів кривих Едвардса.

Тема роботи: удосконалення методу факторизації Лєнстра з використанням кривих Едвардса.

Мета роботи: розробка та математичне обґрунтування вибору форми кривих Едвардса для методу факторизації Лєнстра.

Задача роботи: проаналізувати опубліковані результати використання методу Лєнстра на кривих Едвардса. Проаналізувати параметри методу Лєнстра, розглянути можливість модифікації методу на еліптичних кривих у формі Едвардса над кільцем лишків Z_n. Дослідити модифікований алгоритм Лєнстра на еліптичних кривих у формі Едвардса в залежності від параметрів таких еліптичних кривих.

Об'єкт дослідження: інформаційні процеси в системах криптографічного захисту.

Предмет дослідження: криптографічні властивості методу Лєнстра на еліптичних кривих у формі Едвардса.

Методи дослідження: методи теорії еліптичних кривих, абстрактної алгебри та методи теорії алгоритмів факторизації.

У результаті роботи встановлена залежність властивостей еліптичних кривих у формі Едвардса над кільцем $n = pq$. Досліджено властивості кривих у формі Едвардса в залежності від параметрів еліптичної кривої, в тому числі наявність особливих точок. Отримано оцінки кількості таких точок для всіх можливих випадків значень коефіцієнтів кривої Едвардса над кільцем $n = pq$. Встановлено, що

найбільшу кількість особливих точок має клас кривих Едвардса з квадратичним параметром. Тому в роботі запропоновано обирати параметри a та d так, щоб відповідні криві Едвардса над кільцем $n = pq$ містили найбільшу кількість особливих точок. На основі цього був запропонований модифікований алгоритм Лєнстра з використанням цих кривих.

МЕТОД ЛЄНСТРА, КРИВІ ЕДВАРДСА, ОСОБЛИВІ ТОЧКИ

ABSTRACT

The thesis contains: 54 pages, 6 figures, 7 tables, 13 sources.

In this thesis, an analysis was made of literary sources relating to the theory of elliptic curves. The published results of using the Lenstra method on Weierstrass curves and Edwards curves were considered. And also an analysis was made of the parameters of the Edwards curves.

The theme of this thesis is iman provement of the Lenstra factorization method using Edwards curves.

The goal of this thesis is development and mathematical substantiation of the choice of the shape of the Edwards curves for the Lenstra factorization method.

The task of this work is to analyze the published results of the Lenstra method on the Edwards curves. Analyze the parameters of the Lenstra method, consider the possibility of modifying the method on elliptic curves in the form of Edwards over the ring Z_n. Investigate the modified Lenstra algorithm on elliptic curves in the form of Edwards depending on the parameters of these elliptic curves.

The object of the research is information processes in cryptographic protection systems.

The subject of the research is cryptographic properties of the Lenstra method on elliptic curves in the form of Edwards.

Methods of research are methods of the theory of elliptic curves, abstract algebra and methods of the theory of factorization algorithms.

As a result of this work, the dependence of the properties of elliptic curves in the form of Edwards over the ring $n = pq$ was established. The properties of these curves are investigated, depending on the parameters of the elliptic curve, including the presence of exceptional points. Estimates of the number of such points are obtained for all possible cases of the values of the coefficients of the Edwards curve over the ring $n = pq$. It is established that the class of Edwards

curves with a quadratic parameter has the largest number of exceptional points. Therefore, it is proposed to choose the parameters a and d so that the Edwards quadratic curves over the ring $n = pq$ contain the largest number of exceptional points. Based on this, a modified Lenstra algorithm using these curves was proposed.

LENSTRA METHOD, EDWARDS CURVES, EXCEPTIONAL POINTS

ЗМІСТ

ВСТУП

Актуальність дослідження. Криптографічна стійкість алгоритмів та методів захисту інформації ґрунтується на складності розв'язання задачі факторизації — розкладання заданого числа великої розмірності на прості множники. Факторизація великих чисел є обчислювально складною задачею.

Метод Лєнстра [1],[2],[3] є третім по швидкості роботи після загального методу решета числового поля та методу квадратичного решета. Він має субекспоненціальну складність. В основі алгоритму лежить використання еліптичної кривої та її редукція за цілим модулем. Час роботи методу є пропорційним до часу додавання точок еліптичної кривої. Таким чином можна зробити висновок: використовувати для реалізації методу еліптичні криві такого виду, щоб операція додавання точок на цих кривих виконувалася найшвидше. Криві у формі Едвардса мають таку властивість.

Класичний метод факторизації Лєнстра ґрунтується на одній із властивостей еліптичних кривих у формі Вейєрштрасса, якої немає у кривих Едвардса. Особливість ґрунтується на тому, що у кривих Вейєрштрасса існує точка, що не є розв'язком рівняння відповідної еліптичної кривої — нескінченно віддалена точка, що не має координат. Тому повністю перенести метод Лєнстра, що використовує криві у формі Едвардса не є можливим.

На разі достаньою умовою для взлому криптосистеми RSA та їй подібних криптосистем є існування швидких та ефективних алгоритмів факторизації чисел. Тому задача побудови таких алгоритмів буде актуальною ще довгий проміжок часу, поки використовуються RSA-подібні криптосистеми.

Мета дослідження: розробка та математичне обґрунтування вибору форми кривих Едвардса для методу факторизації Лєнстра.

Завдання дослідження:

1) проаналізувати опубліковані результати використання методу Лєнстра на кривих Едвардса;

2) проаналізувати параметри методу Лєнстра, розглянути можливість модифікації методу на еліптичних кривих у формі Едвардса над кільцем лишків Z_n;

3) дослідити модифікований алгоритм Лєнстра на еліптичних кривих у формі Едвардса в залежності від параметрів еліптичних кривих.

Об'єкт дослідження: інформаційні процеси в системах криптографічного захисту.

Предмет дослідження: криптографічні властивості методу Лєнстра на еліптичних кривих у формі Едвардса.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи теорії еліптичних кривих, абстрактної алгебри та методи теорії алгоритмів факторизації.

Наукова новизна отриманих результатів полягає у застосуванні такого класу кривих Едвардса, що зможуть забезпечити швидкодію методу Лєнстра.

Практичне значення результатів полягає у використанні отриманих результатів для проведення факторизації цілих чисел виду $n = pq$ з використанням методу Лєнстра на кривих Едвардса.

1 АКТУАЛЬНІСТЬ ЗАДАЧІ ФАКТОРИЗАЦІЇ ТА АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ФАКТОРИЗАЦІЇ ЦІЛИХ ЧИСЕЛ

Процес розкладання великих чисел на множники є досить складним для сучасних можливостей ком'ютерів. На сьогоднішній день найшвидші алгоритми для факторизації чисел потребуть експоненціального часу виконання. Відомо багато алгоритмів факторизації, але кожен із них має свої переваги та недоліки. У цьому розділі будуть розглянуті відомі алгоритми розкладання цілих чисел на прості множники: метод перебору можливих дільників, метод факторизації Ферма, $p-1$ метод Поларда, метод Лєнстра на еліптичних кривих у формі Вейєрштрасса та метод Лєнстра на кривих Едвардса. Основна увага присвячена двом останнім алгоритмам. У розділі представлені результати тестів на факторизацію різнорозрядних чисел, щоб наглядно побачити за яких умов краще всього використовувати ці алгоритми.

1.1 Метод перебору дільників

Даний алгоритм є найпростішим методом факторизації чисел. Суть алгоритму полягає у тому, що відбувається ділення числа n на всі цілі числа, що лежать в інтервалі від 2 до квадратного кореня n. Після кожного ділення обчислюється залишок від ділення числа, що факторизується, на кожне із чисел $[2,...,\sqrt{n}]$. Якщо буде знайдено залишок, що дорівнює нулю, то у цьому випадку знайдемо дільник числа n.

Для реалізації цього алгоритму можемо використовувати звичайний список із простими числами або можемо просто генерувати псевдопрості числа. Процес створення та збереження послідовності простих чисел є дуже затратним, тому займає дуже багато пам'яті та часу. Щоб вирішити цю

проблему можемо використовувати числа такого виду :

$$2,3,6t \pm 1, \text{ де } t \text{ це цілі числа більше нуля.}$$

Така послідовність містить у собі кілька дільників, тому можемо зробити трохи більше ділень, ніж необхідно.

Розглянемо алгоритм факторизації перебору дільників:

вхід: складене ціле число n.

вихід: нетривіальний дільник d числа n.

1) Якщо $n \equiv 0 \mod 2$, то повертаємо $d = 2$.
2) Якщо $n \equiv 0 \mod 3$, то повертаємо $d = 3$.
3) Покладемо
   $d = 3$,
   $r = 2$.
4) Поки $d < \sqrt{n}$, то виконуємо
   а) покладемо $d = d + r$;
   б) якщо $n \mod d = 0$, то повертаємо d;
   в) покладемо $r = r - 6$.

Таблиця 1.1 – Алгоритм перебору дільників

Число n	**Час факторизації**
169	3,32 мс
124711	5,64 мс
4068289	6,35 мс
1337362643	18,45 мс
5562989473183	46,63 мс
135176122544191	350,23 мс
1351761225441923	2,0250 с
9407594505751939379	270,54 с

Як бачимо, що при переході від 51 бітного числа до 64 бітного, швидкість різко зменшилася приблизно у 135 разів. Якщо далі

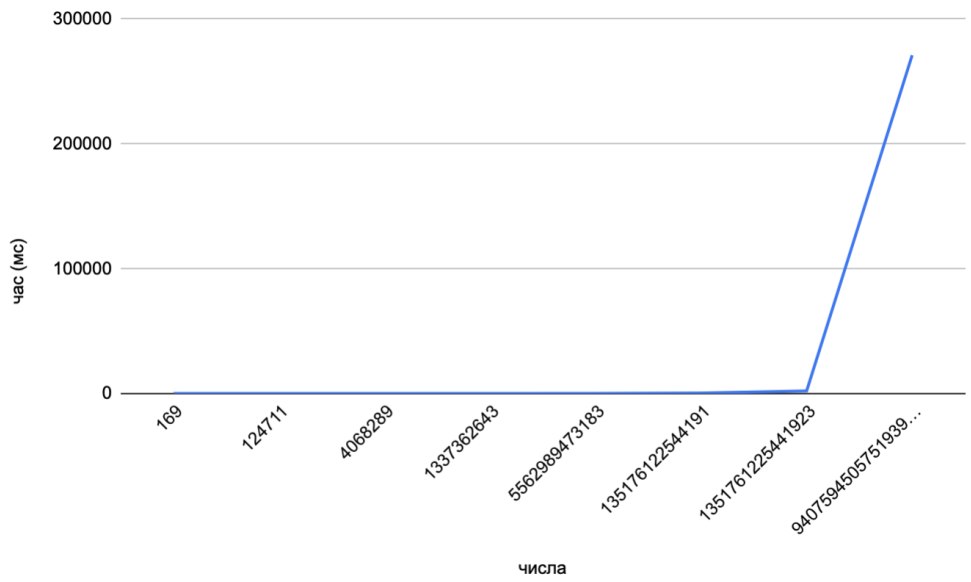

Рисунок 1.1 – швидкодія алгоритму перебору дільників

продовжувати збільшувати бітність n, яке збираємося факторизувати, то швидкість буде падати ще швидше. Часова складність цього методу дорівнює

$$O(\sqrt{n}).$$

1.2 Метод Ферма

Метод факторизації Ферма на практиці не застосовується для факторизації дуже великих чисел. В основі цього методу лежить теорема про представлення числа у вигляді різниці двох квадратів. Використовується стратегія представлення числа n у вигляді різниці двох непослідовних квадратів $a^2 - b^2$, де a,b — невід'ємні цілі числа. Потім ми можемо швидко факторизувати n у вигляді $(a - b)(a + b)$. Сам алгоритм дуже добре застосовувати у випадку, коли числа a та b мають невелику різницю у розмірності.

Метод по-суті складається із двох кроків. Для початку треба знайти цілу частину квадратного кореня для числа n: $\lceil n \rceil = g$. При цьому g має бути найменшим таким числом, що $g^2 - n$ більше нуля. Далі для кожного

$t \in \mathbb{N}$ будемо обчислювати $(\lceil n \rceil + t)^2 - n$ та перевіряти чи є розраховане число квадратом. Якщо ні, то переходимо до наступної ітерації t.

Розглянемо детальніше кожен крок методу за допомогою алгоритму:

вхід: непарне складене ціле число n.

вихід: нетривіальний дільник числа n.

1) Шукаємо найменше ціле число $g : \lceil n \rceil = g$.

2) Якщо $g^2 = n$, то g — дільник n. Кінець алгоритму.

3) Покладемо $a = g$ і $w = a^2 - n$, лічильник t дорівнює 0.

4) Якщо w — повний квадрат, то шукаємо $b = \sqrt{w}$, тоді отримуємо дільник $a + b$. Кінець алгоритму.

5) Лічильник $t = t + 1$, $a = a + 1$, $w = a^2 - n$. Переходимо до 4-го пункту.

Розглянемо швидкість факторизації для різних складених цілих чисел.

Таблиця 1.2 – Алгоритм факторизації Ферма

Число n	**Час факторизації**
169	1 мс
124711	3,67 мс
4068289	1 мс
1337362643	10,345 мс
5562989473183	4,4 с
135176122544191	2,146 с
1351761225441923	5,15 с
9407594505751939379	6,4 с

Виконуючи тести швидкості роботи цього методу, дійсно було помітно, що він є ефективним тільки тоді, коли різниця між дільниками дуже мала. Деякі числа, що були квадратами, розкладалися менше ніж за 1мс. У випадку великої різниці розмірності дільників швидкість методу різко падає.

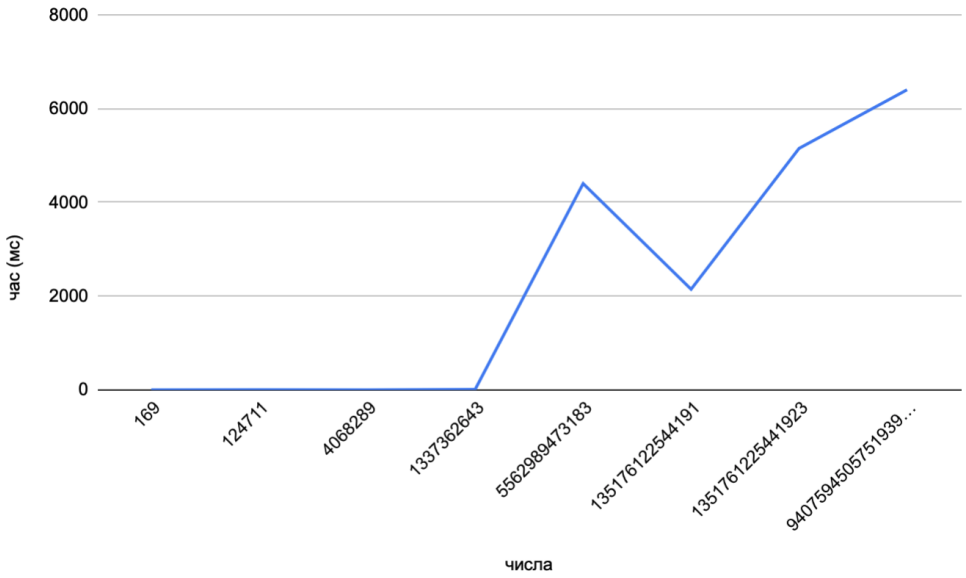

Рисунок 1.2 – швидкодія методу Ферма

1.3 $p-1$ метод Поларда

Цей метод заснований на малій теоремі Ферма. Він є спеціалізованим алгоритмом для цілих чисел, що мають певний дільник p, де $p-1$ є *B-гладким* для певного відносно невеликого B. Якщо спробувати використовувати цей метод на *B-негладких* цілих числах, то це призведе до збою роботи алгоритму.

Розглянемо $p-1$ метод Поларда по крокам:

вхід: складене ціле число n.

вихід: нетривіальний дільник p для числа n.

1) Обираємо границю гладкості для числа B.

2) Обираємо ціле число a.

3) Для кожного просто числа q, що міститься нижче границі гладкості B виконуємо:

а) обчислюємо число $g = \lfloor \frac{ln(n)}{ln(q)} \rfloor$;

б) покладемо $a = a^{q^g} \mod n$.

4) Покладемо $gcd(a-1,n) = p$.

5) Якщо у цьому випадку p таке, що знаходиться у границях

$1 < p < n$, то знайшли нетривіальний дільник для числа n.

6) Якщо такого числа не було знайдено, то повертаємося до кроку 3.

Цей метод не буде ефективним, якщо не використовувати певну продуману стратегію для вибору чисел a.

Розглянемо результати тестів факторизації для різнорозрядних складених чисел та подамо результати до таблиці.

Таблиця 1.3 – Алгоритм факторизації $p-1$ Поларда

Число n	**Час факторизації**
169	1,56 мс
124711	3,45 мс
4068289	10,34 мс
1337362643	36,23 мс
5562989473183	40,34 мс
135176122544191	67,15 мс
1351761225441923	70,32 мс
9407594505751939379	60,53 мс

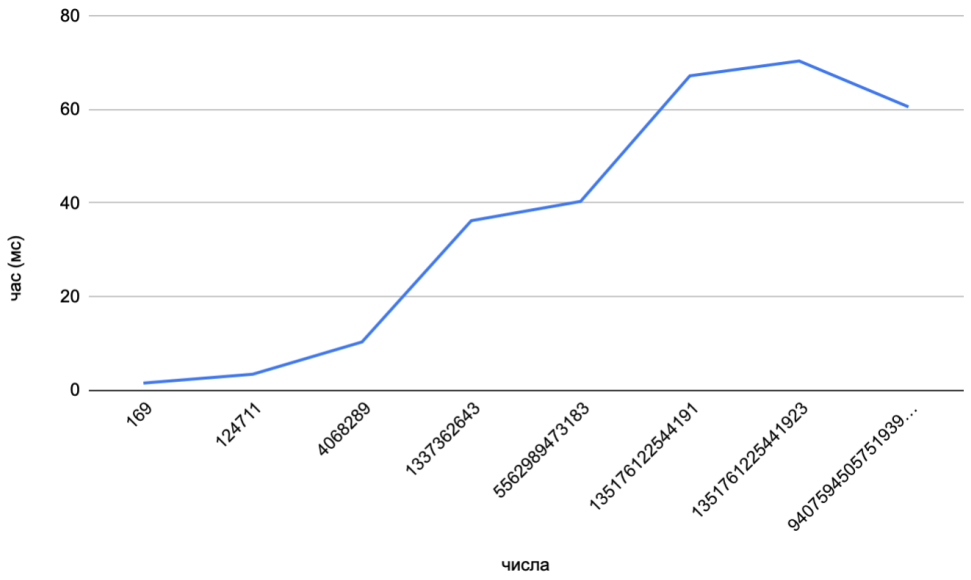

Рисунок 1.3 – швидкодія $p-1$ методу Поларда

У тестах найбільша кількість десяткових знаків дорівнювала 19-м. У багатьох літературних джерелах рекомендують застосовувати цей метод для чисел кількість десяткових знаків яких менше 22. У цьому випадку його швидкість буде максимальною.

Якщо p — дільник числа n і при цьому p є *B-гладким*, то часова складність цього методу дорівнює

$$O\left(B\frac{ln(n)}{ln(B)}\right).$$

1.4 Метод Лєнстра на еліптичних кривих у формі Вейєрштрасса

Прообразом для алгоритму Лєнстра є $p-1$ метод Поларда, що базується на тому, що можна обрати таке натуральне число a, щоб для певного $p|n$ порядок в групі Z_p^* був досить малим. Головною особливістю цього методу є те, що його неможливо застосувати, якщо для нетривіального дільника p число $p-1$ не є складеним. Отже, число n можна обрати так, щоб алгоритм Поларда було неможливо застосувати.

Алгоритм Поларда вже був описаний по крокам реалізації у пункті 1.3 цього розділу. Коротко опишемо його математичну суть:

Мета методу — знаходження простих дільників для складеного числа n. Нехай один з простих дільників p числа n такий, що всі прості дільники числа $p-1$ є невеликими і не перевищують деякого числа A.

Нехай a — натуральне число, $(a,p)=1$. Тоді використовуючи малу теорему Ферма маємо:

$$a^{(p-1)} = 1 \mod p$$

У цьому випадку $p \mid a^{(p-1)} - 1$. А отже, $(a^p - 1,n) = p$

Число p для нас невідоме. Тоді нехай $t_1,t_2,...,t_r$ — прості числа до r, $e_1,e_2,...,e_r$ — невеликі прості числа. Обчислимо :

$$\mathrm{k}=\prod_{i=1}^{r} t_i^{e_i} \tag{1.1}$$

Алгоритм буде працювати при умові, якщо :

$$(p-1) \mid k \tag{1.2}$$

При виконанні умови (1.2) маємо:

$$a^k \equiv 1 \bmod p \text{ , тому } (a^p - 1,n) = p \tag{1.3}$$

Нехай $(a,p) = 1$, тоді $\mathrm{ord}(a \bmod p) = l \mid (p-1)$. У цьому випадку для виконання умови (1.3), достатньо виконання

$$\mathrm{ord}(a \bmod p) \mid k \tag{1.4}$$

Бачимо, що обравши a так, щоб його порядок в групі Z_p^* був малим, то так можна буде знайти дільник p для n, використовуючи умову (1.3). Ймовірність виконання умови (1.4) для випадкового числа a дорівнює

$$\frac{\sum\limits_{d \mid (\mathrm{k,p\text{-}1})} \varphi(d)}{p-1}.$$

Лєнстра запропонував метод, що має в рази ширший спектр використання. Головна його властивість у тому, що група, у якій він працює, для однакових чисел p може бути побудована не одним способом, тому метод Лєнстра може працювати не лише у групі Z_p^*.

В методі Лєнстра замість мультиплікативної групи Z_p^* використовують групу точок еліптичної кривої над кінцевим полем F_p, а замість числа a використовують певну точку кривої. За теоремою Хассе кількість точок кривої $N(E_p)$ знаходиться в межах $p + 1 - 2\sqrt{p} \leq N(E_p) \leq p + 1 + \sqrt{p}$. Тому ми можемо знайти криву, що

має порядок з великою кількістю невеликих дільників. У такому випадку ймовірність вибрати точку кривої з невеликим порядком, що є дільником числа k, є великою. Якщо група точок кривої E_p циклічна, то ймовірність вибору точки, що нас влаштовує, дорівнює :

$$\frac{\sum\limits_{d|f} \varphi(d)}{N(E_p)} \text{ , де } f = (k, N(E_p)).$$

Зауважимо , якщо $N(E_p)|k$, то досягнемо успіху з імовірністю 1. В цьому випадку $(k, N(E_p)) = N(E_p)$, тому маємо :

$$\frac{\sum\limits_{d|f} \varphi(d)}{N(E_p)} = \frac{\sum\limits_{d|N(E_p)} \varphi(d)}{N(E_p)} = \frac{N(E_p)}{N(E_p)} = 1 \text{ , де } f = (k, N(E_p)).$$

Коректність роботи алгоритму Лєнстра забезпечує така теорема:

Теорема 1.1. *Нехай E: $y^2 = x^3 + bx + c$, де $b,c \in Z$ — деяка еліптична крива і при цьому виконується умова $(4b^3+27c^2, n)=1$. P_1 та P_2 — це точки, що належать кривій E, $P_1 \neq P_2$ та їх знаменники координат є взаємно простими із n. Тоді точка, що утвориться при операції суми $P_1 + P_2$ має координати, знаменники яких є взаємно простими із n тоді та тільки тоді, коли для будь-якого простого p, що є дільником для числа n, сума точок $P_1 mod p + P_2 mod p$ на кривій $E mod p$ не є рівною точці, що є нескінченно віддаленою.*

Розглянемо сам алгоритм Лєнстра:

Вхід: n — складене.

Вхід: p — дільник n.

1) Випадково обираємо b, x_0, y_0 у проміжку від 2 до n.

2) Робимо обчислення $c = (y_0^2 - x_0^3 - bx_0) \mod n$.

Крива задана у формі Вейєрштрасса :

E: $y^2 = x^3 + bx + c$, де $b,c \in Z$. Точка P(x_0, y_0) належить цій кривій.

3) Далі обчислюємо $D = (4b^3+27c^2, n)$.

Якщо D знаходиться у проміжку від 1 до n невключно, то ми знайшли дільник $p = D$. Алгоритм завершує роботу.

Якщо $D = n$, то повертаємось до кроку 1) та знову обираємо нове значення для b.

4) Обираємо k, що має вигляд k=$\prod_{i=1}^{r} t_i^{e_i}$, де t_1,t_2,...,t_r — всі прості числа до r, e_1,e_2,...,e_r — невеликі прості числа. Або обираємо число k так, щоб воно складалося із невеликих простих дільників: k=НСК(2,. . . ,M) для деякого додатного числа M.

5) Далі використовуємо схему Горнера для обчислення kP за формулами додавання точок еліптичної кривої у формі Вейєрштрасса. Якщо під час обчислень при додаванні точок $P_1(x_1, y_1)$ та $P_2(x_2, y_2)$ НСД D для точки $P_3(x_3, y_3) = P_1 + P_2$ виявилося у проміжку від 1 до n невключно, тобто

$$D = \begin{cases} (\mathrm{x}_2\text{-}x_1,\mathrm{n}) & , P_1 \neq \mathrm{P}_2 \\ (\mathrm{y}_1,\mathrm{n}) & , P_1 = P_2 \end{cases}$$

то $p = D$ і алгоритм завершує роботу.

Якщо $D = 1$, то проводимо обчислення далі та повертаємось до кроку 4) і при цьому збільшуємо значення k або ж повертаємось до кроку 1) та обираємо нову еліптичну криву.

Згідно з даними, що знаходяться у роботах [2, 3], час роботи цього алгоритму такий самий, як у найкращих алгоритмах факторизації.

Розглянемо швидкодію цього методу для декількох цілих складених чисел.

Час роботи алгоритму може покращуватися або погіршуватися, так як все залежить від точки, що береться на кривій випадково, та від обранної еліптичної кривої.

Таблиця 1.4 – метод Лєнстра на еліптичних кривих у формі Вейєрштрасса

Число n	**Час факторизації**
169	2,223 мс
124711	3,634 мс
4068289	6,32 мс
1337362643	8,324 мс
5562989473183	17,342 мс
135176122544191	120,332 мс
1351761225441923	534,34 мс
9407594505751939379	80,3 с

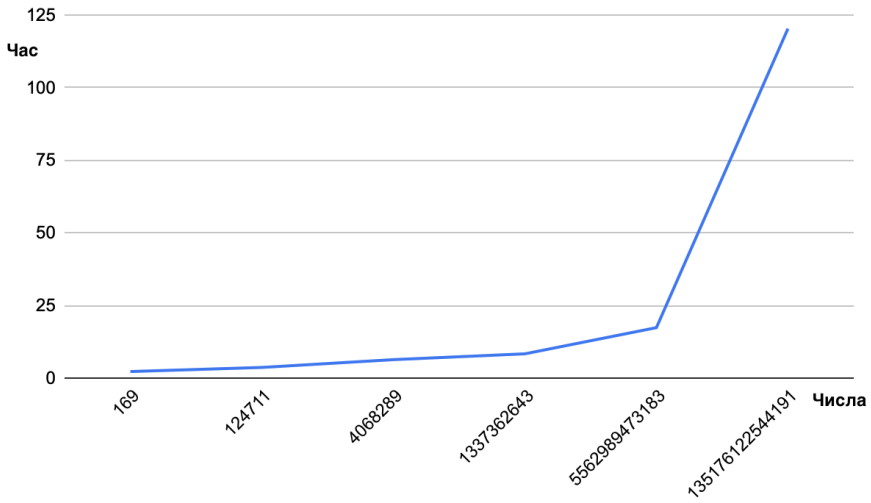

Рисунок 1.4 – швидкодія методу Лєнстра

1.5 Метод Лєнстра на кривих у формі Едвардса

Розглянемо алгоритм Лєнстра, який модифікували у роботі [5], для використання його на повних кривих Едвардса. Для кривих Едвардса у роботі був побудований наступний алгоритм:

$$E : x^2 + y^2 = 1 + dx^2y^2, \quad \left(\frac{d}{n}\right) = -1.$$

вхід: складене натуральне число n.

вихід: нетривіальний дільник p для числа n.

1) Навмання обираємо $x^{'}$ та $y^{'}$ в інтервалі від 2 до $n-1$.

2) Обчислити $R_1 = (x^{'},n)$ та $R_2 = (y^{'},n)$. Якщо ж один із НСД лежить у інтервалі від 1 до n невключно, то ми знайшли p і завершили роботу алгоритму.

3) Обчислити $(x^{'})^2 + (y^{'})^2 - 1$.

4) Обчислити $R_3 = ((x^{'})^2 + (y^{'})^2 - 1,n)$. Якщо R_3 лежить у інтервалі від 1 до n невключно, то ми знайшли p і завершили роботу алгоритму. Якщо ж $R_3 = n$, то ми знову повертаємося до кроку 1) та обираємо нові значення $x^{'}$ та $y^{'}$.

5) Якщо

$$\left(\frac{(x^{'})^2 + (y^{'})^2 - 1}{n}\right) = 1,$$

повертаємо до кроку 1) та обираємо нові значення $x^{'}$ та $y^{'}$.

6) Обчислити

$$\left((x^{'})^2 + (y^{'})^2 - 1\right)\left((x^{'})^2(y^{'})^2\right)^{-1}.$$

7) Якщо не існує $\left((x^{'})^2(y^{'})^2\right)^{-1}$ по модулю n, то ми знайшли p та завершили роботу алгоритму.

8) Обрати k та деяке натуральне число N, щоб k мало багато невеликих дільників. Наприклад, $k = \text{НСК}(2,...,N)$.

9) Обчислити kP, використовуючи схему Горнера та універсальний закон додавання точок еліптичної кривої Едвардса. Точки P_1 та P_2 мають координати: $P_1(x_1,y_1)$ і $P_2(x_2,y_2)$. Обчислюючи для них суму, маємо обчислити G_4,G_5,G_6,G_7 по формулам :

$$G_4 = (dx_1x_2y_1y_2 + 1,n),$$

$$G_5 = (1 - dx_1x_2y_1y_2,n),$$

$$G_6 = (y_2y_1 - x_1x_2,n),$$

$$G_7 = (x_1y_2 + x_2y_1,n).$$

10) Якщо під час обчислень суми двох точок виникає ситуація, що один із G_4,G_5,G_6,G_7 лежить у інтервалі від 1 до n невключно, то ми знайдемо фактор p для числа n і завершимо роботу алгоритму.

11) Якщо дійшовши до етапу алгоритму 9) не було знайдено дільник для числа n, то повертаємося до кроку 1) та змінюємо початкові точки або параметр d.

Розглянемо швидкодію методу Лєнстра на кривих Едвардса.

Таблиця 1.5 – метод Лєнстра на кривих у формі Едвардса

Число n	**Час факторизації**
169	2,123 мс
124711	2,63 мс
4068289	4,44 мс
1337362643	2,75 мс
5562989473183	19,34 мс
135176122544191	100,45 мс
1351761225441923	444,54 мс
9407594505751939379	65,56 с

Аналізуючи тести для факторизації запропонованих цілих чисел, дійсно була помітна перевага цього методу у порівнянні з методом, що використовував еліптичні криві у формі Вейєрштрасса. Але потрібно наголосити, що у цьому методі використовувалася класифікація кривих Едвардса, що дещо відрізняється від тієї, що буде розглядатися у наступному розділі. У цій реалізації алгоритму не береться до уваги ще один параметр, який може дозволити покращити швидкодію методу Лєнстра на кривих у формі Едвардса.

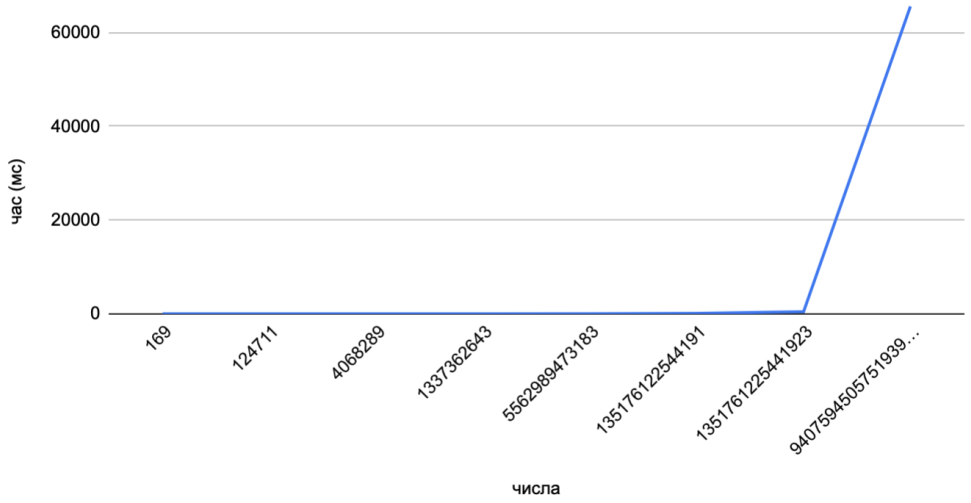

Рисунок 1.5 – швидкодія методу Лєнстра на кривих у формі Едвардса

Висновки до розділу 1

У розділі досліджено та порівняно деякі відомі алгоритми факторизації цілих чисел: метод перебору дільників, метод Ферма, $p-1$ метод Поларда, метод Лєнстра на еліптичних кривих у формі Вейєрштрасса та метод Лєнстра на кривих у формі Едвардса. У кожного із цих методів є свої переваги та недоліки. Проведений огляд показав, що останній метод факторизації з використання повних кривих Едвардса покращує швидкодію методу Лєнстра.

2 ЕЛІПТИЧНІ КРИВІ ЯК ПІДҐРУНТЯ ДЛЯ РЕАЛІЗАЦІЇ МЕТОДУ ЛЄНСТРА

У даному розділі проаналізовано існуючі наукові джерела та виділені основні визначення, теореми та описи, що відносяться до теми роботи, а саме описані основні означення та представлення еліптичних кривих, криві Едвардса та їх класифікація, основні відмінності та переваги кривої Едвардса у порівнянні з кривою у формі Вейєрштрасса.

2.1 Представлення еліптичних кривих та груповий закон

Спочатку введемо деякі означення та теореми з теорії еліптичної криптографії.

Означення 2.1. Множина R є кільцем , якщо на ній задані дві бінарні операції «+» та «·» та виконуються наступні умови :

– операція додавання є комутативною;

– дистрибутивність додавання відносно множення;

– асоціативність множення;

– існує нейтралний елемент "одиниця"у відношенні $(R,«\cdot»)$.

Означення 2.2. Полем називається комутативне кільце F, що має нейтральний елемент та для кожного елемента $a \neq 0$ існує обернений елемент $a^{-1} \in F$.

Означення 2.3. Еліптична крива розглядається над будь-яким полем F. Пара елементів (x,y) таких, що $(x,y) \in F$ називається точкою.

Означення 2.4. Еліптичною кривою над полем F називається множина точок, що задовільняють рівнянню еліптичної кривої та фіктивну точку (якщо це крива у формі Вейєрштрасса), що називається точкою на нескінченності або нейтральною точкою.

Означення 2.5. Нехай E — еліптична крива, тоді порядок кривої $N(E)$ — це порядок абелевої групи, утвореної точками еліптичної кривої відносно введеної операції додавання. Іншими словами — це кількість точок еліптичної кривої.

Означення 2.6. Порядок точки еліптичної кривої — мінімальна кількість разів, скільки потрібно додати цю точку саму з собою, щоб отримати точку на нескінечність (нейтральну точку).

Теорема 2.1. ***Теорема Хассе****. Для еліптичної кривої E заданої над простим полем F, порядок $N(E)$ групи точок даної кривої залежить від розміру поля, що визначається простим числом p і задовольняє нерівності:*

$$p + 1 - 2\sqrt{p} \leq N(E_p) \leq p + 1 + \sqrt{p}.$$

Розглянемо представлення еліптичних кривих. Нехай еліптична крива розглядається над будь-яким полем F. Вона описується рівнянням від двох змінних x та y : по y — у другій степені, по x — у третій.

Загальний вигляд рівняння еліптичної кривої :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Еліптичні криві можна виразити у багатьох формах, з цього випливає, що обчислення на еліптичних кривих можна проводити різними способами. Два найшвидших варіанти існували протягом двадцяти років, вони використовувалися у факторизації з використанням еліптичної кривої та підтверджені простоти числа :

1) Короткі криві Вейєрштрасса $y^2 = x^3 + a_4x + a_6$, з якобіанськими координатами $(X{:}Y{:}Z)$, що представляють $(X/Z^2,Y/Z^3)$, використовувалися для більшості обчислень.

2) Криві Монтгомері $By^2 = x^3 + Ax^2 + x$, де A і B — параметри в F, що задовольняють умовам $B{\neq}0$ і $A^2{\neq}4$. Точки цих кривих представлені у координатах Монтгомері $(X{:}Z)$, що представляють дві

точки $(X/Z, \pm X/Z)$, були кращим поданням для одиничного скалярного множення, і, зокрема, для обчислень в методі Лєнстра.

Картина змінилася з появою кривих Едвардса. Послідовність робіт [6],[7],[8],[9] та [10] показала, що для криптографічних застосувань криві Едвардса містять значно менше операцій множення, ніж короткі криві Вейєрштрасса в якобіанских координатах, і менше великих скалярних множень, ніж криві Монтгомері в координатах Монтгомері.

Далі розглянемо груповий закон еліптичних кривих на прикладі кривих Вейєрштрасса, а саме як вони задовільняють аксіомам, що є необхідними для виконання групової операції. Почнемо з процесу додавання точок.

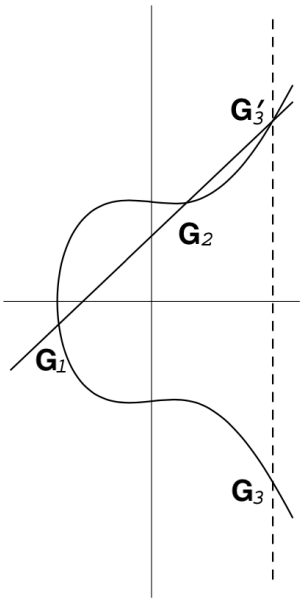

Рисунок 2.1 – додавання точок кривої

Нехай на еліптичній кривій задано дві точки і треба знайти їх суму. Еліптична крива E задається рівнянням кривої Вейєрштрасса :

$$y^2 = x^3 + Ax + B,$$

нехай точки G_1 та G_2 відповідно будуть мати такі координати :

$$G_1 = (x_1,y_1),$$

$$G_2 = (x_2,y_2).$$

Задамо точку G_3 наступним чином :

1) Будуємо пряму L так, щоб вона проходила через точки G_1 та G_2.

2) Пряма L пересікає криву E в точці $G_3^{'}$. Далі віддзеркалюємо цю точку відносно горизонтальної осі координат, так ми отримаємо G_3.

Таким чином ми отримуємо результат додовання двох точок:

$$G_1 + G_2 = G_3(x_3,y_3).$$

Вже зрозуміло, що додавання точок не виконується просто додаванням координат. Розлянемо це детальніше.

Нехай точки не будуть рівні одне одному $G_1 \neq G_2$ і не будуть нескінченно віддаленими. Розглядаємо ту ж лінію, що проведена через точки G_1 та G_2. Нахил кривої через ці точки визначається таким чином:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Нехай координати $x_1 \neq x_2$. Тоді будемо мати таке рівняння кривої L:

$$y = \lambda(x - x_1) + y_1.$$

Якщо підставити це до рівняння еліптичної кривої, то так ми отримаємо перетин кривої та прямої:

$$(\lambda x - \lambda x_1 + y_1)^2 = x^3 + Ax + B,$$

$$x^3 - \lambda^2 x^2 + 2xx_1\lambda^2 - \lambda^2 x_1^2 - y_1^2 - 2\lambda x + 2\lambda x_1 + Ax + B = 0.$$

Це рівняння має 3 корені, що відповідають 3-м точкам перетину прямої L та кривої E. В нашому випадку досить легко знайти корені

цього рівняння, так як ми вже знаємо дві із трьох точок перетину прямої з кривою. В роботі [13] вказаний досить простий спосіб знаходження коренів рівняння такого виду. А саме, якщо ми маємо кубічний многочлен $x^3 + ax^2 + bx + c$ з коренями t_1,t_2,t_3, то

$$x^3 + ax^2 + bx + c = (x - t_1)(x - t_2)(x - t_3) = x^3 - (t_1 + t_2 + t_3)x^2 + \cdots.$$

Тому,

$$t_1 + t_2 + t_3 = -a.$$

Так як ми вже знаємо два корені, то ми можемо знайти третій корінь рівняння:

$$t_3 = -a - t_1 - t_2.$$

Далі отримуємо:

$$x = \lambda^2 - x_1 - x_2$$

та

$$y = \lambda(x - x_1) + y_1$$

Тепер робимо проекцію на горизонтальну вісь координат, для того, щоб отримати точку $G_3(x_3,y_3)$:

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

Для іншого випаду, коли координати $x_1 = x_2$, але при цьому $y_1 \neq y_2$, пряма, що проходить через точки G_1 та G_2, буде знаходитися у вертикальному положені, тобто вона буде перетинати криву у точці, що буде знаходитися на бескінечності. Відображення точки на бескінечність по координатній осі OX дасть ту ж саму точку нескінченності. У цьому випадку отримаємо $G_1 + G_2 = \infty$.

Якщо розглядати випадок накладання точок або коли вони

знаходяться дуже близько одна до одної, то лінія, що буде проходити через них буде наближатися до дотичної. В такому разі, якщо точки збігаються, будемо брати пряму L як дотичну. Можемо знайти нахил прямої L використовуючи звичайне диференціювання рівняння кривої:

$$2y\frac{dy}{dx} = 3x^2 + A,$$

таким чином, можемо знайти нахил

$$\lambda = \frac{3x_1^2 + A}{2y_1}.$$

Якщо ж $y_1 = 0$, то знову отримаємо $G_1 + G_1 = \infty$. Але при цьому є один момент: якщо $y_1 = 0$, то $3x_1^2 + A$ не буде обертатися у нуль. Тому будемо вважати, що $y_1 \neq 0$. Тоді рівняння кривої буде мати такий вигляд як і раніше:

$$y = \lambda(x - x_1) + y_1.$$

Знову підставляємо у вже відоме кубічне рівняння. Тепер маємо лише один корінь x_1, що є подвійним. У цьому випадку отримуємо:

$$x_3 = \lambda^2 - 2x_1,$$

$$y_3 = \lambda x_1 - \lambda x_3 - y_1.$$

Врешті-решт, припустимо, що $G_2 = \infty$. Лінія, що проходить через G_1 і ∞, являє собою вертикальну лінію, що перетинає криву E у точці G_1', що є відображенням G_1 по координатній осі x. У випадку коли відображаємо G_1' по осі OX, щоб отримати $G_3 = G_1 + G_2$, повертаємося до G_1. Отже,

$$G_1 = \infty + G_1$$

для всіх точок G_1 на кривій.

Якщо підсумувати все вище сказане, то отримаємо груповий закон:

Нехай для прикладу крива задається таким рівнянням:

$$y^2 = x^3 + ax + b.$$

Точки G_1 та G_2 належать кривій. $G_1 = (x_1,y_1)$ та $G_2 = (x_2,y_2)$ і вони не дорівнюють нескінченності. Задамо $G_3(x_3,y_3) = G_2 + G_1$. Тоді:

1) У випадку якщо $x_1 \neq x_2$, то отримуємо такі координати для точки G_3:

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = \lambda x_1 - \lambda x_3 - y_1,$$

де коефіцієнт нахилу дорівнює $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.

2) У випадку якщо $x_1 = x_2$, але при цьому $y_1 \neq y_2$, то отримуємо

$$G_1 + G_2 = \infty.$$

3) Якщо точки G_1 та G_2 рівні та $y_1 \neq 0$, то маємо

$$x_3 = \lambda^2 - 2x_1,$$

$$y_3 = \lambda x_1 - \lambda x_3 - y_1,$$

де коефіцієнт нахилу $\lambda = \frac{3x_1^2 + a}{2y_1}$.

4) У останньому випадку точки G_1 та G_2 рівні і $y_1 = 0$, тоді отримуємо

$$\infty = G_1 + G_2.$$

2.2 Координати точок еліптичних кривих

Роль основної математичної функції у криптографії виконує операція множення точки еліптичної кривої на скаляр, що в своїй основі має операцію додавання точок кривої. Отже, на швидкість цієї операції дуже сильно впливає операція додавання точок. Якщо змінити

координати представлення точки кривої, то можна зменшити кількість "важких" операцій та, у свою чергу, збільшити швидкість обчислень.

Криву на площині можна задати за допомогою афінних та проективних координат.

Розглянемо афінні координати. Нехай крива задається над полем p таким чином :

$$E : y^2 = x^3 + a_4x + a_6$$

Для точки (x_1,y_1) на кривій E протилежною є $(x_1,-y_1)$.

Для початку розглянемо додавання двох точок P, Q і $P \neq \pm Q$.

Нехай $P=(x_1,y_1)$, $Q=(x_2,y_2)$, $P+Q=(x_3,y_3)$. У цьому випадку додавання задається таким чином :

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = \lambda(x_1 - x_3) - y_1,$$

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2}.$$

При подвоєнні точки кривої $2P=(x_3,y_3)$ маємо такі результати:

$$x_3 = \lambda^2 - 2x_1,$$

$$y_3 = \lambda(x_1 - x_3) - y_1,$$

$$\lambda = \frac{3x_1^2 + a_4}{2y_1}.$$

Виходячи із цих формул можна легко побачити скільки потрібно операцій для додавання: 6 віднімань, 1 піднесення до квадрату, 1 ділення та 1 множення. Та скільки потрібно операцій для подвоєння точки: 3

віднімання, 1 додавання, 2 піднесення до квадрату, 1 ділення та 1 множення. Найбільшу трудомісткість із перечислених операцій має ділення. За досить великої кількості додавань, стає помітний вплив цієї операції на швидкість роботи криптосистеми. Одним із можливих способів зменшення впливу операції ділення на швидкодію системи, є перехід до проективних координат.

Розглянемо проективні координати. В цих координатах рівняння E має такий вигляд:

$$Y^2Z = X^3 + a_4XZ^2 + a_6Z^3.$$

Точці (X_1,Y_1,Z_1) на E ставиться у відповідність точка з афінними координатами $(\frac{X_1}{Z_1},\frac{Y_1}{Z_1})$, де $Z_1 \neq 0$ і точка на бескінечності має координати (0,1,0). Для точки $(X_1{:}Y_1{:}Z_1)$ протилежною є $(X_1{:}-Y_1{:}Z_1)$.

Додавання точок:

Нехай $P{=}(X_1,Y_1,Z_1)$, $Q{=}(X_2,Y_2,Z_2)$ і $P \neq \pm Q$, а $P{+}Q{=}(X_3,Y_3,Z_3)$. Далі покладемо

$$A = Y_2Z_1 - Y_1Z_2,$$

$$B = X_2Z_1 - X_1Z_2,$$

$$C = A^2Z_1Z_2 - B^3 - 2B^2X_1Z_2$$

Таким чином маємо

$$X_3 = BC,$$

$$Y_3 = A(B^2X_1Z_2 - C) - B^3Y_1Z_2,$$

$$Z_3 = B^3Z_1Z_2.$$

Подвоєння точки:

Нехай $2P{=}(X_3{:}Y_3{:}Z_3)$, тоді маємо

$$A = a_4Z_1^2 + 3X_1^2,$$

$$B = Y_1 Z_1,$$

$$C = X_1 Y_1 B,$$

$$D = A^2 - 8C$$

і

$$X_3 = 2BD,$$

$$Y_3 = A(4C - D) - 8Y_1^2 B^2,$$

$$Z_3 = 8B^3.$$

Таким чином операція ділення тут не задіяна, і час виконання операцій дорівнює часу 12-ти множень та 2-х віднімань для додавання двох різних точок і часу 7-ми множень та 5-х віднімань для подвоєння. Якщо одна із вхідних точок для додавання задається формулою $(X_2{:}Y_2{:}1)$, тобто безпосередньо перетворюється з афінних координат, то вимоги для операції додавання зменшуються до часу виконная 9-ти множень та 2-х віднімань.

2.3 Ізоморфізм множин точок еліптичної кривої

Нехай p та q це непарні цілі числа, $n = pq$ і $gcd(q,p) = 1$. Еліптична крива E задана над Z_n. Тоді існує груповий ізоморфізм

$$E(Z_n) \simeq E(Z_p) \oplus E(Z_q) \text{ [12].}$$

Розглянемо це більш детальніше. Нехай еліптична крива E задана таким рівнянням:

$$y^2 z = x^3 + axz^2 + bz^3, \text{ де } \quad a,b \in Z_n \text{ і } 4a^3 + 27b^2 \in Z_n.$$

Тоді ми можемо розглядати a та b як елементи Z_p та Z_q, де також виконується, що $4a^3 + 27b^2$ належить Z_p^* і Z_q^*. В такому випадку ми можемо

розглядати еліптичну криву над Z_p та Z_q одночасно.

Китайська теорема про лишки стверджує, що існує ізоморфізм кілець

$$Z_n \simeq Z_p \oplus Z_q, \text{ де n=pq.}$$

Тобто маємо:

$$x \mod n \Longleftrightarrow (x \mod p, x \mod q).$$

$$y^2z \equiv x^3 + axz^2 + bz^3 \mod n \Longleftrightarrow$$

$$\begin{cases} y^2z \equiv x^3 + axz^2 + bz^3 \mod p \\ y^2z \equiv x^3 + axz^2 + bz^3 \mod q \end{cases}$$

При цьому існує бієкція

$$\psi : E(Z_n) \longrightarrow E(Z_p) \oplus E(Z_q).$$

Тепер треба зрозуміти чи є це відображення гомоморфізмом? В роботі [12] для вирішення цього питання розглядають точки кривої, які задані в однорідній системі координат. Нехай $(x_i,y_i,z_i) \in E(Z_n)$. Маємо для розгляду такі набори рівнянь:

1)

$$x_3^i = (x_1y_2 - x_2y_1)(y_1z_2 + y_2z_1) + (x_1z_2 - x_2z_1)y_1y_2$$
$$-a(x_1z_2 + x_2z_1)(x_1z_2 - x_2z_1) - 3b(x_1z_2 - x_2z_1)z_1z_2,$$

$$y_3^i = -3x_1x_2(x_1y_2 - x_2y_1) - y_1y_2(y_1z_2 - y_2z_1) - a(x_1y_2 - x_2y_1)z_1z_2$$
$$+a(x_1z_2 + x_2z_1)(y_1z_2 - y_2z_1) + 3b(y_1z_2 - y_2z_1)z_1z_2,$$

$$z_3^i = 3x_1x_2(x_1z_2 - x_2z_1) - (y_1z_2 + y_2z_1)(y_1z_2 - y_2z_1)$$
$$+a(x_1z_2 - x_2z_1)z_1z_2;$$

2)

$$x_3^{ii} = y_1y_2(x_1y_2 + x_2y_1) - ax_1x_2(y_1z_2 + y_2z_1)$$
$$-a(x_1y_2 + x_2y_1)(x_1z_2 + x_2z_1) - 3b(x_1y_2 + x_2y_1)z_1z_2$$
$$-3b(x_1z_2 + x_2z_1)(y_1z_2 + y_2z_1) + a^2(y_1z_2 + y_2z_1)z_1z_2,$$

$$y_3^{ii} = y_2^2y_2^2 + 3ax_1^2x_2^2 + 9bx_1x_2(x_1z_2 + x_2z_1)$$
$$-a^2x_1z_2(x_1z_2 + 2x_2z_1) - a^2x_2z_1(2x_1z_2 + x_2z_1)$$
$$-3abz_1z_2(x_1z_2 + x_2z_1) - (a^3 + 9b^2)z_1^2z_2^2,$$

$$z_3^{ii} = 3x_1x_2(x_1y_2 + x_2y_1) + y_1y_2(y_1z_2 + y_2z_1) + a(x_1y_2 + x_2y_1)z_1z_2$$
$$+a(x_1z_2 + x_2z_1)(y_1z_2 + y_2z_1) + 3b(y_1z_2 + y_2z_1)z_1z_2;$$

3)

$$x_3^{iii} = (x_1y_2 + x_2y_1)(x_1y_2 - x_2y_1) + ax_1x_2(x_1z_2 - x_2z_1)$$
$$+3b(x_1z_2 - x_2z_1)(x_1z_2 - x_2z_1) - a^2(x_1z_2 - x_2z_1)z_1z_2,$$

$$y_3^{iii} = (x_1y_2 - x_2y_1)y_1y_2 - 3ax_1x_2(y_1z_2 - y_2z_1)$$
$$+a(x_1y_2 + x_2y_1)(x_1z_2 - x_2z_1) + 3b(x_1y_2 - x_2y_1)z_1z_2$$
$$-3b(x_1z_2 + x_2z_1)(y_1z_2 - y_2z_1) + a^2(y_1z_2 - y_2z_1)z_1z_2,$$

$$z_3^{iii} = -(x_1y_2 + x_2y_1)(y_1z_2 - y_2z_1) - (x_1z_2 - x_2z_1)y_1y_2$$
$$-a(x_1z_2 + x_2z_1)(x_1z_2 - x_2z_1) - 3b(x_1z_2 - x_2z_1)z_1z_2.$$

Можемо утворити таку матрицю:

$$\begin{pmatrix} x_3^i & y_3^{ii} & z_3^{iii} \\ x_3^i & y_3^{ii} & z_3^{iii} \\ x_3^i & y_3^{ii} & z_3^{iii} \end{pmatrix}$$

Вона є примітивною і кожен її субдетермінант розмірності 2 є рівним нулю.

Якщо ми покладемо G_1,$G_2 \in E(Z_n)$ і $G_1 + G_2 = G_3$. То це буде означати, що існує лінійна комбінація для виходів із формул, що розглядалися вище. Вона є примітивною і допомагає отримати координати для точки G_3. Якщо скоротити всі ці обчислення по $modp$ та $modq$, то ми отримуємо такий самий результат. Бачимо, що точка G_3 є сумою G_1 та G_2 по модулю p та q. Таким чином показали, що відображення ψ є гомоморфізмом [12].

2.4 Еліптичні криві у формі Едвардса та їх класифікація

Нехай F - скінченне поле, (char(F)≠2). Крива у формі Едвардса задається рівнянням в афінних координатах:

$$E : x^2 + y^2 = 1 + dx^2y^2 \text{ , } d \in F\backslash\{0,1\} \qquad (2.1)$$

Нас цікавлять саме криві Едвардса, які мають обмеження на параметр кривої, а саме d не є квадратичним лишком. Це гарантує повноту закону додавання, який заданий над точками кривої (2.1). Сума двох точок з координатами (x_1,y_1), (x_2,y_2) задається формулою:

$$(x_1,y_1) + (x_2,y_2) \Rightarrow (\mathrm{x}_3,y_3)$$

$$x_3 = \frac{(x_1y_2 + x_2y_1)}{(1 + dy_1y_2x_1x_2)}$$

(2.2)

$$y_3 = \frac{(y_1y_2 - x_1x_2)}{(1 - dy_1y_2x_1x_2)}$$

Таким чином, якщо d квадратичний нелишок у полі F, то закон (2.2) буде коректний для будь-яких точок (x_1,y_1), (x_2,y_2), включаючи однакові точки, обернені точки і нейтральну точку = (0,1). Доведено [11], що $\forall y_1,y_2,x_1,x_2 \in F$: $(1 - dy_1y_2x_1x_2) \neq 0$ і $(1 + dy_1y_2x_1x_2) \neq 0$.

Розглянемо класифікацію кривих у формі Едвардса та їх точки. Шляхом введення додаткового параметра a можна задати скручену криву Едвардса :

$$E_{a,d}\text{: } x^2 + ay^2 = 1 + dx^2y^2,\ a,d \in F_p^*\ ,\ \text{p} \neq 2 \qquad (2.3)$$

Модифікований закон додавання точок залишається таким самим, але з додаванням нового параметра a:

$$(x_1,y_1) + (x_2,y_2) = \left(\frac{x_1x_2 - ay_1y_2}{1 - dy_1y_2x_1x_2}\right), \left(\frac{x_1y_2 + ax_2y_1}{1 + dy_1y_2x_1x_2}\right) \qquad (2.4)$$

Якщо точки кривої співпадають, то отримуємо такий закон подвоєння точок :

$$2(x_1,y_1) = \left(\frac{x_1^2 - ay_1^2}{(1 - dy_1^2x_1^2)}\right), \left(\frac{2x_1y_1}{(1 + dy_1^2x_1^2)}\right) \qquad (2.5)$$

Класифікація кривих Едвардса проводиться шляхом різних варіацій пар параметрів a та d кривої (2.3). Можливі такі випадки :

1) $\left(\frac{ad}{p}\right) = -1$.

1.1) $\left(\frac{a}{p}\right) = 1$, $\left(\frac{d}{p}\right) = -1$.

1.2) $\left(\frac{a}{p}\right) = -1$, $\left(\frac{d}{p}\right) = 1$.

2) $\left(\frac{ad}{p}\right) = 1$.

2.1) $\left(\frac{a}{p}\right) = -1$, $\left(\frac{d}{p}\right) = -1$.

2.2) $\left(\frac{a}{p}\right) = 1$, $\left(\frac{d}{p}\right) = 1$.

Маємо такі види кривих :

- Повні криві Едвардса (з умовами п. 1).
- Криві Едвардса з квадратичним параметром (з умовами п. 2.2).
- Скручені криві Едвардса (з умовами п. 2.1).

Розглянемо точки в залежності від класу кривої Едвардса та кількість особливих точок для них.

Повні криві Едвардса:

У цьому випадку існують такі точки: точка, що лежить на осі координатної площини OX $\mathbf{D_0}$ = (-1,0). Вона має порядок 2, це можна перевірити, якщо підставити точку до формули (3); та дві точки, що лежать на координатній осі OY $\pm\mathbf{F_0} = (0,\pm 1/\sqrt{a})$. Ці точки мають порядок 4 та існують при умові, що a квадрат. Якщо ж квадрат d, то точки приймають такий вигляд $\pm\mathbf{F_0} = (0,\pm 1/\sqrt{d})$ [13].

Скручені криві Едвардса :

Теорема 2.2. *Будь-яка скручена крива Едвардса (2.3) біраціонально еквівалентна кривій у формі Монтгомері [13].*

Тому криву Едвардса можна представити таким чином:

$$\mathbf{M}_{A,B} : Bv^2 = u^3 + Au^2 + u, \text{ де}$$

$$A = 2\frac{a+d}{a-d}\ ,\ B = \frac{4}{a-d},$$

$$a = \frac{A+2}{B}\ ,\ d = \frac{A-2}{B},\ A^2 \neq 4.$$

Проводиться заміна координат :

$$y = \frac{u}{v}\ ,\ x = \frac{u-1}{u+1} \Rightarrow u = \frac{1+x}{1-x}\ ,\ v = \frac{u}{y}. \qquad (2.6)$$

Використовуючи **Теорему 1.2**, маємо $(Bad)^2 = (A+2)(A-2)$. Дискрімінант рівняння правої частини — квадрат. Тоді рівняння $0 = u^3 + Au^2 + u$ має три кореня: 0 та $-A \pm \sqrt{A^2-4}/2$, які належать F_p. В свою чергу крій Монтгомері належать такі точки: $\mathbf{D_{M0}}$ = (0,0) та $\mathbf{D_{M12}} = ((A \pm \sqrt{A^2-4}/2,0)$.

Якщо використати заміну координат (2.6), то точка $\mathbf{D_{M0}}$ перейде у точку $\mathbf{D_0}$ = $(-1,0)$, а точки $\mathbf{D_{M12}}$ будуть відображатися у $\mathbf{D_{12}}$ = $(\pm\sqrt{\frac{a}{d}},\infty)$. Знак бескінечності y − координати виникає через

ділення на нуль в заміні $y = \frac{u}{v}$. Точки $\mathbf{D_{12}}$ вважаються особливими. Разом із цими точками виникають ще чотири точки 4-го порядку при умові $p \equiv 3mod4$: $\pm\mathbf{F_{23}} = (\pm\sqrt[4]{\frac{a}{d}},\pm\sqrt{\frac{-1}{\sqrt{ad}}})$ [13].

Як бачимо, що у випадку скрученої кривої Едвардса виникають три точки 2-го порядку із який дві є особливими точками. При умові $p \equiv 3mod4$ додатково можна отримати чотири точки 4-го порядку.

Криві Едвардса з квадратичним параметром:

Так само як і у випадку скручених кривих маємо три точки 2-го порядку з тими ж самими координатами: $\mathbf{D_0} = (-1,\, 0)$, $\mathbf{D_{12}} = (\pm\sqrt{\frac{a}{d}},\infty)$. Додатково виникають дві точки на осі координат OY $\pm\mathbf{F_0} = (0, \pm\, \frac{1}{\sqrt{a}})$, вони мають 4-тий порядок. Якщо із рівняння кривої виділити квадрати :

$$x^2 = \frac{1 - ay^2}{1 - dy^2}\ , \quad y^2 = \frac{1 - x^2}{a - dx^2},$$

то отримуємо вираз для двох особливих точок 4-го порядку $\pm\mathbf{F_1} = (\infty, \pm\, \frac{1}{\sqrt{d}})$. А при $p \equiv 1mod4$ та $ad = c^4$ також є чотири точки 4-го порядку $\pm\mathbf{F_{23}} = (\pm\sqrt[4]{\frac{a}{d}}, \pm\, \sqrt{\frac{-1}{\sqrt{ad}}})$ [13].

Криві з вадратичним параметром мають три точки 2-го порядку, серед яких дві є особливими точками. Також завжди є чотири або вісім точко 4-го порядку, серед яких теж є дві особливі точки.

Перерахуємо переваги та недоліки кривої Едвардса у порівнянні з кривою Вейєрштрасса:

1) Криві Едвардса мають властивість універсальності закону додавання. Операції додавання двох різних точок та подвоєння точки задаються однією формулою :

$$(x_1,y_1) + (x_2,y_2) \Rightarrow (\mathrm{x}_3,y_3)$$

$$x_3 = \frac{(x_1y_2 + x_2y_1)}{(1 + dy_1y_2x_1x_2)}$$

$$y_3 = \frac{(y_1y_2 - x_1x_2)}{(1 - dy_1y_2x_1x_2)}$$

2) Відсутність нескінченно віддаленої точки. За нейтральний елемент береться точка кривої Едвардса, що має координати (0,1).

3) Група E_p є циклічною.

4) Порядок групи E_p ділиться на 4. Ця властивість кривої Едвардса вважається її незначним недоліком, тому що її підгрупа, що має простий великий порядок, на базі якої будуються криптосистеми, буде мати мінімум у 4 рази менше точок, аніж вся група. З цього випливає, що мінімум три чверті точок є "не потрібними".

5) Досить велика швидкість додавання точок кривої. Взагалі кажучи, це найголовніша перевага цих кривих. Виконуючи операцію додавання двох точок, що не є однаковими, ми зробимо у 1,5 рази менше бітових операцій, ніж при цій же операції при використанні криві у формі Вейєрштрасса; під час подвоєння точки кривої загальна кількість операцій над бітами стає ще менше.

6) Стандартизований закону додавання точок. Формули для додавання точок кривої Едвардса мають однаковий вигляд як для подвоєння точки, так і для додавання різних точок. Таким чином, ми отримуємо досить високу захищеність криптосистем на кривих Едвардса проти атак, що визначають число, на яке множиться точка кривої.

Висновки до розділу 2

У цьому розділі проаналізовані джерела та наведені поняття, що використовуються в роботі, а саме описані основні означення щодо еліптичних кривих, груповий закон додавання точок еліптичної кривої, ізоморфізм множин точок еліптичної кривої. Досліджено класи кривих Едвардса в залежності від їх параметрів та переваги цих кривих у порівнянні із кривими Вейєрштрасса.

3 ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ЕЛІПТИЧНИХ КРИВИХ ЕДВАРДСА

У цьому розділі розглянуто залежність властивостей еліптичних кривих у формі Едвардса над кільцем $n = pq$. Досліджено властивості кривих Едвардса в залежності від параметрів кривої, в тому числі наявність особливих точок. Отримано оцінки кількості таких точок для всіх можливих випадків значень коефіцієнтів кривої Едвардса для випадку $n = pq$ та вказано тип кривих, що має їх найбільше. На основі цього запропоновано модифікований алгоритм Лєнстра з використанням цих кривих.

3.1 Особливі точки повних кривих Едвардса над кільцем $n = pq$

Подамо криву Едвардса $E_{a,d,n}$ за допомогою рівняння:

$$E_{a,d,n} : x^2 + ay^2 \equiv 1 + dx^2y^2(mod n).$$

$$E_{a,d,n} : \begin{cases} \mathrm{x}^2 + ay^2 = 1 + dx^2y^2(mod p); \\ \mathrm{x}^2 + ay^2 = 1 + dx^2y^2(mod q). \end{cases} \qquad (3.1)$$

Вона буде класифікована як повна у випадку:

$$\left(\frac{a}{n}\right) = -1, \ \left(\frac{d}{n}\right) = 1 \text{ або}$$

$$\left(\frac{a}{n}\right) = 1, \ \left(\frac{d}{n}\right) = -1.$$

Розглянемо всі можливі комбінації для коефіцієнтів кривої Едвардса, щоб у результаті отримати повну криву Едвардса над кільцем $n = pq$:

"квадратична"×"повна"= "повна":

$$\left(\frac{a}{p}\right) = 1,\ \left(\frac{a}{q}\right) = 1\ , \left(\frac{d}{p}\right) = 1,\ \left(\frac{d}{q}\right) = -1 \Rightarrow \left(\frac{a}{n}\right) = 1\ , \left(\frac{d}{n}\right) = -1,$$

"квадратична"× "повна"= "повна":

$$\left(\frac{a}{p}\right) = 1,\ \left(\frac{a}{q}\right) = -1\ , \left(\frac{d}{p}\right) = 1,\ \left(\frac{d}{q}\right) = 1 \Rightarrow \left(\frac{a}{n}\right) = -1\ , \left(\frac{d}{n}\right) = 1,$$

"повна"× "квадратична"= "повна":

$$\left(\frac{a}{p}\right) = 1,\ \left(\frac{a}{q}\right) = 1\ , \left(\frac{d}{p}\right) = -1,\ \left(\frac{d}{q}\right) = 1 \Rightarrow \left(\frac{a}{n}\right) = 1\ , \left(\frac{d}{n}\right) = -1,$$

"повна"× "квадратична"= "повна":

$$\left(\frac{a}{p}\right) = -1,\ \left(\frac{a}{q}\right) = 1\ , \left(\frac{d}{p}\right) = 1,\ \left(\frac{d}{q}\right) = 1 \Rightarrow \left(\frac{a}{n}\right) = -1\ , \left(\frac{d}{n}\right) = 1.$$

Повна крива Едвардса для простого поля не має особливих точок. Крива з квадратичним параметром у простому полі має 4-ри особливі точки. Введемо позначення кількості звичайних точок для кривих E_p та E_q: $|E_p|$ та $|E_q|$ відповідно. Також введемо позначення кількості особливих точок для E_n: $|E_n|$.

Оцінемо приблизну кількість точок для кожної кривої E_p та E_q за теоремою Хассе:

$$(\sqrt{p} - 1)^2 \leq |E_p| \leq (\sqrt{p} + 1)^2,$$

$$(\sqrt{q} - 1)^2 \leq |E_q| \leq (\sqrt{q} + 1)^2.$$

Загальна кількість точок для кривої E_n: $|E_p| \cdot |E_q|$.

Отримаємо приблизну кількість особливих точок для E_n:

$$E_p \times E_q = E_n, \qquad (3.2)$$

"квадратична"×"повна"= "повна":

$$4|E_q| - 4 = |E_n|, \qquad (3.3)$$

"повна"× "квадратична"= "повна":

$$4|E_p| - 4 = |E_n|. \qquad (3.4)$$

Також повну криву Едвардса над кільцем $n = pq$ можна отримати такими способами:

"скручена"×"повна"= "повна":

$$\left(\frac{a}{p}\right) = 1,\ \left(\frac{a}{q}\right) = -1\ , \left(\frac{d}{p}\right) = -1,\ \left(\frac{d}{q}\right) = -1 \Rightarrow \left(\frac{a}{n}\right) = -1\ , \left(\frac{d}{n}\right) = 1,$$

"скручена"×"повна"= "повна":

$$\left(\frac{a}{p}\right) = -1,\ \left(\frac{a}{q}\right) = -1\ , \left(\frac{d}{p}\right) = 1,\ \left(\frac{d}{q}\right) = -1 \Rightarrow \left(\frac{a}{n}\right) = 1\ , \left(\frac{d}{n}\right) = -1,$$

"повна"×"скручена"= "повна":

$$\left(\frac{a}{p}\right) = -1,\ \left(\frac{a}{q}\right) = 1\ , \left(\frac{d}{p}\right) = -1,\ \left(\frac{d}{q}\right) = -1 \Rightarrow \left(\frac{a}{n}\right) = -1\ , \left(\frac{d}{n}\right) = 1,$$

"повна"×"скручена"= "повна":

$$\left(\frac{a}{p}\right) = -1,\ \left(\frac{a}{q}\right) = -1\ , \left(\frac{d}{p}\right) = -1,\ \left(\frac{d}{q}\right) = 1 \Rightarrow \left(\frac{a}{n}\right) = 1\ , \left(\frac{d}{n}\right) = -1.$$

Скручена крива Едвардса над простим полем має 2 особливі точки. Отримаємо приблизну кількість особливих точок для кривої E_n(3.2):

"скручена"×"повна"= "повна":

$$2|E_q| - 2 = |E_n|, \qquad (3.5)$$

"повна"×"скручена"= "повна":

$$2|E_p| - 2 = |E_n|. \qquad (3.6)$$

3.2 Особливі точки скручених кривих Едвардса над кільцем $n = pq$

Продовжуємо розглядати криву Едвардса E_n (3.1).

Вона буде класифікована як скручена крива, якщо

$$\left(\frac{a}{n}\right) = -1, \ \left(\frac{d}{n}\right) = -1.$$

Розглянемо всі можливі комбінації для коефіцієнтів кривої Едвардса, щоб у результаті отримати скручену криву Едвардса над кільцем $n = pq$:

"квадратична"×"скручена"= "скручена":

$$\left(\frac{a}{p}\right) = 1, \ \left(\frac{a}{q}\right) = -1 \ , \left(\frac{d}{p}\right) = 1, \ \left(\frac{d}{q}\right) = -1 \Rightarrow \left(\frac{a}{n}\right) = -1 \ , \left(\frac{d}{n}\right) = -1,$$

"скручена"×"квадратична"= "скручена":

$$\left(\frac{a}{p}\right) = -1, \ \left(\frac{a}{q}\right) = 1 \ , \left(\frac{d}{p}\right) = -1, \ \left(\frac{d}{q}\right) = 1 \Rightarrow \left(\frac{a}{n}\right) = -1 \ , \left(\frac{d}{n}\right) = -1.$$

У випадку простого поля крива Едвардса з квадратичним параметром має 4 особливі точки, а скручена крива 2 особливі точки. Оцінемо кількість особливих точок для кривої E_n (3.2):

"квадратична"×"скручена"= "скручена":

$$4|E_q| + 2|E_p| - 2 \cdot 4 = |E_n|, \qquad (3.7)$$

"скручена"×"квадратична"= "скручена":

$$2|E_q| + 4|E_p| - 2 \cdot 4 = |E_n|. \qquad (3.8)$$

Розглянемо дві останні комбінації за допомогою яких ми можемо отримати скручену криву Едвардса над кільцем $n = pq$:

"повна"× "повна"= "скручена":

$$\left(\frac{a}{p}\right) = 1,\ \left(\frac{a}{q}\right) = -1\ , \left(\frac{d}{p}\right) = -1,\ \left(\frac{d}{q}\right) = 1 \Rightarrow \left(\frac{a}{n}\right) = -1\ , \left(\frac{d}{n}\right) = -1,$$

"повна"× "повна"= "скручена":

$$\left(\frac{a}{p}\right) = -1,\ \left(\frac{a}{q}\right) = 1\ , \left(\frac{d}{p}\right) = 1,\ \left(\frac{d}{q}\right) = -1 \Rightarrow \left(\frac{a}{n}\right) = -1\ , \left(\frac{d}{n}\right) = -1.$$

У цих випадках ми не будемо мати особливих точок, так як крива E_n складається із декартового добутку повних кривих над простими полями, які не мають особливих точок.

3.3 Особливі точки кривих Едвардса з квадратичним параметром над кільцем $n = pq$

Нехай крива Едвардса E_n задана за допомогою рівняння (3.1).

Вона буде класифікована як крива з квадратичним параметром, якщо

$$\left(\frac{a}{n}\right) = 1,\ \left(\frac{d}{n}\right) = 1.$$

Розглянемо всі можливі комбінації для коефіцієнтів кривої Едвардса, щоб у результаті отримати криву Едвардса з квадратичним параметром над кільцем $n = pq$:

"повна"× "повна"= "квадратична":

$$\left(\frac{a}{p}\right) = 1,\ \left(\frac{a}{q}\right) = 1\ , \left(\frac{d}{p}\right) = -1,\ \left(\frac{d}{q}\right) = -1 \Rightarrow \left(\frac{a}{n}\right) = 1\ , \left(\frac{d}{n}\right) = 1,$$

"повна"× "повна"= "квадратична":

$$\left(\frac{a}{p}\right) = -1,\ \left(\frac{a}{q}\right) = -1\ , \left(\frac{d}{p}\right) = 1,\ \left(\frac{d}{q}\right) = 1 \Rightarrow \left(\frac{a}{n}\right) = 1\ , \left(\frac{d}{n}\right) = 1.$$

У цих випадках крива E_n не буде мати особливих точок. Розглянемо два інші випадки, за допомогою яких може утворитися квадратична крива

над кільцем $n = pq$:

"квадратична"×"квадратична"= "квадратична":

$$\left(\frac{a}{p}\right) = 1,\ \left(\frac{a}{q}\right) = 1\ , \left(\frac{d}{p}\right) = 1,\ \left(\frac{d}{q}\right) = 1 \Rightarrow \left(\frac{a}{n}\right) = 1\ , \left(\frac{d}{n}\right) = 1,$$

"скручена"×"скручена"= "квадратична":

$$\left(\frac{a}{p}\right) = -1,\ \left(\frac{a}{q}\right) = -1\ , \left(\frac{d}{p}\right) = -1,\ \left(\frac{d}{q}\right) = -1 \Rightarrow \left(\frac{a}{n}\right) = 1\ , \left(\frac{d}{n}\right) = 1.$$

Знаємо, що кількість особливих точок для квадратичної кривої дорівнює 4-ом, а для скрученої 2-м. Оцінемо кількість особливих точок для E_n (3.2):

"квадратична"×"квадратична"= "квадратична":

$$4|E_q| + 4|E_p| - 4 \cdot 4 = |E_n|, \qquad (3.9)$$

"скручена"×"скручена"= "квадратична":

$$2|E_q| + 2|E_p| - 2 \cdot 2 = |E_n|. \qquad (3.10)$$

3.4 Застосування результатів для удосконалення методу Лєнстра

Найбільшу кількість особливих точок мають еліптичні криві Едвардса з квадратичним параметром (3.9). Отже, використовуючи їх для факторизації цілих чисел у методі Лєнстра, ми можемо пришвидшити цей метод. Запропонуємо вибір параметрів a та d так, щоб отримати квадратичну криву над кільцем $n = pq$ з максимальною кількістю особливих точок.

Нас цікавить випадок "квадратична"×"квадратична"= "квадратична":

Таблиця 3.1 – класифікація кривих Едвардса над кільцем $n = pq$ в залежності від значень символів Лежандра для параметрів a та d за простими модулями

×	$\left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = 1$	$\left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = -1$	$\left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = 1$	$\left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = -1$
$\left(\frac{a}{q}\right) = 1, \left(\frac{d}{q}\right) = 1$	"квадратична"	"повна"	"повна"	"скручена"
$\left(\frac{a}{q}\right) = 1, \left(\frac{d}{q}\right) = -1$	"повна"	"квадратична"	"скручена"	"повна"
$\left(\frac{a}{q}\right) = -1, \left(\frac{d}{q}\right) = 1$	"повна"	"скручена"	"квадратична"	"повна"
$\left(\frac{a}{q}\right) = -1, \left(\frac{d}{q}\right) = -1$	"скручена"	"повна"	"повна"	"квадратична"

Таблиця 3.2 – оцінка кількості особливих точок для кожного класу кривих Едвардса над кільцем $n = pq$

×	$\left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = 1$	$\left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = -1$	$\left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = 1$	$\left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = -1$
$\left(\frac{a}{q}\right) = 1, \left(\frac{d}{q}\right) = 1$	$4\lvert Ep\rvert + 4\lvert Eq\rvert - 4 \cdot 4$	$4\lvert Eq\rvert - 4$	$4\lvert Eq\rvert - 4$	$2\lvert Ep\rvert + 4\lvert Eq\rvert - 2 \cdot 4$
$\left(\frac{a}{q}\right) = 1, \left(\frac{d}{q}\right) = -1$	$4\lvert Ep\rvert - 4$	0	0	$2\lvert Ep\rvert - 2$
$\left(\frac{a}{q}\right) = -1, \left(\frac{d}{q}\right) = 1$	$4\lvert Ep\rvert - 4$	0	0	$2\lvert Ep\rvert - 2$
$\left(\frac{a}{q}\right) = -1, \left(\frac{d}{q}\right) = -1$	$4\lvert Ep\rvert + 2\lvert Eq\rvert - 2 \cdot 4$	$2\lvert Eq\rvert - 2$	$2\lvert Eq\rvert - 2$	$2\lvert Ep\rvert + 2\lvert Eq\rvert - 2 \cdot 2$

$$\left(\frac{a}{p}\right) = 1,\ \left(\frac{a}{q}\right) = 1\ , \left(\frac{d}{p}\right) = 1,\ \left(\frac{d}{q}\right) = 1 \Rightarrow \left(\frac{a}{n}\right) = 1\ , \left(\frac{d}{n}\right) = 1.$$

Перспективним є використання таких параметрів кривих, щоб їх символи Лежандра за будь-яким простим модулем мали значення 1. Нехай $n = pq$, де p,q — різні прості числа.

$$\begin{cases} (a,n) = 1 \quad , a \text{ — кв. лишок за модулем } n \Rightarrow \left(\frac{a}{n}\right) = 1 \\ (d,n) = 1 \quad , d \text{ — кв. лишок за модулем } n \Rightarrow \left(\frac{d}{n}\right) = 1 \end{cases}$$

Для виконання цих умов параметри a,d мають набувати таких значень:

$$4,9,16,k^2,\ldots \text{ , де } k \in \mathbb{N}\backslash\{1\}.$$

Так як для любого простого p символ Лежандра буде набувати додатного значення для любого k^2, $k \in \mathbb{N}\backslash\{1\}$.

Розглянемо модифікований алгоритм, враховуючи отримані результати.

Метод Лєнстра з використанням кривих Едвардса з квадратичним параметром

$$\mathbf{E}: x^2 + ay^2 = 1 + dx^2y^2,\ \left(\frac{a}{n}\right) = 1,\ \left(\frac{d}{n}\right) = 1,$$

a,$d \in \{4,9,16,k^2,...\}$, де $k \in \mathbb{N}\backslash\{1\}$.

вхід: складене натуральне число n.

вихід: нетривіальний дільник p для числа n.

1) Навмання обираємо $x^{'}$ та $y^{'}$ в інтервалі від 2 до $n-1$. За допомогою $x^{'}$ обчислюємо $y^{'}$. Якщо точки з такою $x^{'}$ координатою немає, то обрати нове значення $x^{'}$.

2) Обчислити $R_1 = (x^{'},n)$ та $R_2 = (y^{'},n)$. Якщо ж один із R_1, R_2 лежить у інтервалі від 1 до n невключно, то ми знайшли p і завершили роботу алгоритму.

3) Обчислити

$$(x^{'})^2 + a(y^{'})^2 - 1.$$

4) Обчислити $R_3 = ((x^{'})^2 + a(y^{'})^2 - 1,n)$. Якщо R_3 лежить у інтервалі від 1 до n невключно, то ми знайшли p і завершили роботу алгоритму. Якщо ж $R_3 = n$, то ми знову повертаємося до кроку 1) та обираємо нове значення $x^{'}$ та $y^{'}$.

5) Якщо

$$\left(\frac{(x^{'})^2 + a(y^{'})^2 - 1}{n}\right) = 1,$$

повертаємо до кроку 1) та обираємо нові значення $x^{'}$ та $y^{'}$.

6) Обчислити

$$\left((x^{'})^2 + a(y^{'})^2 - 1\right)\left((x^{'})^2(y^{'})^2\right)^{-1}.$$

7) Якщо не існує $\left((x^{'})^2(y^{'})^2\right)^{-1}$ по модулю n, то ми знайшли p та

завершили роботу алгоритму.

8) Обрати k та деяке натуральне число N, щоб k мало багато невеликих дільників. Наприклад, $k = \text{НСК}(2,...,\text{N})$.

9) Обчислити kP, використовуючи схему Горнера та універсальний закон додавання точок еліптичної кривої Едвардса (2.4). Точки P_1 та P_2 мають координати: $P_1(x_1,y_1)$ і $P_2(x_2,y_2)$. Обчислюючи для них суму, ми маємо обчислити G_4,G_5,G_6,G_7 по формулам :

$$G_4 = (dx_1x_2y_1y_2 + 1,n),$$

$$G_5 = (1 - dx_1x_2y_1y_2,n),$$

$$G_6 = (x_1x_2 - ay_1y_2,n),$$

$$G_7 = (x_1y_2 + x_2y_1,n).$$

10) Якщо під час обчислень суми двох точок виникає ситуація, що одне із значень G_4,G_5,G_6,G_7 лежить у інтервалі від 1 до n невключно, то ми знайдемо дільник p для числа n і завершимо роботу алгоритму.

11) Якщо до етапу алгоритму 9) не було знайдено дільник для числа n, то повертаємося до кроку 1) та змінюємо початкові точки або параметри d та a.

Висновки до розділу 3

У даному розділі розглянуто залежність властивостей еліптичних кривих у формі Едвардса над кільцем $n = pq$. Досліджено властивості таких кривих в залежності від параметрів еліптичної кривої, в тому числі наявність особливих точок. Отримано оцінки кількості таких точок для всіх можливих випадків значень коефіцієнтів кривої Едвардса для випадку $n = pq$. Встановлено, що найбільшу кількість особливих точок має клас кривих Едвардса з квадратичним параметром. Тому пропонується обирати параметри a та d так, щоб квадратичні криві

Едвардса над кільцем $n = pq$ містили найбільшу кількість особливих точок. На основі цього був запропонований модифікований алгоритм Лєнстра з використанням цих кривих.

ВИСНОВКИ

В даній роботі проаналізовано та стисло описано джерела за тематикою дослідження, а саме основні методи факторизації чисел, зокрема, класичний метод Лєнстра на кривих Вейєрштрасса та метод Лєнстра на кривих Едвардса. Розглянуто еліптичні криві Едвардса з їх класифікацією та наведено основні та необхідні означення з теорії еліптичної кривої.

У роботі досліджено залежність властивостей еліптичних кривих Едвардса над кільцем лишків $n = pq$ від їх параметрів. Досліджено властивості цих кривих в залежності від параметрів еліптичної кривої, в тому числі наявність в них особливих точок. Отримано оцінки кількості таких точок для всіх класів кривих Едвардса над кільцем $n = pq$. Встановлено, що найбільшу кількість особливих точок має клас кривих Едвардса з квадратичним параметром. Тому запропоновано обирати параметри a та d так, щоб квадратичні криві Едвардса над кільцем $n = pq$ містили найбільшу кількість особливих точок. На основі цього був запропонований модифікований алгоритм Лєнстра з використанням цих кривих.

У подальшій роботі планується провести обчислювальні експерименти та дослідити як вибір системи координат представлення точок еліптичної кривої у формі Едвардса впливає на ефективність методу Лєнстра.

ПЕРЕЛІК ПОСИЛАНЬ

1. Lenstra A.K., Lenstra H. W.Jr. Algorithms Algorithms in number theory. //Technical Report 87-008. Chicago: University of Chicago. 1987.

2. Lenstra H. W. Jr. Elliptic curves and number-theoretic algorithms. //Report 86-19. Amsterdam: Mathematisch Instituut, Universiteit van Amsterda. 1986.

3. Lenstra H. W. Jr. Factoring integers with elliptic curves. //Annals of Mathematics. 1987. V. 126. P. 630675.

4. Беспалов О.Ю., Панасюк І.І. Метод Лєнстра та особливості його застосування на кривих Едвардса. Перспективні напрями захисту інформації: матеріали третьої всеукраїнської наук.-пр.конф. – м.Одеса, 02-06 вересня 2017р. – Одеса:ОНАЗ, 2017. – с. 3

5. Беспалов О.Ю., Панасюк І.І. Метод Лєнстра та особливості його застосування на кривих Едвардса. Перспективні напрями захисту інформації: матеріали третьої всеукраїнської наук.-пр.конф. – м.Одеса, 02-06 вересня 2017р. – Одеса:ОНАЗ, 2017. – с. 5-6

6. Daniel J. Bernstein, Peter Birkner, Tanja Lange, Christiane Peters, Optimizing double- base elliptic-curve single-scalar multiplication, in Indocrypt 2007 [42] (2007), 167–182. [Електронний ресурс]. — Режим доступу: http: //eprint.iacr.org/2007/414.

7. Daniel J. Bernstein, Tanja Lange, Faster addition and doubling on elliptic curves, in Asi- acrypt 2007 [32] (2007), 29–50.[Електронний ресурс]. — Режим доступу: http://eprint.iacr.org/2007/286.

8. Daniel J. Bernstein, Tanja Lange, Inverted Edwards coordinates, in AAECC 2007 [17] (2007), 20–27.[Електронний ресурс]. — Режим доступу: http://eprint.iacr.org/2007/410.

9. Daniel J. Bernstein, Tanja Lange, Analysis and optimization of elliptic-curve single-scalar multiplication, in Fq8 [38] (2008), 1–19.[Електронний ресурс]. — Режим доступу: http://eprint.iacr.org/

2007/455

10. Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, Ed Dawson, Twisted Edwards curves revisited, in Asiacrypt 2008 [39] (2008). [Електронний ресурс]. — Режим доступу: http://eprint.iacr.org/2008/522

11. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Con- tract IST–2002–507932 ECRYPT, 2007, PP. 1-20.

12. Washington L. C. Elliptic curves: number theory and cryptography. – CRC press, 2008.

13. Бессалов А.В. Эллиптические кривые в форме Едвардса и криптография: монографія. Киев, КПИ им. Игоря Сикорского, изд. «Политехника». 2017. -272с.