РЕФЕРАТ

ПЗ: 71 сторінка, 12 рисунків, 7 таблиць, 10 посилань

Об’єкт дослідження – алгоритм Сато обчислення порядку еліптичної кривої над полем Галуа характеристики 2.

Мета курсової роботи – аналіз та реалізація алгоритму Сато обчислення порядку еліптичної кривої над полем Галуа характеристики 2.

Алгоритми підрахунку кількості точок еліптичної кривої (порядку кривої) над скінченним полем діляться на два головні типи: *l*-адичні та *p*-адичні. Для розширених полів Галуа доцільно використовувати p-адичні алгоритми, в основі яких покладено підняття еліптичної кривої з необхідною точністю p-адичного представлення.

В роботі розглянуті радичні алгоритми Сато, AGM, SST та MSST. Розроблено програмну реалізацію алгоритму Сато для обчислення порядку еліптичної кривої в спеціалізованому математичному пакеті та обчислено тестовий приклад.

ЕЛІПТИЧНА КРИВА, ПОРЯДОК, ПІДНЯТТЯ ЕЛІПТИЧНОЇ КРИВОЇ, P-АДИЧНІ ЧИСЛА, АЛГОРИТМ САТО.

ЗМІСТ

ВСТУП

Сучасні стандарти цифрового підпису і направленого шифрування засновані на використанні операцій в групах точок еліптичних кривих. Вони забезпечують менші довжини параметрів і, відповідно, більш високу швидкодію при зберіганні заданого рівня стійкості. Чинний український стандарт цифрового підпису ДСТУ 4145-2002 також використовує перетворення в групах точок еліптичних кривих, визначених над полем $GF(2^n)$.

Стійкість криптосистем залежить від правильно підібраних параметрів еліптичної кривої, а одним із найважливіших параметрів кривої є її порядок.

Існує дві великі групи методів визначення порядку еліптичної кривої – l-адичні та p-адичні. Останні показують гарні результати для полів $GF(2^n)$. p-адичні методи є модифікаціями алгоритму Сато, в основі якого лежить механізм підняття еліптичної кривої.

Метою даної роботи є аналіз p-адичних методів визначення порядку еліптичної кривої, які засновані на арифметиці p-адичних чисел та визначення порядку еліптичної кривої над розширеним полем Галуа $GF(2^n)$ за допомогою алгоритму Сато.

1 ЗАГАЛЬНІ ВІДОМОСТІ

1.1 Еліптичні криві

Еліптичні криві отримали своє ім'я від їх відношення до еліптичних інтегралів, що виникають при обчисленні довжини дуги еліпсів. Еліптичні криві відрізняються від еліпсів і мають набагато цікавіші властивості в порівнянні з еліпсами. Еліптична крива - це просто набір точок у площині x-y, які задовольняють рівнянню

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

і це рівняння може бути визначене на дійсному, раціональному, комплексному чи скінченному полі [7]. Це рівняння називається рівнянням Вейєрштрасса.

Еліптична крива E, визначена над полем K, задається рівнянням Вейєрштрасса (1.1), де $a_1, a_2, a_3, a_4, a_5, a_6 \in K$

Іншими словами, нехай K - це будь-яке поле, тоді ми припускаємо $a_1, a_2, a_3, a_4, a_5, a_6 \in K$ та набір K-раціональних точок:

$$E(K) = \left\{ (x, y) \,\middle|\, x, y \in K, y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \right\} \tag{1.2}$$

Якщо працювати з характеристикою, char (K) ≠ 2,3, то допустимі зміни змінних перетворять наведене вище рівняння (1.2) у такий вигляд:

$$y^2 = x^3 + ax + b, \tag{1.3}$$

де $a,\ b \in K$.

Але коли хтось працює з char(K) = 2 або 3, то загальний вигляд рівняння задається згідно з (1.4) та (1.5) відповідно.

$$y^2 + xy = x^3 + a_2x^2 + a_6, \tag{1.4}$$

$$y^2 = x^3 + a_2x^2 + a_6\,. \qquad (1.5)$$

1.2 Задача дискретного логарифмування в групі точок еліптичної кривої

Криптографія еліптичних кривих була введена незалежно Віктором Міллером та Нілом Кобліцем у 1985 році. У той час криптографія еліптичних кривих фактично не розглядалася як перспективна криптографічна техніка. З розвитком часу та подальших досліджень, особливо з боку реалізації, криптографія еліптичних кривих зараз широко впроваджується. Криптографія еліптичних кривих забезпечує менший розмір ключа, економію пропускної здатності та швидкість реалізації, порівняно з криптографією на основі RSA (Rivest-Shamir-Adleman). Найцікавішою особливістю еліптичних кривих є групова структура точок, утворених кривими, де точки на еліптичних кривих утворюють групу. Безпека криптографії еліптичних кривих залежить від задачі дискретного логарифму еліптичних кривих. Проблема дискретного логарифму еліптичної кривої аналогічна задачі звичайного алгебраїчного дискретного логарифму, $l = g^x$, де для l і g неможливо обчислити x. Проблема дискретного логарифму еліптичної кривої стосується вирішення для n відношення $P = nG$. З огляду на точку P і точку G, то дуже важко знайти ціле число n.

Стійкість основного криптографічного перетворення, що використовується при обчисленні цифрового підпису на еліптичній кривій, визначається складністю вирішення завдання дискретного логарифмування в циклічній підгрупі $\langle P \rangle$ великого простого порядку n групи точок еліптичної кривої, тобто складністю рішення рівняння $Q = kP,\ Q \in \langle P \rangle$ відносно k, k – ціле число, $1 < k < n$.

Нагадаємо, що складність рішення задачі, що задається вхідною послідовністю довжиною t бітів, визначається як число бітових операцій $L(t)$, які необхідно виконати для отримання рішення. Якщо функція $L(t)$ являє собою многочлен, то таке завдання має поліноміальну складність і вважається простим. Як приклади таких завдань можна привести задачу зведення цілого числа в ступінь по модулю цілого числа, завдання обчислення найбільшого загального

дільника двох цілих чисел або завдання доказу простоти цілого числа. Якщо функція *L(t)* має вигляд $L(t) = e^{\lambda t}$, де λ - постійна, то кажуть, що завдання має експоненційну складність. Такі завдання вважаються дуже складними і становлять найбільший інтерес для криптографії, що використовує несиметричні алгоритми. В теорії складності розглядаються функції *L(t)*, що мають проміжну швидкість росту. Ці функції залежать від трьох параметрів і мають вигляд

$$L(t,\ v,\ \lambda) = exp(\lambda t^{v}(\log t)^{1-v}), \tag{1.6}$$

де $0 \le v \le 1,\ \lambda > 0$.

При $v = 0$ $L(t,0,\lambda)=t^{\lambda}$ отримуємо поліноміальну складність, при $v = 1$ $L(t, 1,\lambda)=e^{\lambda t}$ маємо експоненційну складність. Якщо ж $0 < v < 1$, то ця проміжна складність називається субекспоненційною. У нашому випадку довжина вхідної послідовності для задач дискретного логарифмування - це довжина двійкового представлення числа n. Тому стосовно до задачі дискретного логарифмування експоненційна складність має порядок зростання n^{λ}, а субекспоненційна складність для завдання дискретного логарифмування має порядок $exp(\lambda(\log n)^{v}(\log\log n)^{1-v})$. Очевидно, що чим менше v, тим простіше в обчислювальному значенні завданню і, отже, практично воно може бути вирішене для великих значень n.

У довільній скінченній циклічній групі завдання дискретного логарифмування можна вирішити за допомогою методу Шенкса або ρ-методом та λ-методом Полларда.

Для реалізації задачі дискретного логарифму в криптографії еліптичної кривої головне завдання полягає в тому, щоб обчислити порядок групи кривих або, іншими словами, кількість точок на кривій. Обчислення, щоб знайти кількість точок на кривій, породило кілька алгоритмів підрахунку точок [13].

1.3 Умови криптографічної стійкості еліптичної кривої

Нехай q = p є простим числом, де $p \geq 5$. Еліптичною кривою над полем F_p є пара $E = (a, b) \in F_p^2$, де $4a^3 + 27b^2 \neq 0$. Точка на кривій E є рішенням $(x, y) \in F_p^2$ таким, що $y^2 = x^3 + ax + b$ або точка на нескінченності O, яка діє як одиничний елемент. Множина точок E над полем F_p позначається $E(F_p)$. Наведена структура називається групою раціональних точок E над полем F_p [4].

Еліптична крива є криптографічно стійкою, якщо вона задовольняє умовам безпеки та ефективності.

Спочатку розглянемо стійкість кривої з точки зору безпеки. Безпека криптосистеми на еліптичних кривих заснована на складності вирішення проблеми дискретного логарифму в $E(F_p)$. На даний момент відомо декілька алгоритмів вирішення дискретних логарифмів. Для того, щоб зробити їх вирішення неможливим, потрібно, щоб еліптична крива задовольняла наступним умовам:

1) $\left|E(F_p^m)\right| = k \times r, r \geq 2^{160}$- просте, k > 0 – ціле;
2) прості числа r і p різні;
3) порядок p в мультиплікативній групі F_p^* із F_r не менше B, де $B \geq 20$.

Перша умова виключає застосування загальних алгоритмів дискретного логарифму. Друга умова робить неможливою аномальну атаку. І, нарешті, остання умова виключає атаки на закриті ключі, такі як відомі атаки Менезеса, Окамото, Ванстоуна, а також атаки Фрея та Рюка [5].

Далі розглянемо криптографічну стійкість криптосистем на еліптичних кривих з точки зору ефективності. Припустимо, що еліптична крива E, що задана над скінченним полем F_p, задовольняє умовам безпеки. Якщо ця крива використовується у криптографічній системі, тоді ефективність цієї системи залежить від ефективності арифметичних операцій у скінченному полі F_p. Тому p має бути малим, наскільки це можливо. Це випливає з теореми Хассе:

$$(\sqrt{\left|E\left(F_p\right)\right| - 1})^2 \le p \le (\sqrt{\left|E\left(F_p\right)\right| + 1})^2 \quad (1.7)$$

Отже, $\left|E\left(F_p\right)\right|$ також має бути невеликим.

Розглянемо першу умову безпеки:

$$\left|E(F_p^m)\right| = k \times r \quad (1.8)$$

де $r \ge 2^{160}$- просте, k > 0 – ціле (кофактор).

Безпека криптосистеми, у якій використовується $E(F_p)$, заснована на складності вирішення проблеми дискретного логарифму у підгрупі порядку r в групі точок еліптичної кривої $E(F_p)$. Таким чином, k має бути малим. Далі ми покращуємо першу умову $\left|E(F_p^m)\right| = k \times r,\ де\ r \ge 2^{160}$- просте, k > 0 – ціле.

Третя умова має на увазі, що ендоморфізм кільця $End(E(F_p))$ еліптичної кривої над алгебраїчним замиканням F_p є уявним квадратичним порядком.

Задача вибору еліптичної кривої, при побудові криптосистеми, є одним з найголовніших завдань, і повинне вирішуватися перш за все.

Важливо, щоб еліптична крива, на якій буде будуватися криптосистема, не виявилась сингулярною, суперсингулярною або аномальною, оскільки в іншому випадку використання таких кривих в криптосистемі призведе до того, що вона виявиться не криптостійкою. Це пов'язано з тим, що особливі властивості таких кривих дозволяють звести задачу дискретного логарифма на еліптичній кривій до задачі дискретного логарифма в скінченному полі. І на відміну від кривих, які не є сингулярними і аномальними, для такого класу кривих, стандартні ключі розміром 20-40 байт будуть вразливі до атак, що дозволить зловмисникам дістати ключ за невелику кількість часу.

Використання еліптичних кривих над дійсними числами призводить до проблеми - відсутності можливості отримання бієкції між вихідними і

зашифрованими даними. Для того щоб полегшити ситуацію і не проводити округлень, необхідно використовувати тільки криві над скінченними полями. І, під еліптичною кривою, в цьому випадку, будемо мати на увазі набір точок, координати яких належать скінченному полю.

Відповідно до вищесказаного, наступним питанням, яке береться до уваги при пошуку еліптичної кривої, є питання про кількість точок цієї кривої, або ж по-іншому, питання про її порядок.

Завдання пошуку еліптичної кривої з певною кількістю точок є досить нетривіальним. Існує кілька способів вирішення такого завдання. Розглянемо деякі з них:

- метод комплексного множення;

- алгоритм Шуфа.

Метод комплексного множення хоч і дозволяє досить ефективно шукати еліптичні криві з необхідною кількістю точок, все ж, на відміну від алгоритму Шуфа, не є універсальним.

У свою чергу, алгоритм Шуфа має досить велику обчислювальну складність ($O(\log^6 q)$) , і, до того ж, містить в собі досить складний математичний апарат.

Логічно було б припустити, що критерієм ефективності буде криптостійкість майбутньої системи, але коли мова йде про криптосистеми, такий параметр, як криптостійкість є очевидним. Саме тому, як критерій ефективності, розглядається швидкість роботи алгоритму криптосистеми в цілому. А для її оптимізації досить прискорити лише найбільш слабкі місця. Одним з таких слабких місць є операція по обчисленню множення по модулю великого числа.

1.4 Визначення порядку кривої над простим полем Галуа

Нехай $E: y^2 = x^3 + bx + c (mod\, p)$ - це еліптична крива. Тоді кількість точок на E, позначена як #E (F_p), задовольняє умовам теореми Хассе. Згідно з теоремою Хассе, кількість точок на E, #E (F_p), задовольняє наступній нерівності.

$$p + 1 - 2\sqrt{p} \le \#E\left(F_p\right) \le p + 1 + 2\sqrt{p} \qquad (1.9)$$

Кількість точок на кривій E називається порядком кривої. Порядок точки визначається кількістю додавань точки самої до себе, доки не буде отримано нескінченність. Порядок будь-якої точки на кривій E ділить порядок кривої E. Якщо порядок кривої має багато дільників або є гладким, то ця крива не є криптографічно надійною. Для криптографії найкращим буде, якщо порядок кривої є великим простим числом. Загалом, знаходження порядку кривої не є тривіальним. У ситуації, коли $p \geq 5$ є простим, для малих p точки можна перерахувати, припускаючи $x=0,1,2,\ldots,p-1$ і простежуючи, коли $x^3 + ax + b$ являє собою квадрат mod p. Коли величина p велика, то неможливо підрахувати точки на кривій, перерахувавши їх.

Є кілька алгоритмів, які можуть вирішити цю проблему. Це алгоритм Шуфа та алгоритм Schoof-Elkies-Atkin (SEA). На кривій E є приблизно p точок і включно з нескінченно віддаленою точкою, загальна кількість точок, що очікується на кривій, становить p+1. Порядок кривої називається "гладким", якщо порядок кривої ділиться багатьма дрібними дільниками, де це може призвести множення точок до тотожності (нескінченно віддалена точка). Тип бажаної кривої має "негладкий" порядок, де порядок кривої ділиться на велике просте число. Метод підрахунку точок Schoof-Elkies-Atkin став досить ефективним для пошуку криптографічних кривих основного порядку над Fp з евристичним часом $O(\log^6 p)$.

1.5 Аналіз методів визначення порядку еліптичної кривої над розширеними скінченними полями характеристики 2

F_q – скінченне поле з кількістю елементів $q = p^n$, $\bar{F}_q$ є алгебраїчним замиканням цього поля. E/F_q – еліптична крива, визначена над полем F_q:

$$E(x,y): y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,\ a_i \in F_q \qquad (1.10)$$

Дано поле F_q^n та набір точок

$$E\left(F_{q^n}\right) = \left\{ (\bar{x}, \bar{y}) \in F_{q^n} \times F_{q^n} \middle| E\left(\bar{x}, \bar{y}\right) = 0 \right\} \cup O \tag{1.11}$$

Постає питання: як ефективно розрахувати кількість точок $\#E(F_q)$?

Застосовується ендоморфізм Фробеніуса:

$$\varphi : \bar{F}_q \to \bar{F}_q : x \to x^q \tag{1.12}$$

Характеристичний поліном Фробеніуса виглядає наступним чином:

$$F^2 - [t] \circ F + \left[q\right] = [0] \tag{1.13}$$

На підставі теореми Хассе:

$$\#E(F_q) = Q + 1 - t, \ \left|t\right| \leq 2\sqrt{q}, \tag{1.14}$$

де t – слід ендоморфізму Фробеніуса.

Постає наступна проблема: як ефективно обчислити t?

Для вирішення цієї проблеми існує два головних підхода: l-адичний та радичний.

l-адичний підхід починається з розгляду наступних виразів:

$$E\left[l\right] = \left\{ P \in E(\bar{F}_q) \middle| l \bullet P = O \right\},$$

$$F^2(P) - \left[t \bmod l\right] \circ F(P) + \left[q \bmod l\right](P) = O. \tag{1.15}$$

Необхідно обчислити t mod l для усіх простих $l \le l_{max}$ із $\prod_{l \le l_{max}} l > 4\sqrt{q}$.

Після цього необхідно отримати t, використовуючи Китайську теорему про остачі.

p-адичний підхід починається з розрахунку наближення p-адичного підняття Фробеніуса. Після цього, використовуючи дані підняття, розраховується t mod p^N. Якщо $p^N > 4\sqrt{q}$, то t є унікально визначеним.

1.6 Висновки до розділу 1

У даному розділі було проаналізовано загальні відомості про еліптичні криві та завдання дискретного логарифму, виявлено умови криптографічної стійкості еліптичної кривої:

1) $\left|E(F_p^m)\right| = k \times r, r \ge 2^{160}$- просте, k > 0 – ціле;
2) прості числа *r* і *p* різні;
3) порядок p в мультиплікативній групі F_p^* із F_r не менше B, де B ≥ 20.

Також виконано аналіз методів визначення порядку еліптичної кривої над розширеними скінченними полями характеристики 2, у результаті якого визначено, що p-адичний підхід краще підходить для розширених полів *GF(2ⁿ)*. Таким чином він викликає більший інтерес, адже чинний український стандарт цифрового підпису ДСТУ 4145-2002 також використовує перетворення в групах точок еліптичних кривих, визначених над полем $GF(2^n)$.

2 ДОСЛІДЖЕННЯ Р-АДИЧНИХ МЕТОДІВ ПІДРАХУНКУ ТОЧОК

2.1 Визначення та базова арифметика р-адичних чисел

Цілим р-адичним числом називається нескінченна послідовність $\{a_0, a_1,...\}$, в якій всі a_i - р-кові цифри. Множина цілих р-адичних чисел позначається Z_p.

Можна уявляти собі послідовності цифр, про які йде мова в цьому визначенні, записаними у вигляді «нескінченної вліво» послідовності: a_0, зліва від нього - a_1, ще лівіше - a_2, і т. д. Тоді кожне натуральне число можна теж розглядати як ціле р-адичне, якщо записати його в р-ковій системі числення, а потім доповнити зліва нескінченним «хвостом» з нулів. Тим самим визначається вкладення N в Z_p. Наприклад, число 39 як елемент Z_5 запишеться так: ...000124.

Над цілими р-адичними числами можна проводити ті ж алгебраїчні операції, що і над цілими числами.

Сумою (відповідно різницею, добутком) цілих р-адичних чисел $(a_0, a_1,...)$ і $(b_0, b_1,...)$ називається ціле р-адичне число, отримане з них за правилами складання (відповідно вирахування, множення) «у стовпчик» в р-ковій системі числення, якщо записати два числа одне під іншим (b_0 під a_0, b_1 під a_1, і т. д.).

Віднімання завжди можна виконати, оскільки з огляду на «нескінченність вліво» р-кових записів завжди можна «зайняти одиницю» в наступному розряді; множення завжди здійснимо, оскільки для знаходження кожної цифри необхідно тільки кінцеве число додавань.

Техніка виконання операцій додавання, віднімання, множення і ділення р-адичних чисел багато в чому нагадує відповідні операції з десятковими дробами, що вивчають у початковій школі. Єдина відмінність у тому, що «займання», «перенiс до іншого розряду», «множення стовпчиком» і т. д. виконуються зліва направо, а не справа наліво. Ось кілька прикладів обчислень в Q_7 [7]:

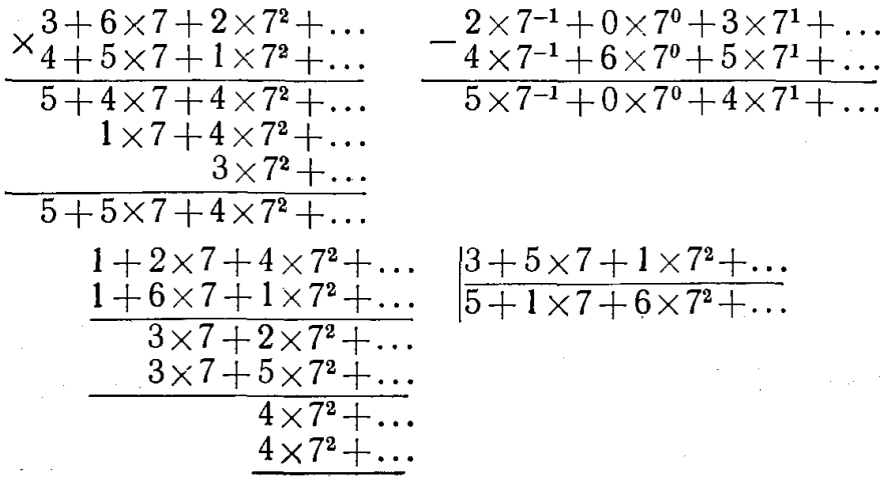


Рисунок 2.1 – Приклади обчислень в Q_7

Оскільки натуральні числа вкладаються в Z_p, а цілі p-адичні числа можна віднімати, цілі числа (тобто різниці натуральних) також вкладаються в Z_p як підкільце; наприклад, число -1 як елемент Z_5 записується у вигляді: ...4444.

Також слід відзначити, що множення на p зводиться до приписування нуля справа, так що ціле p-адичне число ділиться на p тоді і тільки тоді, коли його «остання» (тобто крайня права) цифра є нулем.

P-адичні числа відіграють важливу роль у теорії алгебраїчних чисел. Багато з їхніх плідних властивостей випливають з леми Гензеля, що дозволяє піднімати по модулю p розкладання многочлена. Як наслідок, хоча Q_p є полем з характеристикою нуль, його абсолютно незмінні розширення відображають ту ж структуру, що і алгебраїчні розширення скінченного поля F_p. З іншого боку, завершення алгебраїчного замикання Q_p можна вбудувати як поле, але не як оціночне поле, в C. Отже, p-адичні числа використовуються для подолання розриву між алгебраїчною геометрією скінченного поля та комплексною алгебраїчною геометрією за допомогою так званого принципу Лефшеца [1].

Наприкінці 1999 року Сато зрозумів, що p-адичний підхід, принаймні для малих p, набагато потужніший, ніж існуючі l-адичні методи. Сато не тільки описав p-адичний алгоритм для обчислення кількості точок на звичайній еліптичній кривій над скінченним полем, але також проілюстрував ефективність його

реалізації. Двома найбільш практичними алгоритмами є алгоритм Сато та алгоритм AGM.

2.2 Алгоритм Сато для підрахунку точок кривої

Математичні аспекти еліптичних кривих вивчалися протягом 20-го століття, і використовувались спільно з розкладанням на множники та тестуванням на простоту, і були ключовими складовими в доказі Вільса останньої теореми Ферма.

З моменту, коли для криптографії було запропоновано еліптичні криві незалежно Н. Кобліцем і В. Міллером в 1985 році, багато роботи було виконано для пошуку методів побудови відповідних кривих. Вимога уникати певних нападів на криптосистему полягає в тому, що вибрана крива має груповий порядок, який ділиться на велике просте число.

Кілька спроб вибрати спеціальні види кривих, у яких груповий порядок легко обчислювати у результаті дали незахищені криві. Хоча деякі особливі види все ж можуть бути захищеним, використання повного простору еліптичних кривих широко рекомендується у якості найкращого способу. Однак навіть за допомогою новаторського методу Шуфа було практично неможливо підраховувати точки на кривій, що являє собою криптографічний інтерес, до його покращення Елкісом і Аткіном для випадку великих характеристик.

У 1999 році Т. Сато представив новий метод для підрахунку точок на довільній еліптичній кривій над полем F_q малої характеристики p більше 5. Алгоритм працює в $O(\log^5 q)$ з простою арифметикою, але сильно залежить від p, в той час як вдосконалення методу Шуфа працює в $O(\log^6 q)$ з деякими припущеннями. Таким чином, для фіксованої характеристики, асимптотична поведінка алгоритма Сато працює швидше, ніж у раніше відомих алгоритмів.

Сато винайшов набагато ефективніший алгоритм, базуючись на наступному: замість того, щоб піднімати j до J ізольовано, швидше буде підняти j разом з усіма його поєднаннями j_i одночасно. Справді, запис рівняння $\Phi_p(J_i,J_{i+1})=0$ для $0 \le i < d$ у результаті дає алгебраїчну систему над p-адичним кільцем Z_q без

ендоморфізму Фробеніуса, яку можна швидко розв’язати ітераційним методом Ньютона [7].

Оскільки Сато запропонував ефективний алгоритм підрахунку точок еліптичної кривої для кривих, визначених над скінченними полями малих характеристик $p \geq 5$, деякі роботи з цього питання були розроблені, щоб поширити його на характеристики $p = 2, 3$ і використовувати менше пам'яті. Сато-Скернаа-Тагучі та Харлей-Местре-Гадрі окремо запропонували різні ефективні алгоритми підрахунку точок еліптичних кривих, які називаються алгоритмами SST і AGM, відповідно. Нещодавно Гадрі об'єднав їх у більш ефективний алгоритм, щоб оголосити про модифікований алгоритм SST (MSST). Він модифікує лише етап підйому SST, адаптуючи ідею AGM, і тому він має таку ж складність, що й SST; але це усуває проміжний крок між етапом обчислення підйому та норми в SST і спрощує коди реалізації. Як результат, він працює швидше за постійним чинником, ніж вихідний, хоча його часова складність залишається незмінною.

2.3 Висновки до розділу 2

У даному розділі викладено ознайомлення із арифметикою p-адичних чисел та проведено аналіз алгоритму Сато для підрахунку точок кривої. Алгоритм складається з наступних етапів:

1) підняття j-інваріантів еліптичної кривої;
2) підняття ядра;
3) обчислення кількості точок з використанням результатів попередніх етапів.

Більш детально їх розглянуто у наступному розділі.

3 РЕАЛІЗАЦІЯ АЛГОРИТМУ ПІДНЯТТЯ ЕЛІПТИЧНОЇ КРИВОЇ

3.1 Огляд криптографічних бібліотек

Криптографія - це наука, яка займається проблемами приховування інформації, шифруючи її, і містить набір методів для досягнення такої секретності. За допомогою криптографії ми можемо перетворити нормальний, звичайний текст або інший тип повідомлення таким чином, що він стає незрозумілим для неавторизованих одержувачів. Компетентний одержувач після отримання може конвертувати його в читабельну форму.

До недавнього часу основними споживачами криптографічних рішень стали державні, дипломатичні та військові організації. Розвиток цифрового потоку інформації спричинив значне збільшення областей застосування криптографії. Сьогодні криптографічні методи використовуються для аутентифікації документів та осіб, а також стандартного обміну інформацією. Криптографія також використовується в банківських та мобільних телефонах. Все більшою популярністю користуються інтернет-магазини та онлайн-банкінг.

Цікаво відзначити, що шифри залишаються непорушними приблизно 10 років. Однак ситуація може змінитися з використанням реальних квантових комп'ютерів. Єдиний безпечний спосіб шифрування інформації - це квантова криптографія. У квантовій криптографії ключ захищений принципом невизначеності Гейзенберга. Цей принцип (який є основою квантової механіки) говорить, що вимірювання однієї властивості може вплинути на результати вимірювання іншої властивості. На практиці це означає, що підривний потік фотонів, що вловлюється, змінює свій статус таким чином, що відправник і одержувач можуть його виявити.

Далі коротко описані деякі криптографічні бібліотеки, які можна використовувати для реалізації криптографічних алгоритмів на еліптичних кривих.

Першою бібліотекою є libmcrypt. Це бібліотека, адаптована до багатопотокових середовищ. Хоча її було написано мовою C, вона має дуже

простий у використанні API (інтерфейс прикладного програмування). Ця бібліотека була створена для заміни програми за допомогою функцій mcrypt - це Unix-крипт. І програма, і бібліотека дуже популярні, але вони мають один недолік: хоча вони підтримують різні алгоритми, вони всі симетричні. Зауважте, що libmcrypt може приєднуватися до програм двома способами: статичним та динамічним, і це не змінює спосіб використання API. Найбільш яскравим аспектом цієї бібліотеки є дуже низький рівень функцій, які роблять операції як з буфером даних, так і з блоками. Розробник лише забезпечує бібліотеку даних для шифрування та дешифрування. API цієї бібліотеки являє собою всього два набори функцій для шифрування та дешифрування. Тип алгоритму ми вирішуємо, коли ми ініціюємо цей модуль. Позитивним є те, що бібліотека сама визначає, чи підтримує вона динамічні та статичні модулі.

Інша з цих бібліотек - Borzoi. Borzoi також фокусується тільки на одному типі алгоритму, але тут алгоритми засновані на еліптичних кривих, хоча бібліотека також містить реалізацію симетричного алгоритму AES та одного з алгоритмів генерації цифрового підпису SHA-1. Найважливіші елементи, однак, залишаються класами та об'єктами, пов'язаними з еліптичними кривими, і інші бонуси відіграють допоміжну роль. Головною перевагою цієї бібліотеки є те, що вона намагається відповідати міжнародним стандартам, що, безсумнівно, підвищує її якість. Автор цієї бібліотеки також стверджує, що вона була створена для покращення якості та безпеки коду. Таким чином, ця бібліотека дозволяє використовувати іншу, більш швидку бібліотеку для арифметичних операцій у великих кількостях.

Цікавою ідеєю є бібліотека Crypto++. Вона містить найбільшу кількість алгоритмів серед всіх представлених тут бібліотек. Вона також має добре розроблений API. Ось чому вона застосовується у багатьох комерційних та некомерційних додатках. На жаль, для того, щоб добре працювати з нею, потрібно налаштувати її самостійно. Інший недолік Crypto++ полягає в тому, що компіляція вимагає великих обсягів оперативної пам'яті.

Іншою бібліотекою є Botan. Вона також містить багато алгоритмів, але на відміну від декількох бібліотек, описаних тут, вона включає режими кодування та підтримку міжнародних стандартів. У ній можна маніпулювати даними на високому рівні з API. Тут все є об'єктом або користувальницькими файлами. Botan також дозволяє шифрувати дані на рівні блоків. Botan також пропонує досить гарну документацію. Основним об'єктом цього типу бібліотеки є потік.

Наступною бібліотекою є libgcrypt. Ця бібліотека була створена шляхом вирахування з GnuPG всіх функцій, пов'язаних з криптографією, і працює за алгоритмами, які базуються на відкритих ключах. Це найважливіша особливість цієї криптографічної бібліотеки. Хоча вона не пропонує надто багато криптографічних алгоритмів, вона повністю перевірена з точки зору багатопотокових середовищ. Ця бібліотека також має простий у використанні API, який є повністю уніфікованим та об'єктно-орієнтованим. Libgcrypt підтримує алгоритми шифрування, використовуючи приватні та відкриті ключі, які принципово відрізняються від інших бібліотек.

3.2 Поняття підняття j інваріанта еліптичної кривої

Розглянемо спочатку процес підняття еліптичної кривої над простим полем F_p, хоча він буде таким самим і в разі розширеного поля.

Еліптична крива E над полем F_p, задана рівнянням $y^2=x^3+ax+b$ може бути вкладена в криву E' над полем K. Відображення точки Q кривої E в точку Q' кривої E' називається підняттям точки Q з поля F_p в поле K, при цьому точки кривої $y^2=x^3+ax+b(\mathrm{mod}\ p)$ стануть точками кривої $y^2=x^3+Ax+B$. Таке відображення називається підняттям еліптичної кривої. Сумі точок кривої E' відповідає сума точок кривої E, причому зворотне невірно. Модифікація алгоритму T. Сато розглядає підняття еліптичної кривої з поля F_{p^n} в кільце p-адичних цілих Z_{p^n}. Будь-який елемент Z_{p^n} може бути представлений поліномом $a_{n-1}t^{n-1}+\ldots+a_1t+a_0$, де a_i належать кільцю p-адичних цілих Z_p. Сума і добуток в кільці Z_{p^n} являє собою суму і добуток поліномів, взятих по модулю полінома f(t).

Ступінь даного полінома f(t) дорівнює n, а його редукція по модулю p являє собою незвідний поліном над полем F.

Для обчислення порядку еліптичної кривої над полем F_{p^n} , (p = 2) $y^2 + xy = x^3 + ax + b$, на підставі теореми Хассе використовується формула $\#E = 2^n + 1 - tr(Fr_{2^n})$, де $tr\left(Fr_{2^n}\right)$ - слід n-го ступеня ендоморфізму Фробеніуса. Згідно з оцінкою Хассе $\left|tr(Fr_{2^n})\right| \le 2\sqrt{2^n}$. Для знаходження сліду n-го ступеня ендоморфізму Фробеніуса розглядають відображення малого ендоморфізму Фробеніуса $\sigma : x \alpha x^2$ і представляють n-у ступінь у вигляді послідовності еліптичних кривих $E_0 \leftarrow E_1 \leftarrow E_2 \leftarrow \ldots \leftarrow E_{n-1} \leftarrow E_n$ $E_0 = E_n$. E_0 - базова крива, а всі інші криві отримані одна з іншої застосуванням відображення малого ендоморфізму Фробеніуса. Малий ендоморфізм Фробеніуса може бути перетворений в ізогенії між піднятими кривими $E_0' \leftarrow E_1' \leftarrow E_2' \leftarrow \ldots \leftarrow E_{n-1}' \leftarrow E_n'$ $E_0' = E_n'$. При цьому розглядають дуальні ізогенії в силу їх сепарабельності. В результаті редукція по модулю два кривої E_i', i = 0, 1, ..., n-1 призводить до кривої E_i, i = 0, 1, ..., n-1. Звідси випливає завдання підняти рішення системи рівнянь

$$\begin{cases} \Phi_2(x_0, x_1) \equiv \Phi_2(x_1, x_2) \equiv \ldots \equiv \Phi_2(x_{n-1}, x_0) \equiv 0 \ mod\ 2 \\ x_i \equiv j(E_i) \ mod\ 2 \end{cases} \tag{3.1}$$

до рішень системи

$$\begin{cases} \Phi_2(y_0, y_1) \equiv \Phi_2(y_1, y_2) \equiv \ldots \equiv \Phi_2(y_{n-1}, y_0) \equiv 0 \\ y_i \equiv j(E_i) \ mod\ 2 \end{cases} \tag{3.2}$$

Модулярний поліном, розглянутий в роботі [2]

$$\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 + 2^4 \bullet 3 \bullet 31\left(X^2Y + XY^2\right) - 2^4 3^4 5^3\left(X^2 + Y^2\right) + 3^4 5^3 \bullet 4027XY + 2^8 3^7 5^6 \bullet (X+Y) - 2^{12} 3^9 5$$

,

має властивість, виражену в теоремі, представленій в роботі [3]:

Теорема 1. Нехай E і E' еліптичні криві над полем комплексних чисел, тоді для ізогенії λ: E → E' з циклічним ядром ступеня n необхідно і достатньо, щоб j-інваріант j_E був коренем рівняння $\Phi_n\left(x, j_{E'}\right) = 0$.

Підйом j-інваріанта можливий на основі теореми Lubin-Serre-Tate [2].

Теорема 2. Нехай E еліптична крива над F_{p^n}, її j інваріант $j(E) \notin F_{p^2}$, тоді існує J з кільця Z_{p^n} такий, що $\Phi_p\left(J, \sigma^{-1}(J)\right) = 0, J \equiv j \bmod p$, J є j інваріантом піднятої кривої.

У даній теоремі $\sigma^{-1}(J)$ - це відображення, зворотне відображенню малого ендоморфізму Фробеніуса.

Однак, безпосереднє використання даної теореми вимагає виконання складних обчислень над кільцем Z_{p^n} поля K. Тому на практиці використовують удосконалений метод обчислення J без використання $\sigma^{-1}(J)$. Даний метод полягає в наступному.

1. Піднімаємо j інваріанти j_i, i = 0, 1, …, n-1 циклу кривих $E_0 \leftarrow E_1 \leftarrow E_2 \leftarrow \ldots \leftarrow E_{n-1} \leftarrow E_n$, де крива E_0 збігається з кривою E_n;

2. Обчислюємо j інваріанти j_i, i = 0, 1, ..., n-1 піднятих кривих $E_0' \leftarrow E_1' \leftarrow E_2' \leftarrow \ldots \leftarrow E_{n-1}' \leftarrow E_n' \; E_0' = E_n'$;

3. Вирішуємо систему рівнянь $\Phi_p\left(J_i, J_{i+1}\right) = 0$, в результаті отримуємо підняті j інваріанти.

Всі обчислення проводяться в зазначеному порядку, що дозволяє знайти J_i без обчислення $\sigma^{-1}(J)$.

Описаний метод ефективний тільки для значень p = 2. Це пов'язано з тим, що коефіцієнти модулярного полінома стрімко зростають при значеннях p > 2, крім цього збільшується ступінь полінома.

3.3 Алгоритм підняття j інваріанта за допомогою модифікованих ітерацій Ньютона

Розглянемо послідовність кривих $E_0 \leftarrow E_1 \leftarrow E_2 \leftarrow \ldots \leftarrow E_{n-1} \leftarrow E_n\, E_0 = E_n$, j інваріанти яких пов'язані співвідношенням $j_i^2 \equiv j_{i+1}\, mod\, 2$. Для того, щоб підняти j інваріанти даних кривих, необхідно знайти рішення $y = (y_0, y_1, \ldots, y_{n-1})$ системи

$$\begin{cases} \Phi_2(y_0, y_1) \equiv \Phi_2(y_1, y_2) \equiv \ldots \equiv \Phi_2(y_{n-1}, y_0) \equiv 0 \\ y_i \equiv j(E_i)\ mod\, 2 \end{cases} \tag{3.3}$$

При цьому вважаємо, що j_i, i = 0, 1, ..., n-1 є наближеними коренями системи. За допомогою модернізованих ітерацій Ньютона знаходимо рішення системи із заданою точністю. Для цього алгоритм вирішення рівняння за допомогою ітерацій Ньютона перетворимо в алгоритм розв'язання системи рівнянь за допомогою модернізованих ітерацій Ньютона. Для опису алгоритму модернізованих ітерацій Ньютона розглянемо відображення $g: R^n \to R^n$, яке ставить у відповідність кожному n вимірному вектору $(x_0, x_1, \ldots, x_{n-1})$ вектор $(\Phi_2(x_0, x_1), \Phi_2(x_1, x_2), \ldots, \Phi_2(x_{n-1}, x_0))$. Крім цього розглянемо Якобіанову матрицю A наступного виду:

$$A = \begin{pmatrix} \frac{\partial \Phi_2(j_0, j_0^{n-1})}{\partial x} & \frac{\partial \Phi_2(j_0, j_0^{n-1})}{\partial y} & 0 & \ldots & 0 \\ 0 & \frac{\partial \Phi_2(j_0^{n-1}, j_0^{n-2})}{\partial x} & \frac{\partial \Phi_2(j_0^{n-1}, j_0^{n-2})}{\partial y} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \frac{\partial \Phi_2(j_0^2, j_0)}{\partial x} & 0 & 0 & \ldots & \frac{\partial \Phi_2(j_0^2, j_0)}{\partial y} \end{pmatrix}. \tag{3.4}$$

Позначимо матрицю, зворотну матриці A, як A^{-1}. В результаті отримуємо модернізовані ітерації Ньютона, які дозволяють знайти рішення системи рівнянь, розглянутої вище. Дана формула має вигляд:

$$(y_0, y_{n-1}, \ldots, y_1, y_0)^t = (j_0, j_0^{n-1}, \ldots, j_0^2, j_0)^t - A^{-1} \bullet (\Phi_2(j_0, j_0^{n-1}), \Phi_2(j_0^{n-1}, j_0^{n-2}) \ldots, \Phi_2(j_0^2, j_0))^t \quad (3.5)$$

Елементи матриці A мають наступну властивість:

Твердження: модулярний поліном

$$\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + 2^4 \bullet 3 \bullet 31(X^2Y + XY^2) - 2^4 3^4 5^3 (X^2 + Y^2) + 3^4 5^3 \bullet 4027XY + 2^8 3^7 5^6 \bullet (X + Y) - 2^{12}3$$

при наступному співвідношенні $z_{i+1} = z_i^2$ задовольняє умові

$$\frac{\partial \Phi_2(z_i, z_{i+1})}{\partial x} = \frac{\partial \Phi_2(z_{i+1}, z_i)}{\partial y} \quad (3.6)$$

Доведення. Розглянемо модулярний поліном

$$\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + 2^4 \bullet 3 \bullet 31(X^2Y + XY^2) - 2^4 3^4 5^3 (X^2 + Y^2) + 3^4 5^3 \bullet 4027XY + 2^8 3^7 5^6 \bullet (X + Y) - 2^{12}3$$

.

Нехай $A = 2^4 \bullet 3 \bullet 31$, $B = 2^4 3^4 5^3$, $C = 3^4 5^3 \bullet 4027$, $D = 2^8 3^7 5^6$, $F = 2^{12} 3^9 5^9$.

Тоді модулярний поліном буде мати вигляд:

$$\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + A(X^2Y + XY^2) - B(X^2 + Y^2) + CXY + D*(X + Y) - F$$

. (3.7)

Знайдемо окремі похідні даного модулярного полінома (3.7):

$$\frac{\partial \Phi_2(X, Y)}{\partial x} = 3X^2 - 2XY^2 + A(2XY + Y^2) - 2BX + CY + D,$$

$$\frac{\partial \Phi_2(X, Y)}{\partial y} = 3Y^2 - 2X^2Y + A(X^2 + 2XY) - 2BY + CX + D. \quad (3.8)$$

В отримані вирази (3.8) для окремих похідних підставимо замість змінних X, Y такі вирази: $X = z_i,\ Y = z_{i+1} = z_i^2$. У результаті отримаємо

$$\frac{\partial \Phi_2\left(z_i, z_i^2\right)}{\partial x} = 3z_i^2 - 2z_i z_i^4 + A\left(2z_i z_i^2 + z_i^4\right) - 2Bz_i + Cz_i^2 + D,$$

$$\frac{\partial \Phi_2\left(z_i^2, z_i\right)}{\partial y} = 3z_i^2 - 2z_i^4 z_i + A\left(z_i^4 + 2z_i^2 z_i\right) - 2Bz_i + Cz_i^2 + D\,. \qquad (3.9)$$

Перетворимо праві частини виразів. Отримуємо наступні рівності

$$\frac{\partial \Phi_2\left(z_i, z_i^2\right)}{\partial x} = 3z_i^2 - 2z_i^5 + A\left(2z_i^3 + z_i^4\right) - 2Bz_i + Cz_i^2 + D,$$

$$\frac{\partial \Phi_2\left(z_i^2, z_i\right)}{\partial y} = 3z_i^2 - 2z_i^5 + A\left(z_i^4 + 2z_i^3\right) - 2Bz_i + Cz_i^2 + D\,. \qquad (3.10)$$

Отже,

$$\frac{\partial \Phi_2(z_i, z_i^2)}{\partial x} = \frac{\partial \Phi_2\left(z_i^2, z_i\right)}{\partial y}\ . \qquad (3.11)$$

Дана властивість модулярного полінома дозволяє зменшити кількість операцій множення, які необхідно виконати для обчислення матриці A^{-1}. Для обернення матриці A необхідно обчислювати алгебраїчні доповнення її елементів. В силу того, що матриця має особливий вигляд, обчислення алгебраїчних доповнень зводяться до обчислення добутків елементів відповідних мінорів матриці, що стоять на головній діагоналі. Як уже було відзначено вище, складність обчислення порядку еліптичної кривої за допомогою даного алгоритму є поліноміальною. При використанні даного алгоритму для знаходження матриці, зворотної матриці A, необхідно виконати одну інверсію і $(n^3 + n^2 + 2n)$ операцій

множення. Отже, загальна формула для обчислення складності має вигляд: ($n^3 + n^2 + 2n$) M + 1I, де M - кількість множень, а I - кількість виконуваних інверсій над полем F_{2^n}.

3.4 Підняття еліптичної кривої

Підняття еліптичної кривої в розглянутому алгоритмі здійснюється за рахунок підняття j інваріантів циклу кривих. Розглянемо підняття еліптичної кривої, яка задається рівнянням $y^2 + xy = x^3 + ax^2 + b$. Для кожної такої кривої існує ізоморфне відображення, при якому рівняння вигляду $y^2 + xy = x^3 + ax^2 + b$ зводиться до вигляду $y^2 + xy = x^3 + B$. Якщо відомо рівняння еліптичної кривої, тоді можна обчислити j інваріант цієї кривої по її параметрам. Для еліптичної кривої з параметром B j інваріант обчислюється за формулою: $J = \frac{-1}{B + 432B^2}$.

Якщо j інваріант відомий, то коефіцієнт B можна знайти як корінь полінома $f(x) = 432Jx^2 + Jx + 1$. Для знаходження кореня можна використовувати ітерації Ньютона

$$x_{i+1} = x_i - \frac{432Jx_i + Jx_i + 1}{864Jx_i + J} \tag{3.12}$$

Щоб отримати результат з подвоєною точністю, у якості наближеного кореня розглядають

$$f(x_{i+1}) = 432J\left[\frac{f(x_i)}{f'(x_i)}\right]^2 + f(x_i) - J\left[\frac{f(x_i)}{f'(x_i)}\right] \tag{3.13}$$

В результаті, подвоюючи точність на кожному кроці, можна отримати результат з наперед заданою точністю.

Кількість дій, необхідних для виконання одного кроку в ітераціях Ньютона, дорівнює 3 множенням і 1 інверсії. На кожному наступному кроці кількість множень збільшується до 6, а кількість інверсій не змінюється.

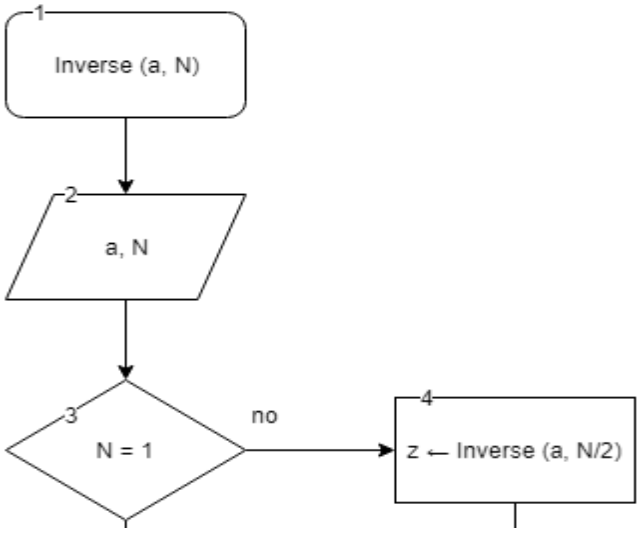
3.5 Реалізація алгоритму

Реалізація алгоритму складається з кількох процедур. Першою процедурою є операція p-адичної інверсії [1]. Вхідними даними цієї процедури є поліном a ∈ Z_q та точність N. Процедура зображена на рисунку 3.1.

```
> Inv_padic:=proc(a,N,MM)
local z,a1,M1,N1,Ns;
if (N=1) then
z:=Powmod(a,(-1),MM,t) mod p;
print(z);
else
z:=Inv_padic(a,ceil(N/2.0),MM);
z:=z+z*(1-a*z);
z:=modpol(z,MM,t,p^N);
print(z);
fi;
z;
end proc;
```

Рисунок 3.1 – Процедура інверсії

Блок-схема процедури зображена на рисунку 3.2.



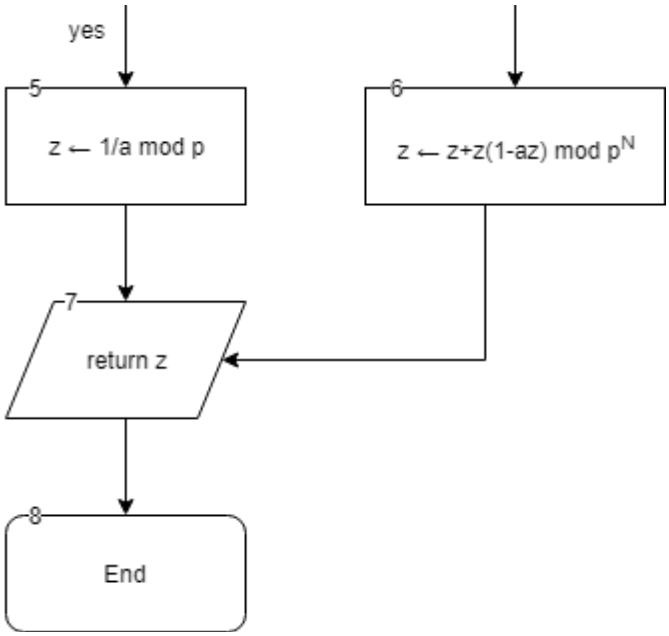


Рисунок 3.2 – Блок-схема процедури інверсії

Розглянемо роботу цієї процедури на прикладі. Нехай $a = 982X^7 + 303X^6 + 724X^5 + 458X^4 + 918X^3 + 423X^2 + 650X + 591$. Поліном поля $M(X) = X^8 + 644X^7 + 842X^6 + 134X^5 + 523X^4 + 21X^3 + 1019X^2 + 562X + 1$, N = 10. Тоді алгоритм обчислює результати, зображені на рисунку 3.3.

$$a$$

$$MM$$

$$N$$

$$t^6 + t^3 + t^2 + t$$

$$2$$

$$6$$

$$22$$

$$854$$

$$z$$

Рисунок 3.3 – Результати роботи процедури інверсії

Для зручності можна згрупувати результати за значенням N наступним чином (табл. 3.1)

Таблиця 3.1 – Результати інверсії

N	z
1	$X^6 + X^3 + X^2 + X$
2	$2X^7 + X^6 + 3X^3 + X^2 + X$
3	$6X^7 + 5X^6 + 4X^4 + 7X^3 + X^2 + X + 4$
5	$22X^7 + 21X^6 + 24X^5 + 4X^4 + 31X^3 + 25X^2 + X + 28$
10	$854X^7 + 373X^6 + 760X^5 + 132X^4 + 863X^3 + 697X^2 + 321X + 60$

Наступна процедура схожа на попередню і виконує обчислення зворотного квадратного кореня. Алгоритм зображено на рисунку 3.4.

```
> Inv_sq_r:=proc(a,z0,MM,N)
if (N<=2) then
  z:=z0;
else
Ns:=ceil((N+1)/2.0);
z:=Inv_sq_r(a,z0,MM,Ns);
w:=(1-a*z*z);
w:=modpol(w,MM,t,2^(N+1));
w:=w/2;
z:=z+z*w;
z:=modpol(z,MM,t,2^N);
z:=sort(expand(z));
print("z=",z);
fi;
z;
end proc;
```

Рисунок 3.4 – Процедура обчислення зворотного квадратного кореня

Блок-схема процедури зображена на рисунку 3.5.

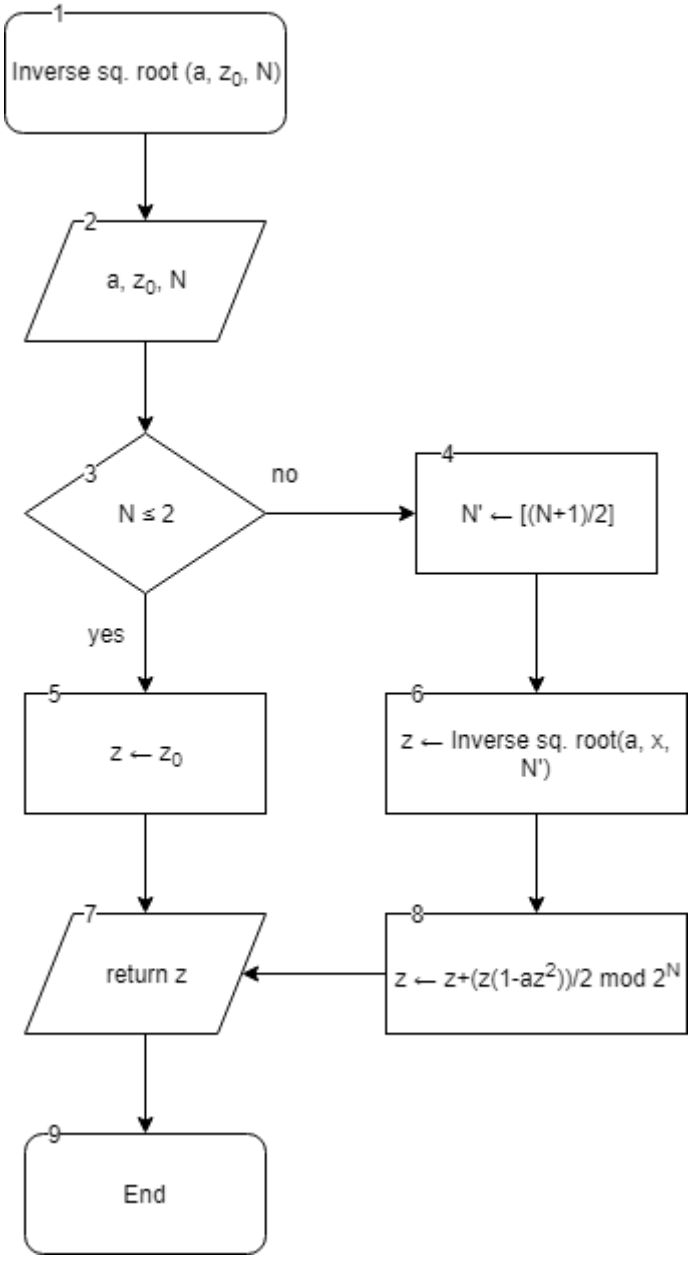


Рисунок 3.5 – Блок-схема процедури обчислення зворотного квадратного кореня

Для прикладу обчислимо зворотний квадратний корінь $a = 823X^7 + 707X^6 + 860X^5 + 387X^4 + 663X^3 + 183X^2 + 12X + 354$. У результаті роботи алгоритма отримаємо наступні результати (табл. 3.2).

Таблиця 3.2 – Результати обчислень зворотного квадратного кореня

N	z
2	$2X^7 + X^6 + 3X^3 + X^2 + X$
3	$6X^7 + 5X^6 + 4X^4 + 7X^3 + X^2 + X + 4$
5	$22X^7 + 21X^6 + 24X^5 + 4X^4 + 31X^3 + 25X^2 + X + 28$
9	$342X^7 + 373X^6 + 248X^5 + 132X^4 + 351X^3 + 185X^2 + 321X + 60$

Наступні дві процедури описують модулярний поліном, що розглянуто у роботі, та його похідну. Вони зображені на рисунках 3.6 та 3.7 відповідно.

```
> F2:=proc(X,Y)
  local c_1,c_2,c_3,c_4,c_5,A,B,C,D,E,F,R,Z,s1,s2,s3,s4,s5;
  c_1:=2^4*3*31:
  c_2:=2^4*3^4*5^3;#162000:
  c_3:=3^4*5^3*4027;#40773375:
  c_4:=2^8*3^7*5^6;#8748000000:
  c_5:=2^12*3^9*5^9;#157464000000000:
s1:=Powmod(X,3,f_t,t)+Powmod(Y,3,f_t,t)-Powmod(X,2,f_t,t)*Powmod(Y,
2,f_t,t) mod p;
s1:=modpol(s1,f_t,t,p);
s2:=(Powmod(X,2,f_t,t)*Y+X*Powmod(Y,2,f_t,t)) mod p;
s2:=modpol(s2,f_t,t,p);
s2:=c_1*s2;

s3:=(Powmod(X,2,f_t,t)+Powmod(Y,2,f_t,t)) mod p;
s3:=modpol(s3,f_t,t,p);
s3:=c_2*s3;

s4:=X*Y;
s4:=modpol(s4,f_t,t,p);
s4:=c_3*s4;

s5:=X+Y;
s5:=modpol(s5,f_t,t,p);
s5:=c_4*s5;

Z:=s1+s2-s3+s4+s5-c_5;

Z:=sort(expand(Z));
end proc;
```

Рисунок 3.6 – Процедура, що описує модулярний поліном

```
> Fs2:=proc(X,Y)
```

```
  local c_1,c_2,c_3,c_4,A,B,C,D,E,F,R,Z,s1,s2,s3,s4,s5;
  c_1:=2^4*3*31:
  c_2:=2^4*3^4*5^3;#162000:
  c_3:=3^4*5^3*4027;#40773375:
  c_4:=2^8*3^7*5^6;#8748000000:

s1:=Powmod(X,2,f_t,t) mod p;
s1:=3*s1-2*X*Y*Y;
s1:=modpol(s1,f_t,t,p);

s2:=Powmod(Y,2,f_t,t) mod p;
s2:=2*X*Y+s2;
s2:=modpol(s2,f_t,t,p);
s2:=c_1*s2;

s3:=2*X;
s3:=modpol(s3,f_t,t,p);
s3:=c_2*s3;

s4:=Y;
s4:=modpol(s4,f_t,t,p);
s4:=c_3*s4;

Z:=s1+s2-s3+s4+c_4;

Z:=sort(expand(Z));
end proc:
```

Рисунок 3.7 – Процедура, що описує похідну модулярного полінома

Процедура Lift_j_Invariants описує:

1. Підняття j інваріантів j_i, i = 0, 1, …, n-1 циклу кривих $E_0 \leftarrow E_1 \leftarrow E_2 \leftarrow \ldots \leftarrow E_{n-1} \leftarrow E_n$, де крива E_0 збігається з кривою E_n;

2. Обчислення j інваріантів j_i, i = 0, 1, ..., n-1 піднятих кривих $E_0' \leftarrow E_1' \leftarrow E_2' \leftarrow \ldots \leftarrow E_{n-1}' \leftarrow E_n' \; E_0' = E_n'$;

3. Вирішення системи рівнянь $\Phi_p(J_i, J_{i+1}) = 0$, в результаті отримуємо підняті j інваріанти.

Процедура зображена на рисунку 3.8.

```
> Lift_j_Invariants:=proc(j,N)
 local i,J,Ns,M,t,D,P,R,R1,S,F,FF,T;
 print("j__,N=",j,N);
  if (N=1) then
   for i from 0 to (n-1) do
     J[i]:=j[i];
   od:
  else
   Ns:=ceil(N/2.0);
   M:=N-Ns;
   J:=Lift_j_Invariants(j,Ns);
   for i from 0 to (n-2) do

     F:=F2(J[i],J[i+1]);
     FF:=Fs2(J[i],J[i+1]);

     print("i,FF,M=",i,FF,M);
     T:=Inv_padic(FF,M,f_t);
     print("T=",T);
     D[i]:=modpol(T*FF,MM,t,p^M);
     P[i]:=modpol(T*((F mod p^N)/p^Ns),MM,t,p^M);
     print("D,P=",D[i],P[i]);
   od;
   R:=modpol(Fs2(J[0],J[n-1]),MM,t,p^M);
   S:=modpol(((F2(J[n-1],J[0]) mod p^N)/p^Ns),MM,t,p^M);
   for i from 0 to min(M,n-2) do
     S:=modpol(S-R*P[i],MM,t,p^M);
     R:=modpol(-R*D[i],MM,t,p^M);
   od;
   R:=modpol(R+Fs2(J[n-1],J[0]),MM,t,p^M);
   R1:=Inv_padic(R,M,f_t);
   P[n-1]:=modpol(S*R1,MM,t,p^M);
   for i from (n-2) by (-1) to 0 do
     P[i]:=modpol(P[i]-D[i]*P[i+1],MM,t,p^M);
   od;
   for i from 0 to (n-2) do
     J[i]:=modpol(J[i]-(p^Ns)*P[i],MM,t,p^M);
     J[i]:=sort(expand(J[i]));
   od;
 fi;
J;
end proc:
```

Рисунок 3.8 – Процедура підняття j-інваріантів

Блок-схема процедури зображена на рисунку 3.9.

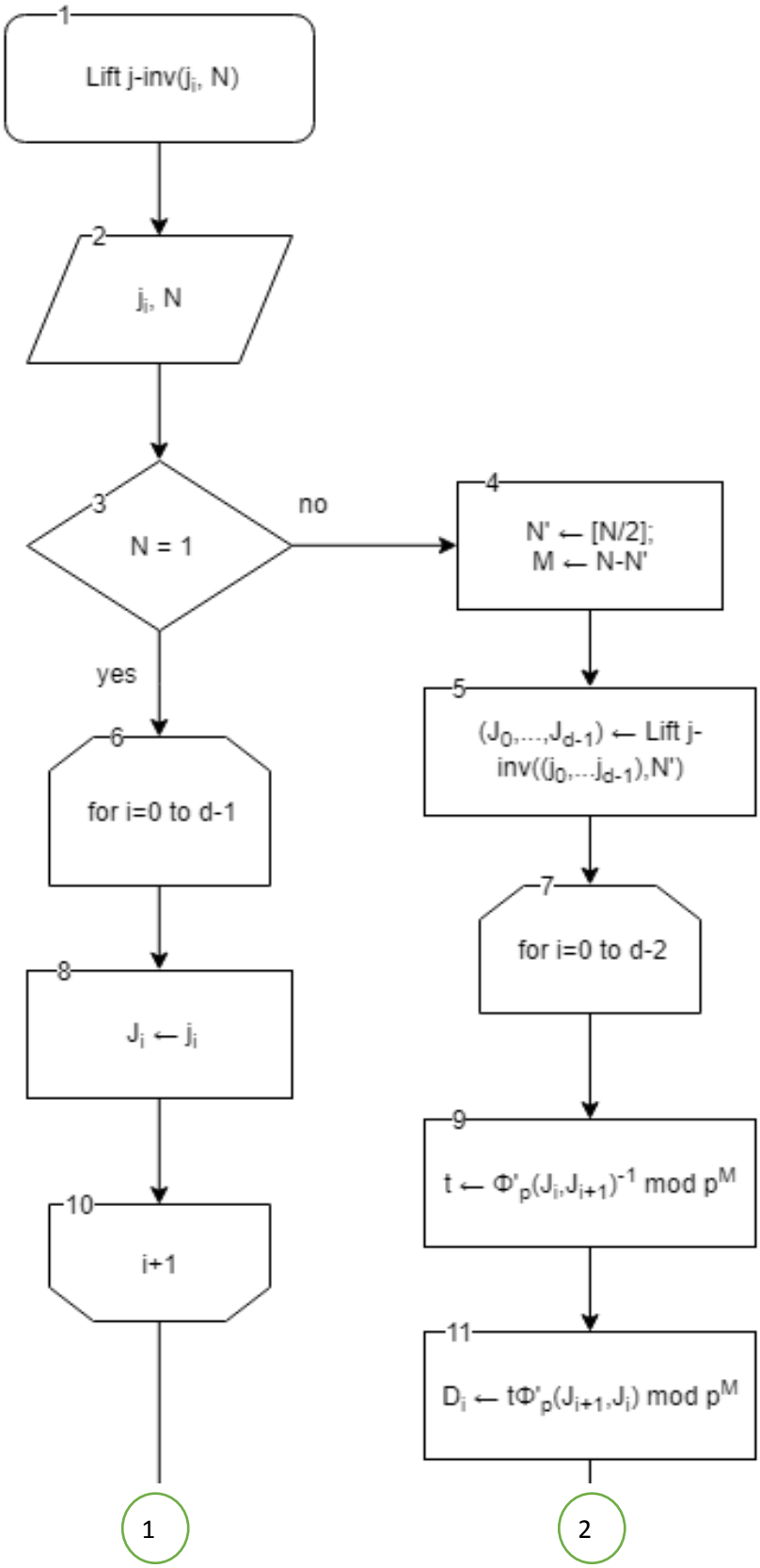


Рисунок 3.9 – Блок-схема процедури підняття j-інваріантів (аркуш 1)

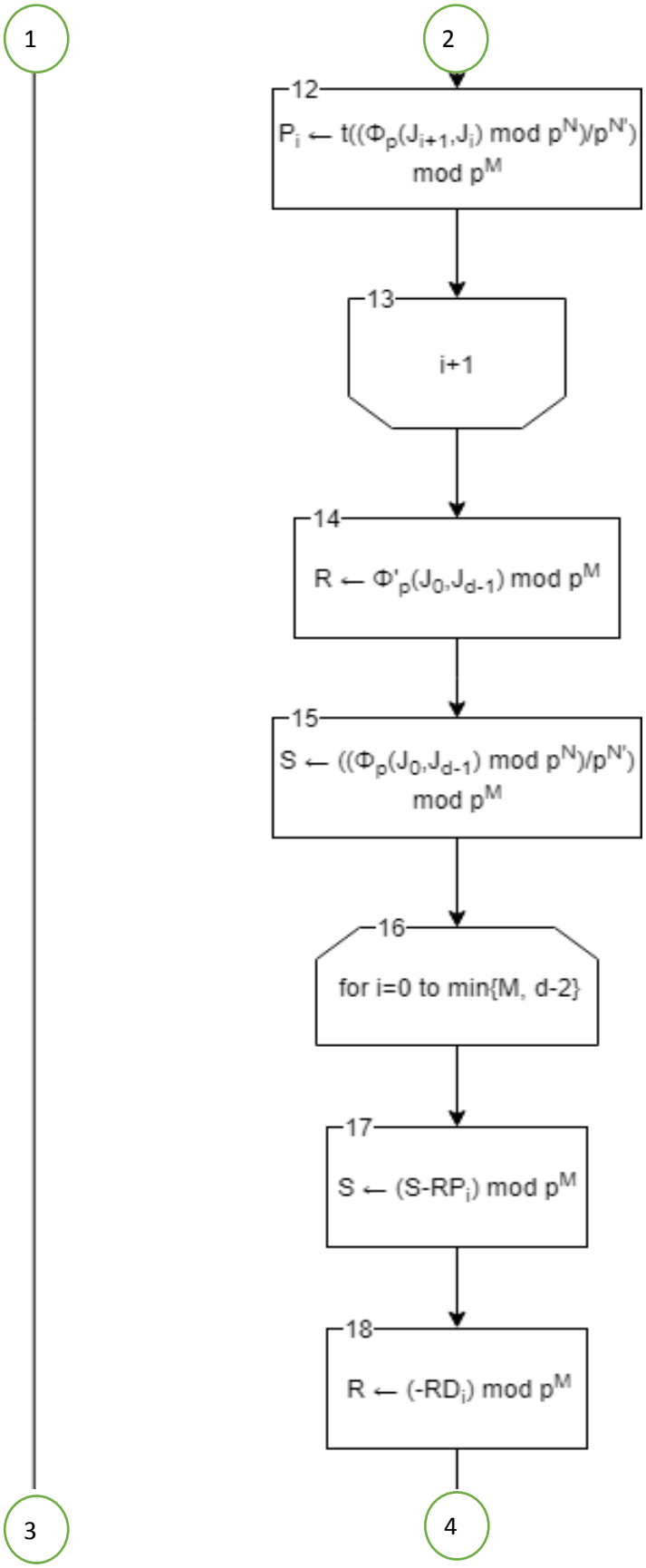


Рисунок 3.9 – Блок-схема процедури підняття j-інваріантів (аркуш 2)

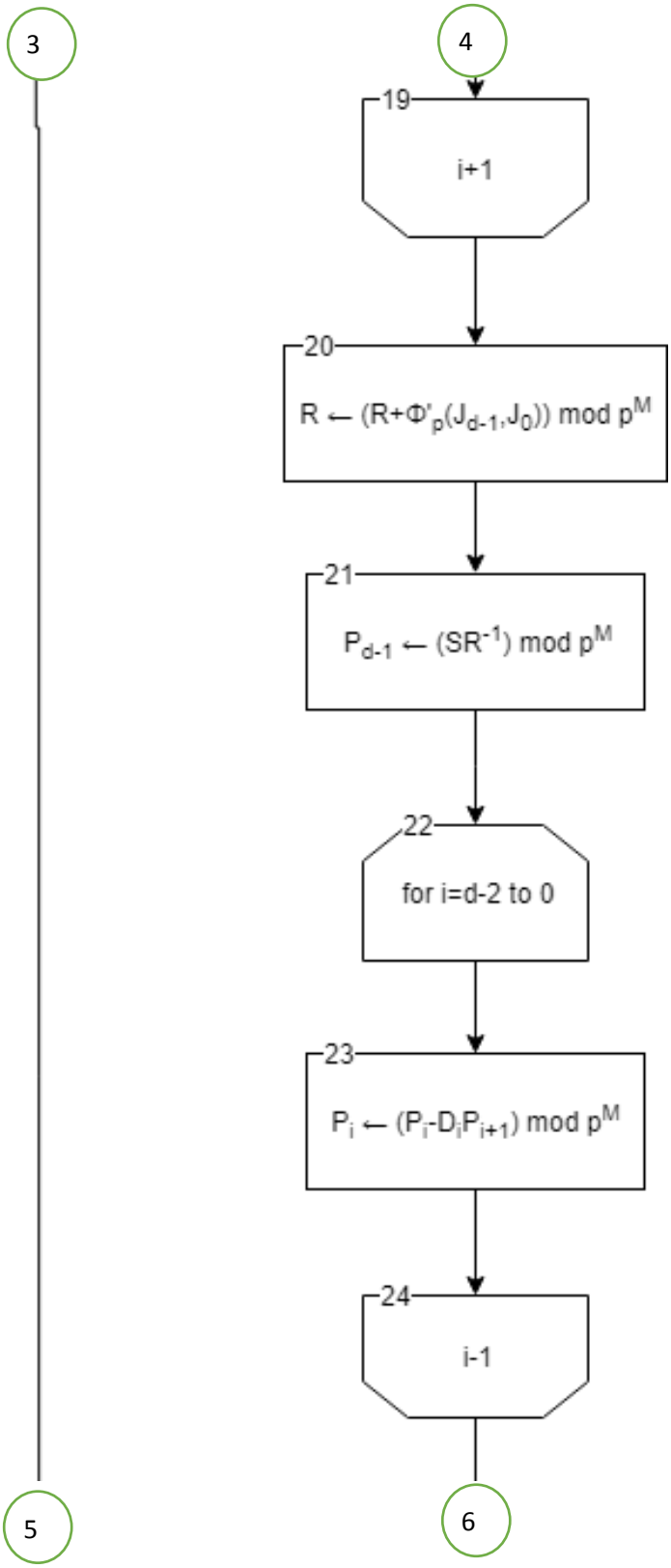


Рисунок 3.9 – Блок-схема процедури підняття j-інваріантів (аркуш 3)

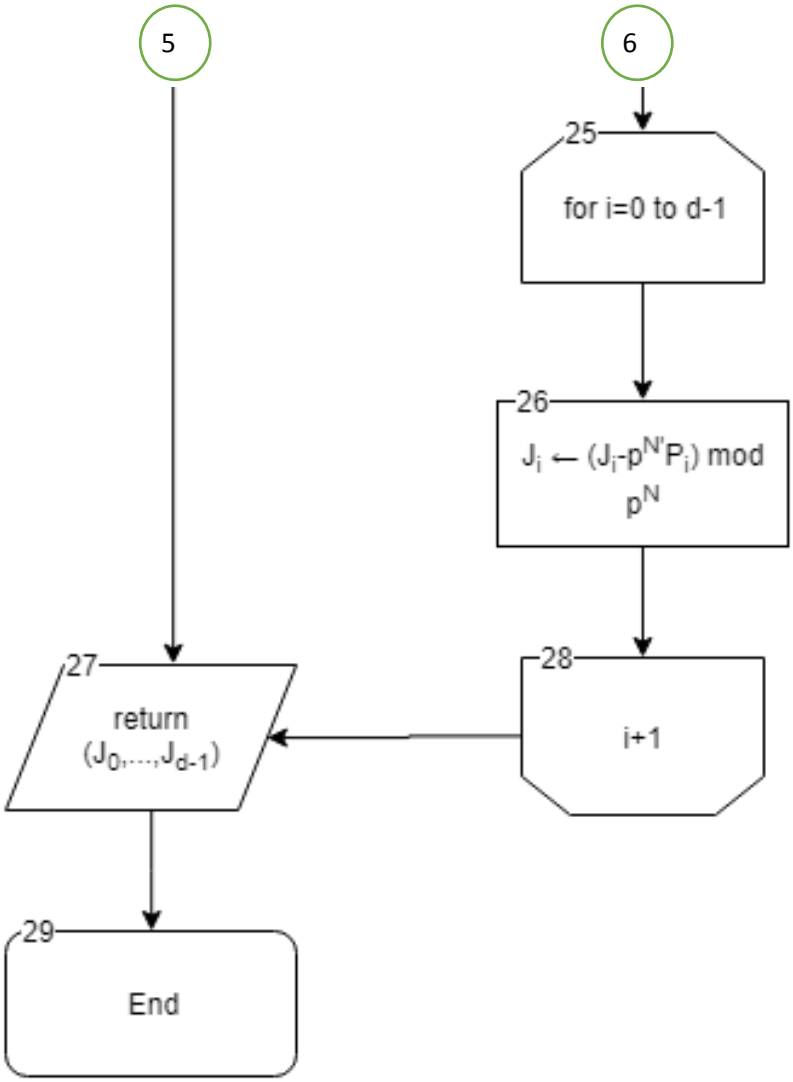


Рисунок 3.9 – Блок-схема процедури підняття j-інваріантів (аркуш 4)

Розглянемо приклад. Нехай p = 7, n = 5 та $F_{p^d} \simeq F_p(t)$ із $t^5 + t + 4 = 0$. Оскільки j-інваріант $j_0 = 3t^4 + 6t^3 + 2t$, то алгоритм обчислює j-інваріант канонічного підняття з точністю N = 10 та поліномом поля $G(T) = T^5 + T + 4$, як

$$J_0 \equiv 249888299T^4 + 236778044T^3 + 9871351T^2 + 169542361T + 26531974 \pmod{p} \quad (3.14)$$

.

Наступним кроком є процедура підняття ядра. У якості вхідних даних вона використовує поліном p-ділення еліптичної кривої є над $Z_q/p^N Z_q$ та точність

N. На виході отримуємо поліном H(x). Блок-схема процедури зображена на рисунку 3.10.

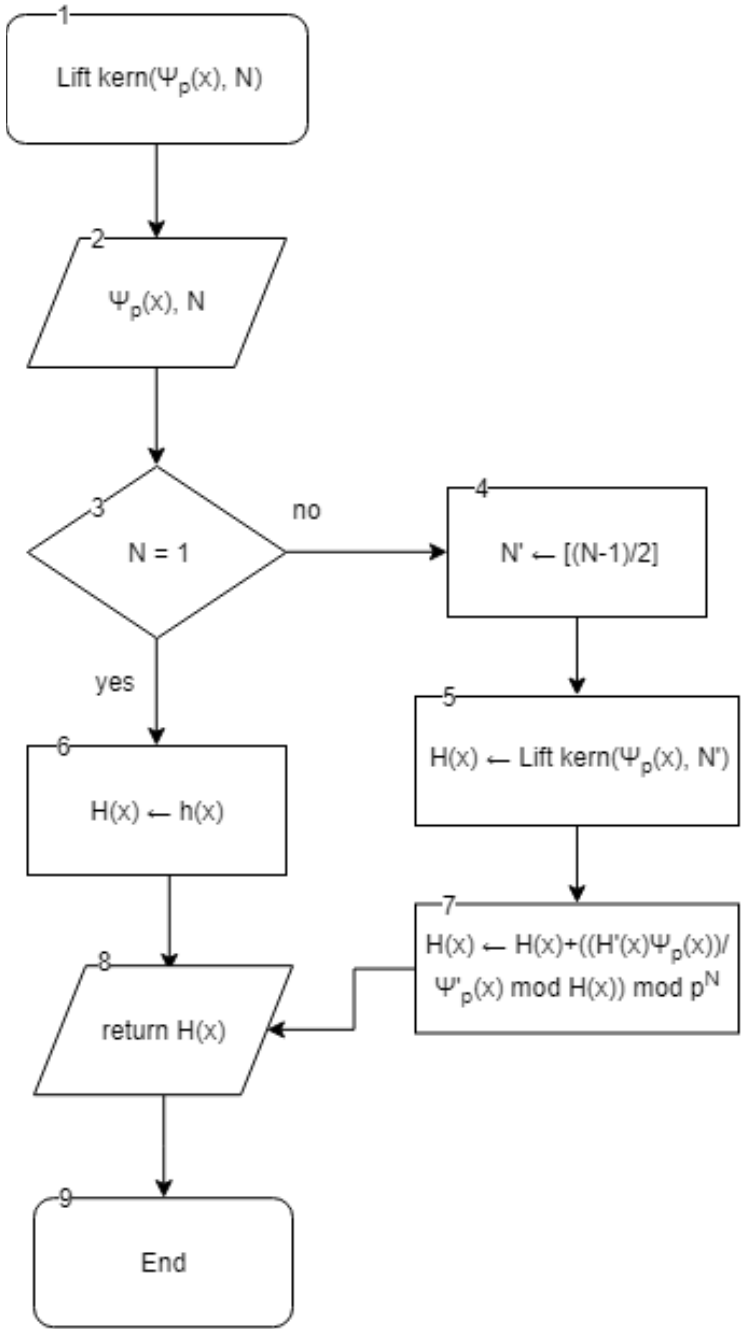


Рисунок 3.10 – Блок-схема процедури підняття ядра

Розглянемо приклад. Нехай p = 7, n = 3, поліном поля $G(T) = T^3 + + T^2 + 4$, а також розглянемо еліптичну криву ε: $y^2 = x^3 + a_4x + a_6$,

де $a_4 \equiv 1409T^2 + 2308T + 2293 \ (mod\, p^4)$ та $a_6 \equiv 139T^2 + 2339T + 2329 \ (mod\, p^4)$.

Поліном р-ділення еквівалентний

$$\text{[very long polynomial]}$$

за модулем p^4, отже результат роботи алгоритму наступний:

$$H(x) \equiv x^3 + \left(502T^2 + 1965T + 742\right)x^2 + \left(1553T^2 + 2106T + 474\right)x + 2329T^2 + 1521T + 2058 \ \left(mod\, p^4\right). \tag{3.15}$$

Останнім кроком є застосування методу Сато для підрахунку точок кривої з використанням усіх попередніх процедур. Вхідними даними є еліптична крива вигляду $y^2 = x^3 + a_4x + a_6$ над F_{p^d}, на виході алгоритму отримуємо кількість точок на даній кривій. Блок-схема алгоритму зображена на рисунку 3.11.

Розглянемо приклад. Нехай p = 5, n = 7, $F_{p^d} \simeq F_p(t)$ із $t^7 + 3t + 3 = 0$. Розглядається еліптична крива $y^2 = x^3 + x + a_6$, де $a_6 = 4t^6 + 3t^5 + 3t^4 + 3t^3 + 3t^2 + 3$.

У результаті роботи алгоритму отримуємо наступні результати: N = 6, $j_0 = 4T^6 + T^5 + 2T^4 + 2T^3$ та $J_0 \equiv 6949T^6 + 6806T^5 + 14297T^4 + 2260T^3 + 13542T^2 + 13130T + 15215 \ (mod\, p^N)$.

Отримуємо поліном

$$H(x) \equiv x^2 + \left(13957^6 + 7906T^5 + 3737T^4 + 9221T^3 + 9207T^2 + 5403T + 7401\right)x + 6090T^6 + 206T^5 + 5259T^4 + 7576T^3 + 3863T^2 + 8903T + 7926 \ (mod\, p^N)$$

.

Використовуючи коефіцієнти цього полінома, алгоритм обчислює значення α та β, за допомогою яких обчислює слід Фробеніуса та кількість точок кривої, у результаті отримуємо: $Tr\left(\varphi_q\right) = 433, \ \left|E(F_{p^d})\right| = 77693.$

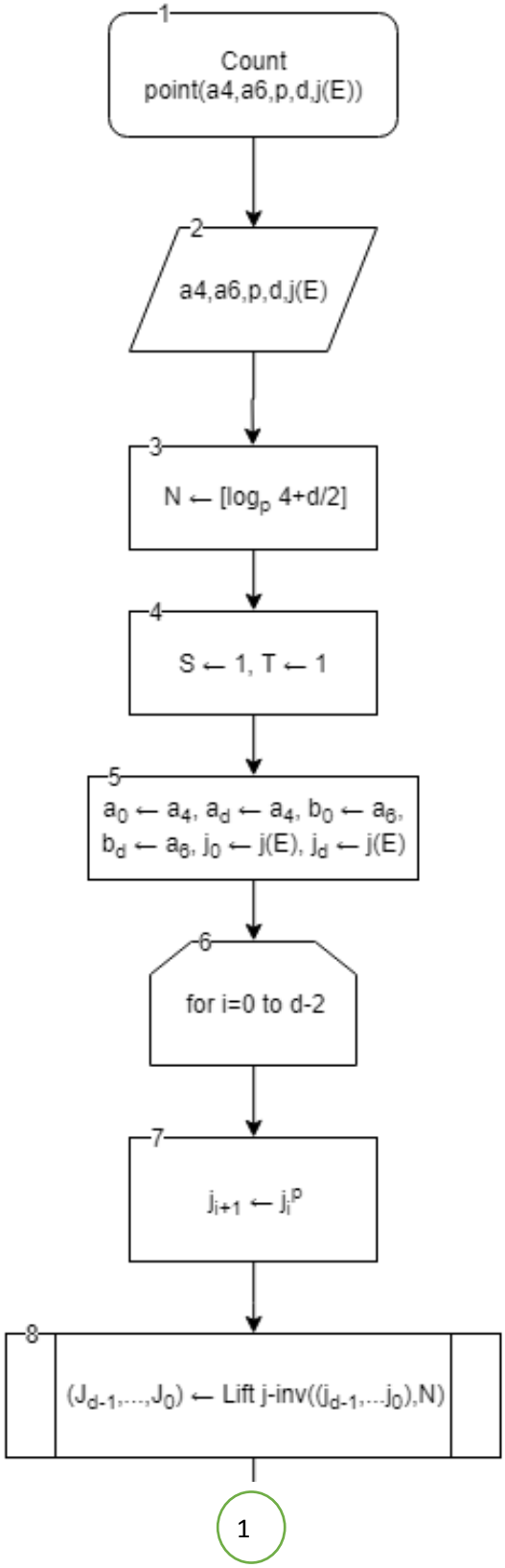


Рисунок 3.11 – Блок-схема алгоритму розрахунку порядку кривої (аркуш 1)

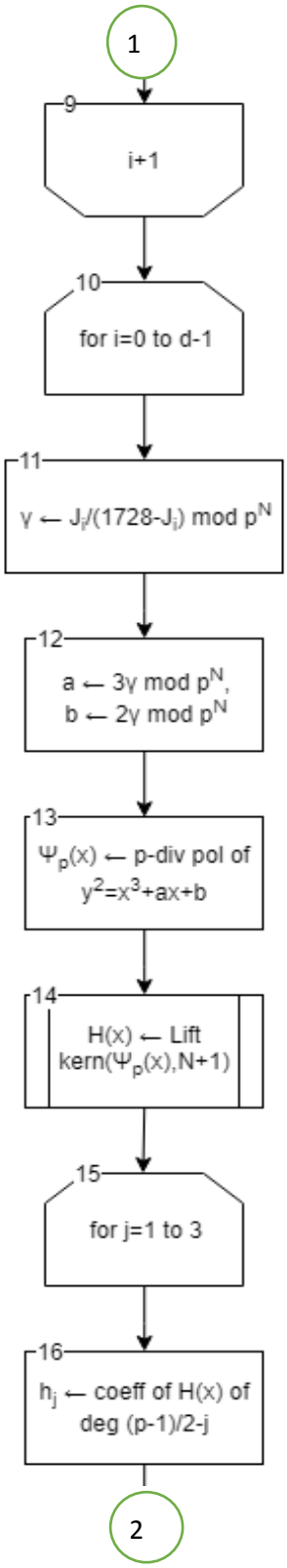


Рисунок 3.11 – Блок-схема алгоритму розрахунку порядку кривої (аркуш 2)

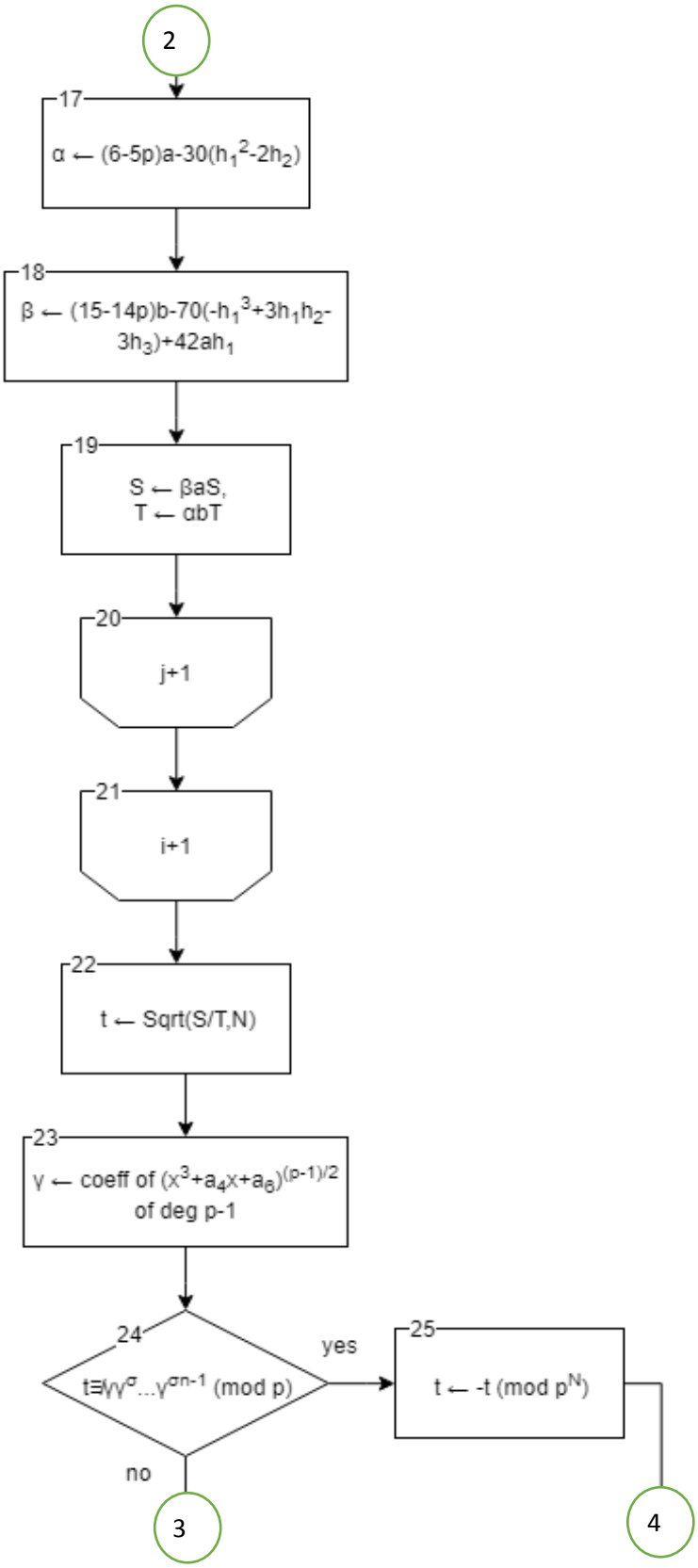


Рисунок 3.11 – Блок-схема алгоритму розрахунку порядку кривої (аркуш 3)

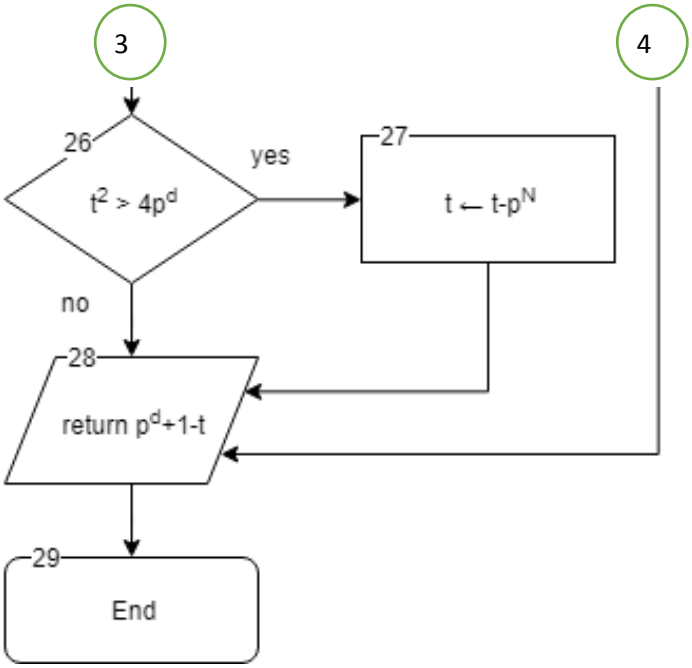


Рисунок 3.11 – Блок-схема алгоритму розрахунку порядку кривої (аркуш 4)

3.6 Висновки до розділу 3

У даному розділі проведено тестові розрахунки підняття еліптичної кривої $y^2 = x^3 + x + a_6$, а також наведено реалізацію алгоритму визначення її порядку. У результаті отримано кількість точок кривої $\left|E(F_{p^d})\right| = 77693$.

4 ОЦІНКА СОБІВАРТОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Собівартість продукції - вартісна оцінка використовуваних в процесі виробництва природних ресурсів, сировини, матеріалів, основних фондів, трудових ресурсів та інших витрат на її виробництво і реалізацію.

Основним нормативним документом, що визначає порядок формування собівартості продукції, є П(С)БО 16. Цей документ окреслює загальні принципи формування собівартості, тоді як безпосередня процедура й специфіка наводяться в галузевих методичних рекомендаціях.

Згідно з п. 11 П(С)БО 16, собівартість реалізованої продукції (робіт, послуг) складається з виробничої собівартості продукції (робіт, послуг), яка була реалізована протягом звітного періоду, нерозподілених постійних загальновиробничих витрат та наднормативних виробничих витрат.

До виробничої собівартості продукції (робіт, послуг) включаються:

- прямі матеріальні витрати;
- прямі витрати на оплату праці;
- інші прямі витрати;
- змінні загальновиробничі та постійні розподілені загальновиробничі витрати.

Загальний час на створення програми складається з різних компонентів. Структура загального часу на створення програмного продукту подана в таблиці 4.1.

4.1 Розрахунок трудомісткості та часу розробки програмного продукту (ПП)

Умовна кількість команд Q визначається за формулою:

$$Q = q \bullet C \tag{4.1}$$

де q – кількість команд у даному програмному продукті (1400).

С - коефіцієнт, який враховує новизну та складність програми.

Таблиця 4.1 – Структура загального часу на створення програмного продукту

№ етапу	Позначення часу даного етапу	Зміст етапу
1	$T_{ПО}$	Підготовка опису завдання.
2	$T_о$	Опис завдання.
3	$T_а$	Розробка алгоритму.
4	$T_{БС}$	Розробка блок-схеми алгоритму.
5	$T_н$	Написання програми мовою програмування
6	$T_п$	Набивання програми.
7	$T_{нт}$	Налагодження і тестування програми.
8	$T_д$	Оформлення документації, інструкції користувачеві, пояснювальної записки.

Таблиця 4.2 – Коефіцієнти розрахунку трудомісткості

Група складності	Ступінь новизни			
	А	Б	В	Г
1	1,38	1,26	1,15	0,69
2	1,30	1,19	1,08	0,65
3	1,20	1,10	1,00	0,60

Новизна визначається за принципом:

А - розробка принципово нових завдань,

Б - розробка оригінальних програм,

В - розробка програм з використанням типових рішень,

Г - разова звичайне завдання.

Складність визначається виходячи з типу вирішуваних завдань:

1 - алгоритми оптимізації і моделювання систем,

2 - завдання обліку, звітності та статистики,

3 - стандартні алгоритми.

Таблиця 4.3 – Коефіцієнти кваліфікації програміста

Стаж програміста	Значення коефіцієнта К
до 2-х років	0,8
від 2 до 3 років	1,0
від 3 до 5 років	1,1 - 1,2
від 5 до 10 років	1,2 - 1,3
понад 10 років	1,3 - 1,5

У відповідності до третьої групи складності та до рівня новизни В визначаємо значення коефіцієнту С. Він рівний 1.00.

Тепер, виходячи з формули (4.1) можна визначити умовне число команд Q.

$$Q = 1400 \bullet 1{,}00 = 1400$$

Трудомісткість розробки програмного продукту (t) визначається за формулою:

$$t=3{,}6\bullet (\eta_{т.в.к})^{1{,}2} \text{ люд.-міс} \qquad (4.2)$$

де t – трудомісткість розробки програмного продукту,

$\eta_{т.в.к}$ - число тисяч команд програмного коду.

Візьмемо $\eta_{т.в.к}$ рівним 2. Тоді $t = 3.6\bullet (2)^{1.2} = 8$ люд.-міс

Загальна тривалість розробки ПП (Т) розраховується за формулою:

$$T=2{,}5\bullet t^{0{,}32} \qquad (4.3)$$

$$T= 2.5 \bullet 8^{0.32} = 5 \text{ міс}$$

Середня кількість виконавців ($PL_{вик}$) розраховується виходячи з трудомісткості та тривалості розробки ПП за формулою:

$$PL_{вик} = t/T \quad (4.4)$$

$$PL_{вик} = 8/5 \approx 1 \text{ чол.}$$

Продуктивність праці групи розробників ПП ($П_р$):

$$П_р = 1000 \bullet \eta_{т.в.к} / t \quad (4.5)$$

$$П_р = 1000 \bullet 2 / 8 = 250 \text{ вихідних команд/люд.-міс}$$

Далі визначаємо час, необхідний для виконання кожного етапу створення програмного продукту:

1. $T_{ПО}$ (час на підготовку опису завдання , год) береться за фактом: $T_{ПО} = 30$ год.

2. $T_о$ (час на опис завдання, год) визначається за формулою:

$$T_о = (Q \bullet B) / (50 \bullet K) \quad (4.6)$$

$$T_о = (1400 \bullet 1,2) / (50 \bullet 0,8) = 42 \text{ год}$$

де В - коефіцієнт урахування змін завдання, коефіцієнт В в залежності від складності завдання і кількості змін обирається в інтервалі від 1,2 до 1,5. Виберемо В=1.2

К – коефіцієнт, що враховує кваліфікацію програміста 1 рік буде рівним К=0.8

3. $T_а$ (час на розробку алгоритму, год) і $T_{БС}$ (час на розробку блок - схеми, год) розраховуємо за формулою:

$$T_а = Q / (50 \bullet K) \quad (4.7)$$

$$T_а = 1400 / (50 \bullet 0.8) = 35 \text{ год}$$

4. $Т_н$ (час написання програми мовою програмування, год):

$$Т_н = (Q \bullet 1.5) / (50 \bullet K) \quad (4.8)$$

$$Т_н = (1400 \bullet 1.5) / (50 \bullet 0,8) = 52,5 \text{ год}$$

5. $Т_{нт}$ (час налагодження та тестування програми, год) визначається за формулою:

$$Т_{нт} = (Q \bullet 4.2) / (50 \bullet K) \quad (4.9)$$

$$Т_{нт} = (1400 \bullet 4.2) / (50 \bullet 0.8) = 147 \text{ год}$$

6. $Т_Д$ (час витрачений на оформлення документації, год) рівний 40 год.

Тепер, знаючи час, витрачений на кожному етапі, можна підрахувати загальний час на створення програмного продукту:

$$T_{заг} = T_{ПО} + T_о + T_а + T_{БС} + T_Н + T_{нт} + T_д \quad (4.10)$$

$$T_{заг} = 30 + 42 + 35 + 52.5 + 147 + 40 = 346.5 \text{ год}$$

4.2 Розрахунок заробітної плати виконавця робіт зі створення програмного продукту

Основна заробітна платня (ЗП, грн) визначається за формулою:

$$ЗП_{осн} = (З \bullet К_т \bullet Т_{заг}) / (Ч_р \bullet Т_{рд}) \bullet (1 + П / 100) \quad (4.11)$$

$$ЗП_{осн} = (3723 \bullet 1 \bullet 346,5) / (21 \bullet 7,9) \bullet (1 + 0,1) = 8553 \text{ грн}$$

З - мінімальна зарплата (3723 грн.);

K_T - тарифний коефіцієнт - 1,00.

$T_{заг}$ - загальний час на створення програмного продукту (год)

$Ч_Р$ - число робочих днів на місяць (21 дні);

$T_{рд}$. - тривалість робочого дня в годинах (7.9 год.).

П - відсоток премії – 10%.

Додаткова заробітна платня (грн.) визначається за формулою:

$$ЗП_{дод} = ЗП_{осн} \bullet Д \quad (4.12)$$

$$ЗП_{дод} = 8553 \bullet 0,1 = 855,3 \text{ грн}$$

де Д – відсоток додаткової заробітної платні, який рівний Д=1%

Загальна заробітна платня визначається як сума основної і додаткової:

$$З_{заг} = ЗП_{осн} + ЗП_{дод} \quad (4.13)$$

$$З_{заг} = 8553 + 855,3 = 9408,3 \text{ грн}$$

Тепер можна підрахувати єдиний соціальний внесок, який нараховується на заробітну плату і складає 22%.

$$В_{єсв} = ((ЗП_{осн} + ЗП_{дод}) \bullet 22) / 100 \quad (4.14)$$

$$В_{єсв} = 2069,82 \text{ грн}$$

4.3 Розрахунок витрат на утримання та експлуатацію ПЕОМ

Основою для розрахунку видатків на утримання та експлуатацію ПЕОМ, що відносяться до даного програмного продукту, є собівартість 1-єї машино-години роботи ПЕОМ, тобто витрати, які виконуються за годину роботи на комп’ютері при створенні чи експлуатації програми, і визначається за формулою:

$$С_{м.год} = В_{сум} / Т_{роб} \text{ (грн./год)} \quad (4.15)$$

де $В_{сум}$ – сумарні річні витрати (грн),

$Т_{роб}$ – час роботи комп’ютера, який визначається як добуток кількості робочих днів на час роботи комп’ютера в день (год), помножені на коефіцієнт (0,9), що позначає ремонт і профілактику обладнання.

$$В_{сум} = В_{ен} + В_{м} + В_{проф} + А + ЗП_{осн} + ЗП_{дод} + В_{єсв} \quad (4.16)$$

Спочатку ми визначимо річні витрати кожного компонента собівартості ($В_{сум}$), до числа яких входять:

Витрати на електроенергію:

$$B_{ЕН} = B_{ПК} + B_{ОСВ} \text{ (грн)} \quad (4.17)$$

де $В_{ПК}$- витрати електроенергії на роботу ЕОМ,

$В_{ОСВ}$ – витрати на освітлення приміщення, які визначаються як:

$$B_{ПК} = T_{Роб.} \bullet Ц \bullet Р \quad (4.18)$$

$$B_{ПК} = 1990,8 \bullet 1,72 \bullet 1,3 = 4451,43 \text{(грн)}$$

$$B_{ОСВ} = 1990,8 \bullet 1,72 \bullet 0.7 = 2396,92 \text{(грн)}$$

де $T_{Роб}$ – тривалість роботи за комп’ютером в рік (год),

Ц - вартість 1 кВт електроенергії (грн), відповідно до тарифу ПАТ «Запоріжжяобленерго» на IV квартал (жовтень-грудень) 2018 року, затвердженого постановою НКРЕКП від 13 квітня 2017 року № 512 із змінами (постанова НКРЕКП №1418 від 27.12.2017 р.).

Р – потужність ПК або освітлювальних приладів.

Тоді: $B_{ЕН} = 4451,43 + 2396,92 = 6848,35$(грн).

Витрати на оплату праці (основної та додаткової) працівникам, які забезпечують функціонування ЕОМ. До них належать:

- інженер

$$ЗП_{осн} = (3723 \bullet 1,54) / 13 \bullet (1 + 0,1) \bullet 12 = 5822 \text{ грн}$$

$$ЗП_{дод} = 5822 \bullet 0,1 = 582,2 \text{ грн}$$

$$В_{єсв} = ((ЗП_{осн} + ЗП_{дод}) \bullet 22) / 100 = 1408,92 \text{ грн}$$

- системний програміст

$$ЗП_{осн} = (3723 \bullet 1,54) / 26 \bullet (1 + 0,1) \bullet 12 = 2911 \text{ грн}$$
$$ЗП_{дод} = 2911 \bullet 0,1 = 291,1 \text{ грн}$$
$$В_{єсв} = ((ЗП_{осн} + ЗП_{дод}) \bullet 22) / 100 = 704,46 \text{ грн}$$

- оператор набору.

$$ЗП_{осн} = (3723 \bullet 1,36) / 10 \bullet (1 + 0,1) \bullet 12 = 6684 \text{ грн}$$
$$ЗП_{дод} = 6684 \bullet 0,1 = 668,4 \text{ грн}$$
$$В_{єсв} = ((ЗП_{осн} + ЗП_{дод}) \bullet 22) / 100 = 1617,52 \text{ грн}$$

Витрати на витратні матеріали ($В_м$) (папір, CD/DVD-диски, картридж тощо.) беруться за фактом і становлять 2% від балансової вартості обчислювальної техніки ($В_б$ = 23000 грн).

$$В_м = В_б \bullet 0,02 \quad (4.19)$$
$$В_м = 23000 \bullet 0,02 = 460 \text{ грн}$$

Витрати на профілактику ($В_{проф}$) становлять 3% від балансової вартості ПЕОМ з периферією ($В_б$).

$$В_{проф} = В_б \bullet 0,03 \quad (4.20)$$
$$В_{проф} = 23000 \bullet 0,03 = 690 \text{ грн}$$

Амортизаційні відрахування в рік (А) визначаються як відношення балансової вартості ПЕОМ ($В_б$) до кількості років експлуатації ($N_р$):

$$A = B_б / N_р \quad (4.21)$$
$$A = 23000 / 3 = 7666.67 \text{ (грн)}$$

Визначимо амортизаційні відрахування за 346,5 годин ($А_Т$):

$$А_Т = (346,5 \bullet 7666,67)/8760 = 303,25 \text{ грн}$$

Визначивши загальну суму витрат $B_{сум}$, одержимо собівартість 1-єї години роботи ЕОМ.

$$В_{сум} = В_{ен} + В_м + В_{проф} + А_Т + ЗП_{осн} + ЗП_{дод} + В_{єсв} \quad (4.22)$$

$$В_{сум} = 6848,35 + 460 + 690 + 303,25 + 5822 + 582,2 + 1408,92 + 2911 + 291,1 + 704,46 + 6684 + 668,4 + 1617,52 = 28991,2 \text{ грн}$$

Витрати на утримання та експлуатацію ПЕОМ, що відносяться до створення даного ПП

Знаючи собівартість 1 години роботи на ПЕОМ і час створення ПП ($Т_{ЗАГ}$), можна визначити витрати на утримання й експлуатацію ПЕОМ при розробці ПП:

$$С_{м.год} = В_{сум} / Т_{роб} \quad (4.23)$$

$$С_{м.год} = 28991,2 / 1990,8 = 14,56 \text{ (грн./год)}$$

$$B_{ПП} = C_{М.год} \cdot T_{заг} \quad (4.24)$$

$$B_{ПП} = 14,56 \cdot 346,5 = 5045.04 \text{ (грн)}$$

4.4 Розрахунок собівартості програмного продукту

Собівартість програмного продукту визначається загальними витратами на виготовлення програмного продукту і обчислюється з використанням таких показників:

1. Основна заробітна плата виконавця робіт зі створення програмного продукту (грн.).

2. Додаткова заробітна плата виконавця робіт зі створення програмного продукту (грн.).

3. Нарахування на заробітну плату (єдиний соціальний податок).

4. Витрати на утримання і експлуатацію ПЕОМ, що відносяться до програмного продукту.

Тепер, додавши значення всіх елементів, можна визначити собівартість (грн.) програмного продукту:

$$С_{пп} = ЗП_{осн} + ЗП_{дод} + В_{єсп} + В_{пп} \quad (4.25)$$

$$С_{пп} = 8553 + 855,3 + 2069,82 + 5045.04 = 16523,16 \text{ грн}$$

4.5 Розрахунок вартості (ціни) програмного продукту

Вартість (ціна) програмного продукту, запропонована розробником, визначається за формулою:

$$Ц = С_{пп} \bullet (1 + Р / 100)*1,2 \quad (4.26)$$

$$Ц = 27758,91 \text{ грн}$$

де $С_{ПП}$ – загальні витрати на створення програмного продукту (грн.),

Р – рентабельність розробки (40 %),

1,2 – коефіцієнт ПДВ (20%).

Таблиця 4.5 - Результати обчислення техніко-економічних показників програмного продукту

Показник	Значення
Кількість команд вихідного коду (команд)	1.4 тис.
Трудомісткість, (люд.-міс.)	8

Продовження таблиці 4.5 - Результати обчислення техніко-економічних показників програмного продукту

Показник	Значення

Продуктивність (вих.ком./люд.-міс.)	250
Кількість виконавців (люд.)	1
Час, потрібний на створення ПП	346,5
Основна заробітна платні виконавця (грн..)	8553
Додаткова заробітна платня (грн..)	855,3
Загальні витрати на утримання і експлуатацію ПЕОМ при виконанні проекту (грн.)	5045.04
Собівартість програмного продукту (грн.)	16523,16
Вартість готового програмного продукту (грн.)	27758,91

4.6 Висновки до розділу 4

В економічній частині дипломної роботи розраховано собівартість програмного продукту (16523,16 грн), визначено його ціну: 27758,91 грн. Розраховано, що період, протягом якого можливо здійснити розробку програмного продукту, складає 346,5 годин.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

В дипломній роботі розглядається програмне забезпечення, розробка якого відбувається у офісному приміщенні.

5.1 Аналіз потенційних небезпек

До потенційних небезпек можна віднести:

- небезпеку ураження електричним струмом через порушення правил електричної безпеки або несправність техніки;
- порушення роботи опорно-рухового апарату внаслідок тривалих статичних навантажень при роботі з ПК;
- нераціональне планування робочого місця, що може призвести до механічних травм, уражень електричним струмом та порушень опорно-рухового апарату;
- негативний вплив недостатнього освітлення робочої зони на зір та продуктивність роботи працюючого, внаслідок несправності освітлювальних приладів або неправильного проектування освітлювальної системи;
- негативний вплив незадовільних параметрів повітряного середовища робочої зони на здоров’я працюючого, внаслідок неправильного проектування системи вентиляції або її несправності;
- небезпеку загоряння у зв'язку із несправністю електричного обладнання, недотримання, або порушення правил протипожежної безпеки обслуговуючим персоналом, що може призвести до пожежі.

5.2 Заходи щодо забезпечення безпеки

Приміщення офісу, в якому відбувається розробка програмного забезпечення, відноситься до приміщень без підвищеної небезпеки ураження електричним струмом.

Різноманітна оргтехніка - комп'ютери, копіри, принтери, касові апарати і т.д. - працює від електрики. Отже, завжди є джерелом можливого ураження струмом. Роботодавець повинен приділяти увагу всім складовим електробезпеки:

- контроль за станом проводки, розеток, вилок, вимикачів і т.п.
- контроль і регулярна модернізація технічної бази.
- навчання і перевірка знань персоналу в частині техніки безпеки і т.д. Офісні працівники в більшості своїй відносяться до I групи по електробезпеці і повинні підтверджувати її раз в 12 місяців.
- регулярні медогляди, що дозволяють своєчасно виявляти симптоми профзахворювань.

Конструктивні заходи забезпечують захист від випадкового дотику до струмопровідних частин за допомогою їх ізоляції та захисних оболонок.

Згідно з ГОСТ 12.1.009-76 (1999) «ССБТ. Электробезопасность. Термины и определения» у приладах II класу захисту використовується подвійна ізоляція - електрична ізоляція, що складається з робочої і додаткової ізоляції.

Оскільки згідно з НПАОП 40.1-1.32-01 «Правила устройства электроустановок. Электрооборудование специальных установок» офісні приміщення у більшості своїй відносяться до класу пожеженебезпечної зони П-IIа (приміщення, в яких містяться тверді горючі речовини), тому передбачений ступінь захисту ізоляції обладнання IP44.

Схемно-конструктивні заходи призначені для забезпечення захисту від ураження електричним струмом при дотику до металевих оболонок, які можуть опинитися під напругою в результаті аварій.

Згідно з ГОСТ 12.1.030-81 (2001) «ССБТ. Электробезопасность. Защитное заземление, зануление» у приміщеннях галузі управління персоналом влаштовується занулення.

Організаційні заходи. Експлуатація електроустановок і електроустаткування проводиться відповідно до НПАОП 40.1-1.01-97 «Правила безпечної експлуатації електроустановок» (далі «ПБЕЕ») та НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів» (далі «ПБЕЕС»).

Аналіз показує, що більшість нещасних випадків, яка фіксується при обслуговуванні електрообладнання, трапляється з організаційних причин, серед яких основними є:

- недостатня навченість персоналу, що обслуговує електроустановки;
- порушення правил будови і безпечної експлуатації електроустановок та правил експлуатації електрозахисних засобів;
- випадковий дотик до неізольованих струмоведучих частин електроустановки;
- помилкова подача напруги в установку, де працюють люди; неправильне розташування пускової апаратури та розподільних пристроїв, захаращеність підходів до них;
- порушення правил виконання робіт в охоронних електричних зонах;
- несправність ізоляції, що призводить до подачі струму на металеві неструмоведучих частини обладнання;
- обрив заземлюючого провідника;
- порушення правил експлуатації електрозахисних засобів або виконання робіт без індивідуальних засобів електрозахисту;
- виконання електромонтажних та ремонтних робіт під напругою;
- застосування проводів і кабелів, які не відповідають умовам виробництва і використовуваного напруги;
- низька якість електроз'єднань в процесі монтажу і ремонту;
- недооцінка небезпеки при обриві і падінні дроти на землю в ситуації, коли працівник знаходяться близько до місця витоку струму (крокова напруга);
- живлення декількох споживачів від загального пускового пристрою з захистом запобіжниками, розрахованими на відключення найбільш потужного з них, або від однієї групи розподільної шафи;
- подача електрики на електроустановку в неробочі періоди; невиконання вимог щодо проведення періодичних випробувань, перевірок

опору заземлюючих пристроїв та ізоляції (обмоток електродвигунів, котушок комутаційної апаратури, реле і т.д.);

- використання електроустановок кустарного виготовлення; неналежний контроль за діями персоналу з боку відповідальних осіб;
- відсутність попереджувальних плакатів, блокувань, огорож в місці проведення електротехнічних робіт;
- використання несправних ручних електроінструментів і переносних світильників.

Відповідальність за організацію безпечної експлуатації електроустановок Правилами покладається на роботодавця, який повинен:

- призначити відповідального за справний стан і безпечну експлуатацію електроустановок;
- створити та укомплектувати електротехнічну службу з числа осіб, які досягли 18-річного віку, які мають відповідну освіту, пройшли медичний огляд і не мають протипоказань;
- розробити і затвердити посадові інструкції працівників та інструкції з безпечного виконання робіт;
- забезпечити навчання і перевірку знань працівників, своєчасний огляд електроустановок та проведення профілактичних, протиаварійних та приймально-здавальних випробувань.

Робота в офісі передбачає переважно працю на стільці або кріслі за столом з офісною технікою. Це може виявитися шкідливим з кількох причин. Удавана зручною поза провокує працівників переробляти, рідко робити перерви, мало рухатися. Сучасна людина може проводити сидячи до 13 годин в день. Додамо 8 годин сну, на рух залишається всього 3 години. Це дуже мало. А тривала малорухлива поза, при сидінні на стільці викликає:

- застої кровообігу.
- порушення постави і хвороби спини, атрофію м'язів.
- кисневе голодування тканин.
- погіршення концентрації уваги.

- підвищення ризику нічного апное (зупинки дихання).
- підвищується ризик діабету і гіпертонії.
- погану моторику кишечника.

І це далеко не весь список хвороб, асоційованих з сидячим способом життя. Медична спільнота кілька років тому відкрито заговорило про Sedentary Death Syndrome - синдромі ранньої сидячій смерті. Цей термін замінив звичне нам слово «гіподинамія».

Загальні ергономічні вимоги встановлено ДСТУ ISO 9241-1:2003 «Ергономічні вимоги до роботи з відеотерміналами в офісі. Частина 1. Загальні положення». Організація робочого місця передбачає: правильне розміщення робочого місця у виробничому приміщенні; вибір ергономічно обґрунтованого робочого положення, виробничих меблів з урахуванням антропометричних характеристик людини; раціональне компонування обладнання на робочих місцях; врахування характеру та особливостей трудової діяльності.

В результаті технічного переоснащення, що базується на впровадженні інформаційних технологій у приміщенні, що знаходиться на другому поверсі виробничого корпусу заплановано встановити комп'ютери. Визначимо скільки комп'ютеризованих робочих місць, оснащених відеодисплейними терміналами (ВДТ) можна встановити у даному приміщенні і як їх розташувати відповідно до встановлених норм та правил з охорони праці. Розміри приміщення: довжина a = 5,1 м, ширина b = 4,1 м, висота h = 3 м.

Перш за все необхідно проаналізувати чи підходить дане приміщення для того, щоб розмістити в ньому комп'ютеризовані робочі місця.

Відповідно до НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин» є неприпустимим розташування приміщень, призначених для роботи з ВДТ у підвалах та цокольних поверхах. Також забороняється розташування вибухонебезпечних приміщень категорії А і Б (НАПБ Б.03.002-2007 «Нормы определения категорий помещений, зданий и наружных установок по взрывопожарной и пожарной безопасности») та виробництв з мокрими технологічними процесами поряд з приміщенням, де

розташовуються ЕОМ (ПЕОМ), а також над такими приміщеннями, або під ними. Окрім того, виробничі приміщення для роботи з ВДТ не повинні межувати з приміщеннями, у яких рівень шуму і вібрації перевищує допустимі значення.

Вибране приміщення відповідає вищезазначеним вимогам, тому переходимо до наступного етапу, а саме, до визначення кількості комп'ютеризованих робочих місць, що можна розмістити в даному приміщенні. Оскільки площа приміщення становить $S_{ПР}$ = 20,91 м^2, а площа, на якій розташовується одне робоче місце з ВДТ, відповідно до вимог ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» повинна становити не менше 6,0 м^2, то в даному приміщенні можна розмістити щонайбільше три комп'ютеризованих робочих місця. Такої кількості достатньо для технічного переоснащення виробництва.

Перевіримо, чи відповідає це число нормативу щодо мінімального об'єму приміщення на одне робоче місце з ВДТ, відповідно до вимог ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ($V_{P.M.Min}$ = 20 м^3). Об'єм приміщення становить 62,73 м^3, а об'єм, що припадає на одне комп'ютеризоване робоче місце - $V^{P.M.}$ = 20,91 м^3. Таким чином норматив щодо об'єму приміщення на одне робоче місце з ВДТ виконується. Отже, можна розмістити в даному приміщенні щонайбільше три комп'ютеризованих робочих місця.

Планування розміщення комп'ютеризованих робочих місць у приміщенні проводимо із врахуванням наступних вимог:

- робочі місця з ВДТ розміщуються на відстані не менше 1 м від стіни зі світловими прорізами;
- відстань між бічними поверхнями ВДТ має бути не менше за 1,2 м;
- відстань між тильною поверхнею одного ВДТ та екраном іншого не повинна бути меншою за 2,5 м;
- прохід між рядами робочих місць має бути не меншим 1 м.

Необхідно також врахувати розміри меблів на комп'ютеризованих робочих місцях, зокрема робочого столу. Відповідно до НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин» рекомендовані розміри столу для робочого місця з ВДТ становлять: висота – 725 мм, ширина – 600-1400 мм, глибина – 800-1000 мм. Приймаємо, що робочий стіл має такі розміри: ширина – 1200 мм, глибина – 800 мм.

Найкраще розмістити комп'ютеризовані робочі місця рядами вздовж стіни з вікнами. Це дасть змогу унеможливити дзеркальне відбиття на екрані ВДТ джерел природного світла (вікон) та потрапляння останніх у поле зору операторів, що погіршує умови їх зорової роботи.

5.3 Заходи щодо забезпечення виробничої санітарії та гігієни праці

Для забезпечення оптимальних параметрів повітряного середовища передбачено виконання вимог ДСН 3.3.6-042-99 «Санітарні норми мікроклімату виробничих приміщень» та ГОСТ 12.1.005-88 (1991) «ССБТ. Общие санитарно-гигиенические требования к воздуху рабочей зоны».

Таблиця 5.1 – Оптимізація значення температурної вологості та швидкості переміщення повітряних мас

Параметри	Оптимальні	Допустимі
Температура °С	20-22	26
Вологість %	40-60	75
Швидкість перен. Повітр. Мас м/с	0,1-0,3	0,5

Офісні приміщення характеризуються специфічним кліматом, який далекий від абсолютно безпечного. На здоров'я персоналу впливають:

- сухе повітря.
- великий вміст пилу.
- недостатня освітленість робочих місць.

- неадекватний тепловий режим (занадто жарко або холодно, занадто великі перепади протягом робочого дня).
- можливе перевищення шумових нормативів (у великих або маленьких приміщеннях).

Порушення гігієнічних нормативів неминуче веде не тільки до хвороб дихальних шляхів, очей і т.д., але і помітно знижує працездатність і мотивацію персоналу. Хороший роботодавець подбає про впровадження в офісі ефективної системи вентиляції і кондиціонування повітря. Також важливо грамотне підтримання її роботи в штатному порядку і обслуговування, включаючи зміну бактерицидних фільтрів. Необхідні регулярні вологі прибирання, провітрювання тощо

Роботи в приміщеннях розробки програмного забезпечення належать до категорії Іб - легка робота, тому встановлені наступні оптимальні значення параметрів мікроклімату:

- у холодний період року: температура 21-23°С; відносна вологість: 40-60%; швидкість переміщення повітря: 0,1 м/с;
- у теплий період року: температура 22-24°С; відносна вологість: 40-60%; швидкість переміщення повітря: 0,2 м/с.

Рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку на робочих місцях у приміщення нормуються згідно ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» та ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

Зниження рівня шуму в приміщенні здійснено за допомогою:

- використання більш сучасного обладнання;
- розташування принтерів та різноманітного устаткування колективного користування на значній відстані від більшості робочих місць працівників;
- переведення жорсткого диска в режим сну (Standby), якщо комп'ютер не працює протягом визначеного часу;

− використання блоків живлення ПК з вентиляторами на гумових підвісках.

5.4 Заходи щодо забезпечення пожежної безпеки

Комплекс протипожежних заходів для приміщення (офісу) обладнаного персональними комп’ютерами з ВДТ розроблений згідно з вимогами НАПБ А. 01.001-2014 «Правила пожежної безпеки в Україні».

Виходячи з аналізу речовин та матеріалів, які використовуються при роботі у приміщенні, відповідно до вимог НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків і зовнішніх установок з взривопожежної і пожежної безпеки», приміщення (офіс), обладнане ВДТ, належить до виробництв категорії «В» з пожежної небезпеки - пространство в помещении, в котором находятся твердые горючие вещества и материалы.

Оскільки приміщення (офіс), обладнане ВДТ, належить до виробництв категорії «В» з пожежної небезпеки, тому згідно з вимогами ДБН В.1.1.7-2002 «Пожежна безпека об’єктів будівництва» воно має II ступінь вогнестійкості.

З технічних та організаційних заходів запобігання пожеж в приміщенні (офісі) обладнаному персональними комп’ютерами з ВДТ передбачені наступні протипожежні заходи. На силовому обладнанні, силових та освітлювальних колах, згідно вимог пункту 3.1 «ПУЕ», встановлені захисні пристрої, що вимикають джерело живлення від ділянки електричного кола, у якій виникло коротке замикання.

Згідно з вимогами НАПБ А.01.003-2009 «Правила улаштування та експлуатації систем оповіщення про пожежу та управління евакуацією людей в будинках та спорудах» і ДБН В.2.5-56:2014 «Системи протипожежного захисту», в приміщенні (офісі) обладнаному персональними комп’ютерами з ВДТ встановлена система пожежної й охоронної сигналізації, яка забезпечує виявлення теплових і димових ознак пожежі і місця виникнення пожежі з точністю до місця розміщення датчика.

Відповідно до вимог НАПБ Б.03.002-2004 «Типові норми належності вогнегасників» для гасіння електрообладнання у приміщенні (офісу) обладнаному персональними комп’ютерами з ВДТ, що знаходиться під напругою, передбачені вуглекислотні вогнегасники типу ВВК-5 в кількості 2 штук. Відстань між вогнегасниками та місцями можливих загорянь не перевищує 10 м.

Передбачені для приміщення (офісу) обладнаного персональними комп'ютерами з візуальними дисплейними терміналами заходи по забезпеченню безпеки, виробничої санітарії, гігієни праці і пожежної безпеки забезпечують безпечні та комфортні умови праці персоналу.

5.5 Заходи щодо забезпечення безпеки у надзвичайних ситуаціях

Ядерні вибухи в атмосфері й більш високих шарах призводять до виникнення потужних електромагнітних полів з довжиною хвиль від 1 до 1000 м і більше. Ці поля через короткочасне існування називають електромагнітним імпульсом (ЕМІ). ЕМІ виникає при ядерному вибусі у воєнний час, у мирний час — при випробуванні ядерної зброї або ядерних аваріях і катастрофах в атмосфері й космосі.

Особливо чутливими до впливу ЕМІ є 6 основних груп об'єктів і систем:

1) системи передачі електроенергії: повітряні ЛЕП, кабельні лінії, різні види з'єднувальних ліній і повітряна електропроводка;

2) системи виробництва, перетворення і накопичення енергії: електростанції, генератори постійного і змінного струму, трансформатори, перетворювачі струмів і напруг, комутатори і розподільні пристрої, електричні батареї і акумулятори, паливні, сонячні й термоелементи;

3) системи регулювання і управління: електромеханічні й електронні датчики та інші елементи автоматики, комп'ютерні установки, мікропроцесори;

4) системи споживання електроенергії: електродвигуни і електромагнітні, нагрівальні, холодильні, вентиляційні, освітлювальні установки та кондиціонери;

5) системи електротяги: електроприводи, напівпровідникові та інші типи перетворювачів;

6) системи радіозв'язку, передачі, зберігання і накопичення інформації: антени, хвилеводи, коаксиальні кабелі, електронні прилади, радіопередавачі, радіоприймачі, установки автономного електропостачання, змішувачі, телефонні апарати, телеграфні установки, заземлені кабелі й проводи, АТС.

Уражаюча дія ЕМІ в приземній області й на землі пов'язана з акумулюванням його енергії довгими металевими предметами, рамними і каркасними конструкціями, антенами, лініями електропередачі та зв'язку, в них виникають сильні наведені струми, які руйнують підключене електронне та інше чутливе устаткування. У районі дії ЕМІ безпосередній контакт людини зі струмопровідними предметами небезпечний.

ЕМІ уражає радіоелектронну і радіотехнічну апаратуру. В провідниках індукуються високі напруги і струми, які можуть призвести до постійних або тимчасових пошкоджень ізоляції кабелів, відключення реле і переривників, пошкодження елементів зв'язку, магнітних запам'ятовуючих пристроїв у ЕОМ і системах передачі даних тощо. Найбільш уразливими елементами обладнання є напівпровідникові прилади — транзистори, діоди, кремневі випрямлячі, інтегруючі ланцюги, цифрові процесори, управляючі й контрольні прилади. Чутливі до пошкодження ЕМІ транзистори звукової частоти, перемикаючі транзистори, інтегруючі ланцюги та ін.

5.6 Висновки до розділу 5

У даному розділі було проведено аналіз потенційних небезпек під час роботи та запропоновано комплекс заходів для покращення умов праці.

ВИСНОВКИ

Арифметика еліптичних кривих відіграє важливу роль у криптографії. Багато досліджень присвячено пошуку швидких алгоритмів виконання групових операцій на еліптичних кривих, а також алгоритмів обчислення кількості точок на еліптичних кривих. Поки що криптографія еліптичних кривих показує себе краще, ніж інші криптографічні схеми. Багато досліджень присвячено аналізу кривих вищого роду або гіпереліптичних кривих.

Алгоритми підрахунку кількості точок еліптичної кривої (порядку кривої) над скінченним полем діляться на два головні типи: *l*-адичні та *p*-адичні.

У роботі було проаналізовано загальні відомості про еліптичні криві та завдання дискретного логарифму, виявлено умови криптографічної стійкості еліптичної кривої:

1) $\left|E(F_p^m)\right| = k \times r, r \geq 2^{160}$- просте, k > 0 – ціле;

2) прості числа *r* і *p* різні;

3) порядок p в мультиплікативній групі F_p^* із F_r не менше B, де $B \geq 20$.

Також виконано аналіз методів визначення порядку еліптичної кривої над розширеними скінченними полями характеристики 2, у результаті якого визначено, що p-адичний підхід краще підходить для розширених полів $GF(2^n)$. Таким чином він викликає більший інтерес, адже чинний український стандарт цифрового підпису ДСТУ 4145-2002 також використовує перетворення в групах точок еліптичних кривих, визначених над полем $GF(2^n)$.

Виходячи з цього, було проведено аналіз алгоритму Сато для підрахунку точок кривої. Алгоритм складається з наступних етапів:

1) підняття j-інваріантів еліптичної кривої;

2) підняття ядра;

3) обчислення кількості точок з використанням результатів попередніх етапів.

Проведено тестові розрахунки підняття еліптичної кривої $y^2 = x^3 + x + a_6$, а також наведено реалізацію алгоритму визначення її порядку. У результаті отримано кількість точок кривої $\left|E(F_{p^d})\right| = 77693$.

Розглянутий алгоритм підняття еліптичної кривої має поліноміальну складність і дозволяє обчислювати коефіцієнти піднятої кривої з необхідною точністю p-адичного представлення для отримання в кінцевому результаті порядку кривої. Ці переваги, а також невисока часова складність обчислень, виділяють цей підхід як один з найбільш перспективних. На ньому базуються такі сучасні алгоритми, як AGM, SST та MSST.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cohen, H. Handbook of Elliptic and Hyperelliptic Curve Cryptography [Текст] / H. Cohen, G. Frey, - Chapman & Hall/CRC, 2006 – 808 с.

2. Fouquet, M. An extention of Satoh's algorithm and its implementation [Текст] / M. Fouquet, P. Gaudry, R. Harley, - J. Ramanujan Math. Soc. 15 2000 - 281–318 с.

3. Gaudry, P. Some remarks on the elliptic curve discrete logarithm [Текст] / P. Gaudry - 2003

4. H. Baier. Efficient Algotithms for Generating Elliptic Curves over Finite Fields Suitable for Use in Cryptography. PhD thesis [Текст] / H. Baier - Darmstadt University of Technology, 2002 – 259 p.

5. H. Baier. How to find Elliptic Curve Groups of Prime Order. Technical Report [Текст] / H. Baier - Darmstadt University of Technology, 2002 – 33 p.

6. Kamarulhaili, H. Elliptic Curve Cryptography and Point Counting Algorithms, Cryptography and Security in Computing [Текст] / H. Kamarulhaili, L.K. Jie, Dr. Jaydip Sen (Ed.), ISBN: 978-953-51-0179-6, 2012 – pp. 91-116

7. Ritzenthaler, C. Point counting on elliptic curves [Текст] / C. Ritzenthaler – UAM (Madrid), 2009 – 28 p.

8. Skjernaa, B. Satoh's Algorithm In Characteristic 2 [Текст] / B. Skjernaa // MATHEMATICS OF COMPUTATION Volume 72, - 2002, - № 241 – pp. 477–487

9. Катренко, Л.А. Охорона праці. Курс лекцій. Практикум: Навчальний посібник [Текст] / Л.А. Катренко, Ю.В. Кіт, І.П. Пістун. – Суми: Університетська книга, 2009. – 540 с.

10. Коблиц, Н. p-адические числа, p-адический анализ и дзета функции [Текст] / Н. Коблиц - М.: Мир, 1982 – 192 с.

11. Ленг, С. Эллиптические функции [Текст] / С. Ленг - Москва, «Наука», 1984 – 309 с.

12. Наказ Міністерства Фінансів України від 31 грудня 1999 р. №318 [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/z0027-00

13. Неласая А.В. Определение порядка группы дивизоров гиперэллиптической кривой [Текст] / А.В. Неласая, В.И. Долгов, С.А. Зайцев // Международная научно-техническая конференция «Компьютерное моделирование и интеллектуальные системы», КМИС-2007, 26-27 марта2007 г. – Запорожье : ЗНТУ. – 2007 – С.173-177.

14. Постанова Кабінету Міністрів України від 26 червня 2013 р. № 444 [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/444-2013-п

15. Тырыгина, Г.А. Выбор эффективного метода подбора эллиптической кривой для реализации на ней криптографической системы [Текст] / Г.А. Тырыгина, Р.Р. Хайбуллин // Молодой ученый. — 2017. — №3. — С. 53-56.