УДК 517.91:004.42

А. Р. Караван
Н. Б. Дубова

АЛГОРИТМИ ОБЧИСЛЕННЯ ДОДАВАННЯ ТА ПОДВОЄННЯ ТОЧОК НА ЕЛІПТИЧНИХ КРИВИХ

Вінницький національний технічний університет;

Анотація

У роботі досліджено математичні основи еліптичних кривих та алгоритми виконання базових операцій над їх точками. Розглянуто правила додавання і подвоєння точок, що забезпечують групову структуру еліптичної кривої. Наведено відповідні математичні формули та описано принципи їх програмної реалізації. Показано значення цих операцій для побудови ефективних обчислювальних методів, що застосовуються у криптографії та теорії чисел.

Ключові слова: еліптична крива, група точок, додавання точок, подвоєння точок, алгоритм, програмна реалізація, криптографія, теорія чисел.

Abstract

The paper investigates the mathematical foundations of elliptic curves and the algorithms for performing basic operations on their points. The rules of point addition and point doubling, which ensure the group structure of an elliptic curve, are considered. Relevant mathematical formulas are presented, and the principles of their software implementation are described. The importance of these operations for constructing efficient computational methods used in cryptography and number theory is demonstrated.

Keywords: elliptic curve, point group, point addition, point doubling, algorithm, software implementation, cryptography, number theory.

Вступ

Еліптичні криві є важливим об’єктом сучасної математики та інформатики, що широко застосовується в теорії чисел і криптографії. Вони задаються рівняннями спеціального виду та утворюють множину точок із визначеними правилами виконання операцій над ними. За умови відсутності особливих точок така множина набуває властивостей алгебраїчної групи.

Особливе значення мають операції додавання та подвоєння точок, оскільки саме вони лежать в основі алгоритмів роботи з еліптичними кривими. Виконання цих операцій дає змогу отримувати нові точки на тій самій кривій і забезпечує можливість побудови ефективних методів обчислення.

У даній роботі розглядаються математичні основи групової структури еліптичних кривих, формули для додавання та подвоєння точок, а також принципи реалізації відповідних алгоритмів. Окрему увагу приділено програмному моделюванню цих операцій та аналізу отриманих результатів.

Математична постановка

Нехай задано еліптичну криву над полем дійсних чисел рівнянням

$$y^2 = x^3 + ax + b \tag{1}$$

де $a,\ b \in \mathbb{R}$, причому виконується умова $4a^3 + 27b^2 \neq 0$ що забезпечує неособливість кривої. Нехай на еліптичній кривій задано точки $P(x_1, y_1), Q(x_2, y_2)$. Потрібно визначити результуючу точку $R = P + Q = (x_3, y_3)$ шляхом застосування групової операції над точками еліптичної кривої. Для випадку додавання різних точок $P \neq Q$ коефіцієнт нахилу прямої між ними обчислюється за формулою

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \tag{2}$$

а координати нової точки визначаються як

$$x_3 = \lambda^2 - x_1 - x_2 \quad (3)$$
$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (4)$$

Для випадку подвоєння точки $P = Q$ коефіцієнт нахилу дотичної визначається формулою

$$\lambda = \frac{3x_1^2 + a}{2y_1} \quad (5)$$

після чого координати точки 2P обчислюються аналогічно. Таким чином, математична задача полягає у визначенні координат результуючої точки еліптичної кривої шляхом реалізації операцій додавання та подвоєння відповідно до правил групової структури.

Алгоритмічна реалізація

Для практичного застосування математичних співвідношень було реалізовано алгоритми додавання та подвоєння точок еліптичної кривої. Програма працює в інтерактивному режимі та дозволяє користувачу обрати необхідну операцію.

Алгоритм роботи програми складається з таких етапів:

1) Введення параметрів еліптичної кривої a
2) Вибір режиму роботи:
   - додавання двох точок;
   - подвоєння точки.
3) Введення координат точки або двох точок залежно від обраного режиму.
4) Перевірка коректності вхідних даних та належності точок еліптичній кривій.
5) Обчислення коефіцієнта нахилу λ відповідно до вибраної операції.
6) Обчислення координат нової точки за математичними формулами.
7) Виведення результату на екран.

Реалізація алгоритму дозволяє автоматизувати виконання обчислень та наочно продемонструвати принцип формування групової структури точок на еліптичній кривій. Отримані результати можуть бути використані для подальшого дослідження методів еліптичної криптографії та чисельних алгоритмів роботи з еліптичними кривими.

Фрагмент коду програми

```
int main() {
    double a;
    int choice;
    cout << "Еліптичні криві: додавання і подвоєння точок\n";
    cout << "Введіть параметр a: ";
    cin >> a;
    cout << "\nОберіть метод:\n";
    cout << "1 - Додавання точок (P + Q)\n";
    cout << "2 - Подвоєння точки (2P)\n";
    cout << "Ваш вибір: ";
    cin >> choice;
    if (choice == 1) {
        Point P, Q;
```

```
    cout << "Введіть точку P (x y): ";
    cin >> P.x >> P.y;
    cout << "Введіть точку Q (x y): ";
    cin >> Q.x >> Q.y;
    Point R = addPoints(P, Q, a, false);
    cout << "Результат P + Q = ("
        << R.x << ", " << R.y << ")\n";
}
```

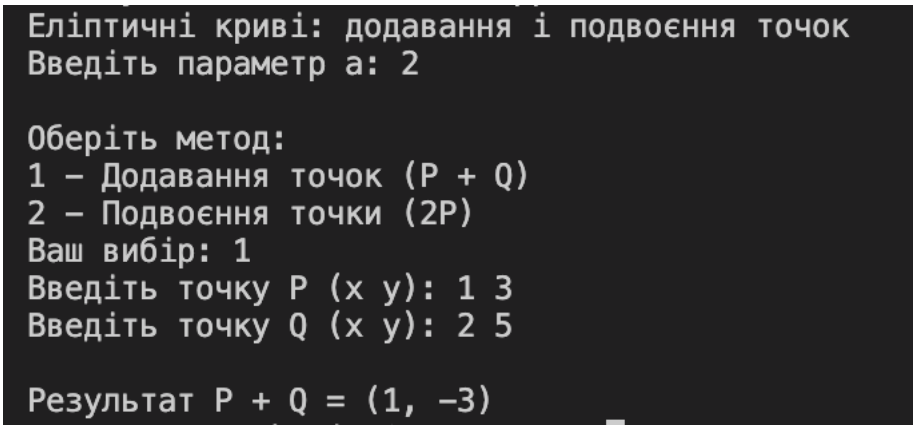

Рис. 1. Результати виконання. Додавання точок

При виконанні операції додавання точок $P(1,3)$ і $Q(2,5)$ було обчислено нахил прямої $\lambda = 2$. Після підстановки у формули отримано нову точку $R(1,-3)$, яка є результатом операції $P + Q$.

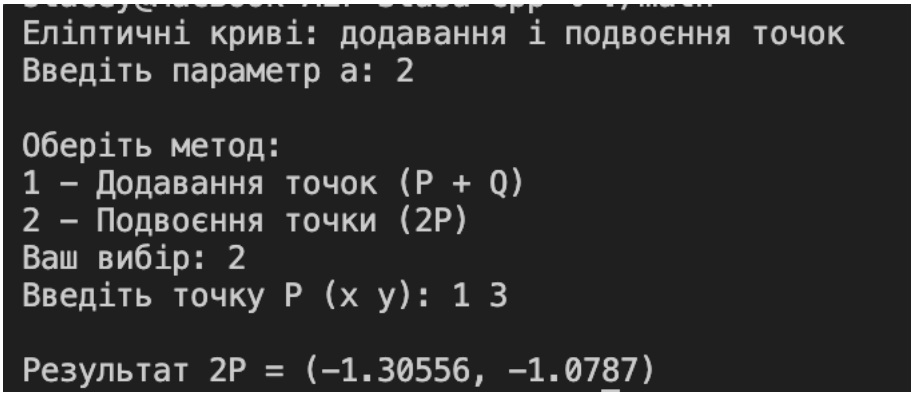

Рис. 2. Результати виконання. Подвоєння точок

При виконанні операції подвоєння точки $P(1,3)$ було використано формулу нахилу дотичної (5). Після обчислень отримано нову точку $R\left(-\frac{47}{36}, -\frac{233}{216}\right)$, яка є результатом операції $2P$

Висновки

У даній роботі було розглянуто основні алгоритми обчислення операцій над точками еліптичної кривої, а саме додавання та подвоєння точок. Встановлено, що ці операції визначаються як геометрично, так і алгебраїчно, та базуються на спеціальних формулах для обчислення координат нових точок.

Було проаналізовано алгоритм додавання двох різних точок, який ґрунтується на побудові прямої через ці точки та знаходженні третьої точки перетину з кривою з подальшим відображенням відносно осі абсцис. Також досліджено алгоритм подвоєння точки, який використовує дотичну до кривої в заданій точці та аналогічний принцип знаходження нової точки.

Одержані результати показують, що операції додавання та подвоєння є базовими для побудови алгебраїчної структури точок еліптичної кривої і можуть бути формалізовані у вигляді чітких обчислювальних алгоритмів. Це підтверджує їх важливість для подальших математичних і прикладних застосувань.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Koblitz N. Elliptic curve cryptosystems // *Mathematics of Computation*. – 1987. – Vol. 48, No. 177. – P. 203–209.
2. Miller V. S. Use of elliptic curves in cryptography // *Advances in Cryptology — CRYPTO'85 Proceedings*. – Springer, Berlin, Heidelberg, 1985. – P. 417–426.

Караван Анастасія Русланівна — студент факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: nastykaravan@gmail.com

Науковий керівник: ***Дубова Надія Борисівна*** – старший викладач, кафедра вищої математики, Вінницький національний технічний університет, м. Вінниця, Хмельницьке шосе, 95, e-mail: dubova_n_b@vntu.edu.ua

Karavan Anastasiia R. — Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: nastykaravan@gmail.com

Supervisor: ***Dubova Nadia B.*** — Senior Lecturer, Department of Higher Mathematics, Vinnytsia National Technical University, Vinnytsia, Khmelnytske Shosse, 95, e-mail: dubova_n_b@vntu.edu.ua