УДК 512.624.2

ВИКОРИСТАННЯ АПАРАТУ ЕЛІПТИЧНИХ КРИВИХ ДЛЯ ФАКТОРИЗАЦІЇ ПОЛІНОМІВ НАД СКІНЧЕННИМ ПОЛЕМ

П. В. Мікава[1, a], Л. В. Ковальчук[1]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

У даній роботі розглянуто алгоритм Ленстра, що дозволяє факторизувати числа, використовуючи апарат еліптичних кривих. Цей алгоритм належить до класу субекспоненціальних методів та входить до трійки найшвидших алгоритмів факторизації. Також розглянута теорема Ленстра, яка забезпечує виконання нетривіальної умови при обчисленнях в алгоритмі. По аналогії, розроблено та доведено теорему Ленстра, яка забезпечить правильність обчислень при подальшій розробці алгоритму Ленстра для факторизації поліномів.

Ключові слова: Алгоритм Ленстра, теорема Ленстра, еліптична крива, факторизація, поліном

Вступ

На сьогоднішній день, алгоритм Ленстра входить до трійки найшвидших алгоритмів факторизації чисел, та розділяє її з такими алгоритмами, як метод квадратичного решета (QS), та метод решета числового поля (NFS). Він базується на використанні апарату еліптичних кривих та належить до класу субекспоненціальних методів. Перед алгоритмом розглянемо теорему Ленстра для чисел. Вона забезпечує правильне обчислення кратних точок, які використовуються у алгоритмі Ленстра. По аналогії з числами, почнемо розробку алгоритму для факторизації поліномів кільця $F_p[x]$. Для цього розробимо та доведемо теорему Ленстра для забезпечення нетривіальної умови при обчисленні кратних точок еліптичної кривої, яка задана над фактор-кільцем $F_p[x]/f(x)$.

1. Алгоритм Ленстра факторизації чисел

Розглянемо існуючі результати щодо факторизації чисел, які отримав Ніл Ленстра. [1]

Позначимо через n непарне складене число та p – простий дільник n. Будемо вважати, що $p > 3$.

Нехай дано еліптичну криву E, яка описується рівнянням $y^2 = x^3 + ax + b,\ \ a, b \in Z$, і точку $P = (x, y)$ на кривій E. Вважаємо, що многочлен x^3+ax+b має різні корені, тобто що $4a^3 + 27b^2 \neq 0$. Для простоти ми припускаємо, що $4a^3 + 27b^2$ не має з n загальних множників, іншими словами, що $x^3 + ax + b$ не має кратних коренів за модулем p для будь-якого простого дільника p числа n (тобто виконується умова: НСД$(4a^3 + 27b^2, n) = 1$).

Нехай потрібно знайти кратну kP для точки P. Існує багато різних способів зробити це за $O(log\, k)$ кроків, кожен з яких – подвоєння точки, або додавання двох різних точок. Оберемо будь-який з прийомів обчислення кратних kP, та будемо розглядати точку P і всі її кратні по модулю n. Вважатимемо, що $P(\mathrm{mod}\, n) = (x(\mathrm{mod}\, n), y(\mathrm{mod}\, n))$ і кожен раз при обчисленні кратної точки kP фактично обчислюємо лише лишки її координат по модулю n. Всі обчисленя при подвоєнні і додаванні точок можна проводити за модулем n, якщо виконана нетривіальна умова: всі знаменники повинні бути взаємно простими з n.

Теорема Ленстра

Нехай E – еліптична крива з рівнянням $y^2 = x^3+ax+b$, де $a, b \in Z$ та НСД$(4a^3+27b^2, n) = 1$. Нехай P_1 та P_2 – дві точки на E, у яких знаменники координат взаємно прості з n, та $P_1 \neq -P_2$. Тоді $P_1 + P_2 \in E$ має координати, у яких знаменники взаємно прості з n, тоді і тільки тоді, коли у n немає простого дільника p, для якого сума точок $P_1(\mathrm{mod}\, p)$ і $P_2(\mathrm{mod}\, p)$ на еліптичній кривій $E(\mathrm{mod}\, p)$ дорівнювала б точці на нескінченності $O(\mathrm{mod}\, p) \in E(\mathrm{mod}\, p)$. Тут $E(\mathrm{mod}\, p)$ позначає еліптичну криву над F_p, яка отримана зведенням по модулю p коефіцієнтів рівняння $y^2 = x^3 + ax + b$.

З доведенням данної теореми можна ознайомитися в книзі [1, стор. 220]

Алгоритм Ленстра

Нехай n – непарне, складене, натуральне число, яке треба розкласти на множники.

Нехай у нас є метод породження пар (E, P), які складаються з еліптичної кривої $y^2 = x^3 + ax + {} + b, a, b \in Z$, і точки $P = (x, y) \in E$.

Перевіряємо, чи буде E еліптичною кривою по модулю будь-якого $p \mid n$. Для цього кубічний многочлен в правій частині рівняння не повинен мати кратних коренів за модулем p. Це справедливо тоді і тільки тоді, коли НСД$(4a^3+27b^2, n) = 1$. Якщо НСД не дорівнює 1 або n, ми отримуємо дільник n. Якщо

[a] geor.polina@gmail.com

цей НСД дорівнює n, то слід обрати іншу еліптичну криву.

Вибираємо два натуральних числа B і C. Тут B – максимальна величина простого дільника цілого числа k, на яке необхідно множити точку P. Число C являється верхньою межею для того простого дільника $p \mid n$, з яким необхідно отримати співвідношення $kP(\mathrm{mod}\, p) = O(\mathrm{mod}\, p)$. Далі вибираємо k по формулі

$$k = \prod_{l \le B} l^{\alpha_l}$$

Тоді, згідно теореми Хассе, якщо $p + 1 + 2\sqrt{p} < C$ і порядок кривої $E(\mathrm{mod}\, p)$ не ділиться ні на яке просте число, більше B, то k кратне цьому порядку і тому $kP(\mathrm{mod}\, p) = O(\mathrm{mod}\, p)$. Працюючи по модулю n, намагаємось обчислювати kP таким чином. Використовуючи метод повторного подвоєння, знаходимо $2, 2(2P), 2(4P), ..., 2^{\alpha_2}P$, потім $3(2^{\alpha_2})P, 3(3(2^{\alpha_2}P)), ..., 3^{\alpha_3}2^{\alpha_2}P$ і т.д., поки не отримаємо $\prod_{l \le B} l^{\alpha_l} P$ (множимо, послідовно переходячи від найменших простих дільників l числа k до найбільших). У цих обчисленнях, при кожному діленні по модулю n застосовуємо алгоритм Евкліда для знаходження зворотнього елемента. Якщо на якійсь стадії алгоритм Евкліда не дає зворотнього елемента, то або знайдений нетривіальний дільник n, або НСД n і цього знаменника дорівнює n. В останньому випадку слід повернутися до початку і обрати іншу пару (E, P). Якщо алгоритм Евкліда завжди дає зворотній елемент, і таким чином, $kP(\mathrm{mod}\, p)$ обчислюється, слід повернутися до початку і обрати іншу пару (E, P).

2. Узагальнення теореми Ленстра для поліномів

Розглянемо випадок для $p > 3$.
Позначимо через $f(x) \in F_p[x]$ – звідний поліном, $\deg f(x) = n$. Нехай дано еліптичну криву над скінченним полем $F_p[x]/f(x)$, яка описується рівняння виду $y^2 = x^3 + ax + b,\ \ a, b \in F_p[x]$.
Вважаємо, що многочлен $y^2 = x^3 + ax + b$ має різні корені, тобто $4a^3 + 27b^2 \neq 0$ Надалі будемо припускати, що $4a^3 + 27b^2$ не має з $f(x)$ загальних множників; іншими словами, що $x^3 + ax + b$ не має кратних коренів за модулем $g(x)$ для будь-якого простого дільника $g(x)$ полінома $f(x)$. На практиці, вибираючи коефіцієнти a, b, ми перевіряємо, чому дорівнює НСД$(4a^3 + 27b^2, f(x))$. Якщо результат більше 1, то ми знайшли нетривіальний дільник $f(x)$ і задача вирішена. Далі будемо припускати, що НСД$(4a^3 + 27b^2, f(x))$=1.

Нехай потрібно знайти кратну kP для точки P. Знайти кратну точку за $O(log\, k)$ кроків можливо двома способами: методом подвоєння точки, або додаванням двох різних точок. Ми будемо розглядати точку P і всі її кратні по модулю $g(x)$. Кожен раз при обчисленні кратної точки kP , фактично будемо обчислювати лише лишки її координат по модулю $g(x)$. Всі обчислення можна проводити за модулем $g(x)$, якщо виконана нетривіальна умова: всі знаменники координат точок повинні бути взаємно прості з $g(x)$.

Теорема Ленстра ($p > 3$)
Нехай E – еліптична крива, яка описується рівнянням:

$$y^2 = x^3 + ax + b,\ \ a, b \in F_p[x]$$

та НСД$(4a^3 + 27b^2, n) = 1$
Нехай P_1 та P_2 – дві точки на E, у яких знаменники координат взаємно прості з $f(x)$, та $P_1 \neq -P_2$. Тоді $P_1 + P_2 \in E$ має координати, у яких знаменники взаємно прості з $f(x)$, тоді і тільки тоді, коли у $f(x)$ немає незвідного дільника $g(x)$, для якого сума точок $P_1(\mathrm{mod}\, g(x))$ і $P_2(\mathrm{mod}\, g(x)$ на еліптичній кривій $E(\mathrm{mod}\, g(x))$ дорівнювала б точці на нескінченності $O(\mathrm{mod}\, g(x)) \in E(\mathrm{mod}\, g(x))$. Тут $E(\mathrm{mod}\, g(x))$ позначає еліптичну криву над полем $F_p[x]/g(x)$.

Доведення.
Нехай всі точки $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, та $P_1 + P_2 \in E$ спочатку мають координати із знаменниками, які взаємно прості з $f(x)$. Необхідно довести, що для будь-якого незвідного дільника $g(x)$ полінома $f(x)$ сума $P_1(\mathrm{mod}\, g(x)) + P_2(\mathrm{mod}\, g(x)) \neq$
$\neq O(\mathrm{mod}\, g(x))$.

Якщо $x_1 \neq x_2(\mathrm{mod}\, g(x))$, то з визначення операції додавання точок на $E(\mathrm{mod}\, g(x))$ слідує, що $P_1(\mathrm{mod}\, g(x)) + P_2(\mathrm{mod}\, g(x)) \neq O(\mathrm{mod}\, g(x))$.

Припустимо, що $x_1 \equiv x_2(\mathrm{mod}\, g(x))$. При $P_1 = P_2$ координати точки $P_1 + P_2 = 2P_1$ та визначаються формулами [1]

$$x_3 = \lambda^2 - 2x \tag{1}$$

$$y_3 = -y + \lambda(x - x_3)$$

$$\lambda = \frac{3x^2 + a}{2y}$$

в яких кожний член замінюється його лишком по модулю $g(x)$. Необхідно показати, що знаменник $2y_1$ дробу в правій частині (1) не ділиться на $g(x)$. Але, якби він ділився на $g(x)$, то і $3x^2 + a$ ділилося б на $g(x)$. Тоді x_1 був би коренем по модулю $g(x)$ як многочлена $x^3 + ax + b$, так і його похідної $3x^2 + a$. Але це суперечить припущенню, що у даного многочлена відсутні кратні корені по модулю $g(x)$. Тепер нехай $P_1 \neq P_2$. Координати точки $P_1 + P_2 = P_3$ визначаються за наступними формулами [1]

$$x_3 = \lambda^2 - x_1 - x_2, \tag{2}$$
$$y_3 = -y_1 + \lambda(x_1 - x_3),$$
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

Так як $x_1 \equiv x_2(\mathrm{mod}\, g(x))$ та $x_1 \neq x_2$, можна записати $x_2 = x_1 + g(x)^r x$, де $r \ge 1$ вибрано так, що ні чисельник, ні знаменник x не діляться на $g(x)$. За

припущенням знаменники координат точки $P_1 + P_2$ не діляться на $g(x)$, тому із формул (2) слідує, що $y_2 = y_1 + g(x)^r y$. З іншого боку

$$y_2^2 = (x_1 + g(x)^r x)^3 + a(x_1 + g(x)^r x) + b \equiv$$
$$\equiv x_1^3 + ax_1 + b + g(x)^r x(3x_1^2 + a) =$$
$$= y_1^2 + g(x)^r x(3x_1^2 + a) (\mathrm{mod}\, g(x)^{r+1}) \qquad (3)$$

Так як
$x_2 \equiv x_1 (\mathrm{mod}\, g(x))$ та $y_2 \equiv y_1 (\mathrm{mod}\, g(x))$,
то $P_1 (\mathrm{mod}\, g(x)) \equiv P_2 (\mathrm{mod}\, g(x))$,
тобто
$P_1 (\mathrm{mod}\, g(x)) + P_2 (\mathrm{mod}\, g(x)) = 2P_1 (\mathrm{mod}\, g(x))$. Очевидно, що $2P_1 (\mathrm{mod} g(x)) = O(\mathrm{mod}\, g(x))$ тоді і тільки тоді, коли $y_1 \equiv y_2 \equiv O(\mathrm{mod}\, g(x))$. Якщо це рівняння виконуються, то

$$y_2^2 - y_1^2 = (y_2 - y_1)(y_2 + y_1) \qquad (4)$$

повинно ділитися на $g(x)^{r+1}$ (тобто повинен ділитися на $g(x)^{r+1}$ чисельник цього виразу). Тому із (3) слідувало б, що $3x_1^2 + a \equiv O(\mathrm{mod}\, g(x))$. Але це неможливо, оскільки $x^3 + ax + b$ не має кратних коренів по модулю $g(x)$, тобто x_1 не може бути загальним коренем цього многочлена і його похідної. Значить, $P_1 (\mathrm{mod}\, g(x)) + P_2 (\mathrm{mod}\, g(x)) \neq O(\mathrm{mod}\, g(x))$, як і стверджувалось.

Зворотньо, нехай
$P_1 (\mathrm{mod}\, g(x)) + P_2 (\mathrm{mod}\, g(x)) \neq O(\mathrm{mod}\, g(x))$
для кожного незвідного дільника $g(x)$ полінома $f(x)$. Фіксуємо деякий поліном $g(x) \mid f(x)$ Формули (1) та (2) показують, що якщо $x_2 \neq x_1 (\mathrm{mod}\, g(x))$, то знаменників, які діляться на $g(x)$ немає. Тому припустимо, що $x_2 \equiv x_1 (\mathrm{mod}\, g(x))$.
Тоді $y_2 \equiv \pm y_1 (\mathrm{mod}\, g(x))$, але так як
$P_1 (\mathrm{mod}\, g(x)) + P_2 (\mathrm{mod}\, g(x)) \neq O(\mathrm{mod}\, g(x))$,
то $y_2 \equiv y_1 \neq O(\mathrm{mod}\, g(x))$.
При $P_2 = P_1$ формули (1) разом з умовою $y_1 \neq O(\mathrm{mod}\, g(x))$ показують, що знаменники координат точки $P_1 + P_2 = 2P_1$ взаємно прості з $g(x)$. Якщо $P_2 \neq P_1$, знову записуємо x_2 у вигляді $x_2 = x_1 + p^r x$, де x не ділиться на $g(x)$, і використовуючи рівняння (3), отримуємо
$\frac{(y_2^2 - y_1^2)}{(x_2 - x_1)} \equiv 3x_1^2 + a (\mathrm{mod}\, g(x))$.
Так як $g(x)$ не ділить $y_1 = y_2 \equiv 2y_1 (\mathrm{mod}\, g(x))$, звідси слідує, що знаменник числа
$\frac{y_2^2 - y_1^2}{(y_1 + y_2)(x_2 - x_1)} = \frac{y_2 - y_1}{x_2 - x_1}$
не ділиться на $g(x)$, і в силу формул (2) знаменники координат точки $P_1 + P_2$ не діляться на $g(x)$. Теорема доведена.

Розглянемо випадок для $p = 2$.

Для цього випадку наведемо формулювання та доведення теореми Ленстра в одну сторону.

Позначимо через $f(x) \in F_2[x]$ – звідний поліном, $\deg f(x) = n$. В даному розділі ми будемо використовувати несуперсингулярну еліптичну криву над кільцем $F_2[x]$. Нехай ця крива описується рівнянням виду $y^2 + xy = x^3 + ax^2 + b,\ \ b \neq 0$, та P_1 і P_2 – дві точки на ній. Визначимо формули для додавання цих точок.

Якщо $P_1 = P_2$, то $P_1 + P_2 = 2P_1$ і визначається по формулам:[2]

$$x = \lambda^2 + \lambda + a \qquad (5)$$
$$y = x^2 + (\lambda + 1)x$$
$$\lambda = x + \frac{y}{x}$$

Якщо $P_1 \neq P_2$, то $P_1 + P_2 = P_3$ і визначається по формулам:[2]

$$x_3 = \lambda^2 + \lambda + a + x_1 + x_2, \qquad (6)$$
$$y_3 = x_3 + y_1 + \lambda(x_3 + x_1),$$
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

Надалі будемо припускати, що b не має з $f(x)$ загальних множників; іншими словами, що $x^3 + ax^2 + b$ не має кратних коренів за модулем $g(x)$ для будь-якого незвідного дільника $g(x)$ полінома $f(x)$. На практиці, вибираючи коефіцієнт b, ми перевіряємо, чому дорівнює НСД$(b(x), f(x))$. Якщо результат більше 1, то ми знайшли нетривіальний дільник $f(x)$ і задача вирішена. Далі будемо припускати, що НСД$(b(x), f(x))$=1.

Теорема Ленстра ($p = 2$)
Нехай E – еліптична крива, яка описується рівнянням:

$$y^2 + xy = x^3 + ax^2 + b,\ \ b \neq 0$$

Нехай P_1 та P_2 – дві точки на E, у яких знаменники координат взаємно прості з $f(x)$, та $P_1 \neq -P_2$, та $P_1 + P_2 \in E$ має координати, у яких знаменники взаємно прості з $f(x)$. Тоді для будь-якого незвідного $g(x)$, такого що $g(x) \mid f(x)$, виконується:
$P_1 (\mathrm{mod}\, g(x)) + P_2 (\mathrm{mod}\, g(x)) \neq O(\mathrm{mod}\, g(x))$

Доведення.
Розглянемо два випадки.

1. Нехай $x_1 \neq x_2 (\mathrm{mod}\, g(x))$
Тоді $P_1 (\mathrm{mod}\, g(x)) \neq P_2 (\mathrm{mod}\, g(x))$ і додавання цих точок виконується за формулою (6). Тоді знаменник у першій координаті $P_1 + P_2$ дорівнює
$x_2^2 - x_1^2 = (x_2 - x_1)^2 \neq O(\mathrm{mod}\, g(x))$,
отже
$P_1 (\mathrm{mod}\, g(x)) + P_2 (\mathrm{mod}\, g(x)) \neq O(\mathrm{mod}\, g(x))$.

2. Нехай $x_1 \equiv x_2 (\mathrm{mod}\, g(x))$.
Тут також можливі два випадки.
2а. Нехай $P_1 = P_2$.
Тоді точка $P_1 + P_2$ визначається за формулою (5),так само і $P_1 (\mathrm{mod}\, g(x)) + P_2 (\mathrm{mod}\, g(x))$. За умовою, знаменник $P_1 + P_2$ не ділиться на $g(x)$, звідси випливає, що $(x_1, g(x)) = 1$, а отже і $(x_1 (\mathrm{mod}\, g(x), g(x)) = 1$, а це означає, що
$P_1 (\mathrm{mod}\, g(x)) + P_2 (\mathrm{mod}\, g(x)) = 2P_1 (\mathrm{mod}\, g(x)) \neq$

$\neq O(\mathrm{mod}\, g(x))$
2б. Нехай
$P_1 \neq P_2$, але $P_1(\mathrm{mod}\, g(x)) = P_2(\mathrm{mod}\, g(x))$.
Якщо при цьому $P_1(\mathrm{mod}\, g(x)) + P_2(\mathrm{mod}\, g(x)) =$
$= O(\mathrm{mod}\, g(x))$,
то $x_1(\mathrm{mod}\, g(x)) = 0$, але тоді $x_1^2 \equiv O(\mathrm{mod}\, g(x))$, тобто x_1 кратний корінь тричлена $x^3 + ax^2 + b$, що суперечить умові при якій ми вводили еліптичну криву.
Тому
$P_1(\mathrm{mod}\, g(x)) + P_2(\mathrm{mod}\, g(x)) \neq O(\mathrm{mod}\, g(x))$.

Висновки

В даній роботі ми розглянули алгоритм Ленстра для факторизації чисел, і теорему що обгрунтовує нетривіальну умову у цьому алгоритмі. Базуючись на цьому ми розробили та довели теорему Ленстра для поліномів кільця характеристики $p > 3$, а також розробили і довели в один бік цю саму теорему для випадку $p = 2$. Завдяки цим результатам ми почали створювати теоретичний фундамент для розробки алгоритму Ленстра для поліномів кільця довільної характеристики.

Перелік використаних джерел

1. Коблиц Н. Курс теории чисел и криптографии. — М. : Научное изд-во ТВП, 2001. — 260 с.
2. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. — М. : КомКнига, 2006. — 280 с.