УДК 512.7

Бойко Д. А.

DOI: https://doi.org/10.18523/2617-70803202011-24

ОБЧИСЛЕННЯ ДИВІЗОРІВ НА ГІПЕРЕЛІПТИЧНІЙ КРИВІЙ ТА ЇХНЄ ПРИКЛАДНЕ ЗАСТОСУВАННЯ НА МОВІ PYTHON

В роботі розглядаються гіпереліптичні криві роду $g > 1$, дивізори на них та їхнє прикладне застосування на мові програмування Python. Наведено основні необхідні означення та відомі властивості про гіпереліптичні криві, представлено поняття поліноміальної функції, переведення його у єдину форму, а також поняття раціональної функції, норми, степеня та спряженого до многочлена. Ці факти потрібні для обчислення порядку точок функцій, тим самим і для швидкого та ефективного обчислення дивізорів. Продемонстровано означення дивізора на гіпереліптичній кривій, наведено основні відомі властивості дивізора. Наведено приклад обчислення дивізора поліноміальної функції, описано зведені та напівзведені дивізори, доведено теореми про існування такого напівзведеного дивізора, котрий не є єдиним, а також існування єдиного зведеного дивізора, який еквівалентний початковому. Зокрема, напівзведений дивізор може бути зображений у вигляді НСД дивізорів двох поліноміальних функцій. Також продемонстрований факт, що кожний зведений дивізор можна єдиним способом зобразити у вигляді пари многочленів $[a(x), b(x)]$, це і є зображенням Мамфорда, наведено декілька прикладів його обчислення.

Описано алгоритм Кантора обчислення суми двох дивізорів, його «композиційної» частини, за допомогою якого утворюється напівзведений дивізор (який не є єдиним), а також редукційної частини, котра зводить напівзведений дивізор у єдиний зведений. Описано особливий випадок «композиційної» частини: подвоєння дивізора, що суттєво зменшує час роботи алгоритму. Доведено коректність алгоритмів, наведено приклади застосувань.

Основним результатом роботи є розробка обчислення дивізора поліноміальної функції, зображення Мамфорда, алгоритму Кантора у вигляді програмного коду на мові програмування Python.

Таким чином, метою роботи є демонстрація можливості легко та ефективно використовувати описані алгоритми для подальшої роботи з дивізорами на гіпереліптичній кривій, в тому числі для розробки криптосистеми, цифрового підпису на основі гіпереліптичних кривих, атаки на таку криптосистему.

Ключові слова: гіпереліптична крива; дивізор; зображення Мамфорда.

Вступ

Робота присвячена обчисленню дивізорів на гіпереліптичній кривій, їхнім прикладним застосуванням. На початку будуть розглянуті необхідні факти про гіпереліптичні криві, які нам знадобляться в подальшому, буде представлений алгоритм обчислення порядків точок поліноміальних функцій, що допоможе нам обчислювати дивізори.

Після цього буде розглянуто саме поняття дивізора та різних операцій з ним: обчислення дивізора поліноміальної функції в точці, зображення Мамфорда для дивізора, обчислення суми двох дивізорів, подвоєного дивізора та процес перетворення напівзведеного дивізора на зведений.

Буде доведено коректність алгоритмів, наведено приклади застосувань, а також кожен з них буде імплементовано в програми на мові Python (які можна знайти в кінці роботи), що дасть можливість ефективно використовувати алгоритми для подальшої роботи з дивізорами.

Означення 1. Нехай $\mathbb{F}$ — поле, а $\overline{\mathbb{F}}$ — його алгебраїчне замикання. **Гіпереліптичною кривою H роду** $g \geq 1$ над полем $\mathbb{F}$ називають рівняння вигляду

$$\mathsf{H} : y^2 + h(x)y = f(x) \text{ в } \mathbb{F}[x, y],$$

де $h(x) \in \mathbb{F}[x]$, $\deg h(x) \leq g$, $f(x) \in \mathbb{F}[x]$ — унітарний, $\deg f(x) = 2g + 1$, а також не існує розв'язків $(x, y) \in \overline{\mathbb{F}} \times \overline{\mathbb{F}}$, які б одночасно задовольняли $y^2 + h(x)y = f(x)$ та його частинні похідні: $2y + h(x) = 0$ і $h'(x)y - f'(x) = 0$.

Означення 2. Нехай $\mathbb{K}$ — розширення поля $\mathbb{F}$ (в тому числі і $\mathbb{K} = \mathbb{F}$).

Множина $\mathbb{K}$-(раціональних) точок на гіпе-

реліптичній кривій H — це множина

$$\mathsf{H}(\mathbb{K}) = \{(x,y) \in \overline{\mathbb{F}} \times \overline{\mathbb{F}} \,|\, y^2 + h(x)y = f(x)\} \cup \{\infty\}.$$

Якщо $P = (x,y)$ — $\mathbb{K}$-(раціональна) точка гіпереліптичної кривої H, то визначимо **протилежну** до неї точку $\widetilde{P}$ як точку з тією самою координатою x, що задовольняє рівняння кривої:

$$\widetilde{P} = (x, -y - h(x)).$$

Якщо $P = \infty$, то покладемо $\widetilde{P} = \infty$. Точка P називається **особливою**, якщо $\widetilde{P} = P$.

Поліноміальні та раціональні функції на гіпереліптичній кривій

Означення 3. Позначимо

$$\mathbb{F}[\mathsf{H}] = \mathbb{F}[x,y]/(y^2 + h(x)y - f(x)),$$

де $(y^2 + h(x)y - f(x))$ позначає ідеал в $\mathbb{F}[x,y]$, породжений цим же многочленом.
Аналогічно визначимо

$$\overline{\mathbb{F}}[\mathsf{H}] = \overline{\mathbb{F}}[x,y]/(y^2 + h(x)y - f(x)).$$

Елемент $\overline{\mathbb{F}}[\mathsf{H}]$ називається **поліноміальною функцією** на гіпереліптичній кривій H.

Для поліноміальної функції $G(x,y) \in \overline{\mathbb{F}}[\mathsf{H}]$ можемо підставити $f(x) - h(x)y$ замість y^2 і отримати єдине зображення функції у вигляді

$$G(x,y) = a(x) - b(x)y, \text{ де } a(x), b(x) \in \overline{\mathbb{F}}[x].$$

Означення 4. Нехай $G(x,y) = a(x) - b(x)y$ — поліноміальна функція в $\overline{\mathbb{F}}[\mathsf{H}]$. **Спряженим** до $G(x,y)$ називають поліноміальну функцію

$$\overline{G}(x,y) = a(x) + b(x)(h(x) + y).$$

Нормою $G(x,y)$ називають поліноміальну функцію

$$N(G) = G \cdot \overline{G}.$$

Лема 1 (властивості норми)**.** *Нехай $G, L \in \overline{\mathbb{F}}[\mathsf{H}]$ – деякі поліноміальні функції. Мають місце такі властивості:*

1. *$N(G)$ — поліноміальна функція в $\overline{\mathbb{F}}[x]$;*
2. *$N(\overline{G}) = N(G)$;*
3. *$N(GL) = N(G) \cdot N(L)$.*

Доведення. Позначимо

$$G(x,y) = a(x) - b(x)y =: a - by,$$

$$L(x,y) = c(x) - d(x)y =: c - dy,$$

де $a(x), b(x), c(x), d(x) \in \overline{\mathbb{F}}[x]$.

$N(G) = G \cdot \overline{G} = (a - by) \cdot (a + b(h+y)) = |y^2 = f - hy| = a^2 + abh - b^2 f \in \overline{\mathbb{F}}[x]$.

$N(\overline{G}) = N(G) \iff \overline{G} \cdot \overline{\overline{G}} = G \cdot \overline{G} \iff \overline{\overline{G}} = G$.

$\overline{\overline{G}} = a + bh + by = a + bh - b(h+y) = a - by = G$.

$N(GL) = GL \cdot \overline{GL}$. Маємо:

$GL = (a - by) \cdot (c - dy) = |y^2 = f - hy| = (ac + bdf) - (bc + ad + bdh)y$.

$\overline{GL} = (ac + bdf) + (bc + ad + bdh)(h + y) = |y^2 + hy = f| = ac + bc(h+y) + ad(h+y) + bd(h+y)^2 = (a + b(h+y)) \cdot (c + d(h+y)) = \overline{G} \cdot \overline{L}$.

Таким чином,
$N(GL) = GL \cdot \overline{GL} = G\overline{G} \cdot L\overline{L} = N(G) \cdot N(L)$.

Означення 5. Поле функцій $\mathbb{F}(\mathsf{H})$ ($\overline{\mathbb{F}}(H)$)— це поле дробів з $\mathbb{F}[\mathsf{H}]$ ($\overline{\mathbb{F}}[\mathsf{H}]$). Аналогічно визначимо поле функцій $\overline{\mathbb{F}}(H)$. Елементи $\overline{\mathbb{F}}(\mathsf{H})$ називають **раціональними функціями** на гіпереліптичній кривій H.

Означення 6. Нехай $R \in \overline{\mathbb{F}}(\mathsf{H})$ — раціональна функція, $P \in \mathsf{H} \backslash \{\infty\}$. Кажуть, що R визначена в точці P, якщо $\exists$ поліноміальні функції $G, L \in \in \overline{\mathbb{F}}[\mathsf{H}]$ такі, що $R = \dfrac{G}{L}$ і $L(P) \neq 0$, тоді значення отримується у вигляді: $R(P) = \dfrac{G(P)}{L(P)}$;
в іншому випадку R не визначена в точці P.

Означення 7. Нехай $G(x,y) = a(x) - b(x)y$ — ненульова поліноміальна функція в $\overline{\mathbb{F}}[\mathsf{H}]$. **Степінь** $G(x,y)$ визначають як:

$$\deg(G) = \max\{2\deg_x(a), 2g + 1 + 2 \cdot \deg_x(b)\}.$$

Означення 8. Нехай $R = \dfrac{G}{L} \in \overline{\mathbb{F}}(\mathsf{H})$ — раціональна функція. Тоді **значення** R в точці $P = \infty$ визначають так:

- якщо $\deg(G) < \deg(L)$, то значення R в точці $P = \infty$ позначається як $R(\infty) = 0$;
- якщо $\deg(G) > \deg(L)$, то значення R в точці $P = \infty$ не визначено;
- якщо $\deg(G) = \deg(L)$, то значення R в точці $P = \infty$ обчислюється як відношення старших коефіцієнтів поліноміальних функцій G, L.

Означення 9. Нехай $R = \dfrac{G}{L} \in \overline{\mathbb{F}}(\mathsf{H})$ — раціональна функція, $P \in \mathsf{H}$. Тоді

- якщо $R(P) = 0$, то R має **нуль в точці** P;
- якщо R не визначена в точці P, то R має **полюс в точці** P, в цьому випадку $R(P) = \infty$.

Означення 10 (порядок функції в точці)**.** Нехай $G(x,y) = a(x) - b(x)y$, де $a(x), b(x) \in \overline{\mathbb{F}}[x]^*$, $P \in \mathsf{H}$. **Порядок поліноміальної функції** G в точці P, який позначається $ord_P(G)$, визначають так:

1. Якщо $P = (x,y)$ — скінченна точка на гіпереліптичній кривій H, то
   а) покладемо r — найвищий степінь $x -$

x_0, який ділить і $a(x)$, і $b(x)$, тобто

$$G(x,y) = (x-x_0)^r(a_0(x) - b_0(x)y);$$

б) якщо $a_0(x) - b_0(x)y_0 \neq 0$, то покладемо $s = 0$. В іншому випадку, s — найвищий степінь $x - x_0$, який ділить норму

$$N(a_0(x) - b_0(x)y) = a_0^2 + a_0b_0h - b_0^2f;$$

в) якщо P — звичайна точка на гіпереліптичній кривій H, то $ord_P(G) = r + s$. якщо P — особлива точка, то $ord_P(G) = 2r + s$.

2. Якщо $P = \infty$, то $ord_P(G) = -\max\{2\deg_x(a), 2g+1+2\deg_x(b)\}$.

Означення 11 (порядок раціональної функції в точці)**.** Нехай $R = \dfrac{G}{L} \in \overline{\mathbb{F}}(\mathsf{H})^*$ — раціональна функція, $P \in \mathsf{H}$. **Порядок раціональної функції** R в точці P обчислюють так:

$$ord_P(R) = ord_P(G) - ord_P(L).$$

Теорема 2. *Нехай $G(x,y) \in \overline{\mathbb{F}}[\mathsf{H}]^*$. Тоді поліноміальна функція G має скінченну кількість нулів та полюсів. Більш того,*

$$\sum_{P\in\mathsf{H}} ord_P(G) = 0.$$

Зауваження 1. Всі отримані вище факти дають змогу легко та ефективно обчислювати порядок точок поліноміальної функції, і тим самим їхні дивізори, про які піде мова далі.

Дивізори

Означення 12. Дивізор на гіпереліптичній кривій H визначають як формальну суму

$$\mathsf{D} = \sum_{P\in\mathsf{H}} m_P P,\ m_P \in \mathbb{Z},$$

де лише скінченна кількість $m_P \in \mathbb{Z}$ не дорівнює 0.

Степенем дивізора D називають суму коефіцієнтів

$$\deg \mathsf{D} = \sum_{P\in\mathsf{H}} m_P \in \mathbb{Z}.$$

Порядком дивізора D у точці P називають число

$$ord_P(\mathsf{D}) = m_P \in \mathbb{Z}.$$

Множина всіх дивізорів, яка позначається $\mathbb{D}$, утворює групу відносно додавання, визначеного правилом

$$\sum_{P\in\mathsf{H}} m_P P + \sum_{P\in\mathsf{H}} n_P P = \sum_{P\in\mathsf{H}} (m_P + n_P)P.$$

Множина всіх дивізорів степеня 0, яка позначається $\mathbb{D}^0$, утворює підгрупу групи $\mathbb{D}$.

Означення 13. Нехай $\mathsf{D}_1 = \sum_{P\in\mathsf{H}} m_P P$, $\mathsf{D}_2 = \sum_{P\in\mathsf{H}} n_P P$ — дивізори на гіпереліптичній кривій H. Найбільший спільний дільник дивізорів D_1 і D_2 визначається як

$$\text{НСД}(\mathsf{D}_1, \mathsf{D}_2) =$$

$$\sum_{P\in\mathsf{H}} \min\{m_p, n_P\}P - \left(\sum_{P\in\mathsf{H}} \min\{m_p, n_P\}\right)\infty.$$

Зазначимо, що $\text{НСД}(\mathsf{D}_1, \mathsf{D}_2) \in \mathbb{D}^0$.

Означення 14. Нехай $R \in \overline{\mathbb{F}}(\mathsf{H})^*$ — ненульова раціональна функція. **Дивізор раціональної функції** R на гіпереліптичній кривій H визначають як

$$div(R) = \sum_{P\in\mathsf{H}} (ord_P R)P.$$

Зазначимо, що якщо $R = \dfrac{G}{L}$, то $div(R) = div(G) - div(L)$. Теорема 2 показує, що дивізор раціональної функції R є скінченною формальною сумою і $\deg(div(R)) = 0$.

Означення 15. Дивізор $\mathsf{D} \in \mathbb{D}^0$ називають **головним дивізором**, якщо $\mathsf{D} = div(R)$ для деякої ненульової раціональної функції $R \in \overline{\mathbb{F}}[\mathsf{H}]^*$.

Множина всіх головних дивізорів, яку позначають $\mathbb{P}$, утворює підгрупу групи $\mathbb{D}^0$, а фактор-групу $\mathbb{J} = \mathbb{D}^0/\mathbb{P}$ називають якобіаном гіпереліптичної кривої H.

Відмітимо також деякі інші властивості дивізора раціональної функції.

Властивості:

1. $div(R) = 0 \iff R = const \not\equiv 0$ в $\overline{\mathbb{F}}(\mathsf{H})$;
2. $div(R_1R_2) = div(R_1) + div(R_2)$ для деяких ненульових раціональних функцій R_1, R_2;
3. $div(R^n) = n \cdot div(R)\ \forall\, n \in \mathbb{N}$;
4. $div(R_1) = div(R_2) \iff R_1 = \alpha R_2$ для деяких ненульових раціональних функцій R_1, R_2 та деякого $\alpha \neq 0$ в $\overline{\mathbb{F}}(\mathsf{H})$.

Приклад 1. Розглянемо поліноміальну функцію $G(x,y) = x - x_0$ та точку $P = (x_0, y_0)$ на деякій гіпереліптичній кривій H. Тоді:

- якщо P — звичайна точка на гіпереліптичній кривій H, то $div(G) = P + \widetilde{P} - 2\infty$;
- якщо ж P — особлива точка на гіпереліптичній кривій H, тобто $P = \widetilde{P}$, то $2P = 0$. Таким чином, $div(G) = 2P - 2\infty$.

Обчислення дивізора поліноміальної функції

Нехай $G = a(x) - b(x)y \in \overline{\mathbb{F}}[\mathsf{H}]$ — ненульова поліноміальна функція, $P \in \mathsf{H}$.

Алгоритм оформлений у вигляді коду на мові Python та описаний в розділі «Імплементація алгоритмів на мові Python». Розглянемо приклад застосування алгоритму.

Приклад 2. Нехай задана гіпереліптична крива

$\mathsf{H} : y^2 + xy = x^5 + 5x^4 + 6x^2 + x + 3$ над полем $\mathbb{F}_7$.

Знайдемо дивізор поліноміальної функції

$$G(x, y) = y^2 + xy + 6x^4 + 6x^3 + x^2 + 6x.$$

Розв'язок. Підставимо в $G\, y^2 = f(x) - h(x)y$, отримаємо: $G(x, y) = x^5 + 11x^4 + 6x^3 + 7x^2 + 7x + 3 \equiv x^5 + 4x^4 + 6x^3 + 3 \pmod 7$.
Звідси бачимо, що

$$a(x) = x^5 + 4x^4 + 6x^3 + 3, b(x) = 0.$$

Наступні точки задовольняють гіпереліптичну криву H: $(1, 1)$, $(1, 5)$, $(2, 2)$, $(2, 3)$, $(5, 3)$, $(5, 6)$, $(6, 4)$ і нескінченно віддалена точка.
Знайдемо порядок поліноміальної функції G в цих точках. Детально розпишемо для першої точки, для інших точок розв'язок надасть нам програма, описана в кінці роботи.

- $P = (1, 1)$:
  - Обчислення r:
    - $r = 5$ очевидно не підходить, бо тоді $a_0(x) = 1$ і тому $(x - 1)^5 = a(x)$, однак це не так;
    - $r = 4$ не підходить, бо $a(x) = (x + 1)(x - 1)^4 + 4x^3 + 5x^2 + 4x + 2 \pmod 7$;
    - $r = 3$ не підходить, бо $a(x) = (x^2 + 3)(x - 1)^3 + 3x^2 - x - 1 \pmod 7$;
    - $r = 2$ не підходить, бо $a(x) = (x^3 + 6x^2 + 3x)(x - 1)^2 + 4x + 3 \pmod 7$;
    - $r = 1$. Тоді $a(x) = (x - 1)(x^4 + 5x^3 + 4x^2 + 4x + 4) \pmod 7$.

    Отже, $r = 1, a_0(x) = x^4 + 5x^3 + 4x^2 + 4x + 4$.
  - Обчислення s: $a_0(1) = 4 \not\equiv 0 \pmod 7$, звідси $s = 0$.
  - Визначимо, чи є P особливою точкою. $\widetilde{P} = |\widetilde{P} = (x, -y - h(x))| = (1, 5) \neq P$,
    тому $ord_P(G) = r + s = 1$.

  Аналогічним чином, визначимо для інших точок.
- $P = (1, 5)$:
  - $a(x) = (x - 1)(x^4 + 5x^3 + 4x^2 + 4x + 4) \pmod 7$. Отже, $r = 1, a_0(x) = x^4 + 5x^3 + 4x^2 + 4x + 4$.
  - $a_0(1) = 4 \not\equiv 0 \pmod 7$, звідси $s = 0$.
  - $\widetilde{P} = (1, 1) \neq P$, тому $ord_P(G) = r + s = 1$.
- $P = (2, 2)$:
  - $a(x) = (x - 2)^2(x^3 + x^2 + 6x + 6) \pmod 7$. Отже, $r = 2, a_0(x) = x^3 + x^2 + 6x + 6$.
  - $a_0(2) = 2 \not\equiv 0 \pmod 7$, звідси $s = 0$.
  - $\widetilde{P} = (2, 4) \neq P$, тому $ord_P(G) = r + s = 2$.
- $P = (2, 3)$:
  - $a(x) = (x - 2)^2(x^3 + x^2 + 6x + 6) \pmod 7$. Отже, $r = 2, a_0(x) = x^3 + x^2 + 6x + 6$.
  - $a_0(2) = 2 \not\equiv 0 \pmod 7$, звідси $s = 0$.
  - $\widetilde{P} = (2, 2) \neq P$, тому $ord_P(G) = r + s = 2$.
- $P = (5, 3)$:
  - $a(x) = (x - 5)^0(x^5 + 4x^4 + 6x^3 + 3) \pmod 7$. Отже, $r = 0, a_0(x) = x^5 + 4x^4 + 6x^3 + 3$.
  - $a_0(5) = 1 \not\equiv 0 \pmod 7$, звідси $s = 0$.
  - $\widetilde{P} = (5, 6) \neq P$, тому $ord_P(G) = r + s = 0$.
- $P = (5, 6)$:
  - $a(x) = (x - 5)^0(x^5 + 4x^4 + 6x^3 + 3) \pmod 7$. Отже, $r = 0, a_0(x) = x^5 + 4x^4 + 6x^3 + 3$.
  - $a_0(5) = 1 \not\equiv 0 \pmod 7$, звідси $s = 0$.
  - $\widetilde{P} = (5, 3) \neq P$, тому $ord_P(G) = r + s = 0$.
- $P = (6, 4)$:
  - $a(x) = (x - 6)^2(x^3 + 2x^2 + x + 3) \pmod 7$. Отже, $r = 2, a_0(x) = x^3 + 2x^2 + x + 3$.
  - $a_0(6) = 3 \not\equiv 0 \pmod 7$, звідси $s = 0$.
  - $\widetilde{P} = (6, 4) = P$, тому $ord_P(G) = 2r + s = 4$.
- $P = \infty$:
  - $ord_P(G) = -\max\{2 \deg_x(a), 2g + 1 + 2 \deg_x(b)\} = -\max\{2 \cdot 5, 2 \cdot 2 + 1\} = -10$.

Таким чином одержали дивізор поліноміальної функції G: $div(G) = 1 \cdot (1, 1) + 1 \cdot (1, 5) + 2 \cdot (2, 2) + 2 \cdot (2, 3) + 4 \cdot (6, 4) - 10 \cdot \infty$.

Напівзведені дивізори

Означення 16. Нехай D_1, D_2 — дивізори на гіпереліптичній кривій H. Якщо $\mathsf{D}_1, \mathsf{D}_2 \in \mathbb{D}^0$, то дивізори D_1 та D_2 називають **еквівалентними** ($\mathsf{D}_1 \sim \mathsf{D}_2$).

Означення 17. Нехай $\mathsf{D} = \sum\limits_{P \in \mathsf{H}} m_P P$ — дивізор. **Носієм дивізора** D називають множину

$$supp(\mathsf{D}) = \{P \in \mathsf{H} \,|\, m_P \neq 0\}.$$

Означення 18. Напівзведеним дивізором називають дивізор вигляду

$$\mathsf{D} = \sum_i m_i P_i - \left(\sum_i m_i\right)\infty, \text{ де}$$

- всі $m_i \geq 0$ і P_i — скінченна точка на гіпереліптичній кривій H така, що якщо $P_i \in supp(\mathsf{D})$, то $\widetilde{P}_i \in supp(\mathsf{D})$;
- якщо $P_i = \widetilde{P}_i \in supp(\mathsf{D})$, то $m_i = 1$ і лише одна з цих точок присутня в сумі.

Лема 3. *Для кожного дивізора* $\mathsf{D} \in \mathbb{D}^0$ *існує (але не єдиний) напівзведений дивізор* D_1 *такий, що* $\mathsf{D} \sim \mathsf{D}_1$.

Доведення. Нехай $\mathsf{D} = \sum_{P \in \mathsf{H}} m_P P$, $(\mathsf{H}_1, \mathsf{H}_2)$ — звуження множини (звичайних, не особливих) точок на гіпереліптичній кривій H таке, що:

1. $P \in \mathsf{H}_1 \iff \widetilde{P} \in \mathsf{H}_2$;
2. якщо $P \in \mathsf{H}_1$, то $m_P \geq m_{\widetilde{P}}$.

Нехай $\mathsf{H}_0 = \{P \in \mathsf{H} : P - \text{особлива точка}\}$. Тоді ми можемо записати, що $\mathsf{D} = \sum_{P \in \mathsf{H}_1} m_P P + \sum_{P \in \mathsf{H}_2} m_P P + \sum_{P \in \mathsf{H}_0} m_P P - m\infty$.

Розглянемо наступний дивізор: $\mathsf{D}_1 = \mathsf{D} - \sum_{P=(x_2,y_2)\in \mathsf{H}_2} m_P div(x - x_2) - \sum_{P=(x_0,y_0)\in \mathsf{H}_0} \left\lfloor \frac{m_P}{2} \right\rfloor div(x - x_0)$.

Тоді $\mathsf{D} \sim \mathsf{D}_1$. Враховуючи приклад 1 на початку розділу, отримаємо: $\mathsf{D}_1 = \mathsf{D} - \sum_{P \in \mathsf{H}_1} \left(m_P - m_{\widetilde{P}}\right) P + \sum_{P \in \mathsf{H}_0} \left(m_P - \left\lfloor \frac{m_P}{2} \right\rfloor\right) P - m_1\infty$, для деякого $m_1 \in \mathbb{Z}$, отже D_1 – напівзведений дивізор.

Зображення напівзведених дивізорів

Лема 4. *Нехай* $P = (x_0, y_0)$ *— звичайна точка на гіпереліптичній кривій* H, $R \in \overline{\mathbb{F}}(\mathsf{H})$ *— ненульова раціональна функція, яка не має полюса в точці* P. *Тоді* $\forall k \geq 0\, \exists!\, c_0, c_1, \ldots, c_k \in \overline{\mathbb{F}}$ *і* $\exists!\, R_k \in \overline{\mathbb{F}}(\mathsf{H})$ *такі, що*

$$R = \sum_{i=0}^{k} c_i (x - x_0)^i + (x - x_0)^{k+1} R_k,$$

причому R_k *не має полюса в точці* P.

Доведення. Існує єдине $c_0 := R(x_0, y_0) \in \overline{\mathbb{F}}$ таке, що P є нулем для $R - c_0$. Звідси отримаємо такий розклад:

$R - c_0 = (x - x_0)R_1$ для деякого $R_1 \in \overline{\mathbb{F}}(\mathsf{H})$ (така раціональна функція є єдиною), для якого $ord_P(R_1) \geq 0$.

Звідси $R = c_0 + (x - x_0)R_1$.

Аналогічно, існує єдине $c_1 := R_1(x_0, y_0) \in \overline{\mathbb{F}}$ таке, що P є нулем для $R_1 - c_1$, тому має місце розклад:

$R_1 - c_1 = (x - x_0)R_2$ для деякого $R_2 \in \overline{\mathbb{F}}(\mathsf{H})$ (така раціональна функція є єдиною), для якого $ord_P(R_2) \geq 0$. Звідси $R_1 = c_0 + (x - x_0)R_2$, тому $R = c_0 + c_1(x - x_0) + (x - x_0)^2 R_2$.

Нарешті отримаємо, $R = \sum_{i=0}^{k} c_i (x - x_0)^i + + (x - x_0)^{k+1} R_k$.

Лема 5. *Нехай* $P = (x_0, y_0)$ *— звичайна точка на гіпереліптичній кривій* H.

Тоді $\forall\, k \geq 1\, \exists!$ *многочлен* $b_k(x) \in \overline{\mathbb{F}}[x]$ *такий, що:*

1. $\deg_x b_k(x) < k$;
2. $b_k(x_0) = y_0$;
3. $b_k^2(x) + b_k(x)h(x) \equiv f(x) \pmod{(x - x_0)^k}$.

Напівзведений дивізор може бути зображений у вигляді НСД дивізорів двох поліноміальних функцій:

Теорема 6. *Нехай* $\mathsf{D} = \sum_i m_i P_i - \left(\sum\limits_i m_i\right)\infty$ *— напівзведений дивізор, де* $P_i = (x_i, y_i)$ *— точка на гіпереліптичній кривій* H, $a(x) = \prod_i (x - x_i)^{m_i}$, $b(x)$ *— єдині многочлени, які задовольняють умови:*

1. $\deg_x b(x) < \deg_x a(x)$;
2. $b(x_i) = y_i\, \forall\, i$, *для яких* $m_i \neq 0$;
3. $a(x) \,|\, (b^2(x) + b(x)h(x) - f(x))$.

Тоді

$$\mathsf{D} = НСД(div(a(x)), div(b(x) - y)) := div(a, b).$$

Доведення. Нехай H_0 — множина особливих точок у $supp(\mathsf{D})$, H_1 — множина звичайних точок у $supp(D)$, $\mathsf{H}_2 = \{\widetilde{P} : P \in \mathsf{H}_1\}$.

Тоді ми можемо записати дивізор D так:

$$D = \sum_{P_i \in \mathsf{H}_0} P_i + \sum_{P_i \in \mathsf{H}_1} m_i P_i - m\infty, \text{ де } m_i, m \in \mathbb{Z}_+.$$

Спершу доведемо, що $\exists!\, b(x)$, яка задовольняє умови теореми. Згідно з лемою 5, для кожної $P_i \in \mathsf{H}_1\, \exists!\, b_i(x) \in \overline{\mathbb{F}}[x]$, яка задовольняє умови:

1. $\deg_x b_i(x) < m_i$;
2. $b_i(x_i) = y_i$;
3. $(x - x_i)^{m_i} \,|\, (b_i^2(x) + b_i(x)h(x) - f(x))$.

Також для кожної $P_i \in \mathsf{H}_0\, \exists!\, b_i(x) = y_i$, яка задовольняє умови:

1. $\deg_x b_i(x) < 1$;
2. $b_i(x_i) = y_i$;
3. $(x - x_i) \,|\, (b_i^2(x) + b_i(x)h(x) - f(x))$.

Тоді за китайською теоремою про остачі для многочленів $\exists!\, b(x) \in \overline{\mathbb{F}}[x]$, $\deg_x b(x) < \sum_i m_i$, такий, що

$$b(x) \equiv b_i(x) \pmod{(x - x_i)^{m_i}}\, \forall\, i.$$

Далі покладемо

$$div(a(x)) = div(\prod_i (x - x_i)^{m_i}) =$$

$$= \sum_{P_i \in \mathsf{H}_0} 2P_i + \sum_{P_i \in \mathsf{H}_1} m_i P_i + \sum_{P_i \in \mathsf{H}_1} m_i \widetilde{P}_i - A\infty$$

і

$$div(b(x) - y) = \sum_{P_i \in \mathsf{H}_0} t_i P_i + \sum_{P_i \in \mathsf{H}_1} s_i P_i +$$

$$+ \sum_{P_i \in \mathsf{H} \setminus (\mathsf{H}_0 \cup \mathsf{H}_1 \cup \mathsf{H}_2 \cup \{\infty\})} m_i P_i - B\infty,$$

де $s_i \geq m_i$ оскільки $(x - x_i)^{m_i}$ ділить норму $N(b(x) - y) = b^2 + hb - f$.

Якщо $P = (x_1, y_1) \in \mathsf{H}_0$, то $(x - x_1) \,|\, (b^2(x) + b(x)h(x) - f(x))$.

Обчислимо похідну норми $N(b(x) - y)$ при $x = x_1$, маємо: $\frac{d}{dx}\left(N(b(x) - y)\right)\Big|_{x=x_1} = (2bb' + b'h + bh' - f')\Big|_{x=x_1} = |b(x_1) = y_1| = b'(x_1)(2y_1 + h(x_1)) + (h'(x_1)y_1 - f'(x_1)) = h'(x_1)y_1 - f'(x_1) \neq 0$, оскільки $2y_1 + h(x_1) = 0$.

Звідси маємо, що $x = x_1$ — простий корінь $N(b(x) - y)$, і тому $t_i = 1 \forall i$. Отже, $\text{НСД}(a(x), b(x) - y) = \sum_{P_i \in \mathsf{H}_0} \min\{t_i, 2\} P_i + \sum_{P_i \in \mathsf{H}_1} \min\{s_i, m_i\} - - \min\{A, B\}\infty = \sum_{P_i \in \mathsf{H}_0} P_i + \sum_{P_i \in \mathsf{H}_1} m_i P_i - m\infty = \mathsf{D}$.

Наслідок 7. *Нехай $a(x), b(x) \in \overline{\mathbb{F}}[x]$ – многочлени такі, що $\deg_x b(x) < \deg_x a(x)$. Якщо $a(x) \,|\, (N(b(x) - y))$, то $div(a, b)$ – напівзведений дивізор.*

Зведені дивізори

Означення 19. Нехай $\mathsf{D} = \sum_i m_i P_i - \left(\sum_i m_i\right)\infty$ — напівзведений дивізор. Якщо $\sum_i m_i \leq g$, де g — рід гіпереліптичної кривої H, то такий дивізор називають **зведеним**.

Означення 20. Нехай $\mathsf{D} = \sum\limits_{P \in \mathsf{H}} m_P P$ — дивізор. **Нормою дивізора** D називають число

$$|\mathsf{D}| = \sum_{P \in \mathsf{H} \setminus \{\infty\}} |m_P|.$$

Теорема 8. *Для кожного дивізора $\mathsf{D} \in \mathbb{D}^0$ існує єдиний зведений дивізор D_1 такий, що $\mathsf{D} \sim \mathsf{D}_1$.*

Доведення. **Існування.** З попередньої леми 5 маємо:

Нехай D' — напівзведений дивізор такий, що $\mathsf{D}' \sim \mathsf{D}$ і $|\mathsf{D}'| \leq |\mathsf{D}|$. Якщо $|\mathsf{D}'| \leq g$, то дивізор вже є зведеним і все доведено.

Припустимо, що це не виконується. Тоді нехай $P_1, P_2, \ldots, P_{g+1}$ — скінченні точки в $supp(\mathsf{D}')$, необов'язково різні. З теореми 6 маємо таке зображення:

$$div(a(x), b(x)) = P_1 + P_2 + \ldots + P_{g+1} - (g+1)\infty.$$

Оскільки $\deg_x b(x) \leq g$, маємо: $\deg(b(x) - y) = 2g + 1$, звідси: $div(b(x) - y) = P_1 + \ldots + P_{g+1} + Q_1 + \ldots + Q_g - (2g+1)\infty$ для деяких скінченних точок $Q_1, \ldots, Q_g$.

Віднявши цей дивізор від D', отримаємо дивізор D'' такий, що $\mathsf{D}'' \sim \mathsf{D}' \sim \mathsf{D}$ і $|\mathsf{D}''| \leq |\mathsf{D}'|$.

Далі ми можемо повторити цей процес і за скінченну кількість кроків отримати напівзведений дивізор D_1, для якого $|\mathsf{D}_1| \leq g$, тобто він є зведеним.

Єдиність. Припустимо, що існує два зведені дивізори такі, що $\mathsf{D}_1 \sim \mathsf{D}_2, \mathsf{D}_1 \neq \mathsf{D}_2$.

Нехай D_3 — напівзведений дивізор, отриманий з леми 5, такий, що $\mathsf{D}_3 \sim \mathsf{D}_1 - \mathsf{D}_2$.

Оскільки $\mathsf{D}_1 \neq \mathsf{D}_2$, то існує точка P така, що $ord_P(\mathsf{D}_1) \neq ord_P(\mathsf{D}_2)$.

Без обмеження загальності припустимо, що $ord_P(\mathsf{D}_1) = m_1 \geq 1$ і або

1. $ord_P(\mathsf{D}_2) = 0$ і $ord_{\widetilde{P}}(\mathsf{D}_2) = 0$, або
2. $ord_P(\mathsf{D}_2) = m_2$, причому $1 \leq m_2 < m_1$, або
3. $ord_{\widetilde{P}}(\mathsf{D}_2) = m_2$, причому $1 \leq m_2 \leq m_1$.

Зокрема, у випадку особливої точки P завжди має місце випадок 1.

Визначимо $ord_P(\mathsf{D}_3)$ в різних випадках. Маємо, що

1. $ord_P(\mathsf{D}_3) = m_1 \geq 1$; $ord_{\widetilde{P}}(\mathsf{D}_2) = 0$, або
2. $ord_P(\mathsf{D}_3) = (m_1 - m_2) \geq 1$;
3. $ord_P(\mathsf{D}_3) = (m_1 - (-m_2)) \geq 1$.

Таким чином, $ord_P(\mathsf{D}_3) \geq 1$ завжди і тому $\mathsf{D}_3 \neq 0, |\mathsf{D}_3| \leq |\mathsf{D}_1 - \mathsf{D}_2| \leq |\mathsf{D}_1| + |\mathsf{D}_2| \leq 2g$.

Нехай $R \in \mathbb{F}(\mathsf{H})^*$ — раціональна функція така, що $div(G) = \mathsf{D}_3$. Оскільки $\mathsf{D}_1 \sim \mathsf{D}_2$ і $\mathsf{D}_3 \sim \mathsf{D}_1 - \mathsf{D}_2$, то D_3 — головний дивізор і з означення маємо, що така раціональна функція R дійсно існує.

Тепер використаємо такий факт: якщо R не має скінченних полюсів, тоді це поліноміальна функція. Звідси

$$R(x, y) = a(x) - b(x)y, \text{ де } a(x), b(x) \in \overline{\mathbb{F}}[x].$$

Оскільки $\deg(y) = 2g + 1$ і $deg\,(R) = |\mathsf{D}_3| \leq 2g$, то маємо, що $b(x) = 0$.

Припустимо, що $\deg_x a(x) \geq 1$, $P = (x_1, y_1)$ — точка на гіпереліптичній кривій H і x_1 — корінь $a(x)$.

Тоді, якщо P — звичайна точка, то P і $\widetilde{P}$ є нулями поліноміальної функції R. Звідси отримуємо суперечність з тим, що D_3 — напівзведений дивізор (не виконується друга умова означення).

Якщо P — особлива точка, то вона має бути нулем поліноміальної функції R хоча б порядку 2. Звідси знову отримуємо суперечність з тим, що D_3 — напівзведений дивізор (не виконується друга умова означення).

Таким чином, $\deg_x a(x) = 0$ і тому $\mathsf{D}_3 = 0$. Отримали суперечність.

Зображення Мамфорда

Якщо в теоремі 6 умову 1 замінити на $\deg_x b(x) < \deg_x a(x) \leq g$, де g — рід гіпереліптичної кривої H, то одержимо, що кожний зведений дивізор $\mathsf{D} = \sum_i m_i P_i - \left(\sum_i m_i\right)\infty$ можна єдиним чином зобразити у вигляді пари многочленів $[a(x), b(x)]$, які задовольняють умови теореми 6, зокрема $a(x)$ — унітарний.

Зображення $[a(x), b(x)]$ називають **зображенням Мамфорда** дивізора D. Для кожного зведеного дивізора D існує єдине таке зображення, доведення випливає з теореми 6. Зокрема, нульовий дивізор зображають у вигляді $div[1, 0]$.

Розглянемо приклад побудови зображення Мамфорда.

Приклад 3. **1)** Якщо $\mathsf{D} = div[x_0, y_0]$ — точка, то $a(x) = x - x_0, b(x) = y_0$.

2) Для гіпереліптичної кривої

$$\mathsf{H} : y^2 = x^5 + 3x^3 + 2x^2 + 3 \text{ над полем } \mathbb{F}_5$$

знайдемо зображення Мамфорда для дивізорів $\mathsf{D}_1 = 1 \cdot (3, 0) + 1 \cdot (1, 2) - 2\infty$ та $\mathsf{D}_2 = 1 \cdot (4, 1) + 1 \cdot (3, 0) - 2\infty$.

Розв'язок. Для дивізора D_1 маємо: $P_1 = (x_1, y_1) = (3, 0), P_2 = (x_2, y_2) = (1, 2)$.

- $a_1(x) = \prod_i (x - x_i)^{m_i} = (x-3)(x-1) \equiv x^2 + x + 3 \pmod 5$.
- Для обчислення $b_1(x)$ врахуємо, що

$$b_1(x_i) = y_i, i \in \{1, 2\};$$

$$\deg b_1 < \deg a_1 = 2;$$

$$a_1 \mid (b_1^2 + b_1 h - f).$$

Таким чином, $b_1(x)$ матиме вигляд: $b_1(x) = c_1 x + c_2$, де $c_1, c_2 \in \{0, \ldots, 4\}$. Перебравши всі можливі варіанти, маємо: $b_1(x) = 4x + 3$.

Отже, зображення Мамфорда для дивізора D_1

$$\mathsf{D}_1 = [x^2 + x + 3, 4x + 3].$$

Для дивізора D_2 маємо: $Q_1 = (x_1, y_1) = (4, 1), Q_2 = (x_2, y_2) = (3, 0)$.

- $a_2(x) = \prod_i (x - x_i)^{m_i} = (x-4)(x-3) \equiv x^2 + 3x + 2 \pmod 5$;
- $b_2(x) = d_1 x + d_2$, де $d_{1;2} \in \{0, \ldots, 4\}$. Перебравши всі можливі варіанти, маємо: $b_2(x) = x + 2$.

Отже, зображення Мамфорда для дивізора D_2

$$\mathsf{D}_2 = [x^2 + 3x + 2, x + 2].$$

Алгоритм Кантора обчислення суми двох дивізорів

«Композиційна» частина. Нехай $\mathsf{D}_1 = div(a_1, b_1)$ та $\mathsf{D}_2 = div(a_2, b_2), a_{1;2}, b_{1;2} \in \mathbb{F}[x]$ — зведені дивізори, які визначені над полем $\mathbb{F}$.

Наступний алгоритм обчислює напівзведений дивізор $\mathsf{D} = div(a, b)$, $a, b \in \mathbb{F}[x]$ такий, що

$$\mathsf{D} \sim \mathsf{D}_1 + \mathsf{D}_2.$$

Алгоритм Кантора: «композиційна» частина

1. $d_1 = \text{НСД}(a_1, a_2) = e_1 a_1 + e_2 a_2, d_1, e_{1;2} \in \mathbb{F}[x]$;
2. $d = \text{НСД}(d_1, b_1 + b_2 + h) = c_1 d_1 + c_2(b + 1 + b_2 + h), d, c_{1;2} \in \mathbb{F}[x]$;
3. $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$, тобто

$$d = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + h) = \text{НСД}(a_1, a_2, b_1 + b_2 + h); \quad (1)$$

4.

$$a = \frac{a_1 a_2}{d^2}; \quad (2)$$

$$b = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \pmod a. \quad (3)$$

Переконаємось у коректності описаного алгоритму.

Теорема 9. *Нехай* $\mathsf{D}_1 = div(a_1, b_1)$ *і* $\mathsf{D}_2 = div(a_2, b_2)$ *— зведені дивізори. Тоді* $\mathsf{D} = div(a, b)$ *– напівзведений дивізор, де* a, b *визначені із рівнянь (2) та (3) відповідно, і* $\mathsf{D} \sim \mathsf{D}_1 + \mathsf{D}_2$.

Доведення. Спочатку переконаємось у тому, що b — многочлен. Використовуючи (1), маємо:

$$\begin{aligned} \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} = \\ \frac{b_2(d - s_2 a_2 - s_3(b_1 + b_2 + h))}{d} + \\ + \frac{s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} = \\ b_2 + \frac{s_2 a_2 (b_1 - b_2) - s_3(b_2^2 + b_2 h - f)}{d}. \end{aligned} \quad (4)$$

Оскільки $d \mid a_2$ та $a_2 \mid (b_2^2 + b_2 h - f)$, то b є дійсно многочленом. Далі, нехай

$$b = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} + sa,$$

де $s \in \mathbb{F}[x]$.

Тоді, використовуючи (1) та $y^2 + hy = f$, одержимо:

$$\begin{aligned} b - y = \\ \frac{s_1a_1b_2 + s_2a_2b_1 + s_3(b_1b_2 + f) - dy}{d} + sa = \\ \frac{s_1a_1b_2 + s_2a_2b_1 + s_3(b_1b_2 + f)}{d} \\ \frac{-s_1a_1y - s_2a_2y - s_3(b_1 + b_2 + h)y}{d} + sa = \\ \frac{s_1a_1(b_2 - y) + s_2a_2(b_1 - y)}{d} + \\ \frac{s_3(b_1 - y)(b_2 - y)}{d} + sa. \end{aligned} \tag{5}$$

З (5) маємо, що $a \,|\, (b^2 + bh - f)$. Дійсно, $(b^2 + bh - f) = (b - y)(b - y - h) = N(b - y) =$ ліва частина (5), тому достатньо показати, що

$$a_1a_2 \,|\, (s_1a_1(b_2-y)+s_2a_2(b_1-y)+s_3(b_1-y)(b_2-y))$$

разом з його спряженим.

Це має місце, оскільки з умов теореми 6 $a_1 \,|\, (b_1^2 + b_1h - f)$ і $a_2 \,|\, (b_2^2 + b_2h - f)$. Оскільки $N(b_i - y) = (b_i - y)(b_i + y + h) = b_i^2 + b_ih - f$, $i \in \{1, 2\}$, то з наслідку 7 теореми 6 отримаємо, що $\mathsf{D} = div(a, b)$ — напівзведений дивізор.

Тепер доведемо, що $\mathsf{D} \sim \mathsf{D}_1 + \mathsf{D}_2$. Мають місце такі два випадки:

1. Нехай $P = (x_1, y_1)$ — звичайна точка на гіпереліптичній кривій H. Розглянемо такі два випадки:
   а) Припустимо, що $ord_P(\mathsf{D}_1) = m_1, ord_{\widetilde{P}_i}(\mathsf{D}_1) = 0, ord_P(\mathsf{D}_2) = m_2, ord_{\widetilde{P}_i}(\mathsf{D}_2) = 0$, де $m_{1;2} \geq 0$. Тоді $ord_P(a_1) = m_1, ord_P(b_1 - y) \geq m_1, ord_P(a_2) = m_2, ord_P(b_2 - y) \geq m_2$.
      i. якщо $m_1 = 0$ або $m_2 = 0$, або ж обидва, то $ord_P(d_1) = 0$, звідки $ord_P(d) = 0$ і $ord_P(a) = ord_P\left(\frac{a_1a_2}{d^2}\right) = ord_P(a_1) + ord_P(a_2) = m_1 + m_2$.
      ii. якщо $m_1 \geq 1$ і $m_2 \geq 1$, то, оскільки $b_1(x_1) + b_2(x_1) + h(x_1) = 2y_1 + h(x_1) \neq 0$, маємо, що $ord_P(d) = 0$ і $ord_P(a) = ord_P\left(\frac{a_1a_2}{d^2}\right) = ord_P(a_1) + ord_P(a_2) = m_1 + m_2$.

      Таким чином, з (5) одержимо, що $ord_P(b - y) \geq m_1 + m_2$, звідси $ord_P(D) = m_1 + m_2$.
   б) Припустимо, що $ord_P(\mathsf{D}_1) = m_1, ord_{\widetilde{P}_i}(\mathsf{D}_2) = m_2$, де $m_1 \geq m_2 \geq 1$. Тоді $ord_P(a_1) = m_1, ord_P(a_2) = m_2, ord_P(d_1) = m_2, ord_P(b_1 - y) \geq m_1, ord_{\widetilde{P}}(b_2 - y) \geq m_2$.

      Звідси $ord_{\widetilde{P}}(b_2-y) = ord_P(b_2+y+h) \geq m_2$, тому $ord_P(b_1+b_2+h) \geq m_2$ або $b_1 + b_2 + h = 0$. Отже, $ord_P(d) = m_2$ і $ord_P(a) = ord_P\left(\frac{a_1a_2}{d^2}\right) = ord_P(a_1) + ord_P(a_2) - 2 \cdot ord_P(d) = m_1 - m_2$, звідси $ord_P(D) = m_1 - m_2$.
2. Нехай $P = (x_1, y_1)$ — особлива точка на гіпереліптичній кривій H. Розглянемо такі два випадки:
   а) Припустимо, що $ord_P(\mathsf{D}_1) = 1, ord_P(\mathsf{D}_2) = 1$.
      Тоді $ord_P(a_1) = 2, ord_P(a_2) = 2, ord_P(d_1) = 2$. $b_1(x_1) + b_2(x_1) + h(x_1) = 2y_1 + h(x_1) = |P -$ особлива точка$| = y_1 + (y_1 + h(x_1)) = 0$, звідки $ord_P(b_1 + b_2 + h) \geq 2$ або $b_1 + b_2 + h = 0$.
      Тому $ord_P(d) = 2$ і $ord_P(a) = ord_P\left(\frac{a_1a_2}{d^2}\right) = ord_P(a_1) + ord_P(a_2) - 2 \cdot ord_P(d) = 0$, звідси $ord_P(\mathsf{D}) = 0$.
   б) Припустимо, що $ord_P(\mathsf{D}_1) = 1, ord_P(\mathsf{D}_2) = 0$.
      Тоді $ord_P(a_1) = 2, ord_P(a_2) = 0$. Звідси $ord_P(d_1) = ord_P(d) = 0$ і $ord_P(a) = ord_P\left(\frac{a_1a_2}{d^2}\right) = ord_P(a_1) + ord_P(a_2) = 2$.
      Оскільки $ord_P(b_1 - y) = 1$, то з (6) випливає, що $ord_P(b - y) \geq 1$. Також з (5) можна одержати, що $ord_P(b - y) \geq 2$ тільки якщо $ord_P(s_2a_2 + s_3(b_2 - y)) \geq 1$.
      Якщо це дійсно виконується, то $ord_P(s_2a_2 + s_3(b_2 - y)) = ord_{\widetilde{P}}(s_2a_2 + s_3(b_2 + y + h)) = ord_P(s_2a_2 + s_3(b_2 + y + h)) \geq 1$ і звідси $ord_P(s_2a_2 + s_3(b_1 + b_2 + h)) \geq 1$ або $s_2a_2 + s_3(b_1 + b_2 + h) = 0$. Тоді з (1) одержимо, що $ord_P(d) \geq 1$. Суперечність.
      Отже, $ord_P(b - y) = 1$, і $ord_P(\mathsf{D}) = 1$.

Розглянемо приклад застосування алгоритму.

Приклад 4. Нехай задані гіпереліптична крива

$$\mathsf{H} : y^2 = x^5 + 3x^3 + 7x^2 + x + 2 \text{ над полем } \mathbb{F}_{11}$$

та два зведені дивізори на ній

$\mathsf{D}_1 = div(a_1, b_1) = div(x^2 + 7x + 10, x + 9)$,
$\mathsf{D}_2 = div(a_2, b_2) = div(x^2 + 10, 7x + 9)$.

Обчислимо напівзведений дивізор D такий, що $\mathsf{D} \sim \mathsf{D}_1 + \mathsf{D}_2$.

Розв'язок.

1. $d_1 = \text{НСД}(a_1, a_2) = 1 = 8x \cdot a_1 + (3x + 10) \cdot a_2$, звідси $e_1 = 8x, e_2 = 3x + 10$;

2. $d = \text{НСД}(d_1, b_1 + b_2 + h) = 1 = 1 \cdot 1 + 0(b + 1 + b_2 + h)$, звідси $c_1 = 1, c_2 = 0$;
3. $s_1 = c_1 e_1 = 1 \cdot 8x = 8x; s_2 = c_1 e_2 = 1 \cdot (3x + 10) = 3x + 10; s_3 = c_2 = 0$;
4. $a = \dfrac{a_1 a_2}{d^2} = a_1 a_2 \equiv x^4 + 7x^3 + 9x^2 + 4x + 1 \pmod{11}$;
   $b = \dfrac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} = s_1 a_1 b_2 + s_2 a_2 b_1 \equiv 4x^2 + 7x + 5 \pmod{a}$.

Отже, отримали напівзведений дивізор $\mathsf{D} = div(a, b) = div(x^4 + 7x^3 + 9x^2 + 4x + 1, 4x^2 + 7x + 5)$.

Особливий випадок «композиційної» частини: подвоєння дивізора. Нехай $\mathsf{D}_1 = div(a_1, b_1), a_1, b_1 \in \mathbb{F}[x]$ — зведений дивізор, визначений над полем $\mathbb{F}$.
Наступний алгоритм обчислює подвоєний напівзведений дивізор

$\mathsf{D} = div(a, b), a, b \in \mathbb{F}[x]$ такий, що $\mathsf{D} \sim 2\mathsf{D}_1$.

Алгоритм Кантора: «композиційна» частина, подвоєння дивізора

1. $d = \text{НСД}(a_1, 2b_1 + h) = s_1 a_1 + s_2(2b_1 + h), d, s_{1;2} \in \mathbb{F}[x]$;
2. $$a = \frac{a_1^2}{d^2};$$
   $$b = \frac{s_1 a_1 b_1 + s_2(b_1^2 + f)}{d} \pmod{a}.$$

Коректність алгоритму слідує з теореми 9. Розглянемо приклад застосування алгоритму.
Приклад 5. Нехай задані гіпереліптична крива

$\mathsf{H} : y^2 = x^5 + 3x^3 + 7x^2 + x + 2$ над полем $\mathbb{F}_{11}$

та зведений дивізор на ній

$\mathsf{D}_1 = div(a_1, b_1) = div(x^2 + 7x + 10, x + 9)$.

Обчислимо напівзведений дивізор D такий, що $\mathsf{D} \sim 2\mathsf{D}_1$.

Розв'язок.

1. $d = \text{НСД}(a_1, 2b_1 + h) = 1 = 2 \cdot a_1 + (10x + 2) \cdot (2b_1 + h)$, звідси $s_1 = 2, s_2 = 10x + 2$;
2. $a = \dfrac{a_1^2}{d^2} = a_1^2 \equiv x^4 + 3x^3 + 3x^2 + 8x + 1 \pmod{11}$;
   $b = \dfrac{s_1 a_1 b_1 + s_2(b_1^2 + f)}{d} = s_1 a_1 b_1 + s_2(b_1^2 + f) \equiv 5x^3 + 2x^2 + 7x + 9 \pmod{a}$.

Отже, отримали напівзведений дивізор $\mathsf{D} = div(a, b) = div(x^4 + 3x^3 + 3x^2 + 8x + 1, 5x^3 + 2x^2 + 7x + 9)$.

«Редукційна» частина. Нехай $\mathsf{D}_1 = div(a_1, b_1), a_1, b_1 \in \mathbb{F}[x]$ — напівзведений дивізор, визначений над полем $\mathbb{F}$.

Наступний алгоритм обчислює (єдиний) зведений дивізор $\mathsf{D} = div(a, b)$, $a, b \in \mathbb{F}[x]$ такий, що

$$\mathsf{D} \sim \mathsf{D}_1.$$

Алгоритм Кантора: «редукційна» частина

1. $$a = \frac{f - b_1 h - b_1^2}{a_1}; \tag{6}$$
   $$b = (-h - b_1) \pmod{a}. \tag{7}$$
2. Якщо $\deg_x a > g$, де g — рід гіпереліптичної кривої H, то покласти $a_1 = a, b_1 = b$ та повернутися до попереднього кроку.
3. Зробити многочлен a унітарним, тобто $a = c^{-1} \cdot a$, де c — старший коефіцієнт a.

Переконаємось у коректності описаного алгоритму.

Теорема 10. *Нехай $\mathsf{D}_1 = div(a_1, b_1)$ — напізведений дивізор. Тоді дивізор $\mathsf{D} = div(a, b)$, отриманий за допомогою алгоритму вище, є зведеним і таким, що $\mathsf{D} \sim \mathsf{D}_1$.*

Доведення. Нехай $a = \dfrac{f - b_1 h - b_1^2}{a_1}$, $b = (-h - b_1) \pmod{a}$. Покажемо, що:

1. $\deg_x a < \deg_x a_1$;
2. $\mathsf{D} = div(a, b)$ — напівзведений дивізор;
3. $\mathsf{D} \sim \mathsf{D}_1$.

Нехай $m = \deg_x a_1, n = \deg_x b_1$, де $m > n, m \geq g+1$, де g — рід гіпереліптичної кривої H. Тоді $\deg_x a = \max\{2g + 1, 2n\} - m$.

- якщо $m > g + 1$, то $\max\{2g + 1, 2n\} \leq 2(m - 1)$, звідки $\deg_x a \leq 2m - 2 - m = m - 2 \leq \deg_x a_1$.
- якщо $m = g+1$, то $\max\{2g+1, 2n\} = 2m-1$, звідки $\deg_x a = 2m - 1 - m = g < \deg_x a_1$.

Покладемо $f - b_1 h - b_1^2 = a_1 a$. Взявши по $\pmod{a}$ з обох сторін, отримаємо, що $f + (b + h)h - (b + h)^2 = f - bh - b^2 = 0 \pmod{a}$, тобто $a \mid (f - bh - b^2)$. З наслідку 7 теореми 6 випливає, що $\mathsf{D} = div(a, b)$ — напівзведений дивізор.

Нехай $\mathsf{H}_0 = \{P \in supp(\mathsf{D}) : P - \text{особлива точка}\}, \mathsf{H}_1 = \{P \in supp(\mathsf{D}) : P - \text{звичайна точка}\}, \mathsf{H}_2 = \{\widetilde{P} : P \in \mathsf{H}_1\}$.
З доведення теореми 6 відомо, що

$$D = \sum_{P_i \in \mathsf{H}_0} P_i + \sum_{P_i \in \mathsf{H}_1} m_i P_i - m\infty.$$

Тоді $div(a_1) = \sum_{P_i \in \mathsf{H}_0} 2P_i + \sum_{P_i \in \mathsf{H}_1} m_i P_i + \sum_{P_i \in \mathsf{H}_1} m_i \widetilde{P}_i - A\infty$ і
$div(b_1 - y) = \sum_{P_i \in \mathsf{H}_0} P_i + \sum_{P_i \in \mathsf{H}_1} n_i P_i + \sum_{P_i \in \mathsf{H}_3} s_i P_i - B\infty$,

де $n_i \geq m_i$ оскільки $a_1 \mid (b_1^2 + b_1 h - f)$, $s_i \geq 1$ і $s_i = 1$ якщо P_i — особлива точка.
$\mathsf{H}_3 = \mathsf{H} \backslash (\mathsf{H}_0 \cup \mathsf{H}_1 \cup \mathsf{H}_2 \cup \{\infty\})$.

Нехай $G \in \overline{\mathbb{F}}[\mathsf{H}]^*$, $div(G) = \sum_{P \in \mathsf{H}} m_P P$. Тоді $div(\overline{G}) = \sum_{P \in \mathsf{H}} m_P \widetilde{P}$. Оскільки $N(b_1 - y) = b_1^2 + b_1 h - f = (b_1 - y)(b_1 + y + h)$, то $div(b_1^2 + b_1 h - f) = div(N(b_1 - y)) = div((b_1 - y)(b_1 + y + h)) = div(b_1 - y) + div(b_1 + y + h) = \sum_{P_i \in \mathsf{H}_0} 2P_i + \sum_{P_i \in \mathsf{H}_1} n_i P_i + \sum_{P_i \in \mathsf{H}_1} n_i \widetilde{P}_i + \sum_{P_i \in \mathsf{H}_3} s_i P_i + \sum_{P_i \in \mathsf{H}_3} s_i \widetilde{P}_i - C\infty$.

Звідси, $div(a) = div(b_1^2 + b_1 h - f) - div(a_1) = \sum_{P_i \in H_{1'}} t_i P_i + \sum_{P_i \in H_{1'}} t_i \widetilde{P}_i + \sum_{P_i \in \mathsf{H}_3} s_i P_i + \sum_{P_i \in \mathsf{H}_3} s_i \widetilde{P}_i - L\infty$, де $t_i = n_i - m_i$ і $\mathsf{H}_{1'} = \{P_i \in \mathsf{H}_1 : n_i > m_i\}$.

Тепер, нехай $b = -h - b_1 + sa$ для деякого $s \in \overline{\mathbb{F}}[x]$. Якщо $P_i = (x_i, y_i) \in \mathsf{H}_{1'} \cup \mathsf{H}_3$, то

$b(x_i) = -h(x_i) - b_1(x_i) + s(x_i)a(x_i) = -h(x_i) - y_i$. Тоді з доведення теореми 6 випливає, що $div(b - y) = \sum_{P_i \in \mathsf{H}_{1'}} r_i \widetilde{P}_i + \sum_{P_i \in \mathsf{H}_3} w_i \widetilde{P}_i + \sum_{P_i \in \mathsf{H}_4} z_i \widetilde{P}_i - M\infty$, де $r_i \geq t_i, w_i \geq s_i$, $w_i = 1$ якщо $P_i \in \mathsf{H}_3$ — особлива точка, $\mathsf{H}_4 = \mathsf{H} \backslash (\mathsf{H}_{1'} \cup \mathsf{H}_3 \cup \{\infty\})$.

Звідси маємо, що:
$div(a, b) = \sum_{P_i \in \mathsf{H}_{1'}} \min\{t_i, r_i\} \widetilde{P}_i + \sum_{P_i \in \mathsf{H}_3} \min\{s_i, w_i\} \widetilde{P}_i - n\infty = \sum_{P_i \in \mathsf{H}_{1'}} t_i \widetilde{P}_i + \sum_{P_i \in \mathsf{H}_3} s_i \widetilde{P}_i - n\infty \sim -\sum_{P_i \in \mathsf{H}'_1} t_i P_i - \sum_{P_i \in \mathsf{H}_3} s_i P_i + m\infty = D - div(b_1 - y)$, звідки $D \sim D_1$.

Повторюючи процес допоки $\deg_x a > g$, в кінці отримаємо, що D — зведений дивізор.

Розглянемо приклад застосування алгоритму.

Приклад 6. Наводимо розгляд прикладу, який ми використовували під час обчислення суми двох дивізорів. Нехай задані гіпереліптична крива $\mathsf{H} : y^2 = x^5 + 3x^3 + 7x^2 + x + 2$ над полем $\mathbb{F}_{11}$ та напівзведений дивізор на ній $\mathsf{D}_1 = div(a_1, b_1) = div(x^4 + 7x^3 + 9x^2 + 4x + 1, 4x^2 + 7x + 5)$. Обчислимо (єдиний) зведений дивізор D такий, що $\mathsf{D} \sim \mathsf{D}_1$.

Розв'язок.

1. $a = \dfrac{f - b_1 h - b_1^2}{a_1} \equiv x + 10 \pmod{11}$;
   $b = (-h - b_1) = -b_1 \equiv 6 \pmod{a}$.
2. $\deg_x a = 1 \not> g = 2$, а також a — унітарний многочлен.

Отже, отримали (єдиний) зведений дивізор
$\mathsf{D} = div(a, b) = div([x + 10, 6])$.

Приклад 7. Наводимо розгляд прикладу, який ми використовували під час обчислення подвоєного дивізора.

Нехай задані гіпереліптична крива $\mathsf{H} : y^2 = x^5 + 3x^3 + 7x^2 + x + 2$ над полем $\mathbb{F}_{11}$ та напівзведений дивізор на ній $\mathsf{D}_1 = div(a_1, b_1) = div(x^4 + 3x^3 + 3x^2 + 8x + 1, 5x^3 + 2x^2 + 7x + 9)$.

Обчислимо (єдиний) зведений дивізор D такий, що $\mathsf{D} \sim \mathsf{D}_1$.

Розв'язок.

1. $$a = \frac{f - b_1 h - b_1^2}{a_1} \equiv 8x^2 + x + 9 \pmod{11};$$
   $$b = (-h - b_1) = -b_1 \equiv 2 \pmod{a}.$$
2. $\deg_x a = 2 \not> g = 2$;
3. Зробимо многочлен a унітарним.
   $c = 8$, $8^{-1} \pmod{11} = 7$, тому $a = x^2 + 7x + 7 \cdot 9 \equiv x^2 + 7x + 8 \pmod{11}$.

Отже, отримали (єдиний) зведений дивізор
$$\mathsf{D} = div(a, b) = div([x^2 + 7x + 8, 2]).$$

Висновки

У роботі було розглянуто поняття дивізора на гіпереліптичній кривій роду $g > 1$, а також певних операцій, пов'язаних з ними. Зокрема, зображення Мамфорда є єдиним у своїй формі, «редукційна» частина алгоритму Кантора обчислює єдиний зведений дивізор, а сам алгоритм є універсальним та може бути застосований для обчислення суми двох дивізорів гіпереліптичної кривої будь-якого роду.

Зауважимо, що він не є дуже ефективним на сьогодні, тому варто розглядати особливі випадки, які залежать від початкових наборів даних, зокрема від вигляду дивізора, що дають змогу вивести явні формули, котрі зменшують час роботи алгоритму. Зокрема, один з таких випадків був розглянутий (подвоєння дивізора), а ще один випадок був частково описаний у прикладі застосування алгоритму Кантора: «композиційна» частина.

Імплементація алгоритмів на мові Python

Алгоритм 1. Обчислення дивізора поліноміальної функції

```
from sympy.polys.domains import ZZ
from sympy.polys.galoistools import (
  gf_add, gf_sub, gf_mul, gf_pow,

  gf_div, gf_rem, gf_eval, gf_degree)

'''
Модифікована версія обчислення степеня п
  оліноміальної функції, оскільки
gf_degree повертає степінь рівний -1 для
   нульової функції
'''
deg = lambda f: max([gf_degree(f), 0])

def ord_ev_step1(a, b, P):
  '''
  Перший крок алгоритму у випадку, коли
  P = (x0, y0) - скінченна точка.
```

```
    Обчислює найвищий степінь r такий, аби
     поліноміальну функцію G
    можна було представити у вигляді: G(x,
    y) = (x-x0)^r (a0(x)-b0(x)y)
    '''
    for r in range(deg(a), 0, -1):
      xx0 = gf_pow([1, -P[0]], r, p, ZZ)
      a0, rem_a = gf_div(a, xx0, p, ZZ)
      b0, rem_b = gf_div(b, xx0, p, ZZ)
      if not rem_a and not rem_b:
        return a0, b0, r
    return a, b, 0

def ord_ev_step2(a0, b0, f, h, P):
    '''
    Другий крок алгоритму у випадку, коли
    P = (x0, y0) - скінченна точка.
    Виконується у випадку, коли a0(x0) -
    b0(x0)y0 != 0 (mod p)
    Обчислює найвищий степінь s для (x -
    x0)^s такий, який ділить
    норму поліноміальної функції G: N(a0(x
    )-b0(x)y) = a0^2+a0b0h-b0^2f
    '''
    a0_2 = gf_pow(a0, 2, p, ZZ)
    b0_2 = gf_pow(b0, 2, p, ZZ)
    a0b0h = gf_mul(gf_mul(a0, b0, p, ZZ),
    h, p, ZZ)
    N = gf_sub(gf_add(a0_2, a0b0h, p, ZZ),
               gf_mul(b0_2, f, p, ZZ),
               p, ZZ)
    for s in range(deg(N), 0, -1):
      xx0 = gf_pow([1, -P[0]], s, p, ZZ)
      if not gf_rem(N, xx0, p, ZZ):
        return s
    return 0

def point_ord(r, s, h, P):
    '''
    Обчислення порядку в точці у випадку,
    коли P = (x0, y0) - скінченна точка.

    ord_P(G) = r+s у випадку, коли P - зви
    чайна точка.
    ord_P(G) = 2r+s у випадку, коли P - ос
    облива точка, тобто
    P = -P [(x0, y0) = (x0, -y0-h(x0))]
    '''
    h_x = gf_eval(h, P[0], p, ZZ)
    try:
      P_y = gf_add([-P[1]], [-h_x], p, ZZ)
    [0]
    except:
      P_y = 0
    P_ = (P[0], P_y)
    return r+s if P_ != P else 2*r + s

def inf_point_ord(a, b, f):
    '''
    Обчислення порядку в точці у випадку,
    коли P = INF
    '''
    return -max([2*deg(a), deg(f)+deg(b)])

def divisor_eval(a, b, f, h, P):
    '''
    Основний блок. Обчислення дивізора для
     заданих точок
    '''
    print(f'P = {P}:')
    if P == 'INF':
      ord_G = inf_point_ord(a, b, f)
    else:
      a0, b0, r = ord_ev_step1(a, b, P)
      s = 0 if gf_eval(a0, P[0], p, ZZ) !=
     0 else ord_ev_step2(a0, b0, f, h, P)
      ord_G = point_ord(r, s, h, P)
    print(f'ord(G) = {ord_G}\n')
    return ord_G

# Потрібні дані про гіпереліптичну криву
   H та поліноміальну функцію G
f = [1, 5, 0, 6, 1, 3]
G = [6, 6, 1, 6, 0]
h = [1, 0];
h_G = [1, 0]
p = 7

a = gf_add(f, G, p, ZZ)
b = gf_sub(h, h_G, p, ZZ)
print(f'a = {a} and b = {b}')

points = [(1, 1), (1, 5), (2, 2), (2, 3)
  , (5, 3), (5, 6), (6, 4),'INF']

'''
Остаточне зображення дивізора поліноміал
  ьної функції G у вигляді
div(G) = [(порядок точки, точка)]
'''
divisor = [(divisor_eval(a, b, f, h, P),
   P) for P in points]
print(f'div(G) = (ord_P(G), P) = {
  divisor}')
```

Алгоритм 2. Обчислення зображення Мамфорда для дивізора

```
from sympy.polys.domains import ZZ
from sympy.polys.galoistools import (
  gf_sub, gf_mul, gf_add_mul, gf_pow,
                                gf_rem,
  gf_eval, gf_LC, gf_degree, gf_strip)
from itertools import product

# Потрібні дані про гіпереліптичну криву
   H
f = [1, 0, 3, 2, 0, 3]
h = [0]
p = 5

# Зображення точок гіпереліптичної криво
  ї H та їх порядків
# P = INF не враховуємо при обчисленні
m = [1, 1]
P = [(4, 1), (3, 0)]

'''
Модифікована версія обчислення степеня п
  оліноміальної функції, оскільки
gf_degree повертає степінь рівний -1 для
   нульової функції
'''
deg = lambda f: max([gf_degree(f), 0])

''' КРОК 1.
Обчислення a, де a = TT(x-x_i)^{m_i}
'''
polynomials = [[1, -i[0]] for i in P]
a = [1]
for i in range(len(polynomials)):
```

```
    a = gf_mul(a, gf_pow(polynomials[i], m
    [i], p, ZZ), p, ZZ)

  '''
  Перевірка виконання умов алгоритму: чи
    deg(u) <= g та чи є многочлен унітарни
    м
  '''
  assert deg(a) <= (deg(f)-1)/2 and gf_LC(
    a, ZZ) == 1, 'deg(a) <= g and lead.
    coef. == 1'


  def polynom_combs(lst, dg):
    '''
    Обчислення всіх комбінацій коефіцієнті
    в для функції b,
    для якої deg(b) < deg(a) <= g
    '''
    for i in range(dg):
      combs = product(lst, repeat=i+1)
      for elem in combs:
        yield gf_strip(elem)

  def eval_checking(P, pol):
    '''
    Перевірка умови: b(x_i) = y_i
    '''
    return all(gf_eval(pol, P[i][0], p, ZZ
    ) == P[i][1] for i in range(len(P)))

  ''' КРОК 2.
  Обчислення b, для якого:
  deg b < deg a <= g,
  b(x_i) = y_i,
  a | (b^2 + hb - f)
  '''
  valid_combs = set(pnts for pnts in
    polynom_combs(list(range(p)), deg(a)))
  candidates = [list(pnts) for pnts in
    valid_combs if eval_checking(P, pnts)]
  for b0 in candidates:
    denom_b0 = gf_sub(gf_add_mul(gf_pow(b0
    , 2, p, ZZ), b0, h, p, ZZ), f, p, ZZ)
    if not gf_rem(denom_b0, a, p, ZZ) and
    deg(b0) < deg(a):
      b = b0
      break

  '''
  Остаточне зображення Мамфорда для дивізо
    ра D
  '''
  D = [a, b]
  print(f'D = {D}.')
```

Алгоритм 3. «Композиційна» частина алгоритму Кантора: обчислення суми двох дивізорів

```
from sympy.polys.domains import ZZ
from sympy.polys.galoistools import (
  gf_add, gf_mul, gf_add_mul, gf_pow,

  gf_quo, gf_rem, gf_gcdex)

# Зображення дивізора D1
a1 = [1, 7, 10]
b1 = [1, 9]

# Зображення дивізора D2
a2 = [1, 0, 10]
b2 = [7, 9]

# Потрібні дані про гіпереліптичну криву
   H
f = [1, 0, 3, 7, 1, 2]
h = [0]
p = 11

''' КРОК 1.
Обчислення d1 = НСД(a1, a2) = e1a1 +
  e2a2,
використовуючи розширений алгоритм Евкліда
'''
e1, e2, d1 = gf_gcdex(a1, a2, p, ZZ)

''' КРОК 2.
Обчислення d = НСД(d1, b1+b2+h) = c1d1 +
   c2(b1+b2+h),
використовуючи розширений алгоритм Евкліда
'''
b1b2h = gf_add(gf_add(b1, b2, p, ZZ), h,
   p, ZZ)

c1, c2, d = gf_gcdex(d1, b1b2h, p, ZZ)

''' КРОК 3.
Узагальнення КРОКу 1 та 2. Задачею було
  пошук:
НСД(a1, a2, b1+b2+h) = s1a1 + s2a2 + s3(
  b1+b2+h)
'''
s1 = gf_mul(c1, e1, p, ZZ)
s2 = gf_mul(c1, e2, p, ZZ)
s3 = gf_mul(c2, e2, p, ZZ)

''' КРОК 4.
Обчислення напівзведеного дивізора у вигляді D = [a, b]
'''

''' КРОК 4.1
Обчислення a = a1a2/d^2
'''
a1a2 = gf_mul(a1, a2, p, ZZ)
d2 = gf_pow(d, 2, p, ZZ)
a = gf_quo(a1a2, d2, p, ZZ)

''' КРОК 4.2
Обчислення b = (s1a1b2 + s2a2b1 + s3(f+
  b1b2))/d (mod a)
'''
s1a1b2 = gf_mul(s1, gf_mul(a1, b2, p, ZZ
  ), p, ZZ)
s2a2b1 = gf_mul(s2, gf_mul(a2, b1, p, ZZ
  ), p, ZZ)
s3fab1b2 = gf_mul(s3, gf_add_mul(f, b1,
  b2, p, ZZ), p, ZZ)

b0 = gf_quo(gf_add(gf_add(s1a1b2, s2a2b1
  , p, ZZ), s3fab1b2, p, ZZ),
            d, p, ZZ)
b = gf_rem(b0, a, p, ZZ)

'''
Остаточне зображення напівзведеного дивізора D
'''
D = [a, b]
```

```
print(f'a={D[0]}, b={D[1]}.')
```

Алгоритм 4. «Композиційна» частина алгоритму Кантора: обчислення подвоєного дивізора

```
from sympy.polys.domains import ZZ
from sympy.polys.galoistools import (
  gf_add, gf_mul, gf_pow,

  gf_quo, gf_rem, gf_gcdex)

# Зображення дивізора D1
a1 = [1, 7, 10]
b1 = [1, 9]

# Потрібні дані про гіпереліптичну криву
   H
f = [1, 0, 3, 7, 1, 2]
h = [0]
p = 11

''' КРОК 1.
Обчислення d = НСД(a1, 2b1+h) = s1a1 +
  s2(2b1+h),
використовуючи розширений алгоритм Евкліда
'''
s1, s2, d = gf_gcdex(a1, gf_add(gf_add(
  b1, b1, p, ZZ),
                                h, p, ZZ),
                     p, ZZ)

''' КРОК 2.
Обчислення напівзведеного дивізора у вигляді D = [a, b]
'''

''' КРОК 2.1
Обчислення a = a1^2/d^2
'''
a1_2 = gf_pow(a1, 2, p, ZZ)
a = gf_quo(a1_2, gf_pow(d, 2, p, ZZ), p,
   ZZ)

''' КРОК 2.2
Обчислення b = (s1a1b1 + s2(b1^2+f))/d (mod a)
'''
s1a1b1 = gf_mul(s1, gf_mul(a1, b1, p, ZZ
  ), p, ZZ)
b1_2 = gf_pow(b1, 2, p, ZZ)
s2b1_2f = gf_mul(s2, gf_add(b1_2, f, p,
  ZZ), p, ZZ)

b0 = gf_quo(gf_add(s1a1b1, s2b1_2f, p,
  ZZ),
            d, p, ZZ)
b = gf_rem(b0, a, p, ZZ)

'''
Остаточне зображення напівзведеного дивізора D
'''
D = [a, b]
print(f'u = {D[0]}, v = {D[1]}.')
```

Алгоритм 5. «Редукційна» частина алгоритму Кантора

```
from sympy.polys.domains import ZZ
from sympy.polys.galoistools import (
  gf_add, gf_sub, gf_sub_mul,
                  gf_quo, gf_rem, gf_pow
  , gf_neg, gf_LC, gf_monic, gf_degree)

# Зображення напівзведеного дивізора D1
a = [1, 7, 9, 4, 1]
b = [4, 7, 5]

# Потрібні дані про гіпереліптичну криву
   H
f = [1, 0, 3, 7, 1, 2]
h = [0]
p = 11

'''
Модифікована версія обчислення степеня поліноміальної функції, оскільки
gf_degree повертає степінь рівний -1 для нульової функції
'''
deg = lambda f: max([gf_degree(f), 0])

''' КРОК 1+2.
Обчислення (єдиного) зведеного дивізора D у вигляді [a, b], де
a = (f-b1h-b1^2)/a1, b = -h -b1 (mod a)

Алгоритм працює до моменту, поки deg(a) > g,
де g - рід гіпереліптичної кривої
'''
while True:
  f_bh = gf_sub_mul(f, b, h, p, ZZ)
  a_red = gf_quo(gf_sub(f_bh, gf_pow(b,
  2, p, ZZ), p, ZZ),
                 a, p, ZZ)

  b_red = gf_rem(gf_add(gf_neg(h, p, ZZ)
  , gf_neg(b, p, ZZ), p, ZZ),
                 a_red, p, ZZ)
  a = a_red
  b = b_red
  if deg(a_red) <= (deg(f)-1)/2:
    break

'''
КРОК 3.
Перевірка, чи є a унітарним,
тобто чи дорівнює 1 старший коефеіцієнт поліноміальної функції
'''
if gf_LC(a, ZZ) != 1:
  a = gf_monic(a, p, ZZ)[1]

'''
Остаточне зображення (єдиного) зведеного дивізора D
'''
D = [a, b]
print(f'a = {D[0]}, b = {D[1]}.')
```

Список літератури

1. Menezes Alfred J., Wu Yi-Hong, Zuccherato Robert J. An elementary introduction to hyperelliptic curves, 1996.
2. Koblitz Neal. Hyperelliptic Cryptosystems. *Journal of Cryptology*. 1989. Vol. 1. Pp. 139–150.
3. Cantor David G. Computing in the Jacobian of a Hyperelliptic Curve. *Mathematics of computation*. 1987. Vol. 48, no. 177. P. 95–101.
4. Galbraith Steven D., Harrison Michael, Mireles Morales David J. Efficient Hyperelliptic Arithmetic using Balanced Representation for Divisors. 2008.
5. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. An Introduction to Mathematical Cryptography, 2008. P. 317–318.
6. Kitamura Izuru, Katagi Masanobu, Takagi Tsuyoshi. A Complete Divisor Class Halving Algorithm for Hyperelliptic Curve Cryptosystems of Genus Two. 2005.

References

1. Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato, *An elementary introduction to hyperelliptic curves* (1996).
2. Neal Koblitz, "Hyperelliptic Cryptosystems", Journal of Cryptology. 1, 139–150 (1989).
3. David G. Cantor, "Computing in the Jacobian of a Hyperelliptic Curve", Mathematics of computation. 48 (177), 95–101 (1987).
4. Steven D. Galbraith, Michael Harrison, David J. Mireles Morales. Efficient Hyperelliptic Arithmetic using Balanced Representation for Divisors, 2008.
5. Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman. *An Introduction to Mathematical Cryptography* (2008), pp. 317–318.
6. Izuru Kitamura, Masanobu Katagi and Tsuyoshi Takagi. *A Complete Divisor Class Halving Algorithm for Hyperelliptic Curve Cryptosystems of Genus Two* (2005).

D. Boiko

APPLICATION OF DIVISORS ON A HYPERELLIPTIC CURVE IN PYTHON

The paper studies hyperelliptic curves of the genus $g > 1$, divisors on them and their applications in Python programming language. The basic necessary definitions and known properties of hyperelliptic curves are demonstrated, as well as the notion of polynomial function, its representation in unique form, also the notion of rational function, norm, degree and conjugate to a polynomial are presented. These facts are needed to calculate the order of points of desirable functions, and thus to quickly and efficiently calculate divisors. The definition of a divisor on a hyperelliptic curve is shown, and the main known properties of a divisor are given. There are also an example of calculating a divisor of a polynomial function, reduced and semi-reduced divisors are described, theorem of the existence of such a not unique semi-reduced divisor, and theorem of the existence of a unique reduced divisor, which is equivalent to the initial one, are proved. In particular, a semi-reduced divisor can be represented as an GCD of divisors of two polynomial functions. It is also demonstrated that each reduced divisor can be represented in unique form by pair of polynomials $[a(x), b(x)]$, which is called Mumford representation, and several examples of its representation calculation are given. There are shown Cantor's algorithms for calculating the sum of two divisors: its compositional part, by means of which a not unique semi-reduced divisor is formed, and the reduction part, which gives us a unique reduced divisor. In particular, special case of the compositional part of Cantor's algorithm, doubling of the divisor, is described: it significantly reduces algorithm time complexity. Also the correctness of the algorithms are proved, examples of applications are given. The main result of the work is the implementation of the divisor calculation of a polynomial function, its Mumford representation, and Cantor's algorithm in Python programming language. Thus, the aim of the work is to demonstrate the possibility of effective use of described algorithms for further work with divisors on the hyperelliptic curve, including the development of cryptosystem, digital signature based on hyperelliptic curves, attacks on such cryptosystems.

Keywords: hyperelliptic curve; divisor; Mumford representation.

Матеріал надійшов 27.06.2020