О сложности двумерной задачи дискретного логарифмирования в конечной циклической группе с эффективным автоморфизмом

Николаев Максим Владимирович
Научный руководитель: к.ф.-м.н. Матюхин Дмитрий Викторович

26 марта, 2014

Определения

- *Определение 1. Задача Дискретного логарифмирования.*
  Дано: группа $G = \langle P \rangle$, $\mathrm{ord}(P) = r$, $Q \in G$.
  Найти: $n \in \{0, ..., r-1\}$ *такое, что* $Q = nP$.

Определения

- *Определение 1. Задача Дискретного логарифмирования.*
  Дано: группа $G = \langle P \rangle$, $\mathrm{ord}(P) = r$, $Q \in G$.
  Найти: $n \in \{0, ..., r-1\}$ *такое, что* $Q = nP$.
- *Определение 2. Двумерная Задача Дискретного логарифмирования.*
  Дано: группа G; $P_1, P_2, Q \in G$, $N_1, N_2 \in \mathbb{N}$, $Q = n_1 P_1 + n_2 P_2$ *для некоторых (неизвестных)* $n_1 \in \{-N_1, \ldots, N_1\}$, $n_2 \in \{-N_2, \ldots, N_2\}$.
  Найти: n_1, n_2 *такие, что* $Q = n_1 P_1 + n_2 P_2$.

Алгоритм решения двумерной задачи дискретного логарифмирования (Gaudry, Schost, 2004)

- Построение Дикого и Домашнего множеств

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

Алгоритм решения двумерной задачи дискретного логарифмирования (Gaudry, Schost, 2004)

- Построение Дикого и Домашнего множеств

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

- Генерация последовательностей

$$x_i P_1 + y_i P_2, (x_i, y_i) \in T, i = 1, 2, \ldots, \quad (1)$$

$$Q + z_j P_1 + w_j P_2, (z_j, w_j) \in T, j = 1, 2, \ldots \quad (2)$$

Алгоритм решения двумерной задачи дискретного логарифмирования (Gaudry, Schost, 2004)

- Построение Дикого и Домашнего множеств

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

- Генерация последовательностей

$$x_i P_1 + y_i P_2, (x_i, y_i) \in T, i = 1, 2, \ldots, \quad (1)$$

$$Q + z_j P_1 + w_j P_2, (z_j, w_j) \in T, j = 1, 2, \ldots \quad (2)$$

- Получение решения задачи

$$x_k P_1 + y_k P_2 = Q + z_l P_1 + w_l P_2, \quad (3)$$

Алгоритм решения двумерной задачи дискретного логарифмирования (Gaudry, Schost, 2004)

- Построение Дикого и Домашнего множеств

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

- Генерация последовательностей

$$x_i P_1 + y_i P_2, (x_i, y_i) \in T, i = 1, 2, \ldots, \quad (1)$$

$$Q + z_j P_1 + w_j P_2, (z_j, w_j) \in T, j = 1, 2, \ldots \quad (2)$$

- Получение решения задачи

$$x_k P_1 + y_k P_2 = Q + z_l P_1 + w_l P_2, \quad (3)$$

- Оценка средней трудоемкости
$\Omega = 2.36\sqrt{N}$, где $N = (2N_1 + 1)(2N_2 + 1)$ [Galbraith, Ruprai, 2009]

Эффективно вычислимый автоморфизм и задача дискретного логарифмирования

- Эффективно вычислимый гомоморфизм

$$\varphi : \ \varphi(g) = \lambda g, \ \forall g \in G$$

Группа G распадается на классы эквивалентности

$$\{g, \varphi(g), ..., \varphi^k(g)\}$$

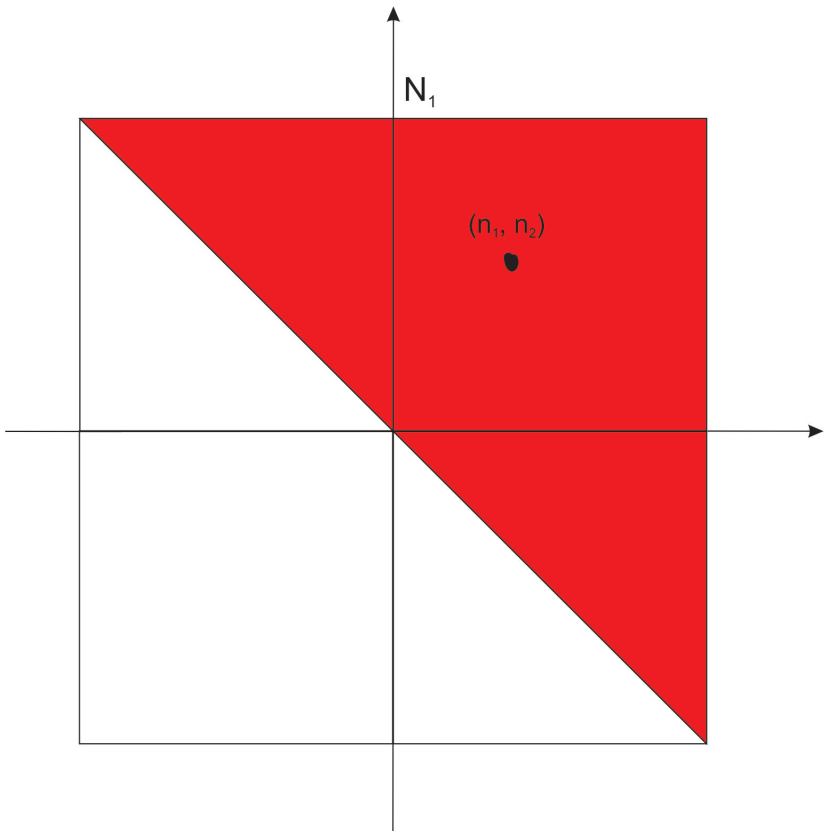
Случай $\#\langle\varphi\rangle = 2$

- Эллиптическая кривая, заданная уравнением $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$

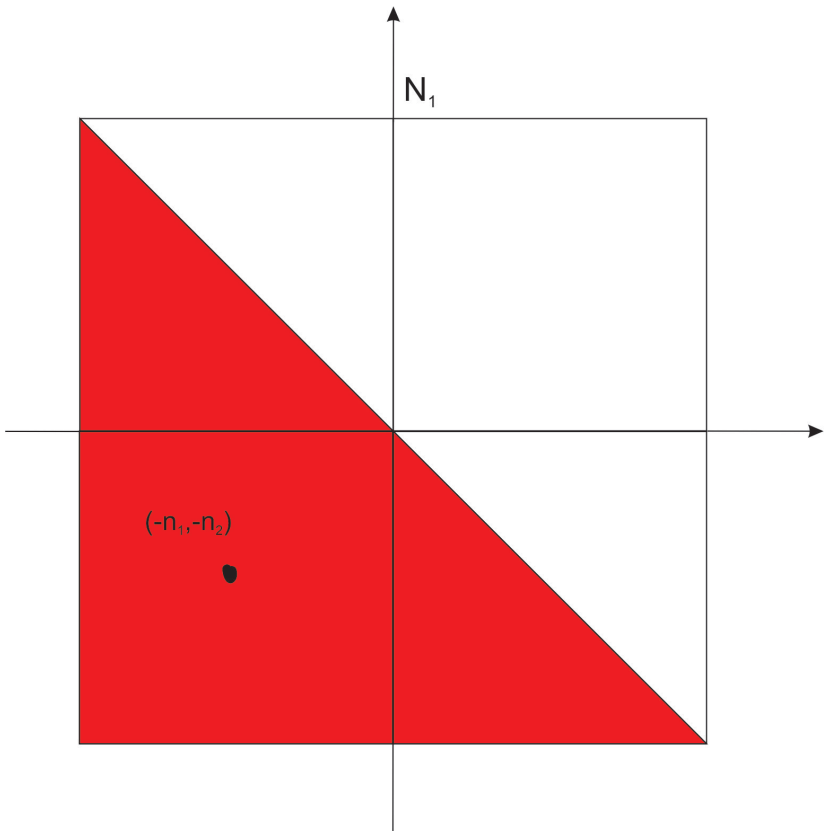
Случай $\#\langle\varphi\rangle = 2$

- Эллиптическая кривая, заданная уравнением $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$
- Эффективный автоморфизм: $\varphi(x, y) = (x, -y)$

Случай $\#\langle\varphi\rangle = 2$



Случай $\#\langle\varphi\rangle = 2$



Результат Лиу [2010]

- Выбор множеств

$$T = \{\{(a,b),(-a,-b)\} : -\frac{17}{20}N_1 \leq a \leq \frac{17}{20}N_1, -\frac{17}{20}N_1 \leq b \leq \frac{17}{20}N_1\}$$

$$W = \{\{(n_1+a, n_2+b),(-n_1-a,-n_2-b)\} : -\frac{N_1}{2} \leq a \leq \frac{N_1}{2}, -\frac{N_1}{2} \leq b \leq \frac{N_1}{2}\}$$

Результат Лиу [2010]

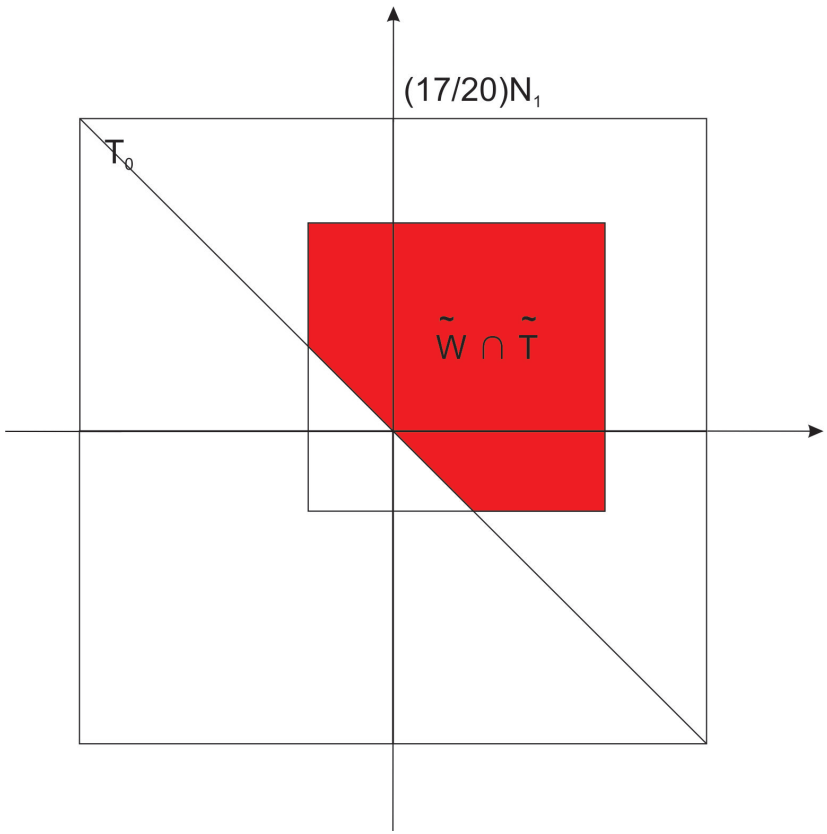
- Выбор множеств

$$T = \{\{(a,b),(-a,-b)\} : -\frac{17}{20}N_1 \le a \le \frac{17}{20}N_1, -\frac{17}{20}N_1 \le b \le \frac{17}{20}N_1\}$$

$$W = \{\{(n_1+a, n_2+b),(-n_1-a,-n_2-b)\} : -\frac{N_1}{2} \le a \le \frac{N_1}{2}, -\frac{N_1}{2} \le b \le \frac{N_1}{2}\}$$

- Средняя трудоемкость решения: $(1.45 + o(1))\sqrt{N}$ групповых операций

Случай $\#\langle\varphi\rangle = 2$



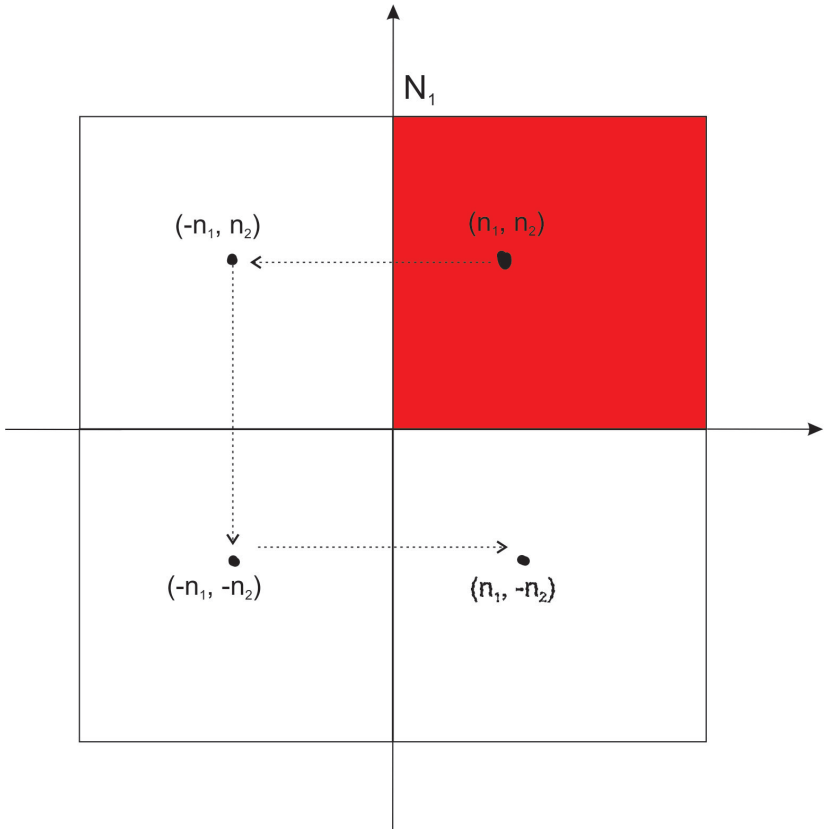
Случай $\#\langle\varphi\rangle = 4$

- Кривая, заданная уравнением $y^2 = x^3 + Ax$, при $p \equiv 1 \bmod 4$

Случай $\#\langle\varphi\rangle = 4$

- Кривая, заданная уравнением $y^2 = x^3 + Ax$, при $p \equiv 1 \bmod 4$
- Эффективный автоморфизм: $\varphi(x, y) = (-x, \alpha y)$, где α — элемент порядка 4 по модулю p, λ — корень уравнения $\lambda^2 \equiv -1 \pmod{n}$

Случай $\#\langle\varphi\rangle = 4$



Результат Лиу [2010]

- Выбор множеств

$$T = \{\{(a,b),(-a,b),(-a,-b),(a,-b)\} : \\ -(1-\tau)N_1 \le a \le (1-\tau)N_1, -(1-\tau)N_1 \le b \le (1-\tau)N_1\}$$

где $\tau = 0.1467$. А также «дикое» множество

$$W = \{\{(n_1+a, n_2+b),(-n_1-a,-n_2-b)\} : \\ -\frac{N_1}{2} \le a \le \frac{N_1}{2}, -\frac{N_1}{2} \le b \le \frac{N_1}{2}\}$$

Результат Лиу [2010]

- Выбор множеств

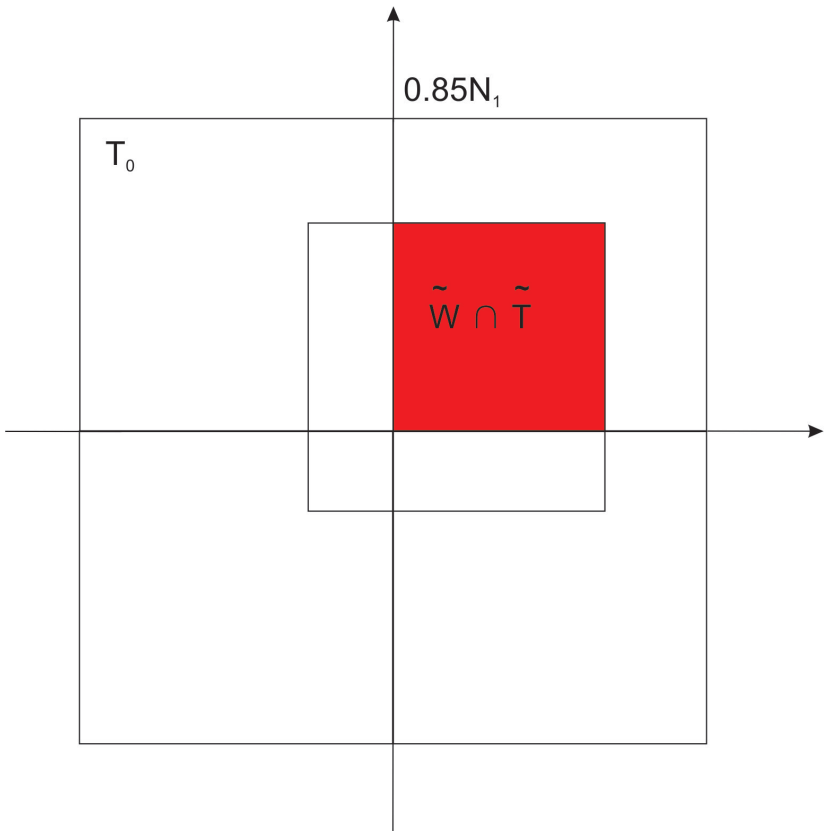
$$T = \{\{(a,b),(-a,b),(-a,-b),(a,-b)\} : \\ -(1-\tau)N_1 \le a \le (1-\tau)N_1, -(1-\tau)N_1 \le b \le (1-\tau)N_1\}$$

где $\tau = 0.1467$. А также «дикое» множество

$$W = \{\{(n_1+a, n_2+b),(-n_1-a,-n_2-b)\} : \\ -\frac{N_1}{2} \le a \le \frac{N_1}{2}, -\frac{N_1}{2} \le b \le \frac{N_1}{2}\}$$

- Средняя трудоемкость решения: $(1.025 + o(1))\sqrt{N}$ групповых операций

Случай $\#\langle\varphi\rangle = 4$



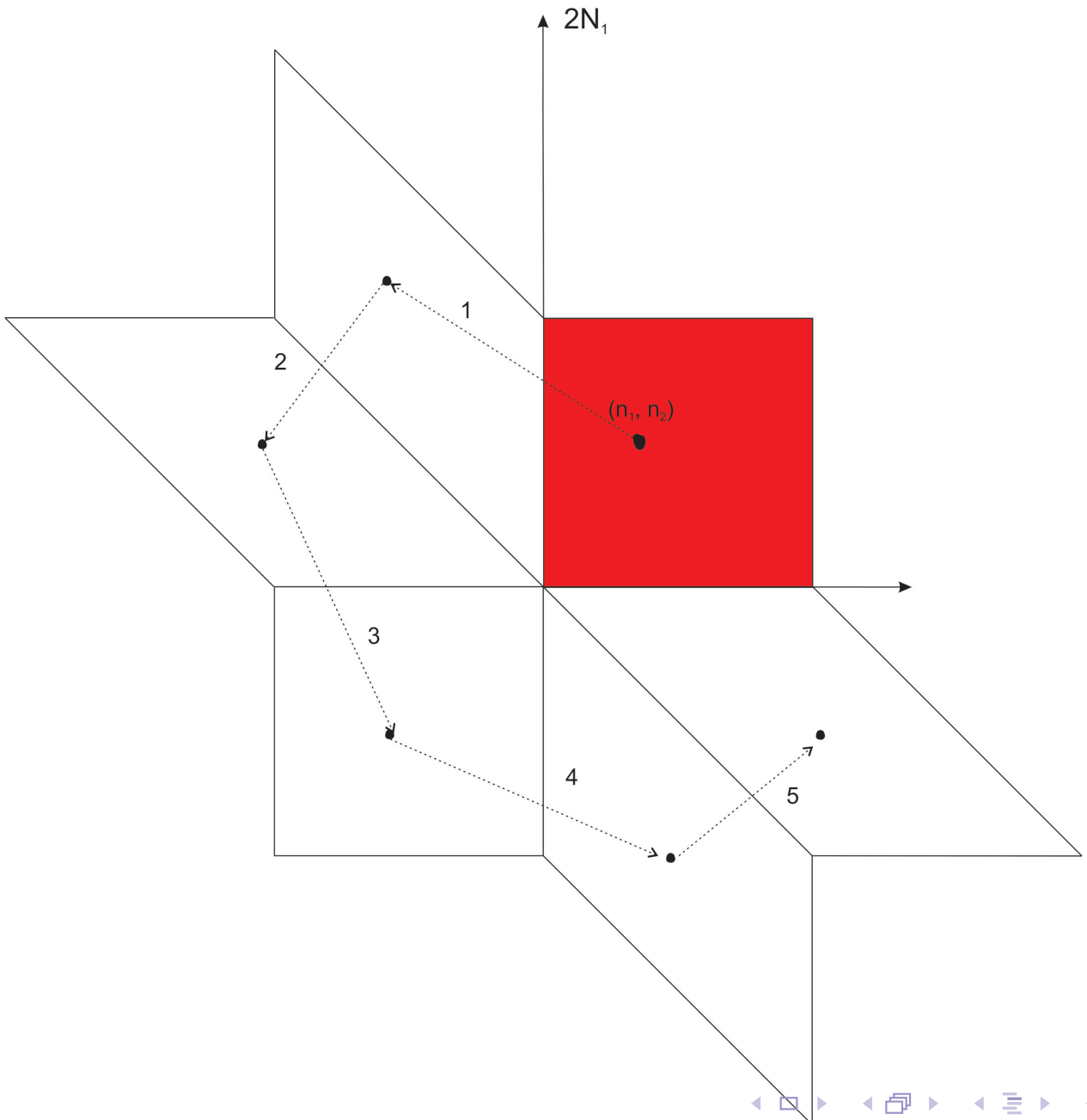
Случай $\#\langle\varphi\rangle = 6$

- Кривая E, заданная над $GF(p)$ уравнением $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$

Случай $\#\langle\varphi\rangle = 6$

- Кривая E, заданная над $GF(p)$ уравнением $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$
- φ порядка 6, $\varphi(x, y) = (\beta x, -y)$, где $\beta \neq 1$ — кубический корень из 1 по модулю p, λ — корень уравнения $\lambda^2 - \lambda + 1 \equiv 0 \pmod n$

Случай $\#\langle\varphi\rangle = 6$



Случай $\#\langle\varphi\rangle = 6$

- Выбор множеств

$$T = \{C(a, b) : -N_1 \leq a \leq N_1, -N_1 \leq b \leq N_1\}.$$

А также «дикое» множество

$$W = \{C(n_1 + a, n_2 + b) : -\frac{N_1}{2} \leq a \leq \frac{N_1}{2}, -\frac{N_1}{2} \leq b \leq \frac{N_1}{2}\}$$

Случай $\#\langle\varphi\rangle = 6$

- Выбор множеств

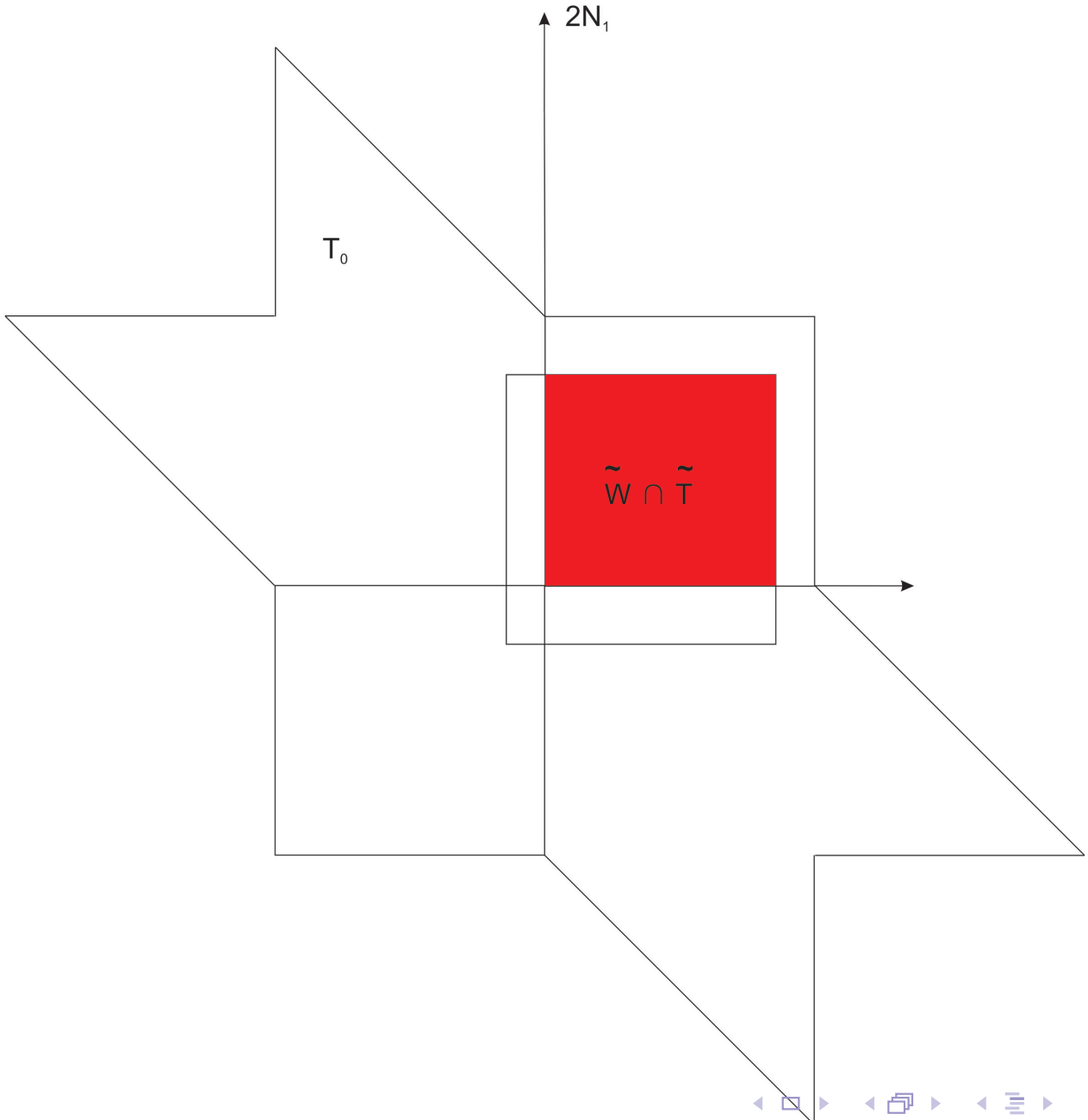
$$T = \{C(a, b) : -N_1 \leq a \leq N_1, -N_1 \leq b \leq N_1\}.$$

А также «дикое» множество

$$W = \{C(n_1 + a, n_2 + b) : -\frac{N_1}{2} \leq a \leq \frac{N_1}{2}, -\frac{N_1}{2} \leq b \leq \frac{N_1}{2}\}$$

- Средняя трудоемкость решения: $(0.9781 + o(1))\sqrt{N}$ групповых операций

Случай $\#\langle\varphi\rangle = 6$



Оценка средней трудоемкости

[Galbraith, Holmes, 2010] Теорема

Пусть есть неограниченное количество шаров (отличающихся только в цвете) и N урн. Мы выбираем шары и перекрашиваем их в красный или синий цвета с вероятностями $q_c (c = 1, 2)$ *и бросаем их в урны. Вероятность попадания в урну a равна* $q_{c,a}$ *и* $q_{c',a}$ *для красных и синих шаров соответственно. Ожидаемое количество шаров, которые необходимо выбрать для того, чтобы получить разноцветные шары в одной урне, равно*

$$\sqrt{\frac{\pi}{2A_N}} + O(N^{1/4})$$

где $A_N = \sum_{c=1}^{2} q_c (\sum_{c'=1, c \neq c'}^{2} q_{c'} (\sum_{a=1}^{R} q_{c,a} q_{c',a}))$

Результаты

Теорема

Пусть G — подгруппа простого порядка n группы точек эллиптической кривой E, заданной над конечным простым полем $GF(p)$ уравнением $y^2 = x^3 + Ax + B$ при $p \equiv 1 \pmod 3$; φ — автоморфизм группы G, $\varphi(x, y) = (x, -y)$, Тогда для любого $\varepsilon > 0$ существует такой алгоритм решения двумерной задачи дискретного логарифмирования в группе G, что при $N_1 = N_2$, $P_2 = \varphi(P_1)$ и случайном равновероятном выборе (n_1, n_2), его средняя трудоемкость не превосходит $(1 + \varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций, где $N = 4N_1N_2, N \to \infty$.

Результаты

- случай кривой, заданной над конечным простым полем $GF(p)$ уравнением $y^2 = x^3 + Ax$ при $p \equiv 1 \pmod 4$

$$(1 + \varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$$

Результаты

- случай кривой, заданной над конечным простым полем $GF(p)$ уравнением $y^2 = x^3 + Ax$ при $p \equiv 1 \pmod 4$

$$(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$$

- случай кривой, заданной над конечным простым полем $GF(p)$ уравнением $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$

$$(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$$

Сравнение с алгоритмом Полларда (случай кривой $y^2 = x^3 + Ax + B$)

- Средняя трудоемколсть алгоритма Полларда: $\sqrt{\frac{1}{2}}\sqrt{\frac{\pi|G|}{2}}$

Сравнение с алгоритмом Полларда (случай кривой $y^2 = x^3 + Ax + B$)

- Средняя трудоемколсть алгоритма Полларда: $\sqrt{\frac{1}{2}}\sqrt{\frac{\pi|G|}{2}}$
- GLV-метод

$$kP = k_1 P + k_2 \varphi(P)$$

$k_1, k_2 \leq C_{GLV}\sqrt{n}$, где $n = ord(P)$

Сравнение с алгоритмом Полларда (случай кривой $y^2 = x^3 + Ax + B$)

- Средняя трудоемколсть алгоритма Полларда: $\sqrt{\frac{1}{2}}\sqrt{\frac{\pi|G|}{2}}$
- GLV-метод

$$kP = k_1 P + k_2 \varphi(P)$$

$k_1, k_2 \leq C_{GLV}\sqrt{n}$, где $n = ord(P)$

- Сравнение с алгоритмом полларда

$$(1+\varepsilon)\sqrt{\frac{\pi N}{2}} < \sqrt{\frac{1}{2}}\sqrt{\frac{\pi|G|}{2}}$$

Сравнение с алгоритмом Полларда (случай кривой $y^2 = x^3 + Ax + B$)

- Средняя трудоемколсть алгоритма Полларда: $\sqrt{\frac{1}{2}}\sqrt{\frac{\pi|G|}{2}}$
- GLV-метод

$$kP = k_1 P + k_2 \varphi(P)$$

$k_1, k_2 \leq C_{GLV}\sqrt{n}$, где $n = ord(P)$

- Сравнение с алгоритмом полларда

$$(1+\varepsilon)\sqrt{\frac{\pi N}{2}} < \sqrt{\frac{1}{2}}\sqrt{\frac{\pi|G|}{2}}$$

- $$C_{GLV} < \frac{1}{2\sqrt{3}(1+\varepsilon)}$$

Сравнение с алгоритмом Полларда

- Средняя трудоемколсть алгоритма Полларда: $\sqrt{\frac{1}{4}}\sqrt{\frac{\pi|G|}{2}}$, в случае кривой $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$ и $\sqrt{\frac{1}{6}}\sqrt{\frac{\pi|G|}{2}}$, в случае кривой $y^2 = x^3 + Ax$ при $p \equiv 1 \bmod 4$

Сравнение с алгоритмом Полларда

- Средняя трудоемколсть алгоритма Полларда: $\sqrt{\frac{1}{4}}\sqrt{\frac{\pi|G|}{2}}$, в случае кривой $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$ и $\sqrt{\frac{1}{6}}\sqrt{\frac{\pi|G|}{2}}$, в случае кривой $y^2 = x^3 + Ax$ при $p \equiv 1 \bmod 4$
- Сравнение с алгоритмом полларда ($y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$)

$$(1+\varepsilon)\sqrt{\frac{\pi N}{4}} < \sqrt{\frac{1}{4}}\sqrt{\frac{\pi|G|}{2}}$$

$$C_{GLV} < \frac{1}{2\sqrt{2}(1+\varepsilon)}$$

Сравнение с алгоритмом Полларда

- Средняя трудоемколсть алгоритма Полларда: $\sqrt{\frac{1}{4}}\sqrt{\frac{\pi|G|}{2}}$, в случае кривой $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$ и $\sqrt{\frac{1}{6}}\sqrt{\frac{\pi|G|}{2}}$, в случае кривой $y^2 = x^3 + Ax$ при $p \equiv 1 \bmod 4$
- Сравнение с алгоритмом полларда ($y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$)

$$(1+\varepsilon)\sqrt{\frac{\pi N}{4}} < \sqrt{\frac{1}{4}}\sqrt{\frac{\pi|G|}{2}}$$

$$C_{GLV} < \frac{1}{2\sqrt{2}(1+\varepsilon)}$$

- Сравнение с алгоритмом полларда ($y^2 = x^3 + Ax$ при $p \equiv 1 \bmod 4$)

$$(1+\varepsilon)\sqrt{\frac{\pi N}{4}} < \sqrt{\frac{1}{6}}\sqrt{\frac{\pi|G|}{2}}$$

$$C_{GLV} < \frac{1}{2\sqrt{3}(1+\varepsilon)}$$

Сравнение с алгоритмом Полларда

Спасибо за внимание!