

Логарифмирование через поднятие

Задачи вычисления логарифма в группе точек эллиптической кривой и в мультипликативной группе конечного поля положены в основу безопасности многих криптосистем, например, стандартов цифровой подписи РФ и США. Для логарифмирования на эллиптической кривой, обладающей группой простого порядка r , наилучшим считается алгоритм Полларда со сложностью $O(\sqrt{r})$. Для логарифмирования в конечном поле \mathbf{F}_p наилучшим считается алгоритм решета числового поля со сложностью $O\left(\exp\left(c^3\sqrt{\ln p(\ln \ln p)^2}\right)\right)$ для $c < 2$. Предлагается подход к вычислению логарифмов, основанный на использовании эллиптической кривой над числовым полем, обладающей достаточно большим рангом. Показано, что задача логарифмирования в конечном поле и на эллиптической кривой сводится к поднятию точки кривой в числовое поле.

1. Теоретические основы

Эллиптическая кривая

$$E(K): y^2 = x^3 + Ax + B, \quad (1)$$

заданная над числовым полем $K = \mathbf{Q}(\sqrt{D_1}, \sqrt{D_2}, \dots, \sqrt{D_m})$, может быть приведена по модулю p , если $\sqrt{D_i} \in \mathbf{F}_p$ (вместо различных D_i , конечно, можно использовать одно алгебраическое число). Целостное кольцо целых элементов поля K обладает однозначным разложением на простые идеалы. Координаты каждой конечной точки кривой $E(K)$ могут быть приведены к паре дробей с целыми рациональными знаменателями. Редукция кривой $E(K)$ по модулю p определена и задает отображение

$$\varphi: E(K) \rightarrow E(\mathbf{F}_p). \quad (2)$$

Обратно, кривая

$$E(\mathbf{F}_p): y^2 \equiv x^3 + Ax + B \pmod{p} \quad (3)$$

может быть вложена в кривую $E(K)$. Отображение точки $Q \in E(\mathbf{F}_p)$ в точку $Q \in E(K)$ назовем *поднятием* точки Q из поля \mathbf{F}_p в поле K , при этом сравнение (3) превращается в равенство (1). Сумме точек $E(K)$ соответствует сумма точек $E(\mathbf{F}_p)$ (обратное утверждение неверно). Поэтому задача вычисления векторного индекса на кривой $E(K)$ соответствует задаче вычисления индекса на кривой $E(\mathbf{F}_p)$ относительно гомоморфных образов образующих кривой $E(K)$.

Кривая (3) допускает изоморфизмы $x \rightarrow xu^2$, $y \rightarrow yu^3$, $A \rightarrow Au^4$, $B \rightarrow Bu^6$. Таким образом, вместо одиночной кривой (3) можно рассматри-

вать семейство изоморфных кривых, каждая из которых может быть вложена в соответствующую кривую $E(K)$.

Нас будет интересовать случай бесконечной группы $E(K)$. Отображение (2) определяется ядром. Пусть $\#E(\mathbf{F}_p) = r$ — большое простое число. Если бесконечная группа $E(K)$ циклична с образующей P_1 , то

$$\text{Ker}(\varphi) = nrP_1,$$

где $n \in \mathbf{Z}$, а точке $P = kP_1$ на кривой $E(\mathbf{F}_p)$ будет соответствовать множество точек $kP_1 + nrP_1$ на кривой $E(K)$.

Предположим, что бесконечная группа $E(K)$ без кручения имеет две образующих P_1 и P_2 , и на кривой $E(\mathbf{F}_p)$ выполняется равенство $\varphi(P_2) = s\varphi(P_1)$. Ядро гомоморфизма включает в себя целочисленные линейные комбинации образующих, кратные r . Кроме того, в ядро входят комбинации образующих, гомоморфный образ которых дает бесконечно удаленную точку, например, $sP_1 - P_2$, $(2s \pmod{r})P_1 - 2P_2$ и т. п. Тогда

$$\text{Ker}(\varphi) = n_1rP_1 + n_2rP_2 + (m \cdot s \pmod{r})P_1 - mP_2,$$

где $n_1, n_2 \in \mathbf{Z}$, $m \in \mathbf{Z}/p\mathbf{Z}$.

Обобщим предыдущее рассуждение на случай k образующих P_1, \dots, P_k . Пусть на кривой $E(\mathbf{F}_p)$ выполняются равенства $\varphi(P_k) = s_1\varphi(P_1) = s_2\varphi(P_2) = \dots = s_{k-1}\varphi(P_{k-1})$. Тогда

$$\text{Ker}(\varphi) = \sum_{i=1}^k n_i r P_i + \sum_{i=1}^{k-1} (m_i s_i \pmod{r}) P_i - \left(\sum_{i=1}^{k-1} m_i \right) \pmod{r} P_k,$$

где $n_i \in \mathbf{Z}$, $m_i \in \mathbf{Z}/p\mathbf{Z}$.

Каноническая высота точки $P \in E(\mathbf{Q})$ определяется [1] как предел

$$\hat{h}(P) = \lim_{m \rightarrow \infty} \frac{h(mP)}{m^2}, \quad (4)$$

где $h(R)$ — длина координаты x точки R в битах, $\hat{h}(P) \in \mathbf{R}$. В соответствии с (4) длина координат точек mR растет пропорционально квадрату от m или пропорционально экспоненте от квадрата длины m . Имеет место равенство $\hat{h}(P) = \frac{h(P)}{2} + O(1)$. Аналогично определяется и каноническая высота на эллиптической кривой $E(K)$ над конечным расширением K поля \mathbf{Q} .

При этом имеют место равенства

$$\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$

$$\hat{h}(mP) = m^2 \hat{h}(P). \quad (5)$$

Равенство (5) устанавливает связь задачи логарифмирования на эллиптической кривой и задачи логарифмирования в конечно порожденной подгруппе группы \mathbf{R}^* ненулевых вещественных чисел.

Каждая точка бесконечного порядка эллиптической кривой $E(K)$ однозначно определяется канонической высотой. Если P — точка кручения, то $\hat{h}(P) = 0$. По теореме Морделла — Вейля ранг кривой $E(K)$ конечен. Индекс $\text{ind}(R)$ каждой точки $R \in E(K)$ может быть представлен как вектор, число координат которого равно рангу кривой. Если P_1, \dots, P_k — образующие групп $E(K)$ бесконечных порядков и $R = \sum_{i=1}^k n_i P_i$, \hat{h} индексы точек P_i

образуют базис k -мерного \mathbf{Z} -модуля. Поэтому индексы точек бесконечного порядка кривой $E(K)$ образуют целочисленную решетку.

Например, эллиптическая кривая $E: y^2 = x^3 + 17$ имеет над \mathbf{Q} ранг 2. Образующие групп бесконечного порядка равны $P_1 = (2, 5)$ и $P_2 = (-2, 3)$, индекс точки бесконечного порядка является двумерным вектором. Точки

$$R_1 = \left(\frac{1466}{169}, -\frac{56857}{2197} \right) \text{ и } R_2 = \left(\frac{94}{25}, \frac{1047}{125} \right)$$

равны $R_1 = 3P_1 - 2P_2$, $R_2 = 2P_1 - 3P_2$, их индексы равны $\text{ind}(R_1) = (3, -2)$, $\text{ind}(R_2) = (2, -3)$. При переходе к расширению $K = \mathbf{Q}(\sqrt{-3})$ кольцо целых имеет вид $\mathbf{Z}[\rho]$, $\rho = \frac{1 + \sqrt{-3}}{2}$, кривая обладает комплексным умножением на

число ρ , задаваемое парой функций $(x, y) \rightarrow (\rho^2 x, -y)$. Поскольку число ρ не является рациональным, то к паре образующих присоединяются (по крайней мере) еще две точки $(-2\rho^2, 3)$ и $(2\rho^2, 5)$. Используя сравнения по модулям различных простых чисел $p \equiv \pm 1 \pmod{6}$, можно показать, что точки $(2, 5)$, $(-2, 3)$, $(-2\rho^2, 3)$ и $(2\rho^2, 5)$ кривой $E(K)$ линейно независимы над \mathbf{Z} .

По определению канонической высоты выполняется равенство $\hat{h}(P) = \hat{h}(-P)$. Поэтому если P и Q — образующие групп бесконечного порядка, то

$$\hat{h}(P + Q) = \hat{h}(P - Q) = \hat{h}(P) + \hat{h}(Q).$$

Следовательно, канонические высоты точек бесконечного порядка эллиптической кривой $E(K)$ образуют решетку, базис которой состоит из канонических высот образующих групп бесконечного порядка.

Пусть $H = (h_{ij})$ — квадратная матрица размера $k \times k$ (k — ранг кривой $E(K)$), где

$$h_{ij} = \frac{\hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j)}{2}$$

и P_1, \dots, P_k — образующие циклических групп бесконечных порядков. Тогда имеет место равенство

$$\hat{h}(n_1P_1 + n_2P_2 + \dots + n_kP_k) = \mathbf{nHn}^T, \quad (6)$$

где $\mathbf{n} = (n_1, \dots, n_k)$ — векторный индекс точки $P = n_1P_1 + \dots + n_kP_k$. Выражение (6) устанавливает связь между канонической высотой произвольной точки кривой $E(K)$, и ее индексом.

2. Использование поля характеристики 0

Задача поднятия точки требует указания всех двоичных разрядов координат точки $E(K)$. В соответствии с (4) длина координат точки пропорциональна квадрату показателя (или экспоненте от квадрата длины показателя). Отсюда следует, что для $k = 1$ задача поднятия является сложной хотя бы потому, что перечисление всех разрядов координат требует экспоненциального времени (даже без учета сложности собственно вычислений). Однако, если ранг k кривой $E(K)$ достаточно велик, то на ней существует значительное количество точек с малой высотой. Ранг эллиптической кривой с комплексным умножением может быть вычислен как кратность нуля функции $L_{E/K}(s)$, где $s = 1$ в предположении, что верна гипотеза Берча и Свиннертона-Дайера [1].

Определим *вес* $w = w(P)$ точки $P \in E(K)$ на точечной решетке как сумму абсолютных значений координат векторного индекса. Если $\text{ind}(P) = (n_1, \dots, n_k)$, то $w(P) = |n_1| + \dots + |n_k|$. Число точек N_w с весом ровно w в соответствии с известным результатом из комбинаторики равно

$$N_w = \frac{k(k+1)\dots(k+w-1)}{w!} = \binom{k+w-1}{w}. \quad (7)$$

Если $k = O(w)$, то число точек с весом не более w можно оценить числом точек с весом w .

Оценим сложность нахождения индекса точки $P \in E(K)$, $P = \sum_{i=1}^k n_i P_i$, если ранг кривой $E(K)$ равен k и вес точки P не превышает w .

Из (6) следует, что $\hat{h}(P) = O(kw^2)$. Для нахождения индекса точки $P \in E(K)$ нужно к точке P прибавлять точки $\pm P_i$ до тех пор, пока не будет получена нулевая каноническая высота. После каждого сложения высота должна уменьшаться. Число сложений точек в ходе вычисления индекса точки P равно $O(kw)$. Наиболее трудоемкой арифметической операцией при сложении точек является умножение. Сложность умножения целых чисел методом Шенхаге — Штрассена равна $O(kw^2 \log(kw^2))$. Пусть поле K является конечным расширением поля \mathbf{Q} , полученное присоединением квадратных

корней из небольших по абсолютной величине чисел D_1, \dots, D_m , причем все D_i являются квадратичными вычетами по модулю p . Координаты точки представляют собой многочлены от 2^m переменных. Сложность умножения координат равна $O(2^m k w^2 \log(k w^2))$. Такую же оценку имеет и сложность сложения точек. Поэтому сложность нахождения индекса точки $P \in E(K)$ равна

$$S = O(2^m k^2 w^3 \log(k w^2)).$$

Пусть поле K является конечным расширением поля \mathbf{Q} , полученное присоединением квадратных корней из небольших по абсолютной величине чисел D_1, \dots, D_m , причем все D_i являются квадратичными вычетами по модулю p . Предположим по аналогии с теоремой Мазура [1] для $E(\mathbf{Q})$, что группа кручения эллиптической кривой $E(K)$ может иметь только гарантированно малый порядок, меньший чем r . Тогда в силу гомоморфизма (2) группа кручения $\text{Tors}E(K)$ состоит из бесконечно удаленной точки, то есть все аффинные точки $E(K)$ имеют бесконечный порядок¹. Поэтому желательно использовать поле K , задаваемое многочленом небольшой степени.

Общий план решения показательного уравнения $P = lQ$ на кривой $E(\mathbf{F}_p)$ может иметь следующий вид.

1. Поднять не менее k аффинных точек $R_i = a_i P + b_i Q$ для некоторых a_i, b_i , из поля \mathbf{F}_p в поле K , определив при этом вид поля K . Не все a_i и не все b_i должны быть нулевыми. Найти образующие P_1, \dots, P_k бесконечных циклических групп $E(K)$.
2. Найти индексы точек R_i в группе $E(K)$ минимизацией канонической высоты.
3. Привести каждую из точек R_i и образующие $E(K)$ по модулю p .
4. Методом гауссова исключения выразить логарифм точки P через логарифм точки Q .

Поднятие на шаге 1 должно обеспечивать минимальный вес точки. Если мощность множества точек веса не более w близка к r , то с вероятностью, близкой к 1, каждую точку кривой $E(\mathbf{F}_p)$ можно поднять так, что ее вес не будет превышать w .

Найдем вначале сложность шагов 2–4. Заменяем в (7) факториалы по формуле Стирлинга и приравняем $\log N_w$ и $\log r$ в предположении, что $k \approx w$. Получим

$$\log r = \log N_w = (k + w) \log(k + w) - k \log k - w \log w \approx 2k \log 2.$$

¹ Теоретически можно было бы в качестве поля K использовать простое трансцендентное расширение $\mathbf{F}_p(t)$ поля \mathbf{F}_p , что облегчило бы поднятие точки. Однако в этом случае группа кручения оказалась бы очень богатой, так как она содержала бы все конечные группы $E(\mathbf{F}_q)$ для $q \in \{p^2, p^3, \dots\}$. Поэтому указанный ниже метод логарифмирования оказывается непрактичным.

Тогда

$$k = \frac{\log_2 r}{2}.$$

Для нахождения логарифма l нужно найти $O(k)$ индексов точек R_i , сложность этой операции (шаг 2) равна

$$O(2^m k^3 w^3 \log(kw^2)) = O(2^m (\log r)^6 \log \log r).$$

Сложность шага 3 оценивается многочленом степени не более 6 от $\log r$, сложность шага 4 оценивается многочленом степени 3 от $\log r$. Итоговая сложность вычисления логарифма на кривой $E(\mathbf{F}_p)$ равна

$$S = O(2^m (\log r)^6 \log \log r) + O(\log r) \cdot (S_1 + S_2)$$

где S_1 — сложность поднятия точки из поля \mathbf{F}_p в поле K так, чтобы вес поднятой точки был минимален, S_2 — сложность нахождения образующих P_i . Если наибольшая из сложностей S_1 и S_2 полиномиальна (субэкспоненциальна, экспоненциальна), то и задача логарифмирования может быть решена указанным методом с полиномиальной (соответственно субэкспоненциальной, экспоненциальной) сложностью. Существование эллиптических кривых над \mathbf{Q} неограниченно большого ранга, вытекает из гипотезы Таниямы [1].

Таким образом, задача дискретного логарифмирования на эллиптической кривой $E(\mathbf{F}_p)$ полиномиально сводится к поднятию точки кривой из поля \mathbf{F}_p в числовое поле K и к нахождению множества образующих кривой $E(K)$. Поднятие выполняется наиболее просто, если вес поднятой точки будет минимален.

Метод поднятия точки из \mathbf{F}_p в K неочевиден. Если определить вес w точки на решетке ранга k образующих бесконечного порядка кривой $E(\mathbf{Q})$ как наибольшее из абсолютных значений координат, то количество точек с весом не более w , равно числу точек k -мерного параллелепипеда с центром в нуле и длиной стороны $2w$ и составляет k^{2w} . В этом случае можно оставаться в рамках поля \mathbf{Q} . Если задача поднятия точки в поле \mathbf{Q} имеет полиномиальную или субэкспоненциальную сложность, то снижение асимптотической сложности задачи логарифмирования по сравнению с алгоритмом Полларда происходит при ранге не менее 3. Таких кривых достаточно много [2].

Аналогичный подход может быть использован и для логарифмирования в мультипликативной группе простого поля. Для решения показательного уравнения $a^u \equiv b \pmod{p}$ выполняется следующая последовательность действий.

1. Выбирается эллиптическая кривая $E(K)$ вида $y^2 = x^3 + Cx^2 + kp$, $Ck \neq 0$, которая в результате редукции по модулю p дает особую кубику.

2. С помощью вычислимого в обе стороны изоморфизма особой кубики и группы \mathbf{F}_p^* находятся точки кубики, соответствующие элементам a и b .
3. Находится ранг кривой $E(K)$ и ее образующие.
4. Далее задача решается так же, как и для эллиптической кривой.

Ранг эллиптической кривой $E(\mathbf{Q})$ мал и обычно не превышает 14 [2]. Для логарифмирования указанным способом нужно иметь большой ранг. Например, если длина порядка группы r равна 200 бит, то оптимальное значение ранга и веса составляют около 100. Для этого можно использовать последовательные квадратичные расширения поля \mathbf{Q} , полученные присоединениями квадратных корней и малых D_i , являющихся квадратичными вычетами по модулю p , или использовать кривую $E(\mathbf{Q})$ достаточно большого ранга. Если кривая обладает комплексным умножением, то присоединение к полю \mathbf{Q} квадратичного целого, определяющего комплексное умножение, приводит по крайней мере к удвоению ранга.

Таким образом, задача логарифмирования на эллиптической кривой над простым полем и в мультипликативной группе простого поля может быть сведена к выбору эллиптической кривой большого ранга над числовым полем и к поднятию точки кривой из конечного поля в числовое поле. Анализ техники решения диофантовых уравнений [3], в частности, уравнений Пелля, подтверждает перспективность указанного подхода для решения задач логарифмирования.

Литература

1. Silverman J. H. The arithmetic of elliptic curves. — GTM, v. 106, Springer-Verlag, 1986.
2. Степанов С. А. Арифметика алгебраических кривых. — М.: Наука, 1991.
3. Zagier D. Large integral points on elliptic curves // Math. Comp., v. 48, 1987, pp. 425–436.