ЭФФЕКТИВНОЕ ВЫЧИСЛЕНИЕ ПОРЯДКА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ НАД КОНЕЧИНЫМ ПОЛЕМ

Д. А. Бодягин

ВВЕДЕНИЕ

Эллиптические кривые на данный момент – один из основных объектов теории чисел. Они представляют огромный интерес. Так, в частности, аппарат эллиптических кривых позволил доказать великую теорему Ферма.

В последнее время эллиптические кривые стали широко применяться в криптографии. Там используются кривые, определенные над некоторым конечным полем, которые порождают удобную для приложений абелеву группу. Тут очень важным оказывается вопрос выбора эллиптических кривых, удовлетворяющих определенным свойствам (обычно эти свойства диктуются требованиями криптографической надежности эллиптической кривой, а также требованием минимизации временных затрат при ее использовании). Эти свойства определяются тем, каков порядок задаваемой группы. В настоящей статье обсуждается вопрос эффективного вычисления этого порядка, а также приводится подробный алгоритм для его вычисления.

Для начала введем несколько определений. Эллиптической кривой мы будем называть множество точек, принадлежащих некоторому полю и удовлетворяющих следующему уравнению

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

К этим точкам еще добавляется бесконечно удаленная точка, которую мы будем обозначать символом O. Мы будем обозначать эллиптическую кривую через $E[\mathbf{K}]$, где $\mathbf{K}$ – поле, над которым она определена. В случае, когда характеристика поля не равна двум или трем, то уравнение можно привести к следующему виду:

$$y^2 = x^3 + ax + b.$$

В дальнейшем мы будем рассматривать уравнение только такого вида. Известно, что точки эллиптической кривой образуют абелеву группу, где бесконечно удаленная точка играет роль нейтрального элемента. Общепринято обозначать групповую операцию на эллиптической кривой символом «+».

По теореме Хассе порядок эллиптической кривой E над полем $\mathbf{F}_q$ из q элементов вычисляется по формуле $\#E = q + 1 - t$, где t – так называемый след Фробениуса, удовлетворяющий условию $|t| \le 2\sqrt{q}$. Кроме того, все точки эллиптической кривой над алгебраическим замыканием $\overline{\mathbf{F}}_q$ удовлетворяют характеристическому уравнению

$$\left(x^{q^2}, y^{q^2}\right) - [t](x^q, y^q) + [q](x, y) = O, \qquad (1)$$

где запись $[n](x,y)$ означает прибавление к точке (x,y) самой себя n раз.

Здесь мы не будем приводить обоснования всех приведенных фактов, все доказательства можно найти в [1].

МЕТОД ШУФА

Метод Шуфа – это единственный известный на сегодняшний день алгоритм (не считая его модификаций) для вычисления порядка эллиптической кривой, который выполняется за полиномиальное время. Основная его идея заключается в том, что сначала вычисляется не сам порядок эллиптической кривой, а остатки при делении его на маленькие простые числа. Потом, используя китайскую теорему об остатках, из этих остатков получают сам порядок.

Мы не будем в деталях описывать работу этого алгоритма. Остановимся лишь вкратце на основных его этапах. Подробности можно будет найти в [2].

Пусть l – простое число. Рассмотрим равенство (1) для ненулевых точек из подгруппы l-кручения $E[l]$ кривой $E[\mathbf{F}_q] : E[l]^* = E[l] \setminus \{O\}$. Обозначим через q_l, t_l остатки от деления q и t на l. Поскольку для точек из $E[l]$ выполняется равенство $[l]P = O$, то равенство (1) переписывается в виде:

$$\varphi^2(P) - [t_l]\varphi(P) + [q_l]P = O, \qquad (2)$$

где $\varphi : (x, y) \mapsto (x^q, y^q)$ – эндоморфизм Фробениуса. Теперь, чтобы найти искомое t_1, будем перебирать все значения $\tau \in \{0,1,\cdots,l-1\}$ и для каждого из них проверять выполнение этого равенства непосредственно. Как только мы находим такое τ, что (2) выполнено для некоторой точки $P \in E[l]$, то останавливаемся, поскольку это и будет наше искомое t_1.

Для того чтобы рассматривать это уравнение только для точек из $E^*[l]$, мы будем все вычисления производить по модулю так называемого многочлена деления $f_l(x)$, все корни которого являются x-выми координатами точек из $E^*[l]$.

УЛУЧШЕНИЯ АЛГОРИТМА ШУФА

Приведенный алгоритм – это стандартный алгоритм Шуфа для вычисления порядка эллиптической кривой. Несмотря на то, что сложность его полиномиальная, она все-таки слишком велика. Так, анализ показал, что если не использовать быстрой арифметики, то эта сложность оказывается равной $O(\log^8 q)$. Поэтому для реальных приложений, где требуются кривые над полями порядка 200 – 300 бит, вычисление порядка кривой займет несколько часов. Таким образом, очень актуален вопрос о возможных улучшениях алгоритма Шуфа. В оставшейся части статьи мы приведем некоторые усовершенствования алгоритма, которые были нами получены.

1. Уменьшение числа операций для каждой итерации алгоритма

Анализ сложности алгоритма показал, что наиболее трудоемкая его часть – это вычисление x^q, y^q, x^{q^2} и y^{q^2} по модулю $f_l(x)$. Вся остальная часть алгоритма по сложности имеет тот же порядок, что и эти вычисления. Таким образом, если мы сможем избавиться от них, то существенно ускорим алгоритм.

Как известно, все точки из $E[l]$ имеют координаты из алгебраического замыкания $\overline{\mathbf{F}}_q$. Но иногда случается, что некоторые из них имеют x-вую координату из основного поля $\mathbf{F}_q$. Это означает, что уравнение $f_l(x)=0$ имеет корень в $\mathbf{F}_q$. Тогда из уравнения кривой следует, что сама точка будет принадлежать либо $E(\mathbf{F}_q)$ (если $y \in \mathbf{F}_q$) либо $E(\mathbf{F}_{q^2})$. В первом случае мы получаем, что в нашей кривой есть точка порядка l, а значит порядок кривой делится на l. Далее, по теореме Хассе автоматически находится значение t_l; $t_l \equiv q+1 (\mathrm{mod}\, l)$. Во втором случае просто воспользуемся следствием из теоремы Хассе, утверждающим , что t_1 и t_2 – порядки кривой $E(\mathbf{F}_q)$ и $E(\mathbf{F}_{q^2})$ соответственно, связаны между собой по следующим формулам.

$$t_2 = t_1^{\,2} - 2q.$$

Отсюда сразу получаем, что $t_l \equiv -q-1 (\mathrm{mod}\, l)$, то есть l – делитель сопряженной кривой.

Для того же, чтобы проверить, имеет ли место такой случай, нам необходимо проверить, имеет ли уравнение $f_l(x)=0$ корни в $\mathbf{F}_q$, а это делается очень просто: нам достаточно вычислить НОД$(x^q - x, f_l(x)) = h(x)$. если он не равен единице, то значит корни есть. Поскольку нам в любом случае x^q вычислить необходимо, то такая проверка не скажется на

сложности алгоритма, но зато если вдруг она выполнится, то нам не придется вычислять остальные выражения, что ускорит работу алгоритма приблизительно в 4 раза.

Остался пока нерешенным только один вопрос: пусть оказалось, что $h(x) \neq 1$, то есть наша проверка выполнилась. Это значит, что все точки с x-выми координатами, являющимися корнями уравнения $h(x) = 0$ принадлежат $E[l]$. Но тогда пока неясно, будут ли их y-вые координаты лежать в $\mathbf{F}_q$. Если будут, то, как несложно проверить, $(x^3 + ax + b)^{\frac{q-1}{2}}$ будет равен единице. Значит, нам необходимо осуществить проверку, равен ли НОД($(x^3 + ax + b)^{\frac{q-1}{2}} - 1$, $h(x)$) единице или нет. Если не равен, то найдется искомое $y \in \mathbf{F}_q$, а значит $t_l \equiv q + 1 (\mathrm{mod}\, l)$, иначе $t_l \equiv -q - 1 (\mathrm{mod}\, l)$.

Поскольку в качестве l мы берем маленькие простые числа, то вероятность того, что порядок кривой разделится на одно из них, очень велика, а значит, делать такое улучшение имеет смысл.

2. Применение алгоритма Шенкса

Теперь рассмотрим еще одну возможность ускорить алгоритм. Сложность вычисления t_l – остатка при делении следа Фробениуса t на l – равна O(l^7) битовых опреаций или O(l^5) операций на эллиптической кривой. Нахождение каждого следующего остатка уменьшает число вариантов для порядка кривой приблизительно в l раз. Таким образом, оказывается, что в некоторый момент различных вариантов для порядка кривой оказывается настолько мало, что гораздо эффективнее каким-то образом их всех перебрать, нежели дальше продолжать вычислять остатки методом Шуфа. Наиболее эффективным методом для вычисленя порядка кривой, если имеется небольшое число вариантов, является метод Шенкса. Его сложность – O($n^{1/2}$ log n) операций на кривой, где n – число возможных вариантов. Таким образом, можно существенно ускорить алгоритм, если вместо нескольких последних вычислений t_l вычислить порядок кривой методом Шенкса.

Теперь произведем довольно грубую оценку, до каких пор следует продолжать вычислять порядок кривой по алгоритму Шуфа, а потом оставшуюся часть сделать по алгоритму Шенкса, чтобы суммарное время работы было минимальным. Для начала вычислим время работы алгоритма Шенкса. Предположим, что Шуфом мы не досчитали k простых чисел: l_1, l_2, …, l_k. Тогда у нас будет около $\prod_{i=1}^{k} l_i$ вариантов для порядка

кривой, а значит, что сложность алгоритма Шенкса – $O\left(\sqrt{\prod_{i=1}^{k} l_i}\,\ln\prod_{i=1}^{k} l_i\right)$.
Предполагая, что все эти простые числа асимптотически равны и равны l, получаем сложность $O(kl^{k/2}\ln l)$.

Значение k будет оптимальным, если при увеличении или уменьшении его на единицу общее время работы алгоритма увеличится. Вычислим разность между сложностями для двух соседних k. Она равна

$$(k+1)l^{\frac{k+1}{2}}\ln l - kl^{\frac{k}{2}}\ln l - l^5 = \ln l\cdot l^{\frac{k}{2}}\left((k+1)\sqrt{l} - k\right) - l^5.$$

Минимум достигнется, когда эта разность окажется равной нулю. При всех $k \geq 9$ эта разность будет больше нуля и с уменьшением k эта разность убывает. Так что нам необходимо брать $k \leq 9$. На практике, это k сильно зависит от числа бит в q и деталей реализации. Тут указано только ориентировочное значение. Так, например, в тестовой программе оптимальные значения для k, вычисленные эмпирически, составляют при 100-битном q – семи, а при 200-битном – восьми.

Использование алгоритма Шенкса позволяет существенно ускорить нахождение порядка эллиптической кривой. Так, для эллиптических кривых над полем порядка 250 бит получается ускорение приблизительно в 2 раза, что очень существенно.

Автором статьи была разработана программа на C++ с использованием библиотеки многозначной арифметики NTL. При помощи этой программы порядок эллиптической кривой над полем из 256 бит на компьютере Pentium 4 1600 МГц был посчитан приблизительно за 3 часа.

Литература

1. *Lang S.* Diofantine Analysis / Springer-Verlag, 1978.
2. *Schoof R.* Counting points on elliptic curves over finite fields // J. Theories des Nombres de Bordeaux. №7. 1995 С. 219 – 254.
3. *Cohen H.* A course in computational algebraic number theory / Springer-Verlag, 1993.

МОДЕЛЬ КОРРЕКЦИИ ОШИБОК ДЛЯ ИНДЕКСА ПОТРЕБИТЕЛЬСКИХ ЦЕН

А. А. Босько

ВВЕДЕНИЕ

Модель коррекции ошибок обладает преимуществами перед другими подходами построения моделей по макроэкономическим показателям, которые в большинстве случаев не являются стационарными. В боль-