смежности в самом начале программы. Дальнейшая работа уже не зависит от количества вершин и связей (ребер) между ними.

Из всего следует, что графы являются очень универсальным средством, которое помогает нам как в решении задач при изучении высшей математики, так и в программировании для написания наиболее оптимального кода. И умение сочетать различные дисциплины и изучать практические стороны различных тем — отличный способ совершенствоваться и достигать наилучшего результата.

ЛИТЕРАТУРА

1. Пацей, Н.В. Основы алгоритмизации и программирования: учеб.-метод. пособие для студентов специальности «Информационные системы и технологии (издательско-полиграфический комплекс)» / Н.В. Пацей. — Минск: БГТУ, 2010. — 289 с.

2. Новиков, Ф. А. Дискретная математика: Учебник для вузов. 3-е изд. Стандарт третьего поколения. — СПб.: Питер, 2017. — 334 с.

УДК 519.171

Студ. В. В. Хорхалёв
Науч. рук. И. К. Асмыкович
(кафедра высшей математики, БГТУ)

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ИХ ПРИЛОЖЕНИЯ В КРИПТОГРАФИИ

На протяжении более сотни лет эллиптические кривые исследовались лишь узкими специалистами в области теории чисел. Но в 1985 г. одновременно и независимо Н. Коблиц и В. Миллер предложили использовать эллиптические кривые для построения криптосистем с открытым ключом. После этого интерес к эллиптическим кривым стремительно возрос. Эллиптические кривые применяются в разных областях криптографии таких, как теория кодирования, генерация псевдослучайных последовательностей, алгоритмическая теория чисел для построения тестов на простоту и, для создания метода факторизации целых чисел Ленстры.

Пусть F_q, $q = p^k$, конечное поле характеристики $p \geq 2$. Эллиптической кривой над полем F_q называется множество точек $(x, y) \in F_q \oplus F_q$, удовлетворяющих уравнению Вейерштрассе [1]:

$$y^2 + ay + b = x^3 + cx^2 + dx + e.$$

К множеству точек эллиптической кривой также добавляется точка, называемая точкой в бесконечности и обозначаемая символом ∞. Если характеристика поля $p \geq 3$ (а мы будем рассматривать именно этот случай), уравнение, путем замены переменных, может быть

преобразовано в уравнение, называемое сокращенным уравнением Вейерштрассе:

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

где $a, b \in F_q$.

Для эллиптической кривой могут быть вычислены ее дискриминант Δ и инвариант j:

$\Delta = -16(4a^3 + 27b^2)$;

$$j = \frac{1728(4a)^3}{b},$$

Заметим: $1728 = 2^6 \cdot 3^3$. [2]

Кривая называется неособой, если $\Delta \neq 0$ и, как следствие, многочлен $x^3 + ax + b$, стоящий в правой части уравнения кривой, не имеет кратных корней. Мы будем рассматривать только неособые кривые. Инвариант j определяет изоморфизм кривых: две кривые с одинаковым инвариантом являются изоморфными.

Арифметические операции с точками на эллиптической кривой

На множестве точек E неособой эллиптической кривой может быть определена групповая операция суммирования +, с помощью которой это множество становится аддитивной абелевой группой. Нулем этой группы является бесконечно удаленная точка ∞, а обратным элементом к точке $P = (x,y) \in E$ будет являться точка $-P = (x,-y)$. Опишем геометрическое определение операции суммирования. Пусть $P_1(x_1, y_1)$ и $P_2(x_2, y_2)$ – произвольные точки, и $P_3(x_3, y_3)$ обозначает сумму этих точек $P_3 = P_1 + P_2$. Через точки $P_1(x_1, y_1)$ и $P_2(x_2, y_2)$ проведем прямую L. Третью точку пересечения с эллиптической кривой обозначим через $P'(x'_3, y'_3)$. Такая точка обязательно существует, т.к. пересечение произвольной прямой с эллиптической кривой имеет либо одну, либо 3 точки пересечения. Определим сумму трех точек $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ и $P_3'(x'_3, y'_3)$ равной нулю (бесконечно удаленной точке):

$P_1 + P_2 + P' = \infty$

Тогда $P_3 = P_1 + P_2 = -P'$, откуда $x_3 = x'_3$, $y_3 = -y'_3$. Для вычисления координат точки P_3, найдем параметры прямой $L : y = kx + d$:

$$\kappa = \frac{y_2 - y_1}{x_2 - x_1}, \; d = y_1 - kx_1$$

Подставляя выражение для L в уравнение, получим

$x^3 + cx^2 + ax + b - (kx + d)^2 = 0$

Сумма координат $x_1 + x_2 + x_3$ должна быть равна коэффициенту при x^2, взятому с противоположным знаком:

$$x_1 + x_2 + x_3 = k^2 - c = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - c,$$

откуда получим формулу для координат суммы [1]:

$$\begin{cases} x_3 = k_2 - x_1 - x_2 - c \\ y_3 = k(x_1 - x_3) - y_1 = k(2x_1 + x_2 - k^2 + c) - y_1 \end{cases}$$

где для сокращенного уравнения значение параметра с равно 0. Если точки P1 и P2 совпадают, то прямая L является касательной

в т.P_1 и угловой коэффициент прямой L можно найти, дифференцируя

уравнение по x. Общие формулы для коэффициента k получат вид [1]:

$$k = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, \text{если } P1 \neq P2, \\ \frac{3x_1^2 + a}{2y_1}, \text{если } P1 = P2 \end{cases}$$

Формулы для координат удвоенной точки можно получить, подставляя $x_2 = x_1$, $y_2 = y_1$:

$$\begin{cases} x_3 = k^2 - 2x_1 - c \\ y_3 = k(x_1 - x_3) - y_1 = k(3x_1 - k^2 + c) - y_1 \end{cases}$$

где опять для сокращенного уравнения значение параметра с равно 0. Группа точек эллиптической кривой над полем F_q обозначается символом $EC(F_q)$, а ее мощность (количество элементов) символом $\#EC(F_q)$.

Известно, что группа точек эллиптической кривой либо является циклической (т.е. найдется точка $P \in EC$ такая, что все точки являются кратными этой точки), либо $E(F_q) =\sim Z_{n1} \oplus Z_{n2}$, где $n_1 | n_2$, и $n_1 | q - 1$.

Поскольку, арифметика эллиптических кривых не содержит прямых формул для вычисления кратного kQ для заданной точки Q(x1,y1), то эту операцию выполняют с использованием операций сложения, вычитания и удвоения точки. Для этого надо представить число k в двоичной системе исчисления $k = b_t\, b_{t-1} \ldots b_0$, $b_i \in \{0, 1\}$, потом вычислить все точки 2Q, 4Q, ... , $2^t \cdot Q$ и подсчитать сумму тех точек $2^i \cdot Q$, для которых $b_i = 1$.

Пример

Выберем эллиптическую кривую, задаваемую a = 1, b = 1 над полем F_{23}. Уравнение кривой примет вид:

$$y^2 = x^3 + x + 1.$$

Выберем точки A = (9, -7), B = (6, -4).

Вычислим значение выражения A - 3B:

3B = B + 2B;

2B = (k^2 – 2x, k(3x – k^2) – y = (-10, -7);

3B = (6, -4) + (-10, -7) = (7, 11);

A - 3B = $(9,-7)-(7,11)=(9,-7)+(7,-11)=(11,3)$.

ЛИТЕРАТУРА

1. Ш.Т. Ишмухаметов, Р.Г. Рубцова Математические основы защиты информации: Электронное учебное пособие для студентов института вычислительной математики и информационных технологий. – Казань, 2012 г. – 138 с.

2. Ю. Г. Прохоров Эллиптические кривые и криптография: учеб. для вузов – Москва: Механико-математический факультет МГУ, 2007 г. – 144 с.

УДК 519.171

Студ. В.А. Андреюк, Е.А. Баран
Науч. рук. А. А. Якименко
(кафедра высшей математики, БГТУ)

ИСТОРИЯ МАТЕМАТИЧЕСКИХ ОБОЗНАЧЕНИЙ

Слово математика пришло к нам из древнегреческого, где означало "учиться", "приобретать знания. Математика – это первая наука, которую смог освоить человек. Самой древней деятельностью был счёт. Некоторые первобытные племена подсчитывали количество предметов с помощью пальцев рук и ног, а так же палочек. Можно сказать, что 1 палочка – это первый математический символ.

С древнегреческого «символ» (греч. *symbolon* – признак, примета, пароль, эмблема) – знак, который связан с обозначаемой им предметностью так, что смысл знака и его предмет представлены только самим знаком и раскрываются лишь через его интерпретацию.

С открытием математических правил и теорем ученые придумывали новые математические обозначения, знаки. Математические знаки - это условные обозначения, предназначенные для записи математических понятий, предложений и выкладок.

1. Знаки сложения, вычитания