Доп. дисциплины

Магистры весна 2021

Занятие 5

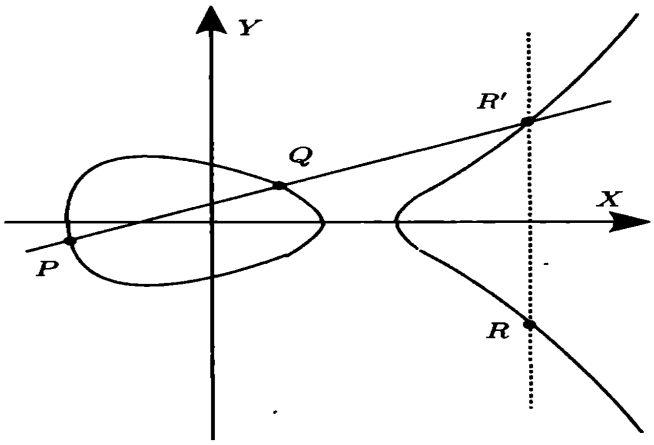
ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ НАД ПОЛЯМИ ГАЛУА

08.04.2021

Эллиптическая кривая над полем действительных чисел

Определение операции на эллиптической кривой. *Пусть P и Q точки на эллиптической кривой. Проведем через них прямую и пусть R' будет третьей точкой пересечения прямой с эллиптической кривой. Тогда точка R, симметричная точке R' относительно оси абсцисс OX, будет искомой суммой P + Q = R. При этом нейтральным элементом является бесконечно удаленная точка E. Обратной к точке P будет точка –P – симметричная точке P относительно оси абсцисс.*

Очевидно, что операция сложения коммутативна P + Q = Q + P, поскольку прямая, проведенная через точки P и Q, и прямая, проведенная через точки Q и P – одна и та же. Все это изображено на рисунке ниже.



Теперь найдем аналитическое выражение для суммы двух точек, через их координаты. Пусть $P = (x_1, y_1), Q = (x_2, y_2), R = (x_3, y_3)$. Рассмотрим два случая.

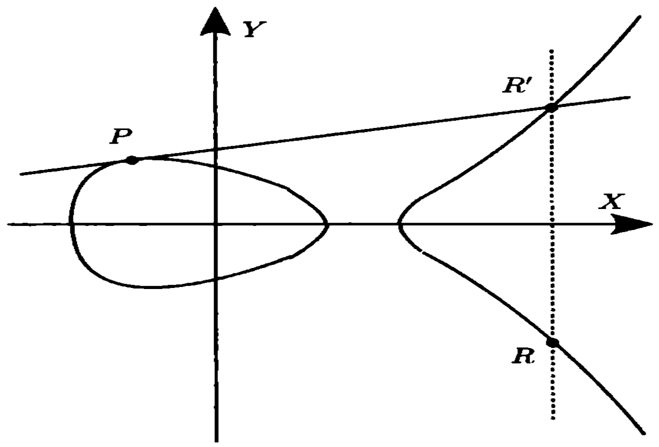
Случай 1. $P \neq Q$.

Итоговый ответ такой

$$\begin{cases} x_3 = k^2 - (x_1 + x_2) \\ y_3 = -k(x_3 - x_1) - y_1 \end{cases}, k = \frac{y_2 - y_1}{x_2 - x_1}.$$

Случай 2. Сумма точки сама с собой P = Q.

Геометрически все изображено ниже



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

Эллиптические кривые над полями Галуа

Теорема. (Хассе) *Если эллиптическая кривая задана над полем, содержащим q элементов, то число точек на ней удовлетворяет неравенству*

$$|q + 1 - \#L| \le 2\sqrt{q}.$$

Мы будем производить вычисления для небольших полей и, по возможности, не вручную, а средствами языка Julia, текущая версия 1.4.1 официальный сайт https://julialang.org/ с подключением пакета Nemo, текущая версия 0.17.5.

Решим типовые задачи.

Задача 1. Эллиптическую кривую f(x,y) над полем GF(13) привести к каноническому виду g(x,y)

$$f(x, y): y^2 + 7xy + 5y = x^3 + 7x^2 + 8x + 9.$$

Решение. а) В левой части выделим полный квадрат

$$y^2 + 2\cdot 10xy + (10x)^2 - (10x)^2 + 5y = x^3 + 7x^2 + 8x + 9 \Rightarrow (y + 10x)^2 + 5y = x^3 + 3x^2 + 8x + 9$$

И осуществим замену y1 = y +10x

$$(y1)^2 + 5y1 = x^3 + 3x^2 + 6x + 9.$$

б) Еще раз выделим слева квадрат и сделаем замену y2 = y1 + 9

$$(y2)^2 = x^3 + 3x^2 + 6x + 12.$$

в) Выделим полный куб в правой части

$$x^3 + 3x^2 + 3x + 1 + 3x + 11 = (x+1)^3 + 3(x+1) + 8$$

и осуществим замены x1 = x + 1 и получим канонический вид кривой

$$g(x1, y2): (y2)^2 = (x1)^3 + 3x1 + 8.$$

Задача 2. Вычислить количество точек на кривой $y^2 = x^3 + 3x + 8$ над полем GF(13).

Решение. Теорема Хассе говорит о том, что на кривой должно быть 14 точек плюс-минус 7, т.е. от 7 до 21 точек.

Вначале найдем дискриминант. Вычисления будем производить средствами языка Julia 1.4.1 и ее пакета Nemo 0.17.5

```
julia> using Nemo

Welcome to Nemo version 0.17.5

Nemo comes with absolutely no warranty whatsoev

julia> F=GF(13)

Galois field with characteristic 13

julia> 4*(F(3))^3 + 27*(F(8))^2

3
```

Дискриминант не нулевой, кривая не сингулярная.

```
julia> using Nemo
Welcome to Nemo version 0.17.5
Nemo comes with absolutely no warranty whatsoever
julia> F=GF(13)
Galois field with characteristic 13
julia> for i in 0:12
              for j in 0:12
                     s= (F(i))^2
                     s1= (F(j))^3+3*F(j)+8
                     if s == s1
                       print("(",j, ",",i, "),")
              end
              end
              end
(12,2),(2,3),(1,5),(9,6),(9,7),(1,8),(2,10),(12,11)
```

Ответ. Кривая $y^2 = x^3 + 3x + 8$ над полем GF(13) содержит 9 точек:

$$(x, y) \in \{E, (12, \pm 2), (2, \pm 3), (1, \pm 5), (9, \pm 6)\} = \{E, (1, \pm 5), (2, \pm 3), (9, \pm 6), (12, \pm 2)\}.$$

Задача 3. Найти элемент наибольшего порядка кривой $y^2 = x^3 + 3x + 8$ над полем GF(13).

Решение. Так как точек всего 9, то максимальный порядок равен 3 или 9. Имеем список точек $L = \{E, (1, \pm 5), (2, \pm 3), (9, \pm 6), (12, \pm 2)\}$.

В качестве точки P выберем, для начала, $P = (x_1, y_1) = (1, 5)$. Тогда

$$\begin{cases} x_3 = k^2 - 2x_1 \\ y_3 = k(x_1 - x_3) - y_1 \end{cases}, k = \frac{3x_1^2 + a}{2y_1} \Rightarrow \begin{cases} x_3 = (-2)^2 - 2 \cdot 1 \\ y_3 = -2(1-2) - 5 \end{cases}, k = \frac{3 \cdot 1^2 + 3}{2 \cdot 5} = 6 \cdot 4 = 11 = -2 \Rightarrow \begin{cases} x_3 = 2 \\ y_3 = 10 \end{cases}.$$

Таким образом, $P=(x_1,y_1)=(1,5);Q=(x_2,y_2)=(2,10)$. Ищем сумму 3P = P + Q, применяем формулу

$$\begin{cases} x_3=k^2-(x_1+x_2) \\ y_3=-k(x_3-x_1)-y_1 \end{cases}, k=\frac{y_2-y_1}{x_2-x_1} \Rightarrow k=\frac{10-5}{2-1}=5 \Rightarrow \begin{cases} x_3=5^2-(1+2) \\ y_3=-5(9-1)-5 \end{cases} \Rightarrow \begin{cases} x_3=9 \\ y_3=7 \end{cases}.$$

Следовательно, $3P=(9,7)\neq E$, значит порядок элемента P равен 9.

Ответ. Элемент P = (1,5) эллиптической кривой $y^2=x^3+3x+8$ над полем GF(13) имеет порядок 9.

Задача 4. Возьмем кривую $y^2+y=x^3+ax+b, a=t^2+1, b=t^4+t+1$ над полем $GF(2^8)$

```
julia> using Nemo
[ Info: Precompiling Nemo [2edaba10-b0f1-5616-af89-8c11ac63239a]
Welcome to Nemo version 0.17.5
Nemo comes with absolutely no warranty whatsoever
julia> T, t = FiniteField(2, 8, "t")
(Finite field of degree 8 over F_2, t)
```

Мы создали поле $GF(2^8)$ над которым задан знаменитый шифр AES.

1 шаг. Вычислим дискриминант $D=4a^3+27b^2, a=t^2+1, b=t^4+t+1$.

```
julia> a=t^2+1; b=t^4+t+1; D=4*a^3+27*b^2
t^4+t^3
```

Теперь проверим вручную.

Так как характеристика равна 2, то 4 = 0, 27 = 1, и, значит,

$$D=b^2=(t^4+t+1)^2=t^8+t^2+1.$$

Так как

```
julia> t^8
t^4+t^3+t^2+1
```

то $D=t^8+t^2+1=t^4+t^3+t^2+1+t^2+1=t^4+t^3\neq 0$.

2 шаг. Вычислим количество точек на нашей кривой. Теорема Хассе говорит о том, что на кривой должно быть 257 точек плюс-минус 32, т.е. от 225 до 289. Реально окажется 257. Очень редкий вид кривой.

Будем использовать t - примитивный элемент поля $GF(2^8)$. Он имеет порядок 255. Мы не можем представить 0 в виде степени примитивного элемента. Поэтому рассмотрим две отдельные программки для нуля.

Первая программа для y = 0.

```
julia> using Nemo
```

```
Welcome to Nemo version 0.17.5
Nemo comes with absolutely no warranty whatsoever
julia> T, t = FiniteField(2, 8, "t")
(Finite field of degree 8 over F_2, t)

julia> for i in 1:255
       s= (t^i)^3+(t^2+1)*(t^i) + t^4 +t+1
       if s == 0
       println(t^i)
       end
       end
t^4+t^3
```

Получаем одно решение.

Вторая программа для x = 0.

```
julia> for i in 1:255
       s= (t^i)^2+t^i
       if s == t^4+t+1
       println(t^i)
       end
       end
t^7+t^6+t^4
t^7+t^6+t^4+1
```

Получилось еще 2 решения, т.е. уже 3. А если добавить бесконечно удаленную точку, то получим 4 точки.

Теперь основная программа для $255 \cdot 255 = 65025$ случаев. Здесь s1 – это значения, которые принимает левая часть уравнения кривой, а s – какие значения пробегает правая часть.

```
julia> for l in 1:1
       l=l-1
       for i in 1:255
       for j in 1:255
              s= (t^j)^3+(t^2+1)*(t^j) + t^4 +t+1
              s1= (t^i)^2+t^i
              if s == s1
                l=l+1
       end
       end
       end
       println(l)
       end
253
```

Ответ. Кривая $y^2 + y = x^3 + (t^2 + 1)x + t^4 + t + 1$ над полем $GF(2^8)$ содержит 253+4 = 257 точек.

ЛИТЕРАТУРА

1. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2017. - URL: https://e.lanbook.com/reader/book/111097/
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. - СПб.: Лань, 2011. - URL: https://e.lanbook.com/reader/book/68466