Доп. дисциплины

Магистры весна 2021

Занятие 4

ВЫЧИСЛЕНИЯ В ПОЛЯХ ГАЛУА

01.04.2021

Пусть неприводимый многочлен f(x) над полем GF(p) имеет степень n. Рассмотрим множество P остатков от деления на многочлен f(x). Т.к. многочлен f(x) имеет степень n, то его остатки имеют степень не выше n – 1, и, значит, имеют вид

$$a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\ldots+a_1x+a_0, a_i\in GF(p), i=0,1,\ldots,n-1.$$

Т.к. в поле GF(p) ровно p элементов, а коэффициентов у любого остатка n штук, то различных остатков ровно p^n.

На множестве остатков P введем операции сложение и умножения.

Суммой двух остатков a + b является остаток от деления на многочлен f(x) обычной суммы многочленов a + b. Аналогично произведением двух остатков ab является остаток от деления на f(x) обычного произведения многочленов ab.

Эта конструкция полностью аналогична построению поля остатков Z_p. Только вместо простого числа p используется неприводимый многочлен f(x).

Например, над полем GF(5) рассмотрим неприводимый многочлен f(x) = x^3 + x + 1. Остатки от деления на многочлен x^3 + x + 1 имеют степень не выше двух, поэтому различных остатков будет 5^3 = 125.

При вычислениях поле остатков от деления на неприводимый многочлен f(x) можно интерпретировать как присоединение к полю GF(5) корня α многочлена f(x). Тогда новый элемент α будет удовлетворять соотношению $\alpha^3+\alpha+1=0\Rightarrow\alpha^3=-\alpha-1$. Тогда каждый остаток от деления на многочлен f(x) можно записать в виде

$$a_2\alpha^2+a_1\alpha+a_0, a_2, a_1, a_0\in GF(5).$$

Пример 1. *Вычислим произведение двух элементов в поле P = GF(5³):*

$$(\alpha^2+2)\cdot(2\alpha^2-3\alpha+4)=2\alpha^4-3\alpha^3+8\alpha^2-6\alpha+8.$$

Т.к. $\alpha^3=-\alpha-1\Rightarrow\alpha^4=-\alpha^2-\alpha$, то получаем

$$2\alpha^4-3\alpha^3+8\alpha^2-6\alpha+8=2(-\alpha^2-\alpha)-3(-\alpha-1)+8\alpha^2-6\alpha+8=6\alpha^2-5\alpha+11=\alpha^2+1$$

Пример 2. *Сколько примитивных элементов в поле GF(127)*

Примитивным элементом поля называется элемент, чьи мультипликативные степени исчерпывают все ненулевые элементы поля.

Другими словами – это порождающий элемент мультипликативной подгруппы поля. В любом поле Галуа примитивный элемент существует.

Т.к. в поле GF(127) имеет всего 127 элементов, то ненулевых из них ровно 126. Поэтому число примитивных элементов будет равно количеству чисел, взаимно простых с числом 126. Что бы его найти вычисляем функцию Эйлера от числа 126:

$$\varphi(126) = \varphi(2*3^2*7) = \varphi(2)*\varphi(3^2)*\varphi(7) = (2-1)*(3^2-3)*(7-1) = 36\,.$$

Таким образом, примитивных элементов ровно 36. Если мы будем искать примитивный элемент наугад, то вероятность найти его с первой попытки равна 36/126 = 2/7. Это примерно 30%.

К счастью, для малых простых чисел, а 127 – малое простое число, обычно подходят уже элементы 2 или 3. Так как 126= 2*9*7, то чтобы выяснить является ли 2 примитивным элементом по модулю 127 достаточно проверить, что $2^{18} \neq 1, 2^{42} \neq 1, 2^{63} \neq 1(\bmod 127)$. Однако, уже 2^7 = 128=1(mod127). Следовательно, элемент 2 – не примитивный элемент по модулю 127.

Проверим, что элемент 3 – примитивный элемент по модулю 127, т.е., что $3^{18} \neq 1, 3^{42} \neq 1, 3^{63} \neq 1(\bmod 127)$.

Проведем для этого вычисления в среде Julia, текущая версия 1.4.1 официальный сайт https://julialang.org/:

```
julia> [3^18 3^42 3^63] .% 127
1?3 Array{Int64,2}:
 4  -32  -35
```

Видно, что все значения не 1 и, значит, 3 – примитивный элемент по модулю 127.

Теперь поясним код нашей микроскопической программы:

`[3^18 3^42 3^63]` – мы задали вектор строку из 3-элементов;

Знак `.% 127` - означает взятие по модулю 127, точка перед ним, что операция производится покоординатно.

`4  -32  -35` - результат, который тоже выводится как вектор строка.

Логарифм Якоби и его применение

Если g – примитивный элемент поля Галуа $GF(\mathrm{p}^n)$ и $a = g^i, b = g^j$, то $ab = g^i g^j = g^{i+j}$, где $(i+j)\bmod(\mathrm{p}^n - 1)$.

Возникает проблема со сложением элементов поля Галуа.

$$a + b = g^i + g^j = g^i(1 + g^{j-i})\,.$$

Нам нужно знать чему равна сумма $1 + g^{j-i}$.

Определение. *Логарифмом Якоби называется соотношение*

$$1+g^n = g^{L(n)},$$

где L(n) и есть логарифм Якоби. В случае, если $1+g^n = 0$, *то L(n)=#, т.е. логарифм не определен.*

Логарифм Якоби очень полезен при вычислениях в Полях Галуа.

МОДЕЛЬНЫЕ ЗАДАЧИ

Для многочлена $f(x) = x^2 + x + 1, GF(5)$ решить несколько типичных задач.

1 задача. *Проверить неприводимость многочлена f(x) над полем GF(5).*

Решение. Так как многочлен имеет 2-ю степень, то неприводимость означает отсутствие корней. Проверим это прямым вычислением с использованием Julia

```
julia> function f(p)
       for i in 1:p
       print((i^2+i+1)%p, ",")
       end
       end
f (generic function with 1 method)

julia> f(5)
3,2,3,1,1,
```

Видим, что среди значений нуля нет, значит многочлен неприводим.

2 задача. *Построить поле разложения многочлена f(x).*

Решение. Так как многочлен имеет 2-ю степень, то его поле разложения – это поле Галуа $GF(5^2)$. Для работы с полями Галуа проект Julia имеет вспомогательный пакет Nemo – подключаем его:

```
julia> using Nemo
Welcome to Nemo version 0.17.4
Nemo comes with absolutely no warranty whatsoever
```

Есть также специализированный пакет GaloisFields v1.0.1.

Но мы будем использовать Nemo, поскольку в нем много функций абстрактной алгебры и теории чисел.

У пакета Nemo есть одна методическая особенность. Полями Галуа в нем называются простые поля Галуа GF(p), которые реализуются как кольца вычетов по простому модулю. Произвольные поля Галуа называются конечными полями.

Поле можно задать двумя способами. Первый способ как абстрактное поле, с неизвестным нам порождающим многочленом:

```
julia> R, x = FiniteField(5, 2, "x")
(Finite field of degree 2 over F_5, x)
```

Но мы можем легко выяснить какой это многочлен

```
julia> x^2
x+3
```

Значит $x^2 = x + 3 \Rightarrow x^2 - x - 3 = x^2 + 4x + 2$, т.е. многочлен “не наш”, а $g(x) = x^2 + 4x + 2$. С чем связан выбор многочлена?

По-видимому, с тем, что его корень x – примитивный элемент поля. Проверим это. В поле $GF(5^2)$ 24 ненулевых элемента, 24 = 8*3. Чтобы x был примитивным элементом нужно проверить два неравенства $x^{12} \neq 1, x^8 \neq 1$:

```
julia> x^12
4
julia> x^8
2*x+1
```

Действительно, x – примитивный элемент.

Задача 3. *Найти примитивный элемент поля* $GF(5^2)$*, заданного как поле разложения многочлена* $f(x) = x^2 + x + 1, GF(5)$.

Решение. Используем второй способ задания поля Галуа. Вначале создадим кольцо T многочленов над поле вычетов, а потом зададим расширение простого поля Галуа, как поля разложения U нашего многочлена

```
julia> T, t = PolynomialRing(ResidueRing(ZZ, 5), "t")
(Univariate Polynomial Ring in t over Integers modulo 5, t)
julia> U, z = FiniteField(t^2+t + 1, "z")
(Finite field of degree 2 over F_5, z)
```

Проверим является ли элемент z примитивным. К сожалению, нет:

```
julia> z^8
4*z+4
julia> z^12
1
```

Проверим элемент y = z+1. Тоже не подходит:

```
julia> y=z+1
z+1
julia> y^8
z
julia> y^12
1
```

Проверим y = z+2. “Упорство и труд – все перетрут!” - подходит

```
julia> y=z+2
z+2
julia> y^8
4*z+4
```

```
julia> y^12
4
```

Итак, y = z+2 – примитивный элемент нашего поля.

Задачи 4 - 5. *Составить таблицу степеней примитивного элемента и таблицу логарифма Якоби.*

Решение. Вычислим все 24 степени элемента y:

```
julia> y=z+2
z+2
julia> for i in 1:24
       print(y^i, ",")
       end
z+2,3*z+3,z+3,4*z,4*z+1,3,3*z+1,4*z+4,3*z+4,2*z,2*z+3,4,4*z+3,2*z+2,4*z+2,z,
z+4,2,2*z+4,z+1,2*z+1,3*z,3*z+2,1
```

Составим объединенную таблицу – первая строка – показатели степеней примитивного элемента y, вторая строка – значение его степеней, третья - логарифм Якоби, который строится просто просмотром первых двух строк. Например, как найти L(10), по определению логарифма $1+y^{10}=y^{L(10)}$. Находим $y^{10}=2z \Rightarrow y^{10}+1=2z+1=y^{21}$, таким образом L(10)=21. Отметим, т.к. 0 не является степенью примитивного элемента, то в 12-столбце вместо значения логарифма стоит символ запрета или останова в машинах Тьюринга – знак #.

В итоге получаем:

i	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
y^i	z+2	3z+3	Z+3	4z	4z+1	3	3z+1	4z+4	3z+4	2z	2z+3	4
L(i)	3	9	17	5	15	12	23	4	22	21	19	#

13	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**
4z+3	2z+2	4z+2	z	Z+4	2	2z+4	Z+1	2z+1	3z	3z+2	1
8	11	13	20	16	6	10	1	14	7	2	18

Задача 6. *Используя таблицы степеней и логарифмов Якоби решить над полем* $GF(5^2)$ *:*

а) систему линейных уравнений

$$\begin{cases} x+(\alpha+1)\,y-z=2 \\ (-\alpha+1)\,x+2\,y+z=3 \\ x+2y+3z=\alpha^2+5 \end{cases},$$

б) квадратное уравнение $(\alpha+1)\,x^2+(\alpha^2+2\alpha+1)\,x+\alpha^2+1.$

Решение. В наших обозначениях $\alpha = z, \alpha^2 = 4z + 4$. Придется также поменять и обозначения неизвестных, иначе и неизвестное и коэффициент будут обозначены одинаково. Неизвестные назовем a,b,c.

а) Решить систему линейных уравнений

$$\begin{cases} a + (\mathrm{z}+1)\,\mathrm{b} + 4c = 2 \\ (4z+1)\,\mathrm{a} + 2b + c = 3 \\ a + 2b + 3c = 4z + 4 \end{cases}.$$

Составим расширенную матрицу нашей системы, коэффициенты зададим как степени примитивного элемента y, используя таблицу из задач 4-5 и решим ее методом Гаусса, т.е. исключением неизвестных:

$$\begin{pmatrix} 1 & y^{20} & y^{12} & y^{18} \\ y^5 & y^{18} & 1 & y^6 \\ 1 & y^{18} & y^6 & y^8 \end{pmatrix}.$$

Поскольку $y^{24} = 1$, то умножим вторую строку на y^{19} и строка приобретет вид $(1, y^{13}, y^{19}, y)$, сама матрица

$$\begin{pmatrix} 1 & y^{20} & y^{12} & y^{18} \\ 1 & y^{13} & y^{19} & y \\ 1 & y^{18} & y^6 & y^8 \end{pmatrix}.$$

Умножим 1-ю строку 4 и прибавим ко 2-й и 3-й

$$\begin{pmatrix} 1 & y^{20} & y^{12} & y^{18} \\ 0 & y^{13} + 4y^{20} & y^{19} + 4y^{12} & y + 4y^{18} \\ 0 & y^{18} + 4y^{20} & y^6 + 4y^{12} & y^8 + 4y^{18} \end{pmatrix}$$

Теперь нам нужно представить 6 сумм в виде степеней примитивного элемента y. Не забудем, что $y^{24} = 1, 4 = y^{12}$:

$$y^{13} + 4y^{20} = y^{13} + y^{12}y^{20} = y^{13} + y^8 = y^8(1 + \mathrm{y}^5) = \mathrm{y}^{8+L(5)} = y^{8+15} = y^{23}$$

$$y^{19} + 4y^{12} = y^{19} + y^{24} = 1 + y^{19} = y^{L(19)} = y^{10}$$

$$y + 4y^{18} = y + y^{30} = y + y^6 = y(1 + \mathrm{y}^5) = \mathrm{y}^{1+L(5)} = y^{16}$$

$$y^{18} + 4y^{20} = y^{18} + y^{12}y^{20} = y^{18} + y^8 = y^8(1 + \mathrm{y}^{10}) = \mathrm{y}^{8+L(10)} = y^{8+21} = y^5$$

$$y^6 + 4y^{12} = y^6 + y^{24} = 1 + y^6 = y^{L(6)} = y^{12}$$

$$y^8 + 4y^{18} = y^8 + y^{30} = y^8 + y^6 = y^6(1 + \mathrm{y}^2) = \mathrm{y}^{6+L(2)} = y^{15}$$

Матрица приобретает вид

$$\begin{pmatrix} 1 & y^{20} & y^{12} & y^{18} \\ 0 & y^{23} & y^{10} & y^{16} \\ 0 & y^5 & y^{12} & y^{15} \end{pmatrix}.$$

Умножим 2-ю строку на y, а 3-ю на y^{19} и получим

$$\begin{pmatrix} 1 & y^{20} & y^{12} & y^{18} \\ 0 & 1 & y^{11} & y^{17} \\ 0 & 1 & y^{7} & y^{10} \end{pmatrix}$$

Умножим 2-ю строку на $4y^{20} = y^{12}y^{20} = y^{8}$ и прибавим к 1-й и на $4 = y^{12}$ и прибавим к 3-й в итоге получим

$$\begin{pmatrix} 1 & 0 & y^{12}+y^{19} & y^{18}+y \\ 0 & 1 & y^{11} & y^{17} \\ 0 & 0 & y^{7}+y^{23} & y^{10}+y^{5} \end{pmatrix}.$$

Теперь нужно 4 суммы представить в виде степеней примитивного элемента y:

$$y^{12}+y^{19} = y^{12}(1+\mathrm{y}^{7}) = \mathrm{y}^{12+L(7)} = y^{12+23} = y^{11},$$
$$y^{18}+y = y(1+\mathrm{y}^{17}) = \mathrm{y}^{1+L(17)} = y^{1+16} = y^{17},$$
$$y^{7}+y^{23} = y^{7}(1+\mathrm{y}^{16}) = \mathrm{y}^{7+L(16)} = y^{7+20} = y^{3},$$
$$y^{10}+y^{5} = y^{5}(1+\mathrm{y}^{5}) = \mathrm{y}^{5+L(5)} = y^{5+15} = y^{20}.$$

Почти итоговая матрица

$$\begin{pmatrix} 1 & 0 & y^{11} & y^{17} \\ 0 & 1 & y^{11} & y^{17} \\ 0 & 0 & y^{3} & y^{20} \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & y^{11} & y^{17} \\ 0 & 1 & y^{11} & y^{17} \\ 0 & 0 & 1 & y^{17} \end{pmatrix}.$$

Осталось последнее преобразование. 3-ю строку умножаем на $4y^{11} = y^{12+11} = y^{23} = y^{-1}$ и прибавляем к 1-й и 2-й строкам и получаем

$$\begin{pmatrix} 1 & 0 & 0 & y^{17}+y^{16} \\ 0 & 1 & 0 & y^{17}+y^{16} \\ 0 & 0 & 1 & y^{17} \end{pmatrix} \Rightarrow \begin{cases} a = y^{17}+y^{16} = z+4+z = 2z+4 \\ b = 2z+4 \\ c = z+4 \end{cases}.$$

Ответ. *Система имеет единственное решение (2z+4, 2z+4, z+4).*

б) *Решить квадратное уравнение* $(\alpha+1)\mathrm{x}^2 + (\alpha^2+2\alpha+1)\mathrm{x} + \alpha^2+1$.

Решение. В наших обозначениях уравнение изменит вид, неизвестную опять назовем символом ‘a’ и перейдем к степеням примитивного элемента y, и, попутно, избавимся от коэффициента при старшем члене:

$$(\mathrm{z}+1)\mathrm{a}^2 + za + 4z = y^{20}a^2 + y^{16}a + y^{4} \Rightarrow a^2 + y^{20}a + y^{8}.$$

Так как у поля GF(25) характеристика не равна 2, то можно воспользоваться формулой решения квадратного уравнения.

В поле характеристики 2 нужно просто перебирать все элементы поля и проверять являются они корнями или нет!

Напишем формулу решения квадратного уравнения

$$a = \frac{-y^{20} + \sqrt{(y^{20})^2 - 4y^8}}{2} = \frac{4y^{20} + \sqrt{y^{40} + y^8}}{y^{18}} = y^6[y^{12+20} + \sqrt{y^8(1+y^8)}] = .$$

$$= y^{14} + y^6\sqrt{y^{8+L(8)}} = y^{14} + y^6\sqrt{y^{12}}$$

Очевидно $\sqrt{y^{12}} = \pm y^6$, т.е. y^6 и $-y^6 = 4y^6 = y^{12}y^6 = y^{18}$.

Получаем два решения

$y^{14} + y^6y^6 = y^{12}(1+y^2) = y^{12+L(2)} = y^{12+9} = y^{21} = 2z+1,$

$y^{14} + y^6y^{18} = 1 + y^{14} = y^{L(14)} = y^{11} = 2z+3.$

Ответ. Два решения {2z+1, 2z+3}.

Второе решение. Подходящее для полей характеристика 2 – полный перебор всех ненулевых элементов поля. Проверка того есть ли среди них корни нашего многочлена $(z+1)a^2 + za + 4z$

. Выполним его в пакете Nemo языка Julia.

```
julia> using Nemo
Welcome to Nemo version 0.17.4
Nemo comes with absolutely no warranty whatsoever

julia> T, t = PolynomialRing(ResidueRing(ZZ, 5), "t")
(Univariate Polynomial Ring in t over Integers modulo 5, t)

julia> U, z = FiniteField(t^2+t + 1, "z")
(Finite field of degree 2 over F_5, z)

  julia> for a in
[z+2,3*z+3,z+3,4*z,4*z+1,3,3*z+1,4*z+4,3*z+4,2*z,2*z+3,4,4*z+3,2*z+2,4*z
+2,z,z+4,2,2*z+4,z+1,2*z+1,3*z,3*z+2,1]
             print((z+1)*a^2+z*a+4*z, ",")
             end

       ОТВЕТ есть два нуля
3*z+4,4*z+3,4*z+2,4*z+1,z+4,z+4,4*z+2,4*z,2*z+4,3*z+3,
0,4*z+1,z+1,4*z+4,4,2*z+4,2*z+2,4,3*z+3,4*z+3,
0,2*z+2,3*z+4,z+1,
```

Есть два нуля, в точности те, что мы нашли выше. Они отмечены красным цветом.