Часть I

Конечные поля или поля Галуа. I

Разделы

Поле $GF(p)$

- $\mathbb{Z}$ — кольцо целых чисел евклидово (целостное унитальное + возможно деление с остатком $\Rightarrow$ существование НОД!),
- p — простое число.
- $(p) = \{\, np \mid n \in \mathbb{Z} \,\} = p\mathbb{Z} = \{0, \pm p, \pm 2p, \ldots\}$ — *идеал*
- $\mathbb{Z}/(p) = \{\, \overline{0}, \overline{1}, \ldots, \overline{p-1} \,\}$ — кольцо вычетов по модулю этого идеала = классы остатков от деления на p:

$$\left.\begin{array}{ll} \overline{0} & = 0 + p\mathbb{Z}\,, \\ \overline{1} & = 1 + p\mathbb{Z}\,, \\ \ldots & \ldots\ldots \\ \overline{p-1} & = (p-1) + p\mathbb{Z}\,. \end{array}\right\} \Rightarrow \mathbb{Z} = \overline{0} \cup \overline{1} \cup \ldots \cup \overline{p-1}.$$

Черту над символами классов вычетов часто не ставят.

Поле $GF(p)$

- $\mathbb{Z}$ — кольцо целых чисел евклидово (целостное унитальное + возможно деление с остатком $\Rightarrow$ существование НОД!),
- p — простое число.
- $(p) = \{\, np \mid n \in \mathbb{Z} \,\} = p\mathbb{Z} = \{\, 0, \pm p, \pm 2p, \dots \}$ — *идеал*
- $\mathbb{Z}/(p) = \{\, \overline{0}, \overline{1}, \dots, \overline{p-1} \,\}$ — кольцо вычетов по модулю этого идеала = классы остатков от деления на p:

$$\left.\begin{array}{ll} \overline{0} & = 0 + p\mathbb{Z}\,, \\ \overline{1} & = 1 + p\mathbb{Z}\,, \\ \dots & \dots\dots \\ \overline{p-1} & = (p-1) + p\mathbb{Z}\,. \end{array}\right\} \Rightarrow \mathbb{Z} = \overline{0} \cup \overline{1} \cup \dots \cup \overline{p-1}.$$

Черту над символами классов вычетов часто не ставят.

Поскольку p — простое, то $\mathbb{Z}/(p)$ — не просто кольцо, а поле (возможно деление без остатка на любой ненулевой элемент). Это простейшее *поле Галуа*, обозначение — $\mathbb{F}_p$ или $GF(p)$; все операции в нём — по $\mod p$.

Поле $\mathbb{F}_3 = \mathbb{Z}/(3)$ и факторкольцо $\mathbb{Z}/(4)$

$\mathbb{F}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}/(4)$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	**0**	2
3	0	3	2	1

Дважды два равно нулю!
Однако, поле из 4-х элементов существует...

Характеристика поля

Пусть $\Bbbk$ — произвольное поле, 1 — единица $\Bbbk$. Складываем их:
$1 = 1\,, \quad 2 = 1 + 1\,, \quad \ldots.$

В конечном поле всегда найдётся первое k такое, что
$\underbrace{1 + \ldots + 1}_{k \text{ раз}} = \mathbf{0}$. Тогда

$$k = \text{порядок аддитивной группы поля } \Bbbk =$$

$$= \textit{характеристика поля } \Bbbk \stackrel{\text{def}}{=} \operatorname{char} \Bbbk$$

$\{\,0,\ 1,\ 2,\ \ldots,\ \operatorname{char}\Bbbk - 1\,\}$ — минимальное подполе в поле $\Bbbk$.

Если все суммы вида $1 + \ldots + 1$ различны, то $\operatorname{char}\Bbbk = 0$.

Примеры: $\mathbb{Q}$, $\mathbb{R}$ — поля нулевой (или бесконечной :)) характеристики.

Бесконечное поле с положительной характеристикой

$\Bbbk$ — произвольное (конечное или бесконечное) поле. Построим:

1. $\Bbbk[x]$ — кольцо многочленов от формальной переменной x: $\{\, P(x) = a_0 + a_1 x + \ldots + a_n x^n \,\}$, $a_0, \ldots, a_n \in \Bbbk$, $n \in \mathbb{N}$, $a_n \neq 0$; $\Bbbk[x] \leftrightarrow \{(a_0, \ldots, a_n) \in \Bbbk^n \mid n \in \mathbb{N}\}$.

2. $\Bbbk(x)$ — поле рациональных функций над $\Bbbk$; в нём:
   элементы — "дроби" P/Q (если $Q \neq 0$), где $P, Q \in \Bbbk[x]$;
   умножение — $(P/Q) \cdot (U/V) = (PU)/(QV)$;
   эквивалентность — $P_1/Q_1 = P_2/Q_2$, если $P_1 Q_2 = P_2 Q_1$;
   сложение — дроби можно приводить к общему знаменателю и складывать:
   $$P/Q + U/V = (PV)/(QV) + (QU)/(QV) = (PV + QU)/(QV);$$
   включение — Поскольку $\Bbbk[x] \subset \Bbbk(x)$, то каждый многочлен P отождествляется с $P/1$.

Если в качестве $\Bbbk$ взять конечное поле $\mathbb{F}_p$, то $\mathbb{F}_p(x)$ — бесконечное поле положительной характеристики p.

Сильное упрощение вычислений в поле положительной характеристики

Лемма

В поле характеристики $p > 0$ выполнено тождество

$$(a+b)^p \; = \; a^p + b^p.$$

Доказательство

В любом коммутативном кольце верна формула для бинома

$$(a+b)^p \; = \; a^p + C_p^1 a^{p-1} b + \ldots + C_p^{p-1} a b^{p-1} + b^p.$$

Но при $i = 1, \ldots, p-1$ числитель коэффициента $C_p^i = \frac{p!}{i!(p-i)!}$ делится на p, а знаменатель — нет, $\therefore$ $C_p^i \equiv_p 0$.

Следствие

В поле характеристики $p > 0$ справедливо $(a+b)^{p^n} \; = \; a^{p^n} + b^{p^n}$.

Мультипликативная группа и примитивный элемент поля $\mathbb{F}_p$

$\mathbb{F}_p^* \stackrel{\text{def}}{=} \mathbb{F}_p \setminus \{0\}$ — *мультипликативная группа поля* $\mathbb{F}_p$.

Утверждение

$\mathbb{F}_p^*$ — циклическая группа порядка $p-1$ по умножению.

Как любая конечная циклическая группа, $\mathbb{F}_p^*$ содержит *генератор* = *примитивный элемент* α:

- любой элемент $\beta \in \mathbb{F}_p^*$ является некоторой его натуральной степенью: $\beta = \alpha^i$, $i \in \{1, \ldots, p-1\}$;
- причём $1 = \alpha^{p-1}$ — т.е. $\alpha^i \neq 1$ для $1 \leqslant i \leqslant p-2$.

Утверждение

Группа $\mathbb{F}_p^*$ имеет $\varphi(p-1)$ примитивных элементов.

Функция Эйлера

$\varphi(n)$ — *функция Эйлера* — количество чисел из интервала $[1, \ldots, n-1]$, взаимно простых с n:

$$\varphi(1) = 1 \text{ (по определению)}, \ \varphi(2) = 1, \ \varphi(3) = \varphi(4) = 2,$$
$$\varphi(5) = 4, \ \varphi(6) = \big|\{1, 5\}\big| = 2, \ \ldots$$

Свойства (p — простое число):

- $\varphi(n) \leqslant n - 1$ и $\varphi(p) = p - 1$;
- $\varphi(n^m) = n^{m-1}\varphi(n)$, т.е. $\varphi(p^m) = p^{m-1}(p-1)$;
- $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$, где $d = \text{НОД}(m, n)$, откуда: если m и n взаимно просты, то $\varphi(mn) = \varphi(m)\varphi(n)$ ($\varphi(\cdot)$ — *мультпликативная функция*).

Пример: $\varphi(15) = \varphi(3 \cdot 5) = \varphi(3)\varphi(5) = (3-1)(5-1) = 8$, $\varphi(16) = \varphi(2^4) = 2^3 \cdot \varphi(2) = 8$.

Первые 99 значений $\varphi(\cdot)$ и степени генератора

$\varphi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Пусть в $\mathbb{F}_p^*$ α — генератор; $\alpha^{-1} = ?$

$$\alpha^{p-1} = 1 \;\Rightarrow\; \alpha^p = \alpha^1 = \alpha \;\text{ и }\; \alpha^{-1} = \alpha^{-1} \cdot \alpha^{p-1} = \alpha^{p-2}.$$

Например, в $\mathbb{F}_5$: $\alpha^{-1} = \alpha^3$.

Как найти примитивные элементы поля $\mathbb{F}_p$?

Если примарное разложение $(p-1)$ —

известно — элемент $\alpha \in \mathbb{F}_p$ будет примитивным iff $\alpha^k \not\equiv_p 1$ для каждого делителя k числа $p-1$.

неизвестно — эффективного алгоритма не найдено (используют таблицы, вероятностные алгоритмы...).

Если α — примитивный элемент поля $\mathbb{F}_p$, то любой другой его примитивный элемент может быть получен как степень α^k, где k — целое число, взаимно простое с $p-1$.

Неприводимые многочлены

Утверждение

Кольцо многочленов $\Bbbk[x]$ *над полем* $\Bbbk$ *— евклидово.*

Теорема

Каждый элемент евклидова кольца однозначно с точностью до перестановок разлагается в произведение простых (неразложимых) элементов.

Простые (неразложимые) элементы $\Bbbk[x]$ — *неприводимые многочлены*.

Вопросы для полей:

1. какие многочлены над ними неприводимы?
2. как находить неприводимые многочлены?

Неприводимые многочлены над $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$:

в поле $\mathbb{C}$ — только многочлены 1-й степени;

в поле $\mathbb{R}$ —

1. многочлены 1-й степени,
2. многочлены 2-й степени с отрицательным дискриминантом;

в поле $\mathbb{Q}$ — существуют неприводимые многочлены произвольной степени.

Далее нас будут интересовать неприводимые многочлены в конечных полях.

Неприводимые многочлены над $\mathbb{F}_2$

Пример

Дано: поле $\mathbb{F}_2 = \langle \{0,1\}, +_2, \cdot_2 \rangle$.
Требуется: найти все неприводимые многочлены степеней 2, 3, 4 над ним.

Вторая степень: $x^2 + ax + b$

Ясно, что $b = 1$, иначе $x^2 + ax = x(x+a)$ $\Rightarrow$ ищем неприводимый многочлен в виде $x^2 + ax + 1$.
Если

$a = 0$, то $x^2 + 1 = (x+1)^2$;

$a = 1$, то получаем неприводимый многочлен.

$\therefore$ над $\mathbb{F}_2$ существует единственный неприводимый многочлен степени 2: $x^2 + x + 1$.

Неприводимые многочлены над $\mathbb{F}_2$

Третья степень: $x^3 + ax^2 + bx + 1$

(почему свободный член не равен нулю?)

Исключая, как сделано ранее, делимость на $x + 1$, получаем условие $a + b \neq 0$, т.е.

$$\left[\begin{array}{l} a = 0, \ b = 1\,, \\ a = 1, \ b = 0\,. \end{array} \right.$$

$\therefore$ над $\mathbb{F}_2$ существует два неприводимых многочлена степени 3:

$$x^3 + x^2 + 1 \ \text{ и } \ x^3 + x + 1\,.$$

Неприводимые многочлены над $\mathbb{F}_2$

Четвёртая степень: $x^4 + ax^3 + bx^2 + cx + 1$

Исключение делимости на $x+1$ приводит к условию $a+b+c=1$, т.е. имеется 4 варианта, которые дают 3 решения:

a	b	c	многочлен	
0	0	1	x^4+x+1	
0	1	0	x^4+x^2+1	— приводимый
1	0	0	x^4+x^3+1	
1	1	1	$x^4+x^3+x^2+x+1$	

Откуда взялся ещё один приводимый многочлен?
Найдены многочлены, у которых нет линейных делителей (степени 1). Но многочлен 4-й степени может разлагаться в произведение двух неприводимых многочленов 2-й степени:

$$x^4+x^2+1 = (x^2+x+1)^2.$$

Неприводимые многочлены над $\mathbb{F}_3$

Поле $\mathbb{F}_3 = \langle \{0, 1, 2\}, +_3, \cdot_3 \rangle \Rightarrow$ кольцо многочленов $\mathbb{F}_3[x]$.
Многочлены порядка 1:

$$\begin{array}{ll} x & 2x \\ x+1 & 2x+1 \\ x+2 & 2x+2 \end{array}$$

Какие из них неприводимы? Все!

Неприводимые многочлены порядка 2 в $\mathbb{F}_3[x]$ (они не имеют корней 0, 1, 2):

$$\begin{array}{ll} x^2+1 & 2x^2+2 \\ x^2+x+2 & 2x^2+x+1 \\ x^2+2x+2 & 2x^2+2x+1 \end{array}$$

Существование и нахождение неприводимых многочленов

Теорема (о существовании неприводимых многочленов)

Для любых натурального n и простого p над $\mathbb{F}_p$ существует неприводимый многочлен степени n.

— докажем позже.

Вопрос

Как в кольце $\mathbb{F}_p[x]$ найти неприводимый многочлен?

Ответ: нет эффективных алгоритмов 
(из таблиц, алгоритм из 5-й главы «Алгебры» Ван дер Вардена, алгоритм Берлекэмпа...)

Если многочлен не имеет корней, это ещё не значит, что он неприводим. Почему?

Зачем нужны неприводимые многочлены?

Используя неприводимые многочлены, можно строить новые конечные поля — *расширения* простых полей $\mathbb{F}_p$:

1. Выбираем простое p и фиксируем поле
$$\mathbb{F}_p = \langle \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}, +_p, \cdot_p \rangle.$$
2. Рассматриваем кольцо $\mathbb{F}_p[x]$ многочленов над ним.
3. Выбираем натуральное n и неприводимый многочлен
$$P(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{F}_p[x].$$
4. Идеал $(P(x))$ порождает факторoccмножество $\mathbb{F}_p[x]/(P(x))$, элементы которого суть совокупность $\{R(x)\}$ остатков от деления многочленов $f \in \mathbb{F}_p[x]$ на $P(x)$:
$$f(x) = Q(x) \cdot P(x) + R(x).$$

Утверждение

Множество $\{R(x)\}$ является полем Галуа $GF(p^n)$.

Построение конечных полей...

Доказательство

1. *Кольцо многочленов* $\mathbb{F}_p[x]$ *евклидово, идеал* $(P(x))$ *— максимальный* $\Rightarrow$ $\{R(x)\}$ *— поле.*
2. *Его мощность* $\big|\{R(x)\}\big|$ $=$ *число многочленов над* $\mathbb{F}_p$ *степени не выше* $n-1$, *т.е.* $\big|\{R(x)\}\big| = p^n$.

Поле $\{R(x)\} = GF(p^n)$ называется *расширением n-й степени поля* $\mathbb{F}_p$; альтернативное обозначение — $\mathbb{F}_p^n$.

Вопрос

Почему в обозначении $\mathbb{F}_p^n$ *не используется многочлен* $P(x)$, *с помощью которого построено поле?*

Теорема

Любое конечное поле изоморфно какому-нибудь полю Галуа $\mathbb{F}_p^n$.

Пример: построение поля $\mathbb{F}_3^2$

Выберем неприводимый многочлен в $\mathbb{F}_3[x]$: $x^2 + 1$.
Искомое поле есть

$$\mathbb{F}_3^2 \cong \mathbb{F}_3[x]/(x^2+1) = \\ = \{\,0,\ 1,\ 2,\ x,\ x+1,\ x+2,\ 2x,\ 2x+1,\ 2x+2\,\}.$$

Можно составить таблицы сложения и умножения в этом поле с учётом $x^2 = -1 \equiv_3 2$.
Например:

$$\begin{aligned} (x+1)+(x+2) &= 2x, & x\cdot(2x) &= 1,\\ (2x+1)+x &= 1, & (2x+1)\cdot x &= x+1, \end{aligned}$$

и т.д.

Построение поля $\mathbb{F}_3^2$...

Заметим, что, например,

$$\begin{aligned} (x+1)^1 &= x+1, & (x+1)^5 &= 2x+2, \\ (x+1)^2 &= 2x, & (x+1)^6 &= x, \\ (x+1)^3 &= 2x+1, & (x+1)^7 &= x+2, \\ (x+1)^4 &= 2, & (x+1)^8 &= 1. \end{aligned}$$

Это значит, что $x+1$ — примитивный элемент (мультипликативной группы) поля $\mathbb{F}_3^2$.

Вопрос

Что будет, если при построении поля вместо x^2+1 взять другой неприводимый в $\mathbb{F}_3[x]$ многочлен? Например, $2x^2+x+1$?

Ответ: получится поле, изоморфное построенному.

Как найти примитивные элементы поля $\mathbb{F}_p^n$?

$f(x)$ — примитивный элемент (генератор) группы $\mathbb{F}_p^{n*}$, если

1. $\left(f(x)\right)^{p^n-1} = 1$ и $\left(f(x)\right)^i \neq 1$ для $0 < i < p^n - 1$,
2. для любого многочлена $g(x) \in \mathbb{F}_p^{n*}$ найдётся степень i такая, что $g(x) = \left(f(x)\right)^i$, $i \in \{0, 1, \ldots, p^n - 1\}$.

Если α — примитивный элемент поля $GF(q)$, то любой другой примитивный элемент может быть получен как степень α^k, где k — целое взаимно простое с $q-1$ $\Rightarrow$ количество примитивных элементов поля $\mathbb{F}_p^n$ равно $\varphi(p^n - 1)$.

Например, в 9-элементном поле $\mathbb{F}_3^2$ имеется $\varphi(8) = 4$ примитивных элемента, образованных степенями 1, 3, 5, 7 (числа, взаимно простые с 8) уже найденного генератора:

$$x + 1,\ (x+1)^3 = 2x + 1,\ (x+1)^5 = 2x + 2,\ (x+1)^7 = x + 2.$$

Я что-то не понимаю: неприводимые многочлены — это примитивные элементы?

Ведь было: для поиска и тех, и других нет эффективных алгоритмов...

- Неприводимые многочлены ищут в кольце многочленов $\mathbb{F}_p[x]$ над простым полем $\mathbb{F}_p$ — например, чтобы построить его расширение.
- Примитивные элементы ищут в мультипликативной группе поля — например, чтобы иметь удобное представление ненулевых элементов $\mathbb{F}_p^n$ через степени генератора.

Замечание: в поле $GF(p^n)$ понятие «неприводимый многочлен» не имеет смысла: там любой многочлен делится на любой ненулевой.

Например, в $\mathbb{F}_3[x]/(x^2+1)$: $\dfrac{x+1}{2x+1} = x.$

Может ли приводимый многочлен быть примитивным элементом?

1. Возьмём поле $\mathbb{F}_2 = \{0, 1\}$.
2. Возьмём неприводимый над $\mathbb{F}_2$ многочлен $x^3 + x + 1$.
3. Построим поле $F = \mathbb{F}_2[x]/(x^3 + x + 1) \cong \mathbb{F}_2^3$; оно содержит все полиномы из $\mathbb{F}_2[x]$ степени не выше 2.
4. Многочлен $P(x) = x^2 + x$ — приводим в любом кольце, в т.ч. в $\mathbb{F}_2[x]$, и он принадлежит F.
5. Является ли $P(x)$ — примитивным элементом поля F?

Мультипликативная группа поля F содержит $2^3 - 1 = 7$ элементов, это простое число $\Rightarrow$ в мультипликативная группе все $\varphi(7) = 6$ неединичных элеметов — генераторы $\Rightarrow$ ответ на оба вопроса — **ДА**!

Всегда ли неприводимый многочлен есть примитивный элемент?

1. Возьмём поле $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$.
2. Возьмём неприводимый над $\mathbb{F}_5$ многочлен $x^2 + x + 1$.
3. Построим поле $F = \mathbb{F}_5[x]/(x^2 + x + 1) \cong \mathbb{F}_5^2$; оно содержит только полиномы 0-й и 1-й степеней из $\mathbb{F}_5[x]$.
4. Все многочлены 1-й степени неприводимы, имеют вид $ax + b$ и их — 20 шт.
   Все ли они — примитивные элементы поля F?

Мультипликативная группа поля F содержит $5^2 - 1 = 24$ элемента из которых $\varphi(24) = 8$ примитивных $\Rightarrow$ не все многочлены 1-й степени — генераторы $\Rightarrow$
ответ на оба вопроса — **НЕТ**!

Когда x есть примитивный элемент?

Вопрос: когда корень x (сам неприводимый многочлен!) неприводимого над $\mathbb{F}_p$ многочлена $a(x)$ будет примитивным элементом мультипликативной группы поля $\mathbb{F}_p[x]/(a(x))$?

Ответ: корень нормированного неприводимого многочлена $a(x)$ будет примитивным элементом мультипликативной группы поля $\mathbb{F}_p[x]/(a(x))$ iff $a(x)$ *примитивен*, т.е. $t = p^n - 1$ — наименьший показатель, при котором $a(x) \mid x^t - 1$ (или, эквивалентно, $a(x)$ — м.м. для x).

Пример: неприводимый над $\mathbb{F}_2$ многочлен $x^3 + x + 1$ примитивен: $(x^{2^3-1} + 1)/(x^3 + x + 1) = x^4 + x^2 + x + 1$, но

$x^m + 1 \not\vdots\, x^3 + x + 1$ ни при каком $m = 4, 5, 6$. Поэтому

$$\mathbb{F}_2^*[x]/\left(x^3 + x + 1\right) = \Big\{ x^0 = 1,\ x,\ x^2,\\ x^3 = x + 1,\ x^4 = x^2 + x,\ x^5 = x^2 + x + 1,\ x^6 = x^2 + 1 \Big\}.$$

Разделы

Алгоритм Евклида —

— применяют для нахождения НОД(a, b) натуральных a и b.

Наблюдение: общий делитель пары чисел (a, b), то остаётся им и для пары $(a - b, b)$ (считаем, что $a \geqslant b$).

Отсюда:

- пары чисел (a, b) и $(a - kb, b)$ $(q \in \mathbb{Z})$ имеет одинаковые общие делители;
- вместо $a - kb$ можно взять остаток r_0 от деления нацело a на b: $a = bq + r_0$, $q \in \mathbb{Z}$, $0 \leqslant r_0 < b$;
- затем, переставив числа в паре, можно повторить процедуру; она закончится, т.к. числа в паре уменьшаются, но остаются неотрицательными.

В результате: за конечное число шагов образуется пара $(\mathbf{r_n}, 0)$. Ясно, что НОД$(a, b) = r_n$.

Алгоритм Евклида: общая схема $(a \geqslant b)$

НОД $(a, b) \boxed{=}$

Шаг (-2): $r_{-2} = a$ — полагаем для удобства;

Шаг (-1): $r_{-1} = b$ — полагаем для удобства;

Шаг 0: $r_{-2} = r_{-1}q_0 + r_0$ — делим r_{-2} на r_{-1}, остаток r_0;

Шаг 1: $r_{-1} = r_0 q_1 + r_1$ — делим r_{-1} на r_0, остаток r_1;

… *всегда делим с остатком бóльшее число на меньшее, оставляем меньшее (оно становится бóльшим) и остаток (он становится меньшим)*;

Шаг n: $r_{n-2} = r_{n-1}q_n + r_n$ — делим r_{n-2} на r_{n-1}, остаток r_n;

Шаг $n+1$: $r_{n-1} = r_n q_{n+1} + 0$ — деление нацело $\Rightarrow$ **останов**.

Всегда $r_{-2} \geqslant r_{-1} > r_0 > r_1 > \ldots > r_n \geqslant 1$. $\boxed{=} r_n$.

Алгоритм Евклида: пример

НОД $(252, 105) \boxed{=}$

Шаг (-2): $r_{-2} = 252$;

Шаг (-1): $r_{-1} = 105 \Rightarrow (252, 105)$;

Шаг 0: $252 = 105 \cdot 2 + 42 \Rightarrow (105, 42)$;

Шаг 1: $105 = 42 \cdot 2 + 21 \Rightarrow (42, 21)$;

Шаг 2: $42 = 21 \cdot 2 + 0 \Rightarrow (\mathbf{21}, 0)$.

$\boxed{=} 21$.

$$\text{НОД}\,(a, b, c) = \text{НОД}\,(a, (\text{НОД}\,(b, c))$$

Соотношение Безу

Утверждение (соотношение Безу)

Для любых натуральных a, b и $d = \text{НОД}(a, b)$ найдутся целые коэффициенты Безу x, y такие, что $d = ax + by$.

Доказательство

Рассматриваем алгоритм Евклида с конца к началу:
$d = r_n = r_{n-2} - r_{n-1}q_n$, затем, подставляя сюда значение $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$, получаем

$$d = -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} = \alpha r_{n-3} + \beta r_{n-2}$$

для некоторых $\alpha, \beta \in \mathbb{Z}$ и т.д.

Для нахождения по паре чисел (a, b) их НОД и коэффициентов Безу применяют *расширенный алгоритм Евклида*.

Расширенный алгоритм Евклида —

— повторяет схему (простого) алгоритма Евклида, в котором на каждом шаге:

1. дополнительно вычисляются x_i и y_i по формулам

$$x_i = x_{i-2} - q_i x_{i-1}, \quad y_i = y_{i-2} - q_i y_{i-1}, \qquad i = 0, 1, \ldots;$$
$$x_{-2} = y_{-1} = 1, \quad x_{-1} = y_{-2} = 0;$$

2. справедливо соотношение

$$r_i = r_{i-2} - q_i r_{i-1} = (a x_{i-2} + b y_{i-2}) - q_i (a x_{i-1} + b y_{i-1}) =$$
$$= a(x_{i-2} - q_i x_{i-1}) + b(y_{i-2} - q_i y_{i-1}) = a x_i + b y_i.$$

Расширенный алгоритм Евклида: пример

Задача. Найти натуральное d и целые x и y такие, что

$$d = \text{НОД}\,(252, 105) = 252x + 105y.$$

Решение. Имеем $x_i = x_{i-2} - q_i x_{i-1}$, $y_i = y_{i-2} - q_i y_{i-1}$.
Сведём все вычисления в таблицу:

шаг i	r_{i-2}	r_{i-1}	q_i	r_i	x_i	y_i
-2				252	1	0
-1				105	0	1
0	252	105	2	42	1	-2
1	105	42	2	21	-2	5
2	42	21	2	0		

Ответ: $d = 21$, $x = -2$, $y = 5$,
т.е. найдено разложение $21 = (-2) \cdot 252 + 5 \cdot 105$.

Задача

В поле $\mathbb{Z}/(101)$ *решить уравнение* $4x = 1.$ $(*)$

Решение

1. $4x = 1 + k \cdot 101 = 102, 203, 304, \ldots; \quad x = 304/4 = 76.$
   Это решение перебором.

2. *Поскольку* $101y \equiv_{101} 0$, *вместо* $(*)$ *можно расширенным алгоритмом Евклида решать уравнение*
   $$4x + 101y = 1\,.$$
   В результате работы алгоритма: $4 \cdot 76 + 101 \cdot (-3) = 1.$

Аналогично решаются уравнения

$$ax = c, \qquad ax + by = c$$

(перед решением a, b и c надо поделить на их общий НОД).

Нахождение обратных элементов в расширениях полей $\mathbb{F}_p$

Алгоритм Евклида и его расширенная версия остаётся справедливым в любом евклидовом кольце, следовательно, и в любом поле Галуа.

Поэтому: обратный элемент $y(x)$ для некоторого многочлена $b(x)$ в поле $F = \mathbb{F}_p[x]/(a(x))$ определяется соотношением

$$b(x) \cdot y(x) = 1 \quad \Leftrightarrow \quad a(x) \cdot \chi(x) + b(x) \cdot y(x) = 1\,,$$

которое может быть решено расширенным алгоритмом Евклида для пары многочленов $(a(x), b(x))$ в поле F.

Решение данных уравнений существует всегда: т.к. $a(x)$ — неприводимый многочлен и $\deg b(x) < \deg a(x)$, то НОД $(a(x), b(x)) = 1$.

Пример: найти $(x^2+x+3)^{-1}$ в поле $\mathbb{F}_7[x]/(x^4+x^3+x^2+3)$

Применяя расширенный алгоритм Евклида, решим уравнение

$$(x^4+x^3+x^2+3)\chi(x) + (x^2+x+3)y(x) = 1 \qquad (*)$$

Шаг 0: $r_{-2}(x) = x^4+x^3+x^2+3$,
$r_{-1}(x) = x^2+x+3$,
$y_{-2}(x) = 0$,
$y_{-1}(x) = 1$ — задание начальных значений.

Шаг 1: $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$,
$q_0(x) = x^2+5$,
$r_0(x) = 2x+2$,
$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = -x^2-5$.

Шаг 2: $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$,
$q_1(x) = 4x$,
$r_1(x) = 3, \quad \deg r_1(x) = 0$
$y_1(x) = y_{-1}(x) - y_0(x)q_1(x) = 1 + 4x(x^2+5) =$
$= 4x^3+6x+1$.

Пример... $\mathbb{F}_7^4: \ (x^4+x^3+x^2+3)\chi(x)+b(x)(x^2+x+3) = 1 \ (*)$

Алгоритм заканчивает свою работу на шаге 2, т.к. $r_1(x)=3$ и $\deg r_1(x) = \deg 1 = 0$ (1 — многочлен в правой части $(*)$).

Замечание: при итерациях алгоритма нет необходимости вычислять $\chi_i(x)$ — коэффициент при $x^4+x^3+x^2+3$, — т.к. нас интересует только $y_i(x)$ — коэффициент при x^2+x+3.

Остаток $r_1(x)=3$, отличается от 1 на множитель-константу.

Чтобы получить решение уравнения $(*)$ вычисляем элемент $3^{-1} \equiv_7 5$ и домножаем на него y_1:

$$5y_1(x) = 5(4x^3+6x+1) \equiv_7 6x^3+2x+5.$$

Ответ: в поле $\mathbb{F}_7[x]/\big(x^4+x^3+x^2+3\big)$ —

$$(x^2+x+3)^{-1} = 6x^3+2x+5.$$

Разделы

Векторное пространство: определение

Определение

Абстрактным векторным пространством над полем $\Bbbk = \{1, \alpha, \beta, \dots\}$ называется алгебраическая система $\mathcal{V} = \langle V, \Bbbk; +, \cdot \rangle$, где

- $V = \{0, v, \dots\}$ — произвольное множество,
- $+$ — бинарная операция сложения над V: $V \times V \xrightarrow{+} V$,
- $\cdot$ — бинарная операция умножения элемента («числа») из $\Bbbk$ на элемент («вектор») из V: $\Bbbk \times V \xrightarrow{\cdot} V$,

причём операции $+$ и $\cdot$ удовлетворяют следующим аксиомам:

L1: V — коммутативная группа по сложению, 0 — её нейтральный элемент.

L2: $\alpha \cdot (v_1 + v_2) = \alpha \cdot v_1 + \alpha \cdot v_2$, $(\alpha_1 + \alpha_2) \cdot v = \alpha_1 \cdot v + \alpha_2 \cdot v$, (дистрибутивность $\cdot$ относительно $+$),

L3: $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$ (композиция умножений на два элемента поля совпадает с умножением их произведение, «ассоциативность» операций умножения поля и $\cdot$),

L4: $1 \cdot v = v$ (унитальность).

Координатное пространство

Пример

Пусть $V = \Bbbk^n$ — множество конечных последовательностей длины n элементов поля $\Bbbk$.
'Сложение' и 'умножение на число (из $\Bbbk$)' элементов из V определяются покомпонентно.

Получившаяся структура — векторное пространство.
Его называют *n-мерным координатным пространством* над полем $\Bbbk$.

Дистрибутивность относительно вычитания: $(\alpha - \beta) \cdot v = \alpha \cdot v - \beta \cdot v$:

$$(\alpha - \beta) \cdot v + \beta \cdot v = (\alpha - \beta + \beta) \cdot v = \alpha \cdot v$$

Отсюда получаем, что

- $0 \cdot v = 0$, так как $0 \cdot v = (1 - 1) \cdot v = v - v = 0$
- и $-v = (-1) \cdot v$, так как
$$v + (-1) \cdot v = 1 \cdot v + (-1) \cdot v = (1 - 1) \cdot v = 0 \cdot v = 0.$$

Применение линейной алгебры к изучению конечных полей

Лемма

Поле $\Bbbk$ характеристики $p > 0$ есть векторное пространство над $\mathbb{F}_p$.

Доказательство

сложение — *наследуется операция сложения в поле $\Bbbk$;*

умножение — *поскольку*

$$\mathbb{F}_p \cong F = \{0, 1, 1+1, \ldots, \overbrace{1+\ldots+1}^{p-1}\} \subseteq \Bbbk,$$

то при умножении «числа» из поля $\mathbb{F}_p$ можно заменять на соответствующие элементы из поля F;

аксиомы векторного пространства — *выполняются в силу свойств арифметических операций в поле $\Bbbk$.*

Следствие

Поле Галуа как векторное пространство состоит из p^n элементов.

Поля Галуа как кольца вычетов или векторные пространства

Поле $\mathbb{F}_p^n$ есть конечная АС с элементами-многочленами

$$M_n(x) = \{ a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \} \subset \mathbb{F}_p[x],$$

которую можно рассматривать как

- факторкольцо вычетов по модулю некоторого неприводимого многочлена $f(x)$ степени n над полем $\mathbb{F}_p$:

$$\mathbb{F}_p^n \cong \langle \mathbb{F}_p[x]/(f(x))\, ; +_p, \cdot_p \rangle$$

  или как

- n-мерное координатное пространство над полем $\mathbb{F}_p$:

$$\mathbb{F}_p^n \cong \langle M_n(x), \mathbb{F}_p; +_p, \cdot_p \rangle.$$

Базис в $\mathbb{F}_p^n$

Теорема

Элементы $\{1\}, \{x\}, \ldots, \{x^{n-1}\}$ *образуют базис* $\mathbb{F}_p^n$.

Доказательство

1. Любой элемент $\mathbb{F}_p^n$ *представим в виде линейной комбинации указанных векторов:*

$$\{a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}\} = \\ = a_0\{1\} + a_1\{x\} + \ldots + a_{n-1}\{x^{n-1}\}.$$

2. Обратно, пусть $g(x) = b_0\{1\} + b_1\{x\} + \ldots + b_{n-1}\{x^{n-1}\} = 0$. *Это означает, что многочлен* $g(x)$ *степени* $n-1$ *делится на некоторый многочлен* n*-й степени, что возможно лишь при* $b_0 = b_1 = \ldots = b_{n-1} = 0$, *т.е. система* $\{1\}, \{x\}, \ldots, \{x^{n-1}\}$ *линейно независима.*

$\mathbb{C}$ — расширение поля $\mathbb{R}$

Замечание. Построение поля с помощью вычетов по модулю некоторого неприводимого многочлена и аналоги доказанных теорем справедливы не только в случае конечных полей.

Например:

1. рассмотрим поле действительных чисел $\mathbb{R}$ и кольцо многочленов $\mathbb{R}[x]$ над ним;
2. в $\mathbb{R}[x]$ возьмём неприводимый многочлен $x^2 + 1$;
3. построим поле F как факторкольцо: $F = \mathbb{R}[x]/(x^2 + 1)$;
4. F также и векторное пространство над $\mathbb{R}$; его базис — $\{\{1\}, \{x\}\}$ и каждый его элемент $z \in F$ можно представить в виде $z = a\{1\} + b\{x\}$, $a, b \in \mathbb{R}$;
5. поле F изоморфно полю комплексных чисел
$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R},\ i^2 = -1\},$$
изоморфизм задаётся соответствием $\{1\} \mapsto 1$, $\{x\} \mapsto i$.

Подполя $\mathbb{F}_p^n$

Лемма

Если поле $\mathbb{F}_p^n$ содержит подполе $\mathbb{F}_p^k$, то $k \mid n$.

Доказательство

Если поле $\Bbbk_1$ содержится в поле ($\Bbbk_1 \subset \Bbbk_2$), то элементы $\Bbbk_2$ можно умножать на элементы из $\Bbbk_1$, а результаты складывать.

Поэтому поле $\Bbbk_2$ является векторным пространством над полем $\Bbbk_1$ некоторой размерности d — значит, в нём $|\Bbbk_1|^d$ элементов.

Для нашего случая: $p^n = (p^k)^d$, что и означает $k \mid n$.

Ясно, что $\mathbb{F}_p$ — всегда подполе $\mathbb{F}_p^n$ (случай $k = 1$).

Разделы

Минимальный многочлен

Рассмотрим поле $\mathbb{F}_p^n$, а в нём — какой-нибудь элемент β и будем интересоваться многочленами, для которых этот элемент является корнем.

Определение

Многочлен $m_\beta(x)$ называется *минимальным (м.м.)* или *минимальной функцией для* β, если это нормированный многочлен минимальной степени, из $\mathbb{F}_p[x]$ для которого β является корнем.

Другими словами, должны выполняться три свойства:

1. $m_\beta(\beta) = 0$;
2. $\forall\, f(x) \in \mathbb{F}_p[x] : (\deg f(x) < \deg m_\beta(x) \Rightarrow f(\beta) \neq 0)$;
3. коэффициент при старшей степени в $m_\beta(x)$ равен 1.

Минимальный многочлен из неприводимого

Рассмотрим поле $\mathbb{F}_p^n = \mathbb{F}_p[x]/\left(a(x)\right)$, порождаемое неприводимым многочленом $a(x) = a_0 + a_1 x + \ldots + a_n x^n$ и убедимся, что многочлен $a_n^{-1} a(x)$ — минимальный для элемента $\overline{x} = (\,0,\,1,\,0,\,\ldots,\,0\,) \in \mathbb{F}_p^n$.

Действительно, с одной стороны —

$$a_0 \overline{1} + a_1 \overline{x} + \ldots + a_n \overline{x}^n = \overline{a_0 + a_1 x + \ldots + a_n x^n} = 0,$$

т.е. $\overline{x}$ — корень $a(x)$, а значит и $a_n^{-1} a(x)$.

С другой, пусть $b(x) = b_0 \overline{1} + b_1 \overline{x} + \ldots + b_{n-1} \overline{x}^{n-1} = 0$.
Но тогда $b_0 \overline{1} + b_1 \overline{x} + \ldots + b_{n-1} \overline{x^{n-1}} = 0$, т.е. имеем линейную зависимость между элементами $\left\{ \overline{1},\, \overline{x},\, \ldots,\, \overline{x^{n-1}} \right\}$ — базиса поля $\mathbb{F}_p^n$ как векторного пространства над $\mathbb{F}_p$, откуда $b_0 = b_1 = \ldots = b_{n-1} = 0$.

$$\overline{x^2} = \overline{x}^2 = (0, 0, 1, 0, \ldots, 0), \quad \ldots, \quad \overline{x^{n-1}} = (0, \ldots, 0, 1)$$

Свойства минимальных многочленов

Утверждение

Минимальные многочлены неприводимы.

Доказательство

Пусть $m_\beta(x)$ — *м.м. для* β *и* $m_\beta(x) = m_1(x)m_2(x)$.
Тогда

$$m_\beta(\beta) = 0 \Rightarrow \left[\begin{array}{l} m_1(\beta) = 0 \\ m_2(\beta) = 0 \end{array} \right. ,$$

но $\deg m_1 < \deg m$ *и* $\deg m_2 < \deg m$ $\Rightarrow$ β *не может быть корнем ни* $m_1(x)$, *ни* $m_2(x)$.

Свойства минимальных многочленов...

Утверждение

Пусть в некотором поле Галуа $m_\beta(x)$ *— м.м. для элемента* β*, а* $f(x)$ *— многочлен такой, что* $f(\beta) = 0$.
Тогда $f(x)$ *делится на* $m_\beta(x)$.

Доказательство

Разделим $f(x)$ *на* $m_\beta(x)$ *с остатком:*

$$f(x) = u(x)m_\beta(x) + v(x), \quad \deg v < \deg m.$$

Подставляя в это равенство β*, получаем*

$$0 = f(\beta) = u(\beta)\underbrace{m_\beta(\beta)}_{=0} + v(\beta) = v(\beta),$$

т.е. β *— корень* $v(x)$*, что противоречит минимальности* $m_\beta(x)$.

Свойства минимальных многочленов...

Следствие

Для каждого элемента поля существует не более одного м.м.

Доказательство

Пусть минимальных многочленов два.
Они взаимно делят друг друга, а значит, различаются на обратимый множитель-константу.
Поскольку минимальный многочлен нормирован, эта константа равна 1, т.е. данные многочлены совпадают.

Свойства минимальных многочленов...

Утверждение

Для каждого элемента β поля $\mathbb{F}_p^n$ существует (единственный) м.м. и его степень не превосходит n.

Доказательство

Рассмотрим следующие элементы поля $\mathbb{F}_p^n$: $1, \beta, \beta^2, \ldots, \beta^n$ — их $n+1$ штука, а размерность $\mathbb{F}_p^n$ как векторного пространства равна n $\Rightarrow$ эти элементы линейно зависимы, т.е. существуют такие не все равные 0 коэффициенты $c_0, \ldots, c_n$, что

$$c_0 + c_1\beta + \ldots + c_n\beta^n = 0,$$

$\Rightarrow$ β — корень многочлена $f(x) = c_0 + c_1x + \ldots + c_nx^n$.

Минимальным многочленом для β будет некоторый нормированный неприводимый делитель $f(x)$ (т.е. $f(x) \in \mathbb{F}_p^n$).

Многочлены над конечным полем: свойства

Теорема

Любой ненулевой элемент поля $\mathbb{F}_p^n$ *является корнем многочлена* $x^{p^n-1} - 1$, *т.е.*

$$x^{p^n-1} - 1 = (x - \beta_1) \cdot \ldots \cdot (x - \beta_{p^n-1}),$$

где $\{\beta_1, \ldots, \beta_{p^n-1}\} = \mathbb{F}_p^{n*} = \mathbb{F}_p^n \setminus \{0\}$.

Доказательство

$\mathbb{F}_p^{n*}$ *— циклическая группа по умножению порядка* $p^n - 1$.
Порядок $\deg\alpha$ *любого элемента* $\alpha \in \mathbb{F}_p^{n*}$ *(т.е. порядок циклической подгруппы* $\langle\alpha\rangle$*) по теореме Лагранжа делит порядок группы.*
Поэтому $p^n - 1 = q \cdot \deg\alpha$, $\alpha^{\deg\alpha} = 1$ *и*

$$\alpha^{p^n-1} - 1 = \alpha^{q\deg\alpha} - 1 = (\alpha^{\deg\alpha})^q - 1 = 1^q - 1 = 0.$$

Многочлены над конечным полем: свойства...

Следствие (теорема Ферма)

Все элементы поля $\mathbb{F}_p^n$, не исключая нуля, являются корнями многочлена $x^{p^n} - x$.

Доказательство

Вынесем x за скобку:

$$x^{p^n} - x = x\left(x^{p^n - 1} - 1\right).$$

У второго сомножителя корнями будут все ненулевые элементы, а у первого — 0.

Многочлены над конечным полем: свойства...

Теорема

В кольце многочленов над конечным полем

$$(x^n - 1) \vdots (x^m - 1) \Leftrightarrow n \vdots m.$$

Доказательство

- *Пусть* $n = mk$. *Сделаем замену* $x^m = y$, *тогда* $x^n - 1 = y^k - 1$ *и* $x^m - 1 = y - 1$. *Делимость очевидна.*
- *Предположим, что* $n \not\vdots\, m$, *т.е.* $n = km + r$, $0 < r < m$, *тогда*

$$x^n - 1 = \frac{x^r(x^{mk} - 1)(x^m - 1)}{x^m - 1} + x^r - 1 = \\ = \frac{x^r(x^{mk} - 1)}{x^m - 1}(x^m - 1) + x^r - 1.$$

Многочлены над конечным полем: свойства...

Последнее выражение задает результат деления $x^n - 1$ на $x^m - 1$ с остатком, поскольку $x^{mk} - 1$ делится на $x^m - 1$ по доказанному выше.
Остаток $x^r - 1 \neq 0$ в силу сделанных предположений.
$\therefore$ *$x^n - 1$ не делится на $x^m - 1$.*

Теорема даёт возможность раскладывать многочлены $x^n - 1$ при составных n.
Например, разложим $x^{15} + 1$ в $\mathbb{F}_2[x]$ (где $-1 = +1$):

$$x^{15} + 1 = (x^3 + 1)(x^{12} + x^9 + x^6 + x^3 + 1)\,,$$
$$x^{15} + 1 = (x^5 + 1)(x^{10} + x^5 + 1)\,.$$

Возможность раскладывать многочлены специального вида на неприводимые даёт следующая теорема.

Разложение многочленов на неприводимые

Теорема

Все неприводимые многочлены n-й степени из $\mathbb{F}_p[x]$ делят многочлен $x^{p^n} - x$.

Доказательство

$n = 1$. *Убеждаемся, что $(x-a) \mid (x^p - x)$, где $a \in \mathbb{F}_p$: при $a = 0$ это очевидно, а в остальных случаях доказано, что a — корень многочлена $x^{p-1} - 1 = (x^p - x)/x$.*

$n > 1$. *Строим по неприводимому и (без ограничения общности — нормированному) многочлену $f(x)$ степени n поле $\mathbb{F}_p^n$.*
В этом поле $\overline{x}$ — корень и $f(x)$, и $x^{p^n-1} - 1$, причём $f(x)$ — м.м. для него.
По свойствам м.м. $x^{p^n-1} - 1$ делится на $f(x)$.

Пример: разложение $x^{15}+1 \in \mathbb{F}_2[x]$

Проверяем степени 2:

$$2^4-1=15|15, \quad 2^3-1=7 \nmid 15, \quad 2^2-1=3|15, \quad 2^1-1=1|15,$$

1. $x(x^{15}+1)=x^{2^4}+x$, откуда все неприводимые многочлены 4-й степени будут делителями $x^{16}+x$ и, следовательно, $x^{15}+1$. Таких многочленов 3:
$$x^4+x+1, \quad x^4+x^3+1 \text{ и } x^4+x^3+x^2+x+1.$$
2. $x(x^3+1)=x^{2^2}+x$, откуда все неприводимые многочлены 2-й степени будут делителями x^4+x и, следовательно, x^3+1. Такой многочлен только один: x^2+x+1.
3. $x(x^1+1)=x^{2^1}+x$, откуда (тривиально) единственный неприводимый многочлен 1-й степени $x+1$ делит x^2+x.

Итого: разложение $x^{15}-1$ на неразложимые над $\mathbb{F}_2$ многочлены —

$$x^{15}+1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Многочлены над конечным полем...

Теорема

Любой неприводимый многочлен-делитель $x^{p^n-1}-1$ имеет степень, не превосходящую n.

Если делящий $x^{p^n-1}-1$ неприводимый многочлен имеет степень равную n, то он называется *примитивным многочленом*.

Доказательство

Пусть φ — неприводимый делитель $x^{p^n}-x$ степени k. Тогда $F \stackrel{\text{def}}{=} \mathbb{F}_p/(\varphi)$ — поле, которое рассмотрим как векторное пространство над $\mathbb{F}_p$ с базисом $\left\{\overline{1}, \overline{x}, \ldots, \overline{x^{k-1}}\right\}$.

Многочлены над конечным полем...

Обозначим $\overline{x} = \alpha$*. Поскольку* $(x^{p^n} - x) \vdots \varphi$*, то в* F *имеем* $\alpha^{p^n} - \alpha = 0$.

Любой элемент F *выражается через базис:* $\beta = \sum\limits_{i=0}^{k-1} a_i \alpha^i$.

Возведя обе части этого равенства в степень p^n*, получим*

$$\beta^{p^n} = \left(\sum_{i=0}^{k-1} a_i \alpha^i \right)^{p^n} = \sum_{i=0}^{k-1} a_i \alpha^i = \beta,$$

т.е. β *— корень уравнения*

$$x^{p^n} - x = 0\,. \qquad (*)$$

Итак, каждый элемент поля F *является корнем* $(*)$*, но у* $(*)$ *не более* p^n *различных корней, а* $|F| = p^k$ $\therefore$ $n \geqslant k$.

Многочлены над конечным полем...

Утверждение

Пусть $\beta \in \mathbb{F}_p^n$ *имеет порядок* l, *а его м.м.* $m(x)$ *имеет степень* k.

Тогда ❶ $(p^k - 1) \vdots l$, *а если* $r < k$, *то* ❷ $(p^r - 1) \not\vdots l$.

Доказательство

❶ *По неприводимому многочлену* k*-й степени* $m(x)$ *строим поле из* p^k *элементов. Все его ненулевые элементы, в том числе и* β, *являются корнями уравнения* $x^{p^k-1} - 1 = 0$, *т.е.* $\beta^{p^k-1} - 1 = 0$ *и* $\beta^{p^k-1} = 1$, *но* $\deg \beta = l \Rightarrow l \mid (p^k - 1)$.

❷ *Пусть* $(p^r - 1) \vdots l$ *и* $r < k$. *Тогда* β *— корень уравнения* $x^{p^r} - 1 = 0$, *а т.к.* $m(x)$ *— м.м. для* β, *то* $(x^{p^r} - 1) \vdots m(x)$ *(было доказано)* $\Rightarrow$ *найден неприводимый делитель* $x^{p^r} - 1$ *степени* k, *но* $k > r \Rightarrow$ *противоречие доказанному ранее.*

Многочлены над конечным полем...

Следующая теорема позволяет раскладывать многочлены на множители.

Теорема (свойство корней неприводимого многочлена)

Пусть β — корень неприводимого многочлена $f(x)$ степени n с коэффициентами из $\mathbb{F}_p$. Тогда элементы $\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}$:
❶ *все различны;* ❷ *исчерпывают список всех n корней $f(x)$ (их называют смежными).*

Т.е. чтобы получить все корни неприводимого многочлена, достаточно найти один из них и возводить его последовательно в степень p.

Доказательство

❶ *Покажем, что если β — корень $f(x)$, то β^p — тоже корень.*

Многочлены над конечным полем...

Поскольку $a^p = a$ *для всех* $a \in \mathbb{F}_p$, *то справедливо*

$$\bigl(a_0 + a_1 x + \ldots + a_k x^k\bigr)^p = a_0^p + a_1^p x^p + a_2^p x^{2p} + \ldots + a_k^p x^{kp} = \\ = a_0 + a_1(x^p) + a_2(x^p)^2 + \ldots + a_k(x^p)^k,$$

т.е. для любого многочлена $\varphi(x) \in \mathbb{F}_p[x]$ *выполняется равенство*

$$\bigl(\varphi(x)\bigr)^p = \varphi(x^p). \qquad (*)$$

Отсюда:

$$f(\beta) = 0 \ \Leftrightarrow \ f(\beta)^p = 0 \ \Leftrightarrow \ f(\beta^p) = 0$$

и $\beta,\ \beta^p,\ \ldots,\ \beta^{p^{n-1}}$ *— корни многочлена* $f(x)$.

Многочлены над конечным полем...

❷ *Осталось доказать, что все* $\beta, \beta^p, \ldots, \beta^{p^{n-1}}$ *различны, и тогда (многочлен степени* n *имеет не более* n *корней) можно утверждать, что найдены* ***все*** *корни многочлена* $f(x)$.

Предположим, что $\beta^{p^l} = \beta^{p^k}$ *и без ограничения общности* $l < k$. *Имеем:*

1. $\beta^{p^n} = \beta$;
2. *поскольку*

$$\beta^{p^n} = \beta^{p^k \cdot p^{n-k}} = \left(\beta^{p^k}\right)^{p^{n-k}} = \left(\beta^{p^l}\right)^{p^{n-k}} = \beta^{p^{n-k+l}},$$

   то β *— корень уравнения* $x^{p^{n-k+l}-1} - 1 = 0$.

Из теоремы «Все неприводимые многочлены n*-й степени над* $\mathbb{F}_p$ *являются делителями* $x^{p^n} - x$*» получаем*
$n - k + l \geqslant n \Rightarrow l \geqslant k$ *— противоречие.*

Многочлены над конечным полем: решение уравнений

Пример

Задача. Найти корни неприводимого над $\mathbb{F}_2$ многочлена

$$f(x) = x^4 + x^3 + 1$$

Решение. Один корень получаем немедленно: x (или $\overline{x}$).
По только что доказанной теореме можно выписать остальные:

$$x^2, \qquad x^4 = x^3 + 1, \qquad x^8 = x^6 + 1 = x^3 + x^2 + x.$$

Покажем, что, например, x^2 — действительно корень $f(x)$:

$$f(x^2) = x^4 + x^3 + 1\big|_{x \mapsto x^2} = x^{4\cdot 2} + x^{4+2} + 1\big|_{x^4 \mapsto x^3+1} =$$
$$= (x^3 + 1)^2 + (x^3 + 1)x^2 + 1 = x^6 + \cancel{1} + x^5 + x^2 + \cancel{1} =$$
$$= x^6 + x^5 + x^2 = x^2(x^4 + x^3 + 1) = x^2 \cdot 0 = 0.$$

Как решать уравнения $f(x) = 0$, когда корней нет?

Алгоритм нахождения всех корней полинома $f(x) \in \mathbb{F}_p[x]$

1. Разложить $f(x)$ на неприводимые множители над $\mathbb{F}_p$:
$$f(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_k(x).$$

2. Для каждого многочлена $g_i(x)$, $i = \overline{1, k}$ рассмотреть расширение $\mathbb{F}_p[x]/(g_i(x))$, в котором он будет иметь корни
$$x = \alpha,\ \alpha^p,\ \ldots,\ \alpha^{p^{\deg g_i - 1}}.$$
Записать данные корни как многочлены из $\mathbb{F}_p[x]/(g_i(x))$.

3. Объединить все корни в одном общем расширении $\mathbb{F}_p^m$, где $m = \text{НОК}\,(\deg g_1, \deg g_2, \ldots, \deg g_k)$.

Разделы

Разделы

Разделы

Разделы