Домашнее задание № 3

Раффаэле Делла Пиетра, 675

Задание 1

Сколько решений имеет уравнение $x^{15} = 1$ в поле порядка 17^n в зависимости от n?

Корни уравнения $x^{15} = 1$ образуют мультипликативную группу, поэтому их число должно делить 15. Также эта группа является подгруппой мультипликативной группы поля $\mathbb{F}_{17^n}$,
поэтому её порядок должен делить и $17^n - 1$. Один корень есть всегда — единица. Рассмотрим большее количество корней:

Число корней k	$17^n \mod k$	$n=1$	$n=2$	$n=3$	$n=4$
3	2^n	2	1	2	1
5	2^n	2	4	3	1
15	2^n	2	4	8	1

Таким образом, образуются 4 случая:

$n \mod 4$	0	1	2	3
Число корней	15	1	3	1

Задание 2

Проверить, что $\mathrm{F}_7[x]/(x^2 + x - 1)$ — поле. Вычислить в нём $(1 - x)^{-1}$.

$a(x) = x^2 + x - 1$.

$\mathrm{F}_7[x]/(a(x))$ — поле $\iff$ $a(x)$ не имеет корней.

$$\begin{cases} a(0) \equiv 6 \\ a(1) \equiv 1 \\ a(2) \equiv 5 \\ a(3) \equiv 4 \\ a(4) \equiv 5 \\ a(5) \equiv 1 \\ a(6) \equiv 6 \end{cases} \implies \text{поле.}$$

Ищем обратное:

$(ax + b)(1 - x) = ax - ax^2 + b - bx = -ax^2 + (a - b)x + b = -a(1 - x) + (a - b)x + b = (2a - b)x + b - a = 1.$

$$\begin{cases} 2a \equiv b \\ b - a \equiv 1 \end{cases} \implies \begin{cases} a \equiv 1 \\ b \equiv 2 \end{cases}$$

Задание 3

Многочлен $x^4 + 2x^3 + 2x^2 + 4x + 4$ разложить на неприводимые множители над Z_5.

$a(x) = x^4 + 2x^3 + 2x^2 + 4x + 4$.

Для начала проверим, на какие множители этот многочлен разложится.

$$\begin{cases} a(0) \equiv 4 \\ a(1) \equiv 3 \\ a(2) \equiv 2 \\ a(3) \equiv 4 \\ a(4) \equiv 1 \end{cases} \implies \text{корней нет. Если разложение будет, то только на 2 квадратных множителя.}$$

$x^4+2x^3+2x^2+4x+4 = x^4-3x^3+2x^2-x-1 = x^4-x^3+x^2-2x^3+2x^2-2x-x^2+x-1 = \boxed{(x^2 - x + 1)(x^2 - 2x - 1)}$

Задание 4

При каких простых p многочлен x^4+1 неприводим над $\mathbb{Z}_p$?

Рассмотрим квадратичные вычеты и невычеты в мультипликативной группе$\mathbb{Z}_p$. Всего в этой группе $p-1$ элемент, то есть чётное количество (двойку рассмотрим отдельно). Если a — вычет, то a — некоторая чётная степень порождающего элемента, что очевидно из чётности порядка группы. Если a — невычет, то это нечётная степень порождающего элемента. Таким образом, произведение двух вычетов или двух невычетов — вычет, а произведение вычета и невычета — невычет.
Для $\mathbb{Z}_2$ всё очевидно: $x^4+1 \equiv x^4-1 \equiv \ldots \equiv (x+1)^4 \implies$ приводим.
Для $\mathbb{Z}_p$ где $p>2$ есть несколько случаев.
Если -1 — квадратичный вычет и $a^2 \equiv -1$, то $x^4+1 \equiv x^4-a^2 \equiv (x^2-a)(x^2+a) \implies$ приводим.
Если 2 — квадратичный вычет и $b^2 \equiv 2$, то $x^4+1 \equiv (x^2+1)^2-(bx)^2 \equiv (x^2-bx+1)(x^2+bx+1) \implies$ приводим.
Если -1 и 2 — невычеты, то -2 — вычет и $c^2 \equiv -2 \implies x^4+1 \equiv (x^2-1)^2-(cx)^2 \equiv (x^2-cx-1)(x^2+cx-1) \implies$ приводим.
Таким образом, x^4+1 приводим в любом $\mathbb{Z}_p$.

Задание 5

Найти порядок элемента $1+x^2$ в поле $\mathrm{F}_2[x]/(x^4+x-1)$.

В этом поле в каждом элементе любая степень x от 0 до 3 может быть и не быть в элементе.
$4^2=16 \implies$ порядок группы — 16.
Мультипликативная группа имеет порядок 15. По теореме Лагранжа порядок элемента должен делить порядок группы, поэтому $ord(1+x^2) \in \{1,3,5,15\}$.
Очевидно, порядок $1+x^2$ не равен 1.
$(1+x^2)^3 \equiv x^3+x \implies$ порядок не равен 3.
$(1+x^2)^5 \equiv x^2+x+1 \implies$ порядок не равен 5.
Проверим 15: $(x^2+x+1)^3 \equiv 1 \implies$ порядок $1+x^2$ равен 15.