

# Алгебра 2 2023 Кузнецов

## 1 Листок 1

1. Для каких натуральных  $n$  многочлен  $\frac{x^n-1}{x-1} = 1+x+\dots+x^{n-1}$  неприводим?

По-видимому, имеется в виду неприводимость над полем  $\mathbb{Q}$ .

Во-первых, заметим, что при  $n = ab$  имеет место равенство

$$1 + x + \dots + x^{n-1} = (1 + x + \dots + x^{a-1})(1 + x^a + \dots + x^{a(b-1)}).$$

Или без разложения:

$$\frac{x^{ab} - 1}{x - 1} = \frac{x^a - 1}{x - 1} \frac{x^{ab} - 1}{x^a - 1}.$$

Отсюда следует, что при составном  $n$  многочлен  $\frac{x^n-1}{x-1}$  приводим.

Теперь попробуем доказать, что при простом  $n = p$  многочлен  $\frac{x^n-1}{x-1}$  неприводим. Предположим, что

$$\frac{x^p - 1}{x - 1} = u(x)v(x),$$

где  $u, v$  — непостоянные многочлены с рациональными коэффициентами, причём будем считать, что их старшие коэффициенты равны 1, и  $u$  — непостоянный многочлен с рациональными коэффициентами наименьшей степени, делящий  $\frac{x^p-1}{x-1}$ . Тогда, что

$$u(x) = (x - a_1) \dots (x - a_k),$$

где  $a_1, \dots, a_k$  — попарно различные неединичные корни степени  $p$  из единицы. Поэтому все симметрические многочлены от  $a_1, \dots, a_k$

$$a_1 + \dots + a_k,$$

$$a_1 a_2 + \dots + a_{k-1} a_k,$$

$$\dots$$

$$a_1 \dots a_k$$

рациональны — они являются коэффициентами многочлена  $u$ . Но тогда для любого натурального  $s$

$$u_s(x) = (x - a_1^s) \dots (x - a_k^s)$$

— тоже многочлен с рациональными коэффициентами (поскольку все симметрические многочлены выражаются через элементарные), и он должен быть взаимно прост с  $u$  либо совпадать с  $u$ , ибо иначе наибольший общий делитель этих многочленов будет степени меньше степени  $u$  и будет делить многочлен  $\frac{x^p-1}{x-1}$ . Рассмотрим множество тех  $s \in \{1, \dots, p-1\}$ , для которых

$$\{a_1^s, \dots, a_k^s\} = \{a_1, \dots, a_k\}.$$

Это подгруппа мультипликативной группы  $\mathbb{F}_p$ . Значит, она циклическая, и есть  $h \in \{1, \dots, p-1\}$ , таких, что она порождена  $h$ . Тогда

$$u(x) = (x-a)(x-a^h)(x-a^{h^2}) \dots (x-a^{h^t}).$$

Дальше я не знаю, как закончить это рассуждение. Поэтому будем решать по-другому. Попробуем применить критерий Эйзенштейна.  $q(x) = \frac{x^p-1}{x-1}$  неприводим над  $\mathbb{Q}$  тогда и только тогда, когда неприводим

$$q(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + C_p^{p-1}x^{p-2} + \dots + C_p^2x + p.$$

И применим критерий Эйзенштейна.

2.  $x^n f(\frac{1}{x}) = c_0x^n + c_1x^{n-1} + \dots + c_{n-1}x + c_n$  имеет с  $f(x)$  общий корень — тот, который лежит на единичной окружности (если  $|\alpha| = 1$  и  $f(\alpha) = 0$ , то  $f(\frac{1}{\alpha}) = f(\bar{\alpha}) = 0$ ). Значит, эти многочлены не взаимно просты, и в силу неприводимости  $f$  должны иметь все корни общие. То есть эти многочлены пропорциональны:

$$f(x) = tx^n f\left(\frac{1}{x}\right), t \in \mathbb{Q}.$$

Отсюда  $c_k = tc_{n-k}$  для всех  $k$ . Отсюда  $t^2 = 1$ . Значит,  $t = \pm 1$ . Если  $t = -1$ , то многочлен  $f$  имеет корнем 1, что противоречит неприводимости. Значит,  $t = 1$ . Если  $n$  нечётно,  $n = 2m+1$ , то

$$f(x) = (x^{2m+1} + 1) + c_1(x^{2m} + x) + \dots,$$

и этот многочлен имеет корень  $-1$ , что тоже невозможно в силу его неприводимости. Всё доказано.

3. а) Кажется, это известная теорема. Воспользуемся тем, что мультипликативная группа поля  $\mathbb{F}_p$  циклическая. Значит, она порождается неким  $g \in \mathbb{F}_p$ . Тогда  $\left(\frac{-1}{p}\right) = 1$  тогда и только тогда, когда для некоторого  $s, 0 < s < p-1$  имеет место

$$g^{2s} = -1.$$

Из этого равенства следует  $g^{4s} = 1$ , и получаем:

$2s$  не делится на  $p-1$ ,  $4s$  делится на  $p-1$ .

Отсюда следует, что  $p-1$  делится на 4. Пусть, напротив,  $p-1$  делится на 4. Тогда возьмём  $h = g^{\frac{p-1}{2}}$ . Отсюда  $h^2 = 1$ . Поэтому  $h = \pm 1$ . Но  $h = 1$  быть не может, так как  $g$  — первообразный корень.

- б) Очевидно, следующие утверждения равносильны:

- $\left(\frac{-3}{p}\right) = 1$
- Многочлен  $x^2 + 3$  приводим над  $\mathbb{F}_p$
- Многочлен  $(x+1)^2 + 3 = x^2 + 2x + 4$  приводим над  $\mathbb{F}_p$
- Многочлен  $(x-2)(x^2 + 2x + 4) = x^3 - 8$  разложим над  $\mathbb{F}_p$
- Существует  $\varepsilon \in \mathbb{F}_p, \varepsilon \neq 1$ , такое, что  $\varepsilon^3 = 1$  (поделить на 2 корни уравнения из предыдущего пункта)

Но мультипликативная группа поля  $\mathbb{F}_p$  циклическая. Значит, она порождается неким  $g \in \mathbb{F}_p$ . Тогда  $\varepsilon = g^s, 0 < s < p-1$ . Но тогда  $g^{3s} = 1$ , и  $3s \mid p-1$ . Если  $p-1$  не делится на 3, то  $s$  делится на  $p-1$ , а такое невозможно в силу  $0 < s < p-1$ . Значит,  $p-1$  делится на 3. И обратно — если  $p-1$  делится на 3, то можно положить

$$\varepsilon = g^{\frac{p-1}{3}}.$$

Задача решена.

4.  $K$  содержит примитивный корень из 1 степени 8. Пусть это корень  $g$ . Ясно, что тогда  $g^4 = -1, g^2 = -1/g^2$ . Рассмотрев пример поля комплексных чисел, я подобрал такое:

$$(g + 1/g)^2 = g^2 + 2 + 1/g^2 = g^2 + 2 - g^2 = 2.$$

Теперь рассмотрим 4 случая:

- $p \equiv 1 \pmod{8}$ . Тогда существует примитивный корень из 1 степени 8. Почему? Как мы помним, мультипликативная группа конечного поля  $\mathbb{F}_p$  циклическая. Она порождена элементом  $t \in \mathbb{F}_p$ . Тогда  $t^{\frac{p-1}{8}}$  и есть первообразный корень из 1 степени 8.
- $p \equiv -1 \pmod{8}$ . Это более сложный случай. По задаче 3а,  $-1$  является квадратичным невычетом в  $F_p$ . Значит, многочлен  $x^2 + 1$  неприводим над  $F_p$ , и фактор  $G = F_p[x]/(x^2 + 1)$  является полем из  $p^2$  элементов. Обозначим в этом поле элемент  $x$  как  $i$ ,  $i^2 = -1$ . Итак,  $G = \{a + bi \mid a, b \in F_p\}$ . Пусть  $g$  — первообразный корень в  $G$  (то есть порождающий элемент мультипликативной группы поля  $G$ ). Положим

$$h = g^{(p^2-1)/8}.$$

Тогда  $h^4 = -1$ ,  $h$  — примитивный корень из 1 степени 8 (но, к сожалению, он лежит не в поле  $F_p$ , а в его расширении).

**Утверждение 1.1.** Или  $h + 1/h$ , или  $h - 1/h$  лежит в  $F_p$ .

*Proof.*  $h$  является корнем многочлена  $x^4 + 1$ . Вот 4 корня этого многочлена:  $h, -h, 1/h, -1/h$ . Легко видеть, что они все разные (если, например,  $h = -1/h$ , то  $h^2 = -1$ , а это противоречит равенству  $h^4 = -1$ ). Итак,

$$x^4 + 1 = (x - h)(x + h)(x - 1/h)(x + 1/h).$$

Но  $F_p[h]$  — поле, которое строго больше  $F_p$ , но содержится в  $G$ . Значит, оно совпадает с  $G$ , ведь нет поля характеристики  $p$  с количеством элементов между  $p$  и  $p^2$ . Значит, любой элемент поля  $G$  представляется в виде  $\alpha h + \beta, \alpha, \beta \in F_p$ . Поэтому

$$h^2 = \alpha h + \beta, \alpha, \beta \in F_p.$$

Значит, многочлены  $x^4 + 1$  и  $x^2 - \alpha x - \beta$  не взаимно просты. Поэтому  $x^4 + 1$  делится на какой-то многочлен степени 2 с коэффициентами в  $F_p$ . Возможны лишь такие разложения  $x^4 + 1$  в произведение многочленов второй степени (с коэффициентами из  $F_p$ ):

$$\begin{aligned} x^4 + 1 &= (x^2 - h^2)(x^2 - 1/h^2), \\ x^4 + 1 &= (x^2 - (h + 1/h)x + 1)(x^2 + (h + 1/h)x + 1), \\ x^4 + 1 &= (x^2 - (h - 1/h)x - 1)(x^2 + (h - 1/h)x - 1). \end{aligned}$$

Первый вариант не подходит, поскольку  $h^2$  не может лежать в  $F_p$ , ведь его квадрат равен  $-1$ . Во втором и третьем вариантах либо  $h + 1/h$ , либо  $h - 1/h$  лежит в  $F_p$ . Выяснить, какой же из этих вариантов реализуется, у нас получится позже.  $\square$

Покажем, что не может быть  $h - 1/h \in F_p$ . Пусть  $g = u + vi, u, v \in F_p$ . Тогда

$$\frac{1}{g} = \frac{u - vi}{u^2 + v^2}.$$

Имеем

$$h - 1/h = (u + vi)^{(p^2-1)/8} - \frac{(u - vi)^{(p^2-1)/8}}{(u^2 + v^2)^{(p^2-1)/8}}.$$

Пусть  $h = U + Vi = (u + vi)^{(p^2-1)/8}, U, V \in F_p$ . Тогда

$$h - 1/h = U + Vi - \frac{U - Vi}{(u^2 + v^2)^{(p^2-1)/8}} = U + Vi + \frac{-U + Vi}{(u^2 + v^2)^{(p^2-1)/8}}.$$

Это может лежать в  $F_p$ , только если

$$V + \frac{V}{(u^2 + v^2)^{(p^2-1)/8}} = 0.$$

$V = 0$  быть не может, ведь  $U + Vi = h$ , а  $h$  не лежит в  $F_p$  — потому что  $h^4 = -1$ , а  $-1$  у нас квадратичный невычет. Значит, на  $V$  можно сократить, и

$$(u^2 + v^2)^{(p^2-1)/8} = -1.$$

Но у нас  $(p^2 - 1)/8$  чётное, и из этого равенства следует, что  $-1$  — квадратичный вычет по модулю  $p$ . А это неверно. Итак,  $h - 1/h$  не может лежать в  $F_p$ , и остаётся  $h + 1/h \in F_p$ . Поскольку

$$(h + 1/h)^2 = 2,$$

то всё доказано.

- $p \equiv -3 \pmod{8}$ . Предположим,

$$s^2 \equiv 2 \pmod{p}.$$

По задаче 3а есть  $j \in \mathbb{F}_p$ , такое, что

$$j^2 \equiv -1 \pmod{p}.$$

Рассмотрим  $z = s^{\frac{1+j}{2}}$ . Тогда

$$z^2 = s^{\frac{1+j}{2}} = j.$$

Отсюда ясно, что  $z$  — первообразный корень из 1 степени 8. Мультипликативная группа поля  $\mathbb{F}_p$  циклическая. Она порождена элементом  $t \in \mathbb{F}_p$ . Тогда  $z = t^k, 0 < k < p-1$ . Отсюда  $t^{8k} = 1$ ,  $8k$  делится на  $p-1$ . Но  $p-1$  не делится на 8. Значит,  $4k$  делится на  $p-1$ , и  $z^4 = 1$ . Противоречие с первообразностью  $p$ .

- $p \equiv 3 \pmod{8}$ . Это самый сложный случай. Поначалу можно рассуждать, как в случае  $p \equiv -1 \pmod{8}$ . По задаче 3а,  $-1$  — квадратичный невычет в  $F_p$ . Поэтому так же рассматриваем расширение  $G = F_p[x]/(x^2 + 1)$ . В нём выбираем элемент  $g$ , порождающий мультипликативную группу  $G$ . Полагаем

$$h = g^{(p^2-1)/8}.$$

Как и раньше,  $h^4 = -1$ . Снова получаем, что либо  $h + 1/h$ , либо  $h - 1/h$  лежит в  $F_p$ . И нам надо показать, что в этом случае  $h - 1/h \in F_p$  (тогда получается, что  $-2$  — квадратичный вычет в  $F_p$ , а раз  $-1$  — невычет, то  $2$  — невычет).

Итак, покажем, что  $h + 1/h \notin F_p$ .

Пусть  $g = u + vi, u, v \in F_p$ . Тогда

$$\frac{1}{g} = \frac{u - vi}{u^2 + v^2}.$$

Имеем

$$h + 1/h = (u + vi)^{(p^2-1)/8} + \frac{(u - vi)^{(p^2-1)/8}}{(u^2 + v^2)^{(p^2-1)/8}}.$$

Пусть  $h = U + Vi = (u + vi)^{(p^2-1)/8}, U, V \in F_p$ . Тогда

$$h + 1/h = U + Vi + \frac{U - Vi}{(u^2 + v^2)^{(p^2-1)/8}}.$$

Это может лежать в  $F_p$ , только если

$$V - \frac{V}{(u^2 + v^2)^{(p^2-1)/8}} = 0.$$

$V = 0$  быть не может, ведь  $U + Vi = h$ , а  $h$  не лежит в  $F_p$  — потому что  $h^4 = -1$ , а  $-1$  у нас квадратичный невычет. Значит, на  $V$  можно сократить, и

$$(u^2 + v^2)^{(p^2-1)/8} = 1.$$

На первый взгляд, тут нет никакого противоречия. Но добавим ещё такое замечание:  $u^2 + v^2$  должно быть первообразным корнем в  $F_p$ . Действительно, в поле  $G$  норма  $\|a + bi\| = a^2 + b^2 \in F_p$  мультипликативна (легко проверить). Чтобы порождать мультипликативную группу поля  $G$ ,  $g = u + vi$  должно обладать таким свойством, что  $(u^2 + v^2)^k, k \geq 0$  должно пробегать все элементы в  $F_p$  вида  $a^2 + b^2, a, b \in F_p$ . Поскольку  $a^2 + b^2, a, b \in F_p$  пробегает все вычеты  $\bmod p$  (см. утверждение ниже), то  $u^2 + v^2$  — порождает мультипликативную группу  $F_p$ . А тогда  $(u^2 + v^2)^{(p-1)/2} = -1$ , и в силу нечётности  $\frac{p+1}{4}$

$$(u^2 + v^2)^{(p^2-1)/8} = -1.$$

Противоречие.

**Утверждение 1.2.**  $a^2 + b^2, a, b \in F_p$  пробегает все элементы  $F_p$ .

*Proof.* Ясно, что в виде  $a^2 + b^2$  можно представить любой квадратичный вычет в  $F_p$  (надо взять  $b = 0$ ). Осталось показать, что в таком виде можно представить хотя бы один квадратичный невычет  $s \in F_p$  — ведь любой другой квадратичный невычет представляется в виде  $cz^2, z \in F_p$  (потому что частное двух квадратичных невычетов — квадратичный вычет). Ясно, что есть квадратичный вычет  $s$ , такой, что  $s + 1$  — квадратичный невычет (если бы это было не так, то по индукции бы получили, что  $0, 1, 2, \dots, p-1$  — все квадратичные вычеты, что неправда). Тогда  $s = a^2, s + 1 = a^2 + 1$ , и мы представили квадратичный невычет  $s$  в виде суммы двух квадратов. Доказательство окончено.  $\square$

5. Ясно, что  $K(\sqrt{a} + \sqrt{b}) \subseteq K(\sqrt{a}, \sqrt{b})$ . Покажем, что

$$K(\sqrt{a}, \sqrt{b}) \subseteq K(\sqrt{a} + \sqrt{b}).$$

Имеем

$$\sqrt{a} - \sqrt{b} = \frac{a - b}{\sqrt{a} + \sqrt{b}} \in K(\sqrt{a} + \sqrt{b}).$$

Ну а тогда

$$\sqrt{a} = \frac{1}{2}((\sqrt{a} + \sqrt{b}) + (\sqrt{a} - \sqrt{b})) \in K(\sqrt{a} + \sqrt{b}).$$

И аналогично для  $\sqrt{b}$ . А всё потому, что в поле характеристики, отличной от 2, элемент 2 обратим. А если характеристика поля равна 2, то это не обязательно так. Пример:

6. Потом.

7.  $q$  — степень простого числа. Сколько неприводимых многочленов степени 42 над  $F_q$ ? Решим сначала, когда  $q = p$  — простое число. Пусть  $P_k$  — произведение всех приведённых неприводимых многочленов степени  $k$  над  $F_p$ . Имеем тогда

$$x^{p^{42}} - x = P_1 P_2 P_3 P_6 P_7 P_{14} P_{21} P_{42},$$

$$x^{p^{21}} - x = P_1 P_3 P_7 P_{21}.$$

Отсюда

$$\frac{x^{p^{42}} - x}{x^{p^{21}} - x} = P_2 P_6 P_{14} P_{42}.$$

Далее,

$$\begin{aligned} x^{p^{14}} - x &= P_1 P_2 P_7 P_{14}, \\ \frac{x^{p^{42}} - x}{(x^{p^{21}} - x)(x^{p^{14}} - x)} &= \frac{P_6 P_{42}}{P_1 P_7}. \end{aligned}$$

Далее,

$$\begin{aligned} x^{p^7} - x &= P_1 P_7, \\ \frac{(x^{p^{42}} - x)(x^{p^7} - x)}{(x^{p^{21}} - x)(x^{p^{14}} - x)} &= P_6 P_{42}. \end{aligned}$$

Далее,

$$\begin{aligned} x^{p^6} - x &= P_1 P_2 P_3 P_6, \\ \frac{(x^{p^{42}} - x)(x^{p^7} - x)}{(x^{p^{21}} - x)(x^{p^{14}} - x)(x^{p^6} - x)} &= \frac{P_{42}}{P_1 P_2 P_3}. \end{aligned}$$

Далее,

$$\begin{aligned} x^{p^3} - x &= P_1 P_3, \\ \frac{(x^{p^{42}} - x)(x^{p^7} - x)(x^{p^3} - x)}{(x^{p^{21}} - x)(x^{p^{14}} - x)(x^{p^6} - x)} &= \frac{P_{42}}{P_2}. \end{aligned}$$

Далее,

$$\begin{aligned} x^{p^2} - x &= P_1 P_2, \\ \frac{(x^{p^{42}} - x)(x^{p^7} - x)(x^{p^3} - x)(x^{p^2} - x)}{(x^{p^{21}} - x)(x^{p^{14}} - x)(x^{p^6} - x)} &= P_{42} P_1. \end{aligned}$$

Но  $P_1 = x^p - x$ . Итак,

$$P_{42} = \frac{(x^{p^{42}} - x)(x^{p^7} - x)(x^{p^3} - x)(x^{p^2} - x)}{(x^{p^{21}} - x)(x^{p^{14}} - x)(x^{p^6} - x)(x^p - x)}.$$

Приравняем степени. Получаем, что количество многочленов, входящих в произведение  $P_{42}$ , равно

$$\frac{p^{42} - p^{21} - p^{14} + p^7 - p^6 + p^3 + p^2 - p}{42}.$$

Это как раз то, что мы искали. Но как быть для случая  $F_q$ ?

Итак, решаем задачу в общем случае. Пусть  $Q_k$  — количество неприводимых многочленов степени  $k$  со старшим коэффициентом 1 над  $F_q$ , где  $q$  — степень простого числа. Напишем рекуррентные соотношения для  $Q_k$ :

$$Q_1 = q,$$

$$Q_k = q^k - \sum_{s=1}^k \sum_{\substack{0 < i_1 \leq i_2 \leq \dots \leq i_s \\ i_1 t_1 + \dots + i_s t_s = k \\ t_1 + \dots + t_s > 1}} \binom{Q_{i_1} + t_1 - 1}{t_1} \dots \binom{Q_{i_s} + t_s - 1}{t_s}, k > 1.$$

Поясним, откуда берётся такая рекуррентная формула. Мы вычитаем из общего количества многочленов степени  $k$  со старшим коэффициентом 1 количество приводимых многочленов. Количество приводимых многочленов мы считаем с помощью суммирования по всевозможным разложениям на неприводимые множители.  $i_r$  соответствуют степеням неприводимых множителей,  $t_r$  — количество неприводимых многочленов степени  $i_r$  в разложении.  $\binom{Q_{i_r} + t_r - 1}{t_r}$  — это количество сочетаний с повторениями из  $Q_{i_r}$  различных неприводимых многочленов степени  $i_r$  по  $t_r$ .

А теперь определим последовательность многочленов  $H_k(x)$ :

$$H_1(x) = x,$$

$$H_k(x) = x^k - \sum_{s=1}^k \sum_{\substack{0 < i_1 \leq i_2 \leq \dots \leq i_s \\ i_1 t_1 + \dots + i_s t_s = k \\ t_1 + \dots + t_s > 1}} \frac{(H_{i_1}(x) + t_1 - 1) \dots H_{i_1}(x)}{t_1!} \dots \frac{(H_{i_s}(x) + t_s - 1) \dots H_{i_s}(x)}{t_s!},$$

$$k > 1.$$

Ясно, что  $Q_k = H_k(q)$ , причём, заметим,  $H_k$  не зависит от  $q$ . Если  $q = p$  — простое, то, как мы видели,

$$Q_{42} = \frac{p^{42} - p^{21} - p^{14} + p^7 - p^6 + p^3 + p^2 - p}{42}.$$

Отсюда для простого  $p$

$$H_{42}(p) = \frac{p^{42} - p^{21} - p^{14} + p^7 - p^6 + p^3 + p^2 - p}{42}.$$

Так как простых чисел бесконечно много, то

$$H_{42}(x) = \frac{x^{42} - x^{21} - x^{14} + x^7 - x^6 + x^3 + x^2 - x}{42}.$$

Значит,

$$Q_{42} = H_{42}(q) = \frac{q^{42} - q^{21} - q^{14} + q^7 - q^6 + q^3 + q^2 - q}{42}.$$

Ответ: количество неприводимых многочленов степени 42 над  $F_q$  со старшим коэффициентом 1 есть

$$\frac{q^{42} - q^{21} - q^{14} + q^7 - q^6 + q^3 + q^2 - q}{42}.$$

## 2 Листок 2

1. Не буду решать.



2. Степень расширения  $[\mathbb{Q}[\sqrt{n_1}, \dots, \sqrt{n_m}] : \mathbb{Q}]$  равна произведению степеней  $[\mathbb{Q}[\sqrt{n_1}, \dots, \sqrt{n_{s+1}}] : \mathbb{Q}[\sqrt{n_1}, \dots, \sqrt{n_s}]]$ . А каждая из этих степеней — 1 или 2. Поэтому степень расширения  $[\mathbb{Q}[\sqrt{n_1}, \dots, \sqrt{n_m}] : \mathbb{Q}]$  — это степень двойки. Если бы там был  $\sqrt[3]{2}$ , то было бы

$$[\mathbb{Q}[\sqrt{n_1}, \dots, \sqrt{n_m}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{n_1}, \dots, \sqrt{n_m}] : \mathbb{Q}[\sqrt[3]{2}]] [\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}].$$

Но  $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$  — это 3. А слева степень двойки, она на 3 не делится. Противоречие.

3. Работаем в поле разложения многочлена  $x^3 - x - a$ . Имеем

$$x^3 - x - a = (x - \alpha)(x - \beta)(x - \gamma).$$

Отсюда, приравнявая коэффициенты, получаем

$$\alpha + \beta + \gamma = 0,$$

$$\alpha\beta + \beta\gamma + \alpha\gamma = -1,$$

$$\alpha\beta\gamma = a.$$

Далее, из предыдущих равенств

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \alpha\gamma) = 2,$$

$$\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 = (\alpha\beta + \beta\gamma + \alpha\gamma)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma) = 1.$$

Теперь имеем

$$(3\alpha^2 - 1)(3\beta^2 - 1)(3\gamma^2 - 1) = 27\alpha^2\beta^2\gamma^2 - 9(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3(\alpha^2 + \beta^2 + \gamma^2) - 1 = 27a^2 - 4.$$

Из равенств  $\alpha\beta\gamma = a$ ,  $\alpha^3 - \alpha = a$  получаем

$$\alpha\beta\gamma = \alpha^3 - \alpha,$$

$$\beta\gamma = \alpha^2 - 1.$$

Аналогично,  $\alpha\beta = \gamma^2 - 1$ ,  $\alpha\gamma = \beta^2 - 1$ . Имеем

$$(\alpha - \beta)(\beta - \gamma) = \alpha\beta - \beta^2 - \alpha\gamma + \beta\gamma = (\alpha + \gamma)\beta - \beta^2 - \alpha\gamma = -2\beta^2 - \alpha\gamma = -2\beta^2 - (\beta^2 - 1) = 1 - 3\beta^2.$$

Аналогично,  $(\beta - \gamma)(\gamma - \alpha) = 1 - 3\gamma^2$ ,  $(\gamma - \alpha)(\alpha - \beta) = 1 - 3\alpha^2$ . Итак,

$$4 - 27a^2 = (1 - 3\alpha^2)(1 - 3\beta^2)(1 - 3\gamma^2) = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2.$$

Осталось показать, что  $(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$  лежит в  $F_p$ . Рассмотрим в поле разложения многочлена  $x^3 - x - a$ , то есть  $F_p[\alpha, \beta, \gamma]$ , автоморфизм Фробениуса  $x \rightarrow x^p$ . Как известно, он оставляет на местах элементы  $F_p$  и только их. Кроме того, ясно, что корни многочлена  $x^3 - x - a$  переходят в его же корни, поэтому  $\alpha, \beta, \gamma$  переставляются этим автоморфизмом. Но поскольку эти корни не лежат в  $F_p$ , ни один из них не переходит в себя. А все перестановки множества из трёх элементов, не оставляющие на месте ни один из них, чётные. Поэтому наш автоморфизм производит чётную перестановку  $\alpha, \beta, \gamma$ , а значит, переводит  $(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$  в себя. А кто переходит в себя, тот лежит в  $F_p$ . Всё доказано.

### 3 Листок 3

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
7. Автоморфизм поля  $\overline{\mathbb{F}}_p$ , не являющийся степенью автоморфизма Фробениуса. Алгебраическое замыкание поля  $\mathbb{F}_p$  можно представить как объединение последовательности вложенных друг в друга полей  $\mathbb{F}_{p^{n!}}$ . На каждом из этих полей можно задать какой-то автоморфизм, но он с необходимостью будет степенью автоморфизма Фробениуса. Значит, единственная возможность — задать согласованно на этих подполях степени автоморфизма Фробениуса, но так, чтоб эти степени были разные, но при этом автоморфизмы были согласованы.

Теперь опишем решение формально. Пусть

$$k_n = 1 + p^{1!} + p^{2!} + \dots + p^{(n-1)!}.$$

Зададим на вложенных друг в друга  $\mathbb{F}_{p^{n!}}$  полях автоморфизм  $\phi$  так:

$$\phi(x) = x^{p^{k_n}}, x \in \mathbb{F}_{p^{n!}}.$$

Согласованность следует из того, что при  $m > n$   $k_m - k_n$  делится на  $n!$ . Значит, автоморфизм  $\phi$  на  $\overline{\mathbb{F}}_p$  определён корректно, а быть фиксированной степенью  $M$  автоморфизма Фробениуса он не может, так как на  $\mathbb{F}_{p^{n!}}$  при больших  $n$  минимальная степень Фробениуса, которой является наш автоморфизм, есть  $k_n < p^{n!}$  (то есть наш автоморфизм на  $\mathbb{F}_{p^{n!}}$  есть степень  $k_n$  автоморфизма Фробениуса, или  $k_n + n!$ , или  $k_n + 2n!$ , или  $\dots$ , но никак не нечто иное).