

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ  
ЯРОСЛАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. П.Г. ДЕМИДОВА

С.И. Яблокова

**ОСНОВЫ АЛГЕБРАИЧЕСКОЙ АЛГОРИТМИКИ**  
**Часть 2**

*Учебное пособие*

*Рекомендовано*  
*Научно-методическим советом университета*  
*для студентов, обучающихся по специальности*  
*Компьютерная безопасность*

ЯРОСЛАВЛЬ      2009

УДК 512+519.6  
ББК В14я73+В18я73  
Я 14

*Рекомендовано  
Редакционно-издательским советом университета  
в качестве учебного издания. План 2009 года*

**Рецензенты:**

кафедра алгебры ЯГПУ им. К.Д. Ушинского;  
кандидат физ.-мат. наук, доцент ЯГТУ Е.Р. Матвеев

Я 14 **Яблокова, С.И.** Основы алгебраической алгоритмики. Часть 2 : учеб. пособие  
/ С.И. Яблокова ; Яросл. гос. ун-т. – Ярославль : ЯрГУ, 2009. – 120 с.  
ISBN 978-5-8397-0639-2

Учебное пособие составлено в соответствии с программой курса «Алгебраическая алгоритмика».

Рассматриваются вопросы и методы, связанные с алгебраическими алгоритмами в кольце многочленов. Полученные алгоритмы иллюстрируются примерами.

Издание предназначено для студентов первого и второго курсов, обучающихся по специальности 090102 Компьютерная безопасность (дисциплина «Алгебраическая алгоритмика», блок ОПД), очной формы обучения.

Библиогр.: 4 назв.

УДК 512+519.6  
ББК В14я73+В18я73

ISBN 978-5-8397-0639-2 © Ярославский государственный  
университет им. П.Г. Демидова, 2009

Учебное издание

**Яблокова Светлана Ивановна**

## **Основы алгебраической алгоритмики**

**Часть 2**  
**Учебное пособие**

Редактор, корректор М.В. Никулина  
Компьютерный набор, верстка С.И. Яблоковой

Подписано в печать 27.01.2009 г. Формат 60×84 1/8. Бумага тип.  
Усл. печ. л. 6,97. Уч.-изд. л. 6,0. Тираж 100 экз. Заказ 009/09

Оригинал-макет подготовлен в редакционно-издательском отделе  
Ярославского государственного университета.

Отпечатано на ризографе.

Ярославский государственный университет.  
150000 Ярославль, ул. Советская, 14.

## ПРЕДИСЛОВИЕ

Учебное пособие содержит лекции по курсу "Алгебраическая алгоритмика", изучаемому студентами специальности "Компьютерная безопасность" во втором и третьем семестрах.

Первая часть этого курса изложена в пособии "Основы алгебраической алгоритмики. Часть 1" и вышла в 2008 году. Данная часть содержит 17 параграфов, в которых рассматриваются основные алгебраические алгоритмы в кольце многочленов от одной переменной над полем и над кольцом; вопросы, связанные со структурой конечных полей и колец многочленов над конечными полями.

В приложении, состоящем из 6 параграфов, изложены алгоритмы, связанные в основном с факторизацией многочленов над кольцом  $\mathbb{Z}$  и над конечными полями, такие как алгоритм Кронекера - Шуберта, модулярный алгоритм, алгоритм Берлекэмпла. Эти вопросы, как правило, не излагаются на лекциях в силу большого объема материала курса, но знакомство с ними будет полезно для развития математического кругозора в данной области математики. Кроме того, они могут быть использованы студентами при написании курсовых работ.

Первоначальное намерение автора – включить в эту часть пособия раздел о быстрых алгоритмах цифровой обработки сигналов – осуществить не удалось из-за большого объема данного пособия. Однако автор надеется включить их либо в третью часть пособия по данному курсу, либо в будущее пособие по быстрым алгоритмам для двух специальностей "Математика" и "Компьютерная безопасность".



# §1. ОСНОВНЫЕ СВЕДЕНИЯ О МНОГОЧЛЕНАХ. ЕВКЛИДОВО ДЕЛЕНИЕ МНОГОЧЛЕНОВ

Пусть  $\mathbf{A}$  – коммутативное кольцо без делителей нуля. Рассмотрим многочлены от  $x$  с коэффициентами из  $\mathbf{A}$  (или многочлены от  $x$  над  $\mathbf{A}$ )

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

где  $a_i \in \mathbf{A}$ ,  $i = 0, 1, \dots, n$ . Множество таких многочленов обозначим  $\mathbf{A}[x]$ .

*Старшим коэффициентом* многочлена называется коэффициент при наибольшей степени  $x$ , т.е. при  $x^n$ , если  $f(x)$  – многочлен степени  $n$ . Обозначать старший коэффициент многочлена  $f(x)$  будем символом  $lc(f(x))$ .

Если старший коэффициент многочлена равен единице, то многочлен называется *нормированным* или *унитарным*.

На множестве  $\mathbf{A}[x]$  определим операции сложения и умножения. Пусть

$$f_1(x) = \sum_{i=0}^n a_i x^i, \quad f_2(x) = \sum_{i=0}^m b_i x^i,$$

тогда

$$f_1(x) + f_2(x) = \sum_{i=0}^n a_i x^i + \sum_{i=0}^m b_i x^i = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i,$$

$$f_1(x) f_2(x) = \left( \sum_{i=0}^n a_i x^i \right) \cdot \left( \sum_{j=0}^m b_j x^j \right) = \sum_{k=0}^{m+n} \left( \sum_{i+j=k} a_i b_j \right) x^k.$$

Очевидно, сумма и произведение многочленов с коэффициентами из  $\mathbf{A}$ , снова есть многочлен с коэффициентами из  $\mathbf{A}$ , т.е. введенные операции замкнуты в множестве  $\mathbf{A}[x]$ . Множество  $\mathbf{A}[x]$  является коммутативным кольцом без делителей нуля. Выполнение аксиом кольца не вызывает сомнений. Чтобы убедиться, что в  $\mathbf{A}[x]$  нет делителей нуля, возьмем  $f_1(x) \neq 0$  и  $f_2(x) \neq 0$ , и пусть  $\deg f_1(x) = m$ ,  $\deg f_2(x) = n$ . Тогда  $lc(f_1(x)) = a_m \neq 0$  и  $lc(f_2(x)) = b_n \neq 0$ , и в силу того, что в  $\mathbf{A}$  нет делителей нуля,  $a_m b_n \neq 0$ , но  $a_m b_n = lc(f_1(x) f_2(x))$ , значит,  $f_1(x) f_2(x) \neq 0$ .

Два многочлена

$$f_1(x) = \sum_{i=0}^n a_i x^i \quad \text{и} \quad f_2(x) = \sum_{i=0}^m b_i x^i$$

из кольца  $\mathbf{A}[x]$  равны тогда и только тогда, когда

$$a_0 = b_0, \quad a_1 = b_1, \quad a_2 = b_2, \dots, a_i = b_i, \dots \quad \text{для всех } i.$$

На многочлен можно смотреть как на функцию, которая ставит в соответствие элементу  $a \in \mathbf{A}$  элемент  $f(a)$ . Но равенство многочленов – это не то же самое, что равенство функций. Функции считаются равными, когда они имеют равные значения для каждого элемента из  $\mathbf{A}$ .

Два *разных* многочлена могут определять одну и ту же функцию.

Например, в  $\mathbf{Z}_2[x]$

$$f_1(x) = x^3 - 1 \quad \text{и} \quad f_2(x) = x^5 - 1,$$

очевидно, не равны как многочлены, но

$$f_1(0) = f_2(0) = -1 \equiv 1, \quad f_1(1) = f_2(1) = 0,$$

т.е. они равны как функции в  $\mathbf{Z}_2[x]$ .

Многочлен  $f(x) = x^2 - x$  в  $\mathbf{Z}_2[x]$  равен нулю для всех элементов кольца  $\mathbf{Z}_2$ , поэтому определяет ту же функцию, что и нулевой многочлен  $0 + 0 \cdot x + 0 \cdot x^2 + \dots$ .

В общем случае, если  $\mathbf{A}$  – конечное кольцо с  $n$  элементами

$$\mathbf{A} = \{a_0 = 0, a_1, a_2, \dots, a_{n-1}\},$$

то многочлен

$$f(x) = x(x - a_1)(x - a_2) \cdot \dots \cdot (x - a_{n-1}) \neq 0,$$

но для всех  $x \in \mathbf{A}$  равен нулю, поэтому определяет функцию, равную функции, определяемой нулевым многочленом.



**Определение 1.** Пусть  $f_2(x) \neq 0$ . Многочлен  $f_1(x)$  делится на многочлен  $f_2(x)$ , если существует многочлен  $q(x)$  такой, что

$$f_1(x) = q(x)f_2(x).$$

Обозначение:  $f_2(x) \mid f_1(x)$ .

Очевидно, что если  $f_2(x)$  делит  $f_1(x)$ , то  $\deg f_2(x) \leq \deg f_1(x)$ . Многочлен  $f_2(x)$  называется **делителем** или **сомножителем** многочлена  $f_1(x)$ .

**Теорема 1 (свойство евклидова деления).** Пусть  $\mathbb{A}$  – коммутативное кольцо без делителей нуля. Пусть

$$f_1(x) = \sum_{i=0}^m c_i x^i, \quad \text{и} \quad f_2(x) = \sum_{i=0}^n d_i x^i \neq 0$$

– многочлены степени  $m$  и  $n$  в кольце  $\mathbb{A}[x]$ , и пусть  $d_n = lc(f_2(x))$  обратим в  $\mathbb{A}$ . Тогда существуют единственные многочлены  $q(x)$  и  $r(x)$  в  $\mathbb{A}[x]$  (частное и остаток) такие, что

$$f_1(x) = f_2(x)q(x) + r(x), \quad \deg r(x) < \deg f_2(x).$$

*Доказательство.* Если  $f_1(x) = 0$  или  $\deg f_1(x) < \deg f_2(x)$ , то положим

$$q(x) = 0 \quad \text{и} \quad r(x) = f_1(x).$$

Пусть  $\deg f_1(x) = \deg f_2(x) + k$ , где  $k \geq 0$  (т.е.  $\deg f_1(x) \geq \deg f_2(x)$ ). Определим рекуррентно многочлены  $r_i(x)$  ( $i = k + 1, k, \dots, 0$ ):

$$\begin{aligned} r_{k+1}(x) &= f_1(x), \\ r_k(x) &= r_{k+1}(x) - \frac{c_m}{d_n} x^k f_2(x), & \deg r_k(x) < \deg r_{k+1}(x), \\ r_{k-1}(x) &= r_k(x) - \frac{lc(r_k(x))}{d_n} x^{k-1} f_2(x), & \deg r_{k-1}(x) < \deg r_k(x), \\ &\dots\dots\dots \\ r_1(x) &= r_2(x) - \frac{lc(r_2(x))}{d_n} x f_2(x), & \deg r_1(x) < \deg r_2(x), \\ r_0(x) &= r_1(x) - \frac{lc(r_1(x))}{d_n} f_2(x), & \deg r_0(x) < \deg r_1(x). \end{aligned} \tag{1}$$

На каждом шаге степень вновь полученного многочлена  $r_i(x)$  меньше, чем степень предыдущего  $r_{i+1}(x)$  по крайней мере на единицу, так как старшие коэффициенты у многочленов, стоящих в правых частях равенств (1) равны. Будем считать, что на каждом шаге степень уменьшается на единицу (если это не так, то следующий шаг вычитания просто не делается, так как приходится вычитать 0, т.е. под  $lc(r_i(x))$  понимаем коэффициент при  $x^{m-k+(i-1)}$ ,  $i = k + 1, k, \dots, 1$ ).

Введем обозначения:

$$q_i = \frac{lc(r_{i+1}(x))}{d_n} \quad (i = k, k - 1, \dots, 0),$$

тогда равенства (1) можно переписать в виде

$$\begin{aligned} r_{k+1}(x) &= f_1(x), \\ r_k(x) &= r_{k+1}(x) - q_k x^k f_2(x), \\ r_{k-1}(x) &= r_k(x) - q_{k-1} x^{k-1} f_2(x), \\ &\dots\dots\dots \\ r_1(x) &= r_2(x) - q_1 x f_2(x), \\ r_0(x) &= r_1(x) - q_0 f_2(x). \end{aligned} \tag{2}$$

Сложим левые и правые части равенств (2):

$$r_{k+1}(x) + r_k(x) + \dots + r_1(x) + r_0(x) = f_1(x) + r_{k+1}(x) + \dots + r_1(x) - \\ - (q_k x^k + q_{k-1} x^{k-1} + \dots + q_1 x + q_0) f_2(x),$$

откуда получим

$$r_0(x) = f_1(x) - (q_k x^k + q_{k-1} x^{k-1} + \dots + q_1 x + q_0) f_2(x),$$

т.е.

$$f_1(x) = q(x) f_2(x) + r_0(x),$$

где  $q(x) = q_k x^k + q_{k-1} x^{k-1} + \dots + q_1 x + q_0$ .

При этом

$$\deg r_0(x) \leq \deg r_1(x) - 1 \leq \deg r_2(x) - 2 \leq \dots \leq \deg r_k(x) - k \leq \\ \leq \deg r_{k+1}(x) - (k+1) = \deg f_1(x) - (k+1) = (n+k) - (k+1) = n-1 < \deg f_2(x),$$

т.е.  $r_0(x) = 0$  или  $\deg r_0(x) < \deg f_2(x)$ .

Таким образом, существование многочленов  $q(x)$  и  $r(x)$  ( $= r_0(x)$ ), о которых говорится в теореме, доказано.

Для доказательства единственности предположим, что существует еще одна пара многочленов  $q_1(x)$  и  $r_1(x)$  таких, что

$$f_1(x) = q_1(x) f_2(x) + r_1(x), \quad \deg r_1(x) < \deg f_2(x).$$

Тогда

$$q(x) f_2(x) + r(x) = q_1(x) f_2(x) + r_1(x)$$

или

$$f_2(x) \{q(x) - q_1(x)\} = r_1(x) - r(x), \quad (3)$$

причем  $\deg(r_1(x) - r(x)) < \deg f_2(x)$ . Но в то же время из равенства (3) следует, что

$$f_2(x) \mid \{r_1(x) - r(x)\},$$

значит,  $r_1(x) - r(x) = 0$ , или  $r_1(x) = r(x)$ .

Тогда

$$f_2(x) \{q(x) - q_1(x)\} = 0$$

и в силу  $f_2(x) \neq 0$  и того, что  $\mathbb{A}[x]$  — кольцо без делителей нуля, получаем

$$q(x) - q_1(x) = 0 \quad \text{или} \quad q(x) = q_1(x).$$

Теорема доказана.

В результате мы получили алгоритм евклидова деления многочленов. На каждом шаге этого деления выполняется

$$f_1(x) = f_2(x)(q_k x^k + \dots + q_s x^s) + r_s(x), \quad 0 \leq s \leq k. \quad (4)$$

Пока мы не будем обсуждать вопрос, что делать, если старший коэффициент  $f_2(x)$  не обратим в кольце  $\mathbb{A}$ . Заметим только, что если  $\mathbb{A}$  является полем, то для выполнимости деления достаточно, чтобы  $f_2(x) \neq 0$ .

Если  $\alpha \in \mathbb{A}$ , то можно разделить  $f(x) \in \mathbb{A}[x]$  на  $x - \alpha$  (коэффициент при  $x$  обратим) и получить

$$f(x) = (x - \alpha)q(x) + r(x), \quad \deg r(x) < \deg(x - \alpha) = 1, \quad (5)$$

т.е.  $r(x)$  — константа из кольца  $\mathbb{A}$ .

**Определение 2.** Говорят, что  $\alpha \in \mathbb{A}$  есть *корень* многочлена  $f(x)$ , если  $f(\alpha) = 0$ .



**Теорема 2.** Пусть  $\mathbb{A}$  – коммутативное целостное кольцо,  $f(x) \in \mathbb{A}[x]$  и  $\alpha \in \mathbb{A}$ . Тогда  $\alpha$  является корнем многочлена  $f(x)$  тогда и только тогда, когда  $(x - \alpha) \mid f(x)$ .

**Доказательство.** Если  $f(\alpha) = 0$ , то из (5) следует, что  $r = 0$ , а значит,  $(x - \alpha) \mid f(x)$ .

Обратно. если  $(x - \alpha) \mid f(x)$ , то  $r = 0$ , т.е.  $f(x) = (x - \alpha)q(x)$ . При  $x = \alpha$  получаем

$$f(\alpha) = (\alpha - \alpha)q(\alpha) = 0.$$

**Следствие.** Пусть  $\mathbb{A}$  – целостное кольцо,  $f(x) \in \mathbb{A}[x]$  и  $\alpha \in \mathbb{A}$ . Тогда  $f(\alpha)$  равно остатку от деления  $f(x)$  на  $x - \alpha$ .

Действительно. из (5) получаем

$$f(\alpha) = (\alpha - \alpha)q(\alpha) + r = r.$$

**Определение 3.** Если  $\alpha$  – корень многочлена  $f(x)$  и  $f(x) = (x - \alpha)^m q(x)$ ,  $m \geq 1$ ,  $q(\alpha) \neq 0$ , то  $\alpha$  называется кратностью корня  $\alpha$ .

Если  $m = 1$ , то  $\alpha$  называется простым корнем.

**Теорема 3.** Пусть  $\mathbb{A}$  – целостное кольцо и  $f(x) \neq 0$  – многочлен из  $\mathbb{A}[x]$ . Если степень  $f(x)$  равна  $n$ , то  $f(x)$  имеет не больше  $n$  корней с учетом кратностей. Эти корни лежат в  $\mathbb{A}$  или в бесконечной области.

**Доказательство.** Пусть  $\alpha_1, \alpha_2, \dots, \alpha_s$  – различные корни многочлена  $f(x)$ , кратности их равны  $k_1, k_2, \dots, k_s$  соответственно. Докажем, что  $f(x)$  делится на

$$(x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} \dots (x - \alpha_s)^{k_s}.$$

Так как  $\alpha_1$  – корень  $f(x)$  кратности  $k_1$ , то

$$f(x) = (x - \alpha_1)^{k_1} q_1(x), \quad (6)$$

причем  $q_1(\alpha_1) \neq 0$ . Поскольку  $\alpha_2$  – корень  $f(x)$ , то из (6) получаем

$$0 = f(\alpha_2) = (\alpha_2 - \alpha_1)^{k_1} q_1(\alpha_2),$$

откуда в силу  $\alpha_2 - \alpha_1 \neq 0$  получаем  $q_1(\alpha_2) = 0$ , значит,

$$q_1(x) = (x - \alpha_2)^{k_2} q_2(x), \quad q_2(\alpha_2) \neq 0,$$

поэтому  $\alpha_2$  – корень кратности  $k_2$ . Значит,  $f(x) = (x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} q_2(x)$ .

Продолжая рассуждать таким же образом, предположим, что получено разложение

$$f(x) = (x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} \dots (x - \alpha_{s-1})^{k_{s-1}} q_{s-1}(x). \quad (7)$$

Поскольку  $\alpha_s$  – корень  $f(x)$ , то

$$0 = f(\alpha_s) = (\alpha_s - \alpha_1)^{k_1} (\alpha_s - \alpha_2)^{k_2} \dots (\alpha_s - \alpha_{s-1})^{k_{s-1}} q_{s-1}(\alpha_s),$$

и так как  $\alpha_s$  отличен от  $\alpha_1, \alpha_2, \dots, \alpha_{s-1}$ , получаем, что  $\alpha_s$  – корень многочлена  $q_{s-1}(x)$ , откуда

$$q_{s-1}(x) = (x - \alpha_s)^{k_s} q_s(x),$$

$q_s(\alpha_s) \neq 0$ .

Значит,

$$f(x) = (x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} \dots (x - \alpha_s)^{k_s} q_s(x).$$

Отсюда видно, что  $k_1 + k_2 + \dots + k_s$  не может быть больше, чем  $n = \deg f(x)$ , так как при  $k_1 + k_2 + \dots + k_s = n$  многочлен  $q_s(x)$  является константой, что и заканчивает доказательство теоремы.

Если  $\mathbb{A}$  не является целостным кольцом, то теорема 3 может не выполняться. Рассмотрим, например, кольцо  $\mathbb{Z}_8$ , которое не является целостным. Многочлен  $f(x) = x^2 - 1$  из  $\mathbb{Z}_8[x]$  имеет в  $\mathbb{Z}_8$  четыре различных корня: 1, 3, 5 и 7.



**Следствие.** Пусть  $\mathbf{A}$  – целостное кольцо и  $f(x) \in \mathbf{A}[x]$ . Если степень  $f(x)$  равна  $n$  и  $f(x)$  имеет больше, чем  $n$  корней, то  $f(x) = 0$ .

**Теорема 4.** Пусть  $\mathbf{A}$  – целостное кольцо с единицей. Если  $\mathbf{A}$  состоит из бесконечного числа элементов, то два различных многочлена  $f(x)$  и  $g(x)$  из  $\mathbf{A}[x]$  всегда определяют различные функции.

*Доказательство.* Рассмотрим многочлен

$$d(x) = f(x) - g(x).$$

Если многочлены  $f(x)$  и  $g(x)$  определяют равные функции, то для любого элемента  $x \in \mathbf{A}$  их разность должна быть равна нулю. Отсюда следует, что каждый элемент кольца  $\mathbf{A}$  является корнем многочлена  $d(x)$ , если  $\deg d(x) = n$  (конечное число!), то  $d(x)$  имеет больше, чем  $n$  корней, откуда следует, что  $d(x) = 0$ . Поэтому  $f(x) = g(x)$ .

## §2. МЕТОД ГОРНЕРА И ЕГО ПРИМЕНЕНИЕ

Рассмотрим два эффективных алгоритма, с помощью которых можно:

- (1) вычислить значение многочлена  $f(x)$  в данной точке  $x = \alpha$  и
- (2) вычислить новый многочлен  $f(y)$ , где  $y = x - \alpha$ .

Для обоих алгоритмов воспользуемся методом Горнера. Вспомним этот метод.

Пусть  $\mathbf{A}$  – коммутативное кольцо без делителей нуля (целостное) и  $f(x) \in \mathbf{A}[x]$ :

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0.$$

Пусть  $\alpha \in \mathbf{A}$ . Будем делить  $f(x)$  на  $(x - \alpha)$ , т.е. искать представление  $f(x)$  в виде

$$f(x) = (x - \alpha)q(x) + r, \tag{1}$$

где  $r \in \mathbf{A}$ , а  $\deg q(x) = n - 1$ , т.е.

$$q(x) = b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \dots + b_1 x + b_0. \tag{2}$$

Подставляя (2) в равенство (1), получаем

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = (x - \alpha)(b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \dots + b_1 x + b_0) + r. \tag{3}$$

Приравнявая коэффициенты при одинаковых степенях  $x$  из левой и правой частей равенства (3), получим

$$\begin{aligned} a_n &= b_{n-1}, \\ a_{n-1} &= b_{n-2} - \alpha b_{n-1}, \\ a_{n-2} &= b_{n-3} - \alpha b_{n-2}, \\ &\dots\dots\dots \\ a_1 &= b_0 - \alpha b_1, \\ a_0 &= r - \alpha b_0, \end{aligned}$$

$$\begin{aligned} b_{n-1} &= a_n, \\ b_{n-2} &= a_{n-1} + \alpha b_{n-1}, \\ b_{n-3} &= a_{n-2} + \alpha b_{n-2}, \\ &\dots\dots\dots \\ b_0 &= a_1 + \alpha b_1, \\ r &= a_0 + \alpha b_0 = f(\alpha). \end{aligned} \tag{4}$$

Таким образом,  $f(\alpha)$  вычисляется с помощью вложенной формулы

$$f(\alpha) = a_0 + \alpha\{a_1 + \alpha[a_2 + \dots + \alpha(a_{n-1} + \alpha a_n) \dots]\}. \tag{5}$$

Формулы (4) удобно записывать в виде таблички:

	$a_n$	$a_{n-1}$	$a_{n-2}$	$\dots$	$a_1$	$a_0$
$\alpha$	$a_n$	$b_{n-2} = \alpha a_n + a_{n-1}$	$b_{n-3} = \alpha b_{n-2} + a_{n-2}$	$\dots$	$b_0 = \alpha b_1 + a_1$	$r = \alpha b_0 + a_0$

Мы видим, что для отыскания  $f(\alpha) = r$  по формулам (4) требуется сделать  $n$  операций умножения и столько же сложений, где  $n = \deg f(x)$ . Кроме значения  $f(\alpha)$ , этот алгоритм находит коэффициенты частного – многочлена  $q(x)$ , а значит, может быть использован для быстрого деления  $f(x)$  на  $x - \alpha$ .

**Пример 1.** Вычислить значение многочлена  $f(x) = x^5 - 2x^3 + 3x^2 + x - 1$  из  $\mathbb{Z}_6[x]$  при  $x = 5$ .

Запишем наши вычисления в таблицу, учитывая, что арифметические действия проводятся в кольце  $\mathbb{Z}_6$ :

$$\begin{array}{c|cccccc} & 1 & 0 & -2 & 3 & 1 & -1 \\ \hline \alpha = 5 & 1 & 5 & 5 & 4 & 3 & 2 \end{array}$$

Итак,  $f(x) = (x - 5)(x^4 + 5x^3 + 5x^2 + 4x + 3) + 2$ , значит,  $f(5) = 2$ .

Пусть  $f(x) \in \mathbb{A}[x]$ :

$$f(x) = \sum_{i=0}^n a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0. \quad (6)$$

Требуется получить многочлен  $f(y)$ , где  $x = y + \alpha$ ,  $\alpha \in \mathbb{A}$ . Подставим в (6) вместо  $x$  выражение  $y + \alpha$ :

$$\sum_{i=0}^n a_i x^i = \sum_{i=0}^n a_i (y + \alpha)^i = \sum_{i=0}^n b_i y^i = \sum_{i=0}^n b_i (x - \alpha)^i, \quad (7)$$

где  $b_i$  ( $i = 0, 1, \dots, n$ ) – коэффициенты многочлена  $f(y)$ , которые требуется найти. Из (7) имеем

$$\sum_{i=0}^n a_i x^i = \sum_{i=0}^n b_i (x - \alpha)^i. \quad (8)$$

Правая часть равенства (8) есть многочлен вида

$$b_n (x - \alpha)^n + b_{n-1} (x - \alpha)^{n-1} + \dots + b_1 (x - \alpha) + b_0 =$$

$$= (x - \alpha) \{b_n (x - \alpha)^{n-1} + b_{n-1} (x - \alpha)^{n-2} + \dots + b_1\} + b_0 = (x - \alpha) q_{n-1}(x) + b_0,$$

где  $q_{n-1}(x) = b_n (x - \alpha)^{n-1} + b_{n-1} (x - \alpha)^{n-2} + \dots + b_1$ . Таким образом,  $b_0$  есть остаток от деления  $f(x)$  на  $x - \alpha$ .

Далее, рассмотрим  $q_{n-1}(x)$ :

$$q_{n-1}(x) = (x - \alpha) \{b_n (x - \alpha)^{n-2} + b_{n-1} (x - \alpha)^{n-3} + \dots + b_2\} + b_1 =$$

$$= (x - \alpha) q_{n-2}(x) + b_1,$$

где  $q_{n-2}(x) = b_n (x - \alpha)^{n-2} + b_{n-1} (x - \alpha)^{n-3} + \dots + b_2$ . Значит,  $b_1$  есть остаток от деления  $q_{n-1}(x)$  на  $x - \alpha$ .

Очевидно, этот процесс можно продолжать далее, получая последовательно  $b_2, b_3, \dots, b_n$ ; для этого берем частное, полученное на предыдущем шаге, делим его на  $x - \alpha$ , используя метод Горнера, получаем остаток от деления, равный очередному коэффициенту  $b_i$ , и новое частное, которое используем на следующем шаге.

**Пример 2.** Пусть дан многочлен  $f(x) = x^4 - 3x^3 + 5x^2 - 2x + 1$  из  $\mathbb{Z}[x]$ . Найдем многочлен  $f(y)$ , где  $y = x - 1$ .

Делим  $f(x)$  на  $x - 1$ , используя метод Горнера:

$$\begin{array}{c|ccccc} & 1 & -3 & 5 & -2 & 1 \\ \hline \alpha = 1 & 1 & -2 & 3 & 1 & 2 \end{array},$$

откуда  $f(x) = (x - 1)(x^3 - 2x^2 + 3x + 1) + 2$ , значит,  $b_0 = 2$ . Делим полученное частное  $q_3(x) = x^3 - 2x^2 + 3x + 1$  на  $x - 1$ :



$$\begin{array}{r|rrrr} & 1 & -2 & 3 & 1 \\ \hline \alpha = 1 & 1 & -1 & 2 & 3 \end{array},$$

откуда  $q_3(x) = (x - 1)(x^2 - x + 2) + 3$ , значит,  $b_1 = 3$ .

Частное  $q_2(x) = x^2 - x + 2$  от последнего деления делим на  $x - 1$ :

$$\begin{array}{r|rrr} & 1 & -1 & 2 \\ \hline \alpha = 1 & 1 & 0 & 2 \end{array},$$

откуда  $q_2(x) = (x - 1)x + 2$ , значит,  $b_2 = 2$ .

Полученное частное  $q_1(x) = x$  делим на  $x - 1$ :

$$q_1(x) = 1(x - 1) + 1,$$

откуда  $b_3 = 1$ .

Наконец,  $q_0(x) = 1$  и есть  $b_4$  — последний из искоемых коэффициентов. Таким образом,

$$f(y) = y^4 + y^3 + 2y^2 + 3y + 2.$$

Все проделанные нами вычисления можно записать в одну большую таблицу:

$$\begin{array}{c|ccccc} & 1 & -3 & 5 & -2 & 1 \\ \hline 1 & 1 & -2 & 3 & 1 & 2 = b_0 \\ 1 & 1 & -1 & 2 & 3 = b_1 \\ 1 & 1 & 0 & 2 = b_2 \\ 1 & 1 & 1 = b_3 \\ 1 & 1 = b_4 \end{array}.$$

**Замечание.** В случае  $\alpha = 1$  (как в нашем примере) алгоритм не требует умножений, т.е. содержит только сложения.

Если  $\alpha \neq 1$ , то для вычисления  $b_0$  требуется  $n$  операций умножения и  $n$  операций сложения, для вычисления  $b_1$  —  $(n - 1)$  умножений и  $(n - 1)$  сложений, для вычисления  $b_2$  число умножений (и сложений) равно  $(n - 2)$  и т.д. Значит, общее количество операций умножения (сложения) равно

$$n + (n - 1) + (n - 2) + \dots + 1 = \frac{n(n + 1)}{2}.$$

**Пример 3.** Дан многочлен  $f(x) = x^3 - x^2 + 2x + 1$  из  $\mathbb{Z}_3[x]$ . Найдем  $f(y)$ , где  $y = x - 2$ .

Сразу запишем наши вычисления в общую таблицу (вычисления производятся в кольце  $\mathbb{Z}_3$ ):

$$\begin{array}{c|cccc} & 1 & -1 & 2 & 1 \\ \hline 2 & 1 & 1 & 1 & 0 = b_0 \\ 2 & 1 & 0 & 1 = b_1 \\ 2 & 1 & 2 = b_2 \\ 2 & 1 = b_3 \end{array},$$

**значит,**  $f(y) = y^3 + 2y^2 + y$ .

### §3. ЕВКЛИДОВЫ КОЛЬЦА И ДЕЛИМОСТЬ МНОГОЧЛЕНОВ. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ МНОГОЧЛЕНОВ

Напомним определение евклидова кольца.

**Определение 1.** Пусть  $\mathbf{A}$  — произвольное целостное кольцо, в котором каждому ненулевому элементу  $a$  сопоставлено целое неотрицательное число  $g(a)$  такое, что:

1. если  $a \neq 0$ ,  $b \neq 0$ , то  $g(ab) \geq g(a)$ ;
2. для любых элементов  $a, b \in \mathbb{A}$ , где  $b \neq 0$  существуют элементы  $q, r \in \mathbb{A}$  такие, что

$$a = qb + r,$$

причем  $r = 0$  или  $g(r) < g(b)$ .

Кольцо, удовлетворяющее этим свойствам, называется *евклидовым*.

Функцию  $g(a)$  мы называем *нормой элемента*  $a$ .

В кольце многочленов  $K[x]$  ( $K$  — поле), которое, как мы видели, является целостным, введем норму

$$g(f(x)) = \deg f(x).$$

Очевидно, это целое неотрицательное число, удовлетворяющее требуемым свойствам евклидовой нормы. Действительно, если  $f_1(x), f_2(x) \in K[x]$ ,  $f_2(x) \neq 0$ , то

$$g(f_1(x)f_2(x)) = \deg(f_1(x)f_2(x)) = \deg f_1(x) + \deg f_2(x) \geq \deg f_1(x) = g(f_1(x)),$$

а второе свойство (евклидова делимость многочленов) следует из теоремы 1 §1 и того, что  $K$  – поле.

**Определение 2.** Пусть  $\mathbf{A}$  — целостное кольцо,  $f_1(x), f_2(x) \in \mathbf{A}[x]$  и  $f_2(x) \neq 0$ . Многочлен  $d(x) \in \mathbf{A}[x]$  называется *наибольшим общим делителем* многочленов  $f_1(x)$  и  $f_2(x)$ , если:

- (1)  $d(x)$  делит  $f_1(x)$  и  $d(x)$  делит  $f_2(x)$ ;
- (2) если  $g(x)$  делит  $f_1(x)$  и  $f_2(x)$ , то  $g(x)$  делит  $d(x)$  и  $\deg g(x) \leq \deg d(x)$ .

Наибольший общий делитель (НОД) многочленов можно найти, используя несколько раз теорему о делимости. Соответствующий процесс называется *алгоритмом Евклида для многочленов*:

[illegible]

Поскольку  $\deg f_i(x) < \deg f_{i-1}(x)$  для  $i = 3, 4, \dots, k$ , то процесс деления гарантированно закончится после  $\deg f_2(x)$  шагов.

**Теорема.** Пусть  $\mathbf{A}$  – целостное кольцо и  $f_1(x), f_2(x) \in \mathbf{A}[x]$ , причем  $f_2(x) \neq 0$ . В алгоритме Евклида (1) последний отличный от нуля остаток  $f_k(x)$  является наибольшим общим делителем многочленов  $f_1(x)$  и  $f_2(x)$ .

*Доказательство.* Достаточно проверить, что для любого  $i$  ( $i = 2, 3, \dots, k-1$ )

$$\text{НОД}(f_{i-1}(x), f_i(x)) = \text{НОД}(f_i(x), f_{i+1}(x)). \quad (2)$$

Пусть  $d(x) = \text{НОД}(f_{i-1}(x), f_i(x))$ , тогда  $d(x)$  делит  $f_{i-1}(x)$  и  $f_i(x)$ , следовательно,  $d(x)$  делит и

$$f_{i+1}(x) = f_{i-1}(x) - q_{i-1}(x)f_i(x),$$

таким образом,  $d(x)$  является общим делителем  $f_i(x)$  и  $f_{i+1}(x)$ . Если многочлен  $q(x)$  также делит  $f_i(x)$  и  $f_{i+1}(x)$ , то он делит и

$$f_{i-1}(x) = f_i(x)q_{i-1}(x) + f_{i+1}(x),$$

т.е. является общим делителем многочленов  $f_{i-1}(x)$  и  $f_i(x)$ , следовательно, должен делить их ~~наибольший~~ общий делитель  $d(x)$  и  $\deg q(x) \leq \deg d(x)$ .

Отсюда следует, что  $d(x)$  делится на любой общий делитель многочленов  $f_i(x)$  и  $f_{i+1}(x)$ , следовательно, является их наибольшим общим делителем, т.е. (2) справедливо.

Тогда из (1) имеем

$$\text{НОД}(f_1(x), f_2(x)) = \text{НОД}(f_2(x), f_3(x)) = \text{НОД}(f_3(x), f_4(x)) = \dots =$$

$$\text{НОД}(f_{k-1}(x), f_k(x)) = \text{НОД}(f_k(x), 0) = f_k(x).$$

Заметим, что если  $f_k(x) = \text{НОД}(f_1(x), f_2(x))$ , то для любого обратимого элемента  $a \in \mathbb{A}$  ~~многочлен~~  $af_k(x)$  также будет наибольшим общим делителем  $f_1(x)$  и  $f_2(x)$ , т.е. наибольший общий делитель двух многочленов определен с точностью до умножения на обратимый элемент кольца  $\mathbb{A}$ .

**Определение 3.** Говорят, что многочлены  $f(x)$  и  $g(x)$  из  $\mathbb{A}[x]$  *ассоциированы*, если они ~~отличаются~~ отличаются лишь обратимым множителем из  $\mathbb{A}$ , т.е.

$$f(x) = ag(x),$$

где  $a$  обратим в  $\mathbb{A}$ .

Очевидно, что любой многочлен ассоциирован с одним *нормированным (или унитарным)* многочленом. поэтому если  $f_k(x)$  нормирован, то можно говорить о единственности наибольшего общего делителя.

**Определение 4.** Два многочлена из  $\mathbb{A}[x]$  называются *взаимно простыми*, если любой их ~~наибольший~~ общий делитель есть обратимая в  $\mathbb{A}$  константа.

Поскольку обратимая в  $\mathbb{A}$  константа ассоциирована с 1 этого кольца, то говорят, что НОД двух ~~взаимно~~ простых многочленов есть единичный элемент кольца  $\mathbb{A}$ .

На самом деле, алгоритм Евклида в виде (1) можно провести лишь в том случае, когда на ~~каждом~~ шаге старший коэффициент делителя обратим в кольце  $\mathbb{A}$ . В противном случае деление в таком виде выполнить не удастся. Но если  $\mathbb{A}$  является полем, то трудностей такого рода не ~~возникает~~ возникает, и алгоритм Евклида в виде (1) всегда применим.



#### §4. РАСШИРЕННЫЙ АЛГОРИТМ ЕВКЛИДА ДЛЯ МНОГОЧЛЕНОВ НАД ПОЛЕМ

Пусть  $\mathbb{K}$  — поле и  $f_1(x), f_2(x) \in \mathbb{K}[x]$ , причем  $f_2(x) \neq 0$ . При помощи алгоритма Евклида легко найти  $\text{НОД}(f_1(x), f_2(x))$ , пусть это многочлен  $d(x) \in \mathbb{K}[x]$ . Очевидно, что  $d(x)$  делит любой многочлен вида

$$f_1(x)u(x) + f_2(x)v(x), \quad (1)$$

где  $u(x), v(x)$  — произвольные многочлены из  $\mathbb{K}[x]$ . Рассмотрим множество многочленов вида (1) и выясним, принадлежит ли  $d(x)$  этому множеству. На данный вопрос отвечает следующая теорема.

**Теорема 1.** Пусть  $\mathbb{K}$  — поле и  $f_1(x), f_2(x) \in \mathbb{K}[x]$ , причем  $f_2(x) \neq 0$ . Если  $d(x) = \text{НОД}(f_1(x), f_2(x))$ , то в  $\mathbb{K}[x]$  существуют многочлены  $u(x)$  и  $v(x)$  такие, что

$$f_1(x)u(x) + f_2(x)v(x) = d(x). \quad (2)$$

*Доказательство.* Из всех многочленов вида (1), не равных тождественно нулю, выберем многочлен наименьшей степени, обозначим его  $d(x)$ . Покажем, что  $d(x)$  и есть  $\text{НОД}(f_1(x), f_2(x))$ .

Сначала проверим, что  $d(x)$  делит  $f_1(x)$ . Предположим противное, тогда

$$f_1(x) = d(x)q(x) + r(x),$$

причем  $r(x) \neq 0$  и  $\deg r(x) < \deg d(x)$ . Имеем

$$\begin{aligned} r(x) &= f_1(x) - d(x)q(x) = f_1(x) - \{f_1(x)u(x) + f_2(x)v(x)\}q(x) = \\ &= f_1(x)\{1 - u(x)q(x)\} - f_2(x)v(x)q(x) = f_1(x)\tilde{u}(x) + f_2(x)\tilde{v}(x), \end{aligned}$$

где  $\tilde{u}(x) = 1 - u(x)q(x)$ ,  $\tilde{v}(x) = -v(x)q(x)$ . Значит,  $r(x)$  также имеет вид (1), он ненулевой и степень его меньше степени  $d(x)$ , что противоречит выбору многочлена  $d(x)$ . Поэтому предположение неверно и  $d(x)$  делит  $f_1(x)$ . Аналогично проверяется, что  $d(x)$  делит  $f_2(x)$ . Действительно, в предположении, что это не так, разделим  $f_2(x)$  на  $d(x)$  с остатком

$$f_2(x) = d(x)t(x) + s(x), \quad s(x) \neq 0, \quad \deg s(x) < \deg d(x).$$

Опять имеем

$$\begin{aligned} s(x) &= f_2(x) - d(x)t(x) = f_2(x) - \{f_1(x)u(x) + f_2(x)v(x)\}t(x) = \\ &= -f_1(x)u(x)t(x) + f_2(x)\{1 - v(x)t(x)\} = f_1(x)\hat{u}(x) + f_2(x)\hat{v}(x), \end{aligned}$$

где  $\hat{u}(x) = -u(x)t(x)$ ,  $\hat{v}(x) = 1 - v(x)t(x)$ .

Значит,  $s(x)$  имеет вид (1),  $s(x) \neq 0$  и  $\deg s(x) < \deg d(x)$ , что опять противоречит выбору многочлена  $d(x)$ . Следовательно,  $d(x)$  должен делить  $f_2(x)$ .

Пусть  $g(x)$  также делит  $f_1(x)$  и  $f_2(x)$ , тогда из (2) следует, что  $g(x)$  делит и  $d(x)$ . Значит, выполняются оба условия определения 2 §3 и  $d(x) = \text{НОД}(f_1(x), f_2(x))$ .

**Следствие.** Необходимым и достаточным условием того, что многочлены  $f_1(x)$  и  $f_2(x)$  из  $\mathbb{K}[x]$  взаимно просты, является существование многочленов  $u(x)$  и  $v(x)$  таких, что

$$f_1(x)u(x) + f_2(x)v(x) = 1.$$

Отметим, что многочлены  $u(x)$  и  $v(x)$  в теореме 1 определены неоднозначно. Действительно, если  $u(x), v(x)$  удовлетворяют условию (2), то ему удовлетворяют и многочлены

$$\tilde{u}(x) = u(x) - t(x)f_2(x), \quad \tilde{v}(x) = v(x) + t(x)f_1(x),$$

где  $t(x)$  — произвольный многочлен из  $\mathbb{K}[x]$ . Действительно,

$$\begin{aligned} f_1(x)\tilde{u}(x) + f_2(x)\tilde{v}(x) &= f_1(x)\{u(x) - t(x)f_2(x)\} + f_2(x)\{v(x) + t(x)f_1(x)\} = \\ &= f_1(x)u(x) - t(x)f_1(x)f_2(x) + f_2(x)v(x) + t(x)f_1(x)f_2(x) = f_1(x)u(x) + f_2(x)v(x) = d(x). \end{aligned}$$

Значит, многочлены  $u(x)$  и  $v(x)$  в принципе могут иметь сколь угодно большие степени. Однако степени их можно ограничить снизу.



Запишем полученные рекуррентные формулы с помощью матриц. Формулы (5) для  $i$  и  $i + 1$  запишем в виде

$$\begin{pmatrix} r_i(x) \\ r_{i+1}(x) \end{pmatrix} = \begin{pmatrix} u_i(x) & v_i(x) \\ u_{i+1}(x) & v_{i+1}(x) \end{pmatrix} \begin{pmatrix} f_1(x) \\ f_2(x) \end{pmatrix}, \quad (0 \leq i \leq n). \quad (7)$$

В частности, при  $i = 0, 1$  имеем

$$\begin{pmatrix} u_0(x) & v_0(x) \\ u_1(x) & v_1(x) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

значит, определитель этой матрицы равен 1.

Далее, формулы (6) можно записать в виде

$$\begin{pmatrix} u_i(x) & v_i(x) \\ u_{i+1}(x) & v_{i+1}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i(x) \end{pmatrix} \begin{pmatrix} u_{i-1}(x) & v_{i-1}(x) \\ u_i(x) & v_i(x) \end{pmatrix}.$$

Тогда

$$\begin{vmatrix} u_i(x) & v_i(x) \\ u_{i+1}(x) & v_{i+1}(x) \end{vmatrix} = \begin{vmatrix} 0 & 1 \\ 1 & -q_i(x) \end{vmatrix} \begin{vmatrix} u_{i-1}(x) & v_{i-1}(x) \\ u_i(x) & v_i(x) \end{vmatrix} = - \begin{vmatrix} u_{i-1}(x) & v_{i-1}(x) \\ u_i(x) & v_i(x) \end{vmatrix}$$

для  $i = 1, \dots, n$ . Поскольку первый из этих определителей равен 1, то получаем

$$\begin{vmatrix} u_i(x) & v_i(x) \\ u_{i+1}(x) & v_{i+1}(x) \end{vmatrix} = (-1)^i,$$

но это означает, что матрица, стоящая под знаком определителя, не вырождена, следовательно, обратима, и

$$\begin{pmatrix} u_i(x) & v_i(x) \\ u_{i+1}(x) & v_{i+1}(x) \end{pmatrix}^{-1} = (-1)^i \begin{pmatrix} v_{i+1}(x) & -v_i(x) \\ -u_{i+1}(x) & u_i(x) \end{pmatrix}. \quad (8)$$

Формула (7) при  $i = n$  принимает вид

$$\begin{pmatrix} r_n(x) \\ 0 \end{pmatrix} = \begin{pmatrix} u_n(x) & v_n(x) \\ u_{n+1}(x) & v_{n+1}(x) \end{pmatrix} \begin{pmatrix} f_1(x) \\ f_2(x) \end{pmatrix},$$

откуда в силу (8) получаем

$$\begin{pmatrix} f_1(x) \\ f_2(x) \end{pmatrix} = (-1)^n \begin{pmatrix} v_{n+1}(x) & -v_n(x) \\ -u_{n+1}(x) & u_n(x) \end{pmatrix} \begin{pmatrix} r_n(x) \\ 0 \end{pmatrix}$$

или

$$\begin{aligned} f_1(x) &= (-1)^n v_{n+1}(x) r_n(x), \\ f_2(x) &= (-1)^{n+1} u_{n+1}(x) r_n(x). \end{aligned}$$

Значит,

$$\begin{aligned} f_1(x) &= (-1)^n v_{n+1}(x) d(x), \\ f_2(x) &= (-1)^{n+1} u_{n+1}(x) d(x), \end{aligned} \quad (9)$$

где  $d(x) = \text{НОД}(f_1(x), f_2(x))$ .

Теперь оценим степени многочленов.

В алгоритме Евклида

$$\deg r_{i+1}(x) < \deg r_i(x), \quad 1 \leq i \leq n,$$

поэтому частное  $q_i(x)$  от деления остатка  $r_{i-1}(x)$  на остаток  $r_i(x)$  есть многочлен степени большей либо равной 1, т. е.  $\deg q_i(x) \geq 1$  при  $i \geq 2$ .



Из формул (6) имеем

$$\begin{aligned} u_2(x) &= u_0(x) - q_1(x)u_1(x) = 1 - q_1(x) \cdot 0 = 1, \\ u_3(x) &= u_1(x) - q_2(x)u_2(x) = 0 - q_2(x) = -q_2(x), \\ u_4(x) &= u_2(x) - q_3(x)u_3(x) = 1 + q_2(x)q_3(x), \\ &\dots \end{aligned}$$

Таким образом, степени многочленов  $u_i(x)$  растут с ростом  $i$

$$\deg u_2(x) < \deg u_3(x) < \deg u_4(x) < \dots < \deg u_n(x) < \deg u_{n+1}(x).$$

Но из формул (9) имеем

$$f_2(x) = (-1)^{n+1}u_{n+1}(x)d(x),$$

значит,

$$\deg u_{n+1}(x) \leq \deg f_2(x),$$

отсюда

$$\deg u_n(x) < \deg u_{n+1}(x) \leq \deg f_2(x).$$

Аналогично из формул (6) имеем

$$\begin{aligned} v_2(x) &= v_0(x) - q_1(x)v_1(x) = 0 - q_1(x) = -q_1(x), \\ v_3(x) &= v_1(x) - q_2(x)v_2(x) = 1 + q_1(x)q_2(x), \\ v_4(x) &= v_2(x) - q_3(x)v_3(x) = -q_1(x) - q_3(x)(1 + q_1(x)q_2(x)), \\ &\dots \end{aligned}$$

Значит, степени многочленов  $v_i(x)$  растут с ростом  $i$

$$\deg v_2(x) < \deg v_3(x) < \deg v_4(x) < \dots < \deg v_n(x) < \deg v_{n+1}(x).$$

Из (9) имеем

$$f_1(x) = (-1)^nv_{n+1}(x)d(x),$$

значит,

$$\deg v_{n+1}(x) \leq \deg f_1(x),$$

откуда

$$\deg v_n(x) < \deg v_{n+1}(x) \leq \deg f_1(x).$$

Единственность следует из единственности определения частного и остатка от деления на каждом шаге алгоритма Евклида.

**Пример 1.** Рассмотрим в  $\mathbb{R}[x]$  многочлены

$$f_1(x) = x^4 - x^3 - 5x^2 - x - 6 \quad \text{и} \quad f_2(x) = x^4 - 1$$

и найдем  $u(x), v(x)$  из  $\mathbb{R}[x]$  такие, что

$$f_1(x)u(x) + f_2(x)v(x) = \text{НОД}(f_1(x), f_2(x)).$$

Все наши вычисления можно записать в таблицу

$i$	$q_i(x)$	$u_i(x)$	$v_i(x)$	$r_i(x)$	$u_{i+1}(x)$	$v_{i+1}(x)$	$r_{i+1}(x)$
0	—	1	0	$x^4 - x^3 - 5x^2 - x - 6$	0	1	$x^4 - 1$
1	1	0	1	$x^4 - 1$	1	-1	$-x^3 - 5x^2 - x - 5$
2	$-x + 5$	1	-1	$-x^3 - 5x^2 - x - 5$	$x - 5$	$6 - x$	$24x^2 + 24$
3	$-\frac{1}{24}x - \frac{5}{24}$	$x - 5$	$6 - x$	$24x^2 + 24$			0

(Здесь мы не стали вычислять  $u_4(x)$  и  $v_4(x)$ , поскольку они нам не нужны). Итак, получаем

$$\text{НОД}(f_1(x), f_2(x)) = 24x^2 + 24,$$

причем

$$24x^2 + 24 = (x - 5)f_1(x) + (6 - x)f_2(x).$$

**Пример 2.** Пусть

$$f_1(x) = x^4 + 4x^3 + 6x^2 + 5x + 2, \quad f_2(x) = x^3 + 5x^2 + 2x + 6$$

многочлены из  $\mathbf{Z}_7[x]$ . Найдем  $u(x)$ ,  $v(x)$  из  $\mathbf{Z}_7[x]$  такие, что

$$f_1(x)u(x) + f_2(x)v(x) = \text{НОД}(f_1(x), f_2(x))$$

в  $\mathbf{Z}_7[x]$ .

Выполним деления алгоритма Евклида, учитывая, что вычисления проводятся в кольце  $\mathbf{Z}_7[x]$ :

$$\begin{aligned} f_1(x) &= (x-1)f_2(x) + (2x^2 + x + 1), \\ f_2(x) &= (4x+4)(2x^2 + x + 1) + (x+2), \\ 2x^2 + x + 1 &= (2x+4)(x+2) + 0. \end{aligned}$$

Итак,

$$x+2 = \text{НОД}(f_1(x), f_2(x))$$

в  $\mathbf{Z}_7[x]$ . Теперь найдем многочлены  $u(x)$  и  $v(x)$ :

$$\begin{aligned} u_0(x) &= 1, & v_0(x) &= 0, \\ u_1(x) &= 0, & v_1(x) &= 1, \\ u_2(x) &= 1 - 0 \cdot (x-1) = 1, & v_2(x) &= 0 - 1 \cdot (x-1) = 1-x, \\ u_3(x) &= 0 - (4x+4) \cdot 1 = -4x-4 \equiv 3x+3, & v_3(x) &= 1 - (1-x)(4x+4) \equiv 4x^2+4. \end{aligned}$$

Значит,

$$x+2 = f_1(x)(3x+3) + f_2(x)(4x^2+4)$$

в  $\mathbf{Z}_7[x]$ .

Из теоремы 2 вытекает следующее утверждение.

**Теорема 3.** Если  $f_1(x)$  и  $f_2(x)$  — взаимно простые многочлены над полем  $K$ , то существуют многочлены  $u(x)$  и  $v(x)$  над полем  $K$  такие, что

$$\deg u(x) < \deg f_2(x), \quad \deg v(x) < \deg f_1(x)$$

и

$$1 = f_1(x)u(x) + f_2(x)v(x).$$

**Теорема 4.** Пусть  $f_1(x)$  и  $f_2(x)$  — многочлены с коэффициентами в факториальном кольце  $\mathbf{A}$  с полем частных  $K$ .  $f_1(x)$  и  $f_2(x)$  взаимно просты тогда и только тогда, когда найдутся два многочлена  $u(x)$  и  $v(x)$  с коэффициентами из  $\mathbf{A}$ ,  $\deg u(x) < \deg f_2(x)$ ,  $\deg v(x) < \deg f_1(x)$ , и элемент  $\alpha \in \mathbf{A}$ ,  $\alpha \neq 0$  такие, что

$$\alpha = f_1(x)u(x) + f_2(x)v(x).$$

*Доказательство.* Если  $f_1(x)$  и  $f_2(x)$  взаимно простые многочлены из  $\mathbf{A}[x]$ , то они взаимно просты и в  $K[x]$ . Тогда по теореме 3 найдутся такие  $u(x), v(x) \in K[x]$ , что

$$1 = f_1(x)u(x) + f_2(x)v(x), \tag{10}$$

$$\deg u(x) < \deg f_2(x), \quad \deg v(x) < \deg f_1(x).$$

Коэффициенты  $u(x), v(x)$  принадлежат полю  $K$ . Умножая (10) на общий знаменатель всех коэффициентов многочленов  $u(x)$  и  $v(x)$ , получим

$$\alpha = f_1(x)\tilde{u}(x) + f_2(x)\tilde{v}(x),$$

где  $\tilde{u}(x), \tilde{v}(x) \in \mathbf{A}[x]$ . Умножение на константу, очевидно, не меняет степеней многочленов, поэтому соотношения

$$\deg \tilde{u}(x) < \deg f_2(x), \quad \deg \tilde{v}(x) < \deg f_1(x)$$

сохраняются.

Оценим сложность алгоритма Евклида в  $K[x]$ .



**Лемма.** Если  $n$  — число делений, необходимых для получения НОД  $(f(x), g(x))$  ( $\deg g(x) \leq \deg f(x)$ ), то

$$n \leq 1 + \deg g(x).$$

**Доказательство.** Если  $\{r_i(x)\}_{0 \leq i \leq n+1}$  — последовательность остатков в алгоритме Евклида, примененном к многочленам  $f(x)$  и  $g(x)$ , где

$$r_0(x) = f(x), \quad r_1(x) = g(x), \quad r_{n+1}(x) = 0, \quad r_n(x) \neq 0,$$

то

$$0 \leq \deg r_n(x) < \deg r_{n-1}(x) < \dots < \deg r_1(x) = \deg g(x).$$

На каждом шаге алгоритма Евклида степень остатка уменьшается не менее, чем на единицу, следовательно,

$$n - 1 \leq \deg g(x),$$

откуда

$$n \leq 1 + \deg g(x).$$

Полученная в лемме оценка является наилучшей возможной. Можно указать такие многочлены  $f(x)$  и  $g(x)$ , что  $\deg f(x) = n$ ,  $\deg g(x) = n - 1$ , для нахождения наибольшего общего делителя которых требуется ровно  $n$  делений алгоритма Евклида.

Чтобы построить  $f(x)$  и  $g(x)$ , рассмотрим последовательность многочленов  $\{f_i(x)\}_{i \geq 0}$ :

$$\begin{aligned} f_0(x) &= 1, \\ f_1(x) &= x + 1, \\ f_{i+2}(x) &= x f_{i+1}(x) + f_i(x), \quad i \geq 0. \end{aligned}$$

Таким образом,

$$\begin{aligned} f_2(x) &= x(x + 1) + 1 = x^2 + x + 1, \\ f_3(x) &= x(x^2 + x + 1) + (x + 1) = x^3 + x^2 + 2x + 1, \\ f_4(x) &= x(x^3 + x^2 + 2x + 1) + (x^2 + x + 1) = x^4 + x^3 + 3x^2 + 2x + 1, \\ &\dots \end{aligned}$$

Тогда положим  $f(x) = f_n(x)$ ,  $g(x) = f_{n-1}(x)$  и применим к  $f(x)$  и  $g(x)$  алгоритм Евклида:

$$\begin{aligned} f_n(x) &= x f_{n-1}(x) + f_{n-2}(x), \\ f_{n-1}(x) &= x f_{n-2}(x) + f_{n-3}(x), \\ &\dots \\ f_3(x) &= x f_2(x) + f_1(x), \\ f_2(x) &= x f_1(x) + f_0(x), \\ f_1(x) &= f_1(x) f_0(x). \end{aligned}$$

Итак, алгоритм Евклида потребует ровно  $n$  делений.

На самом деле алгоритм Евклида по числу делений является наилучшим среди всех аналогичных алгоритмов нахождения наибольшего общего делителя двух многочленов.

**Определение.** Пусть  $\mathbb{A}$  — коммутативное кольцо с единицей. Квазиалгоритм на  $\mathbb{A}$  есть отображение  $\varphi$  множества  $\mathbb{A} \times \mathbb{A}$  во вполне упорядоченное множество, обладающее следующим свойством:

для любой пары  $(a, b) \in \mathbb{A} \times \mathbb{A} \setminus \{0\}$  найдется пара  $(q, r) \in \mathbb{A} \times \mathbb{A}$  такая, что

$$a = bq + r \quad \text{и} \quad \varphi(b, r) < \varphi(a, b). \quad (10)$$

Равенство (10) называется *квазиевклидовым* делением  $a$  на  $b$ .

Пусть

$$\mu : K[x] \times K[x] \rightarrow \mathbb{N}$$

– минимальный квазиалгоритм, причем  $\mu$  ставит в соответствие паре многочленов  $f(x), g(x)$  количество квазиевклидовых делений вычисления их наибольшего общего делителя.

Пусть  $\varphi$  – функция, ставящая в соответствие паре многочленов количество делений алгоритма Евклида. Докажем равенство

$$\mu(f, g) = \varphi(f, g). \quad (11)$$

Равенство (11) будем доказывать индукцией по значениям  $\mu(f, g)$ .

Если  $\mu(f, g) = 1$ , т.е. требуется одно квазиевклидово деление, то это означает, что

$$f(x) = g(x)q(x) + 0,$$

т.е.

$$g(x) = \text{НОД}(f(x), g(x)).$$

Очевидно, что в этом случае евклидово деление также одно, значит,  $\varphi(f, g) = 1$ . Итак, в этом случае равенство (11) выполняется.

Предположим, что для  $\mu(f, g) < n$  выполняется равенство (11). Пусть  $\mu(f, g) = n$ . Запишем оптимальное деление в виде

$$f(x) = g(x)q(x) + r(x),$$

а евклидово деление – в виде

$$f(x) = g(x)q_1(x) + r_1(x), \quad \text{где } \deg r_1(x) < \deg g(x).$$

Тогда, очевидно,

$$\begin{aligned} \mu(f, g) &= \mu(g, r) + 1, \\ \varphi(f, g) &= \varphi(g, r_1) + 1. \end{aligned}$$

Покажем, что  $\deg r(x) < \deg g(x)$ , если  $\mu$  – минимальный квазиалгоритм. Предположим, что это неравенство не выполняется. Пусть

$$\deg r(x) > \deg g(x).$$

Тогда следующие евклидовы деления выглядят так:

$$\begin{aligned} g(x) &= 0 \cdot r(x) + g(x), \\ r(x) &= g(x)Q(x) + R(x), \quad \deg R(x) < \deg g(x). \end{aligned} \quad (12)$$

Причем

$$r(x) = f(x) - g(x)q(x) = g(x)q_1(x) + r_1(x) - g(x)q(x) = (q_1(x) - q(x))g(x) + r_1(x),$$

т.е.

$$Q(x) = q_1(x) - q(x), \quad \text{а} \quad R(x) = r_1(x).$$

Так как  $\mu(f, g) < n$ , то по предположению индукции

$$\mu(g, r) = \varphi(g, r),$$

поэтому получаем

$$\mu(f, g) = \mu(g, r) + 1 = \varphi(g, r) + 1.$$

Но из (12) получаем

$$\begin{aligned} \varphi(g, r) &= \varphi(r, g) + 1 \\ \varphi(r, g) &= \varphi(g, r_1) + 1, \end{aligned}$$

значит,

$$\mu(f, g) = \varphi(g, r) + 1 = \varphi(r, g) + 2 = \varphi(g, r_1) + 3 = \varphi(f, g) + 2.$$

Итак,

$$\mu(f, g) = \varphi(f, g) + 2,$$

что противоречит оптимальности квазиалгоритма  $\mu$ . Значит,

$$\deg r(x) \leq \deg g(x).$$

Покажем, что равенство степеней  $r(x)$  и  $g(x)$  также невозможно.

Предположим противное, пусть

$$\deg r(x) = \deg g(x).$$

Тогда

$$\deg r_1(x) < \deg r(x),$$

значит,

$$\deg (r_1(x) - r(x)) = \deg r(x).$$

Из равенства

$$g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x)$$

получаем

$$g(x)(q(x) - q_1(x)) = r_1(x) - r(x), \quad (13)$$

следовательно,

$$\deg (r_1(x) - r(x)) = \deg r(x) = \deg g(x) = \deg \{g(x)(q(x) - q_1(x))\}.$$

Значит,

$$q(x) - q_1(x) = \text{const} \neq 0.$$

Обозначим эту константу  $\frac{1}{k}$ , тогда (13) можно переписать в виде

$$g(x) = k(r_1(x) - r(x))$$

или

$$g(x) = -kr(x) + kr_1(x), \quad \text{причем} \quad \deg kr_1(x) < \deg r(x), \quad (14)$$

т.е. (14) является евклидовым делением многочлена  $g(x)$  на  $r(x)$ .

Теперь имеем

$$\mu(f, g) = \mu(g, r) + 1 = \varphi(g, r) + 1 = \varphi(r, kr_1) + 2. \quad (15)$$

Умножение на числовые множители не меняет числа евклидовых делений многочленов, поэтому

$$\varphi(r, kr_1) = \varphi(-kr, r_1).$$

Кроме того, из

$$g(x) \equiv kr(x) \pmod{r_1(x)}$$

следует

$$\varphi(-kr, r_1) = \varphi(g, r),$$

поэтому (15) можно продолжить

$$\varphi(r, kr_1) + 2 = \varphi(-kr, r_1) + 2 = \varphi(g, r_1) + 2 = \varphi(f, g) + 1.$$

В результате получаем

$$\mu(f, g) = \varphi(f, g) + 1,$$

что противоречит оптимальности квазиалгоритма  $\mu$ .

Итак, единственно возможный случай:

$$\deg r(x) < \deg g(x).$$

Но тогда в силу единственности деления Евклида  $r(x) = r_1(x)$ , значит, квазиалгоритм  $\mu$  совпадает с алгоритмом Евклида  $\varphi$ . Таким образом, доказана следующая теорема.

**Теорема Лазара.** Евклидов алгоритм вычисления наибольшего общего делителя двух многочленов  $f(x), g(x) \in K[x]$  ( $K$  — поле) является оптимальным по числу делений.



## §5. ИНТЕРПОЛЯЦИЯ НАД ПОЛЕМ

Пусть  $K$  – поле. Рассмотрим множество  $n + 1$  наборов

$$(a_i, b_i) \in K \times K, \quad i = 0, 1, 2, \dots, n,$$

где  $a_i$  – все различны. Задача интерполяции состоит в том, чтобы найти многочлен  $f(x) \in K[x]$  такой, что

$$f(a_i) = b_i, \quad i = 0, 1, \dots, n.$$

Здесь мы обсудим два способа решения задачи интерполяции. Начнем с интерполяции Лагранжа.

**Теорема 1.** Пусть  $(a_i, b_i) \in K \times K$ ,  $i = 0, 1, \dots, n$ , где  $K$  – поле,  $a_i$  – различны. Тогда существует единственный многочлен  $f(x) \in K[x]$  степени не большей  $n$  такой, что  $f(a_i) = b_i$  для всех  $i = 0, 1, \dots, n$ .

*Доказательство.* Для доказательства существования такого многочлена воспользуемся интерполяционной формулой Лагранжа

$$f(x) = \sum_{i=0}^n b_i L_i(x), \quad (1)$$

где

$$L_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^n \frac{(x - a_j)}{(a_i - a_j)} = \frac{(x - a_0)(x - a_1) \dots (x - a_{i-1})(x - a_{i+1}) \dots (x - a_n)}{(a_i - a_0)(a_i - a_1) \dots (a_i - a_{i-1})(a_i - a_{i+1}) \dots (a_i - a_n)}. \quad (2)$$

Очевидно,  $L_i(a_j) = 0$  при  $i \neq j$ , так как в числителе (2) встретится сомножитель  $(a_j - a_j)$ , а  $L_i(a_i) = 1$ . Значит,

$$f(a_i) = b_i L_i(a_i) = b_i \quad (i = 0, 1, \dots, n).$$

Кроме того, по построению  $\deg f(x) \leq n$ , так как  $\deg L_i(x) \leq n$  для всех  $i = 0, 1, \dots, n$ .

Теперь докажем единственность. Предположим, что существует другой многочлен  $g(x) \in K[x]$  такой, что  $g(a_i) = b_i$ ,  $i = 0, 1, \dots, n$ . Рассмотрим многочлен  $d(x) = f(x) - g(x)$ , его степень не превосходит  $n$ , так как  $\deg f(x) \leq n$ ,  $\deg g(x) \leq n$ . В то же время

$$d(a_i) = f(a_i) - g(a_i) = b_i - b_i = 0 \quad i = 0, 1, \dots, n,$$

т.е. он имеет  $n + 1$  различных корней. По следствию из теоремы 3 § 1 получаем, что  $d(x) = 0$ , откуда  $f(x) = g(x)$ . Теорема доказана.

**Пример 1.** Найти  $f(x) \in \mathbb{Z}_7[x]$  такой, что

$$f(0) = 3, \quad f(1) = 2, \quad f(2) = 5, \quad f(3) = 4.$$

Построим сначала многочлены  $L_i(x)$  ( $i = 0, 1, 2, 3$ ) по формулам (2):

$$L_0(x) = \frac{(x-1)(x-2)(x-3)}{(0-1)(0-2)(0-3)} = (-6)^{-1}(x-1)(x-2)(x-3) \equiv -6(x^3 - 6x^2 + 4x - 6) \equiv x^3 + x^2 + 4x + 1,$$

$$L_1(x) = \frac{x(x-2)(x-3)}{(1-0)(1-2)(1-3)} = 2^{-1}x(x-2)(x-3) \equiv 4(x^3 - 5x^2 + 6x) \equiv 4x^3 + x^2 + 3x,$$

$$L_2(x) = \frac{x(x-1)(x-3)}{(2-0)(2-1)(2-3)} = (-2)^{-1}x(x-1)(x-3) \equiv -4(x^3 - 4x^2 + 3x) \equiv -4x^3 + 2x^2 + 2x,$$

$$L_3(x) = \frac{x(x-1)(x-2)}{(3-0)(3-1)(3-2)} = 6^{-1}x(x-1)(x-2) \equiv 6(x^3 - 3x^2 + 2x) \equiv 6x^3 - 4x^2 - 2x,$$

в силу  $6^{-1} \equiv 6 \pmod{7}$ ,  $2^{-1} \equiv 4 \pmod{7}$  и того, что все вычисления проводятся в кольце  $\mathbb{Z}_7$ .

По формуле (1) получаем

$$\begin{aligned} f(x) &= 3L_0(x) + 2L_1(x) + 5L_2(x) + 4L_3(x) = 3(x^3 + x^2 + 4x + 1) + 2(4x^3 + x^2 + 3x) + \\ &+ 5(-4x^3 + 2x^2 + 2x) + 4(6x^3 - 4x^2 - 2x) = (3x^3 + 3x^2 + 5x + 3) + (x^3 + 2x^2 + 6x) + \\ &+ (x^3 + 3x^2 + 3x) + (3x^3 - 2x^2 - x) \equiv x^3 + 6x^2 + 6x + 3 \pmod{7}. \end{aligned}$$

Проверка:  $f(0) = 3$ ,  $f(1) = 2$ ,  $f(2) = 5$ ,  $f(3) = 4$  в  $\mathbb{Z}_7$ .

Теперь решим задачу интерполяции с помощью китайской теоремы об остатках.

Так как

$$f(x) = (x - \alpha)q(x) + f(\alpha) \quad \text{для любого} \quad \alpha \in K,$$

то

$$(x - \alpha) \mid (f(x) - f(\alpha)),$$

а следовательно,

$$f(\alpha) = \beta \text{ тогда и только тогда, когда } f(x) \equiv \beta \pmod{(x - \alpha)}.$$

Если на  $\beta$  смотреть как на многочлен – константу, то мы ввели в кольцо  $K[x]$  отношение сравнимости по модулю многочлена. Сравнимость по модулю многочлена  $m(x)$  обладает свойствами, аналогичными свойствам сравнимости по модулю целого числа. Все утверждения относительно сравнимости, полученные для целых чисел, остаются справедливыми для сравнимости по модулю  $m(x)$ .

Теперь задачу интерполяции можно сформулировать в виде:

найти многочлен  $f(x) \in K[x]$  такой, что

$$f(x) \equiv b_i \pmod{(x - a_i)}, \quad i = 0, 1, \dots, n, \quad (3)$$

где  $a_i$  – различные элементы поля  $K$ .

Так как  $a_i$  различны, то многочлены  $x - a_i$ ,  $i = 0, 1, \dots, n$ , различны; следовательно, они попарно взаимно простые. На самом деле мы получаем частный случай китайской теоремы об остатках для многочленов над кольцом  $K[x]$  (см. § 8).

**Теорема 2.** Пусть  $K$  – поле,  $f(x) \in K[x]$ ,  $a \in K$ . Тогда

1.  $f(x) \pmod{(x - a)} \equiv f(a)$ ;
2. если  $f(a) \neq 0$ , то  $f^{-1}(x) \pmod{(x - a)} \equiv f^{-1}(a)$ .

**Доказательство.** Первое утверждение, очевидно, следует из того, что

$$f(x) = (x - a)q(x) + f(a).$$

**Докажем** второе утверждение. Требуется найти единственный многочлен  $v(x) \in K[x]$  такой, что

$$f(x)v(x) \equiv 1 \pmod{(x - a)}. \quad (4)$$

Так как  $\deg v(x) < \deg(x - a) = 1$ , то  $v(x)$  – константа из поля  $K$ .

Поскольку

$$f(x)f^{-1}(a) \equiv \{f(x) \pmod{(x - a)}\}f^{-1}(a) \pmod{(x - a)} \equiv f(a)f^{-1}(a) = 1,$$

$$v(x) \equiv f^{-1}(a) \pmod{(x - a)}.$$

Будем искать  $f(x)$  – решение системы сравнений (3) в виде

$$f(x) = q_0 + q_1(x - a_0) + q_2(x - a_0)(x - a_1) + \dots + q_n(x - a_0)(x - a_1) \dots (x - a_{n-1}). \quad (5)$$

Построим последовательность многочленов  $\{f_i(x)\}_{0 \leq i \leq n}$  таких, что

$$f_i(a_j) = b_j, \quad 0 \leq j \leq i, \tag{6}$$

тогда  $f_n(x)$  удовлетворяет условиям  $f_n(a_j) = b_j, \quad 0 \leq j \leq n$ , т. е. является искомым многочленом  $f(x)$ .

Введем также последовательность многочленов  $\{m_i(x)\}_{0 \leq i \leq n}$  такую, что

$$\begin{aligned} m_0(x) &= 1, \\ m_i(x) &= (x - a_0)(x - a_1) \dots (x - a_{i-1}), \quad 1 \leq i \leq n, \end{aligned} \tag{7}$$

тогда (5) перепишется в виде

$$f(x) = q_0 m_0(x) + q_1 m_1(x) + q_2 m_2(x) + \dots + q_n m_n(x).$$

Последовательность  $\{f_i(x)\}_{0 \leq i \leq n}$  можно теперь строить следующим образом:

$$\begin{aligned} f_0(x) &= b_0, \\ f_i(x) &= f_{i-1}(x) + q_i m_i(x), \quad 1 \leq i \leq n. \end{aligned} \tag{8}$$

Имеем

$$\begin{aligned} b_0 &= f(a_0) = f_0(x) \quad (= q_0), \\ b_1 &= f(a_1) = f_0(a_1) + q_1 m_1(a_1), \\ b_2 &= f(a_2) = f_1(a_2) + q_2 m_2(a_2), \\ &\dots\dots\dots \\ b_n &= f(a_n) = f_{n-1}(a_n) + q_n m_n(a_n), \end{aligned}$$

откуда

$$\begin{aligned} q_0 &= b_0, \\ q_1 &= \{b_1 - f_0(a_1)\} \{m_1(a_1)\}^{-1}, \\ q_2 &= \{b_2 - f_1(a_2)\} \{m_2(a_2)\}^{-1}, \\ &\dots\dots\dots \\ q_n &= \{b_n - f_{n-1}(a_n)\} \{m_n(a_n)\}^{-1}, \end{aligned}$$

т. е.

$$\begin{aligned} q_0 &= b_0, \\ q_i &= \{b_i - f_{i-1}(a_i)\} \{m_i(a_i)\}^{-1}, \quad 1 \leq i \leq n. \end{aligned} \tag{9}$$

В результате получаем алгоритм решения задачи интерполяции с использованием формул (7), (8) и (9), который можно для наглядности записать в виде следующей таблицы:

$a_i$	$b_i$	$m_i(x)$	$b_i - f_{i-1}(a_i) = d_i$	$c_i = \{m_i(a_i)\}^{-1}$	$q_i = c_i d_i$	$f_i(x)$
$a_0$	$b_0$	1	—	—	$b_0$	$f_0(x) = b_0$
$a_1$	$b_1$	$x - a_0$	$b_1 - f_0(a_1)$	$\{m_1(a_1)\}^{-1}$	$q_1$	$f_0(x) + q_1 m_1(x)$
$a_2$	$b_2$	$(x - a_0)(x - a_1)$	$b_2 - f_1(a_2)$	$\{m_2(a_2)\}^{-1}$	$q_2$	$f_1(x) + q_2 m_2(x)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$a_n$	$b_n$	$(x - a_0) \dots (x - a_{n-1})$	$b_n - f_{n-1}(a_n)$	$\{m_n(a_n)\}^{-1}$	$q_n$	$f_{n-1}(x) + q_n m_n(x)$

**Пример 2.** Построить многочлен  $f(x) \in \mathbb{Z}_7[x]$  такой, что

$$f(0) = 3, \quad f(1) = 2, \quad f(2) = 5, \quad f(4) = 4.$$

Запишем наши вычисления в таблицу (вычисления проводятся в  $\mathbb{Z}_7$ ) :

$i$	$a_i$	$b_i$	$m_i(x)$	$d_i$	$c_i$	$q_i$	$f_i(x)$
0	0	3	1	—	—	3	3
1	1	2	$x$	6	1	6	$3 + 6x$
2	2	5	$x(x - 1)$	4	4	2	$3 + 6x + 2(x^2 - x)$
3	3	4	$x(x - 1)(x - 2)$	6	6	1	$3 + 4x + 2x^2 + x(x - 1)(x - 2).$

Таким образом,

$$f(x) = 3 + 4x + 2x^2 + x^3 - 3x^2 + 2x = x^3 - x^2 + 6x + 3 \equiv x^3 + 6x^2 + 6x + 3 \pmod{7}.$$

**Пример 3.** Построить многочлен  $f(x) \in \mathbb{Q}[x]$  такой, что

$$f(-1) = -2, \quad f(1) = -2, \quad f(2) = 10, \quad f(3) = 38.$$

Получим следующую таблицу:

$i$	$a_i$	$b_i$	$m_i(x)$	$d_i$	$c_i$	$q_i$	$f_i(x)$
0	-1	-2	1	—	—	-2	-2
1	1	-2	$x + 1$	0	1/2	0	-2
2	2	10	$(x + 1)(x - 1)$	12	1/3	4	$-2 + 4(x^2 - 1)$
3	3	38	$(x + 1)(x - 1)(x - 2)$	8	1/8	1	$4x^2 - 6 + (x + 1)(x - 1)(x - 2),$

Итак,

$$f(x) = 4x^2 - 6 + (x^2 - 1)(x - 2) = x^3 + 2x^2 - x - 4.$$



## §6. ФАКТОРКОЛЬЦО $K[x]/(m(x))$

Нам потребуется несколько определений.

**Определение 1.** Пусть  $\mathbf{A}$  – целостное кольцо. Многочлен  $v(x)$  кольца  $\mathbf{A}[x]$ ,  $v(x) \neq 0$ , называется *обратимым*, если существует такой многочлен  $u(x)$ , что

$$v(x)u(x) = 1 \quad \text{в} \quad \mathbf{A}[x].$$

**Определение 2.** Пусть  $\mathbf{A}$  – целостное кольцо. Многочлен  $f(x) \in \mathbf{A}[x]$  называется *простым*, если из условия

$$f(x) = f_1(x)f_2(x)$$

следует, что либо  $f_1(x)$ , либо  $f_2(x)$  является обратимым в  $\mathbf{A}[x]$ .

**Определение 3.** Пусть  $\mathbf{A}$  – целостное кольцо. Многочлен  $f(x) \in \mathbf{A}[x]$  называется *неприводимым*, если из

$$f(x) = f_1(x)f_2(x)$$

следует, что либо  $f_1(x)$ , либо  $f_2(x)$  является многочленом нулевой степени, т.е. константой кольца  $\mathbf{A}$ .

Очевидно, что всякий простой многочлен неприводим. Обратное утверждение в общем случае неверно. Но если  $\mathbf{A}$  является полем, то все обратимые многочлены являются многочленами нулевой степени, т.е. константами, значит, для того чтобы  $f(x)$  был простым, необходимо, чтобы хотя бы один из многочленов  $f_1(x)$ ,  $f_2(x)$  был константой, т.е. над полем понятия простого и неприводимого многочлена совпадают.

### Примеры.

1. Многочлен  $2x^2 + 2$  неприводим над полем  $\mathbb{R}$ .

2. Многочлен  $2x^2 + 2$  неприводим над кольцом  $\mathbb{Z}$ , но простым над  $\mathbb{Z}$  не является, так как  $2x^2 + 2 = 2(x^2 + 1)$ , но ни 2, ни  $x^2 + 1$  не являются обратимыми в кольце  $\mathbb{Z}[x]$ .

3. Многочлен  $x^2 + 1$  неприводим над полями  $\mathbb{R}$ ,  $\mathbb{Q}$  и над кольцом  $\mathbb{Z}$ . Над полем  $\mathbb{C}$  он приводим:  $x^2 + 1 = (x - i)(x + i)$ .

4. Многочлен  $2x^2 + 4x + 6$  неприводим над полем  $\mathbb{Z}_7$ , он является простым над  $\mathbb{Z}_7$ , так как  $2x^2 + 4x + 6 = 2(x^2 + 2x + 3)$  и 2 – обратимо в  $\mathbb{Z}_7$  ( $2^{-1} \equiv 4 \pmod{7}$ ).

Пусть  $K$  – поле. Точно так же, как определялось отношение сравнимости по модулю целого числа в  $\mathbb{Z}$ , можно определить отношение сравнимости по модулю некоторого многочлена в кольце  $K[x]$ .

Пусть

$$m(x) = x^n + m_{n-1}x^{n-1} + \dots + m_1x + m_0$$

– нормированный многочлен в  $K[x]$  степени  $n > 0$ . Для любого многочлена  $f(x) \in K[x]$ , поделив его на  $m(x)$ , получим

$$f(x) = m(x)q(x) + r(x), \quad \deg r(x) < \deg m(x).$$

Остаток  $r(x)$  назовем *вычетом* многочлена  $f(x)$  по модулю многочлена  $m(x)$ , т.е.

$$r(x) \equiv f(x) \pmod{m(x)}.$$

Если  $f(x) \equiv 0 \pmod{m(x)}$ , то  $f(x) = m(x)q(x)$ , т.е.  $m(x) \mid f(x)$ .

Определим *отношение эквивалентности по модулю  $m(x)$*  в кольце  $K[x]$  следующим образом:

$f_1(x) \equiv f_2(x) \pmod{m(x)}$  тогда и только тогда, когда

$$m(x) \mid \{f_1(x) - f_2(x)\}.$$



Нетрудно проверить, что это действительно отношение эквивалентности в кольце  $K[x]$ . Свойство рефлексивности очевидно, так как

$$m(x) \mid \{f(x) - f(x)\}$$

для любого  $f(x) \in K[x]$ , значит,  $f(x) \equiv f(x) \pmod{m(x)}$ .

Далее, если

$$m(x) \mid \{f_1(x) - f_2(x)\}, \quad \text{то} \quad m(x) \mid \{f_2(x) - f_1(x)\},$$

т.е. из  $f_1(x) \equiv f_2(x) \pmod{m(x)}$  следует  $f_2(x) \equiv f_1(x) \pmod{m(x)}$ , значит, выполнено свойство симметричности.

Осталось проверить свойство транзитивности. Если

$$f_1(x) \equiv f_2(x) \pmod{m(x)} \quad \text{и} \quad f_2(x) \equiv f_3(x) \pmod{m(x)},$$

то  $m(x) \mid \{f_1(x) - f_2(x)\}$  и  $m(x) \mid \{f_2(x) - f_3(x)\}$ . Но тогда

$$m(x) \mid \{(f_1(x) - f_2(x)) + (f_2(x) - f_3(x))\}$$

т.е.

$$m(x) \mid \{f_1(x) - f_3(x)\},$$

т.е.  $f_1(x) \equiv f_3(x) \pmod{m(x)}$ .

Определим факторкольцо  $K[x]/(m(x))$  как множество классов эквивалентности (или классов вычетов) по модулю многочлена  $m(x)$ . К одному классу относятся все те многочлены из кольца  $K[x]$ , которые сравнимы по модулю  $m(x)$ . Обозначать класс, которому принадлежит многочлен  $f(x)$ , будем  $[f(x)]_{m(x)}$ . В каждом классе эквивалентности по модулю  $m(x)$  имеется единственный представитель — многочлен, степень которого меньше степени многочлена  $m(x)$ , обозначим его  $r_{m(x)}[f(x)]$ , тогда класс эквивалентности состоит из многочленов

$$r_{m(x)}[f(x)] + m(x)g(x),$$

где  $g(x)$  — произвольный многочлен из  $K[x]$ .

Сложение и умножение классов определим формулами:

$$[f_1(x)]_{m(x)} + [f_2(x)]_{m(x)} = [f_1(x) + f_2(x)]_{m(x)},$$

$$[f_1(x)]_{m(x)} \cdot [f_2(x)]_{m(x)} = [f_1(x) \cdot f_2(x)]_{m(x)}.$$

Т.е. берутся представители соответствующих классов, над которыми проводится операция сложения или умножения, затем в качестве результата берется класс, которому принадлежит полученный многочлен.

Нетрудно проверить, что эти две операции превращают множество  $K[x]/(m(x))$  в кольцо. При этом поле  $K$  можно рассматривать как подмножество кольца  $K[x]/(m(x))$ , отождествляя  $a \in K$  с  $[a]_{m(x)}$ . Если  $[a]_{m(x)} = [b]_{m(x)}$ , т.е.  $a \pmod{m(x)} \equiv b \pmod{m(x)}$ , то

$$m(x) \mid a - b,$$

но  $\deg m(x) \geq 1$ , а  $\deg(a - b) = 0$ , значит,  $a - b = 0$ , откуда  $a = b$  в  $K$ . Значит, функция, отображающая  $a$  из  $K$  на  $[a]_{m(x)}$  из  $K[x]/(m(x))$ , взаимно однозначна, и мы можем отождествлять  $a \in K$  с  $[a]_{m(x)}$ .

В  $K[x]/(m(x))$  рассмотрим следующие классы эквивалентности:

$$[1]_{m(x)}, [x]_{m(x)}, [x^2]_{m(x)}, \dots, [x^{n-1}]_{m(x)},$$

которые для краткости записи обозначим соответственно

$$\bar{1}, \bar{x}, \bar{x^2}, \dots, \bar{x^{n-1}}.$$

(Представителями этих классов, имеющими наименьшую степень, являются соответственно многочлены  $1, x, x^2, \dots, x^{n-1}$ .)

Тогда каждый элемент кольца  $K[x]/(m(x))$  имеет вид

$$\overline{f(x)} = [f(x)]_{m(x)} = r_{m(x)}[f(x)] + m(x)q(x) \equiv c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1} \pmod{m(x)} =$$

$$c_0\bar{1} + c_1\bar{x} + c_2\overline{x^2} + \dots + c_{n-1}\overline{x^{n-1}},$$

где  $c_i \in K$  ( $i = 0, 1, \dots, n-1$ ).

Обратно, любой элемент вида

$$d_0\bar{1} + d_1\bar{x} + d_2\overline{x^2} + \dots + d_{n-1}\overline{x^{n-1}} \equiv d_0 + d_1x + d_2x^2 + \dots + d_{n-1}x^{n-1} \pmod{m(x)},$$

где  $d_i \in K$  ( $i = 0, 1, \dots, n-1$ ), очевидно, принадлежит факторкольцу  $K[x]/(m(x))$ .

Обозначим через  $\alpha$  класс  $[x]_{m(x)} = \bar{x}$ . Тогда каждый элемент нашего факторкольца имеет вид

$$c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_{n-1}\alpha^{n-1},$$

где  $c_i \in K$  ( $i = 0, 1, \dots, n-1$ ). Поэтому можно представлять элементы факторкольца  $K[x]/(m(x))$  как многочлены кольца  $K[x]$ , вычисленные в точке  $\alpha = \bar{x}$ , причем  $m(\alpha) = 0$ , так как  $m(\alpha) = [m(x)]_{m(x)} = [0]_{m(x)}$ . Факторкольцо  $K[x]/(m(x))$  также теперь можно обозначать  $K[\alpha]$ .

**Пример 1.** Пусть  $K = \mathbb{R}$ . Нормированный многочлен  $m(x) = x^2 + 1$  неприводим в кольце  $\mathbb{R}[x]$ . Каждый элемент факторкольца  $\mathbb{R}[x]/(x^2 + 1)$  имеет вид

$$a + b\bar{x}, \quad a, b \in \mathbb{R}, \quad \bar{x} = [x]_{m(x)=x^2+1}.$$

Заметим, что

$$\bar{x} \cdot \bar{x} \equiv x^2 \pmod{(x^2 + 1)} \equiv -1,$$

поэтому естественно ввести обозначение

$$i = \bar{x} = [x]_{x^2+1}.$$

Тогда операции сложения и умножения выполняются следующим образом:

$$(a + b\bar{x}) + (c + d\bar{x}) = (a + c) + (b + d)\bar{x},$$

$$(a + b\bar{x})(c + d\bar{x}) = ac + ad\bar{x} + bc\bar{x} + bd\overline{x^2} = (ac - bd) + (ad + bc)\bar{x},$$

т.е. точно так же, как они проводятся в поле  $\mathbb{C}$ :

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Более того,  $\mathbb{R}[x]/(x^2 + 1)$  является полем, так как если  $a \neq 0$  или  $b \neq 0$  (т.е.  $a + b\bar{x}$  — ненулевой элемент факторкольца), то

$$(a + b\bar{x}) \cdot \left( \frac{a - b\bar{x}}{a^2 + b^2} \right) = 1,$$

поэтому  $\frac{a - b\bar{x}}{a^2 + b^2} = (a + b\bar{x})^{-1}$ , т.е. любой ненулевой элемент обратим в факторкольце  $\mathbb{R}[x]/(x^2 + 1)$ .

Значит, факторкольцо  $\mathbb{R}[x]/(x^2 + 1)$  выглядит точно так же, как  $\mathbb{C}$ .

**Пример 2.** Пусть  $K = \mathbb{Z}_2$ . Рассмотрим нормированный многочлен  $m(x) = x^2 + x + 1$  из  $\mathbb{Z}_2[x]$ . Он неприводим в  $\mathbb{Z}_2[x]$ , так как его нельзя представить в виде произведения двух многочленов первой степени, поскольку у него нет в  $\mathbb{Z}_2$  корней.

Рассмотрим факторкольцо  $\mathbb{Z}_2[x]/(x^2 + x + 1)$ . Это кольцо содержит следующие классы:

$$[0] = \bar{0}, \quad [1] = \bar{1}, \quad [x] = \bar{x}, \quad [x+1] = \overline{x+1}.$$

Все операции над этими элементами выполняются по модулю  $m(x) = x^2 + x + 1$ . Например,

$$\bar{x} + \overline{x+1} = x + (x+1) \pmod{x^2 + x + 1} \equiv 1 = \bar{1}, \quad \text{так как } 2 \equiv 0 \pmod{2},$$

$$\bar{x} \cdot \overline{x+1} = x(x+1) \pmod{x^2 + x + 1} = x^2 + x \pmod{x^2 + x + 1} \equiv -1 \equiv 1 = \bar{1},$$

следует

$$\bar{x}^{-1} = \overline{x+1} \quad \text{и} \quad (\overline{x+1})^{-1} = \bar{x}$$

в  $\mathbb{Z}_2[x]/(x^2 + x + 1)$ .

В результате получаем, что все ненулевые элементы факторкольца  $\mathbb{Z}_2[x]/(x^2 + x + 1)$  обратимы, значит, оно является полем. Таким образом, мы построили поле, в котором четыре элемента.

**Пример 3.** Пусть  $K = \mathbb{Z}_2$ . Рассмотрим нормированный многочлен  $m(x) = x^2 + 1$  из  $\mathbb{Z}_2[x]$ . Этот многочлен приводим в  $\mathbb{Z}_2[x]$ .

Действительно,

$$x^2 + 1 \equiv (x+1)^2 \pmod{2}.$$

Факторкольцо  $\mathbb{Z}_2[x]/(x^2 + 1)$  содержит те же 4 класса, что и факторкольцо примера 2. Все операции над классами выполняются по модулю  $m(x) = x^2 + 1$ . Так,

$$\bar{x} \cdot \overline{x+1} = x(x+1) \pmod{x^2 + 1} = x^2 + x \pmod{x^2 + 1} \equiv x+1 = \overline{x+1},$$

$$\bar{x} \cdot \bar{x} = x^2 \pmod{x^2 + 1} \equiv -1 \equiv 1 = \bar{1},$$

$$\overline{x+1} \cdot \overline{x+1} = (x+1)(x+1) \pmod{x^2 + 1} = x^2 + 1 \pmod{x^2 + 1} \equiv 0 = \bar{0},$$

значит, класс  $\overline{x+1}$  не обратим в кольце  $\mathbb{Z}_2[x]/(x^2 + 1)$ .

**Теорема.** Пусть  $K$  – поле и  $m(x)$  – нормированный многочлен из кольца  $K[x]$ . Тогда  $K[x]/(m(x))$  есть коммутативное кольцо с единицей. Оно является полем тогда и только тогда, когда  $m(x)$  неприводим в  $K[x]$ .

**Доказательство.** То, что  $K[x]/(m(x))$  является коммутативным кольцом с единицей, следует из того, что  $K[x]$  является коммутативным кольцом с единицей. Проверка соответствующих аксиом проводится так же, как для числовых факторколец.

Докажем второе утверждение теоремы. Пусть многочлен  $m(x)$  неприводим в  $K[x]$ . Покажем, что  $K[x]/(m(x))$  является полем, т.е. любой ненулевой элемент этого факторкольца обратим. Пусть  $[f(x)]_{m(x)}$  – класс эквивалентности из  $K[x]/(m(x))$ , отличный от класса  $[0]_{m(x)}$ . Возьмем представитель этого класса, имеющий наименьшую степень, т.е. степень, меньшую  $\deg m(x)$ , пусть  $p(x) = r_{m(x)}[f(x)]$ ,  $\deg p(x) < \deg m(x)$ . Поскольку  $m(x), p(x) \in K[x]$  и  $m(x)$  неприводим, то многочлены  $p(x)$  и  $m(x)$  взаимно просты в  $K[x]$  ( $m(x)$  не может делить  $p(x)$ , так как имеет большую степень).

Используя расширенный алгоритм Евклида (см. § 4), можно найти такие многочлены  $u(x)$ ,  $v(x)$ , что

$$p(x)u(x) + m(x)v(x) = 1, \quad \deg u(x) < \deg m(x),$$

или

$$p(x)u(x) \equiv 1 \pmod{m(x)}.$$

Рассмотрим класс многочлена  $u(x)$  в  $K[x]/m(x)$ :  $[u(x)]_{m(x)}$ . Имеем

$$[f(x)]_{m(x)} \cdot [u(x)]_{m(x)} = p(x)u(x) \pmod{m(x)} \equiv 1 = [1]_{m(x)},$$

т. е. класс  $[u(x)]_{m(x)}$  является обратным для класса  $[f(x)]_{m(x)}$ .

Обратно, пусть  $K[x]/(m(x))$  есть поле. Покажем, что  $m(x)$  неприводим в  $K[x]$ . Предположим противное, пусть  $m(x)$  приводим, т.е.

$$m(x) = m_1(x)m_2(x),$$

где  $0 < \deg m_1(x) < \deg m(x)$ ,  $0 < \deg m_2(x) < \deg m(x)$ . Значит,  $[m_1(x)]_{m(x)} \neq [0]_{m(x)}$  и  $[m_2(x)]_{m(x)} \neq [0]_{m(x)}$ , но их произведение равно  $[0]_{m(x)}$ . Действительно,

$$[m_1(x)]_{m(x)} \cdot [m_2(x)]_{m(x)} = [m_1(x)m_2(x)]_{m(x)} = [m(x)]_{m(x)} = [0]_{m(x)}.$$

В поле нашлись делители нуля. Противоречие. Значит, наше предположение о приводимости  $m(x)$  неверно.

Эта теорема дает нам способ построения новых полей:

для этого следует рассмотреть кольцо многочленов  $K[x]$  над полем  $K$ , выбрать в  $K[x]$  неприводимый многочлен  $m(x)$  и построить факторкольцо  $K[x]/(m(x))$ .

Поле  $K[x]/(m(x))$  называется простым расширением поля  $K$ .



## §7. ВЫЧИСЛИТЕЛЬНЫЕ СХЕМЫ, ИСПОЛЬЗУЮЩИЕ ИНТЕРПОЛЯЦИЮ

Ранее мы рассмотрели модульную арифметику для целых чисел, с помощью которой можно "вычислять" арифметические действия над большими целыми числами, выбирая в качестве модулей несколько взаимно простых чисел и вместо действий с самими числами выполняя действия с их остатками по выбранным модулям. При этом окончательный результат восстанавливается, если использовать китайскую теорему об остатках и априорную оценку результата вычислений. Этот же метод применим и к вычислению значений выражений, аргументами которых являются многочлены. При этом для восстановления значений можно использовать интерполяцию.

Пусть требуется вычислить выражение

$$f(x) = f(g_1(x), g_2(x), \dots, g_l(x))$$

над  $K[x]$ , где  $K$  — поле и  $g_j(x) \in K[x]$  ( $j = 1, 2, \dots, l$ ).

Если вычислять это выражение в  $K[x]$  "трудно", то можно работать над полями  $K[x]/(m_s(x))$  для различных  $s$ , где  $m_s(x) = x - a_s$ ,  $a_s \in K$ , очевидно, неприводимый над  $K[x]$  многочлен. В этом случае мы должны знать границу для  $\deg f(x)$ , чтобы затем правильно восстановить  $f(x)$ .

Пример. если известно, что  $\deg f(x) \leq n$ , то  $s$  принимает значения  $1, 2, \dots, n+1$ . Кроме того, стоит отметить, что поскольку  $m_s(x) = x - a_s$ , то  $K[x]/(m_s(x))$  совпадает с  $K$  для любого  $s$ .

Для  $s = 1, 2, \dots, n+1$  сначала вычисляем  $g_j(a_s)$ ,  $j = 1, 2, \dots, l$  (при условии, что  $a_s$  выбраны так, что все  $f_s = f(g_1(a_s), g_2(a_s), \dots, g_l(a_s))$  определены) и вычисляем

$$f(a_s) = f(g_1(a_s), g_2(a_s), \dots, g_l(a_s)) = b_s.$$

Далее при помощи интерполяции по выбранным точкам  $(a_s, b_s)$ ,  $s = 1, 2, \dots, n+1$  находим функцию  $f(x)$  такую, что

$$f(a_s) = b_s, \quad s = 1, 2, \dots, n+1.$$

Пример 1. В  $\mathbb{Z}_7[x]$  вычислим произведение многочленов  $f_1(x) = 3x + 4$  и  $f_2(x) = 2x^2 + 5x + 1$ , используя описанный выше способ.

Степень произведения  $f_1(x)f_2(x)$  не выше 3, поэтому следует выбрать четыре точки. Возьмем  $a_1 = 0$ ,  $a_2 = 1$ ,  $a_3 = 2$  и  $a_4 = 3$ . Вычислим  $f_1(x) \pmod{(x - a_s)} \cdot f_2(x) \pmod{(x - a_s)}$ ,  $s = 1, 2, 3, 4$  над  $\mathbb{Z}_7$ :

$$f_1(0) \cdot f_2(0) = 4 \cdot 1 = 4 = b_1,$$

$$f_1(1) \cdot f_2(1) \equiv 0 \cdot 1 = 0 = b_2,$$

$$f_1(2) \cdot f_2(2) \equiv 3 \cdot 5 \equiv 1 = b_3,$$

$$f_1(3) \cdot f_2(3) \equiv 6 \cdot 6 \equiv 1 = b_4.$$

Применим к полученным парам чисел интерполяционный алгоритм, основанный на китайской теореме об остатках:

$i$	$a_i$	$b_i$	$m_i(x)$	$d_i$	$c_i$	$q_i$	$f_i(x)$
1	0	4	1	—	—	4	4
2	1	0	$x$	3	1	3	$4 + 3x$
3	2	1	$x(x-1)$	5	4	6	$4 + 3x + 6(x^2 - x)$
4	3	1	$x(x-1)(x-2)$	1	6	6	$4 - 3x + 6x^2 + 6(x^3 - 3x^2 + 2x)$

Значит,

$$f(x) = 4 - 3x + 6x^2 + 6x^3 - 4x^2 + 5x \equiv 6x^3 + 2x^2 + 2x + 4$$

в  $\mathbb{Z}_7[x]$ .

Интерполяцией мы смогли воспользоваться потому, что задача решалась в поле. Если подобную задачу решать в кольце, то придется изменить тактику.

Пусть требуется вычислить выражение

$$f(x) = f(g_1(x), g_2(x), \dots, g_l(x))$$

над  $\mathbb{Z}[x]$ , где  $f(x), g_j(x)$  ( $j = 1, 2, \dots, l$ ) – многочлены из кольца  $\mathbb{Z}[x]$ . Используем следующее соображение: если

$$p(x) = \sum_{i=0}^n p_i x^i$$

– многочлен из кольца  $\mathbb{Z}[x]$ ,  $m$  – целое положительное число, то

$$p(x) \pmod{m} = \sum_{i=0}^n p_i \pmod{m} x^i.$$

Предположим, что все коэффициенты многочлена  $f(x) = \sum_{i=0}^k a_i x^i$  удовлетворяют неравенствам  $0 \leq a_i \leq m_1 m_2 m_3 \dots m_s$ , где  $m_1, m_2, \dots, m_s$  –  $s$  попарно взаимно простых модулей. Тогда для нахождения  $f(x)$  можно сделать следующее:

1) для  $j = 1, 2, \dots, s$  (считаем, что  $g_i(x) \pmod{m_j}$  определены для  $i = 1, 2, \dots, l$ ) вычислить

$$f_j(x) = f(g_1(x) \pmod{m_j}, g_2(x) \pmod{m_j}, \dots, g_l(x) \pmod{m_j}) \pmod{m_j}$$

над  $\mathbb{Z}_{m_j}[x]$ ;

2) решить китайскую задачу об остатках для многочленов

$$f(x) \equiv f_j(x) \pmod{m_j}, \quad j = 1, 2, \dots, s,$$

отыскивая наименьшее неотрицательное решение.

**Пример 2.** В  $\mathbb{Z}[x]$  найдем произведение многочленов  $f_1(x) = 2x + 4$ ,  $f_2(x) = 3x^2 + 5x - 2$ ,  $f_3(x) = x + 3$ .

Все коэффициенты произведения  $g(x) = f_1(x)f_2(x)f_3(x)$  не превосходят 100, поэтому в качестве модулей возьмем  $m_1 = 3$ ,  $m_2 = 5$  и  $m_3 = 7$  ( $3 \cdot 5 \cdot 7 > 100$ ).

Для  $m_1 = 3$  получаем

$$g_1(x) = \{f_1(x) \pmod{3} \cdot f_2(x) \pmod{3} \cdot f_3(x) \pmod{3}\} \pmod{3} = (2x + 1)(2x + 1)x \pmod{3} = x^3 + x^2 + x$$

Для  $m_2 = 5$  произведение равно

$$\begin{aligned} g_2(x) &= \{f_1(x) \pmod{5} \cdot f_2(x) \pmod{5} \cdot f_3(x) \pmod{5}\} \pmod{5} = \\ &= (2x + 4)(3x^2 - 2)(x + 3) \pmod{5} = x^4 + 2x^2 + 1. \end{aligned}$$

Наконец, для  $m_3 = 7$  получаем

$$\begin{aligned} g_3(x) &= \{f_1(x) \pmod{7} \cdot f_2(x) \pmod{7} \cdot f_3(x) \pmod{7}\} \pmod{7} = \\ &= (2x + 4)(3x^2 + 5x - 2)(x + 3) \pmod{7} = 6x^4 + 5x^3 + 5x^2 + 5x - 3. \end{aligned}$$

В результате следует решить систему

$$\begin{cases} g(x) \equiv x^3 + x^2 + x \pmod{3}, \\ g(x) \equiv x^4 + 2x^2 + 1 \pmod{5}, \\ g(x) \equiv 6x^4 + 5x^3 + 5x^2 + 5x - 3 \pmod{7}. \end{cases}$$

Очевидно, что  $g(x) = ax^4 + bx^3 + cx^2 + dx + e$ , где коэффициенты есть решения следующих пяти систем сравнений:

$$\begin{cases} a \equiv 0 \pmod{3}, \\ a \equiv 1 \pmod{5}, \\ a \equiv 6 \pmod{7}, \end{cases} \quad \begin{cases} b \equiv 1 \pmod{3}, \\ b \equiv 0 \pmod{5}, \\ b \equiv 5 \pmod{7}, \end{cases} \quad \begin{cases} c \equiv 1 \pmod{3}, \\ c \equiv 2 \pmod{5}, \\ c \equiv 5 \pmod{7}, \end{cases} \quad \begin{cases} d \equiv 1 \pmod{3}, \\ d \equiv 0 \pmod{5}, \\ d \equiv 5 \pmod{7}, \end{cases} \quad \begin{cases} e \equiv 0 \pmod{3}, \\ e \equiv 1 \pmod{5}, \\ e \equiv -3 \pmod{7}. \end{cases}$$

Применяя к каждой системе китайскую теорему об остатках, получаем

$$a = 6, \quad b = 40, \quad c = 82, \quad d = 40, \quad e = -24$$

(очевидно, что свободный член должен быть отрицательным), т.е.

$$g(x) = 6x^4 + 40x^3 + 82x^2 + 40x - 24.$$

**В качестве обоснования такого использования китайской теоремы об остатках для решения системы полиномиальных сравнений**

$$\begin{cases} f(x) \equiv f_1(x) \pmod{m_1}, \\ f(x) \equiv f_2(x) \pmod{m_2}, \\ \dots\dots\dots \\ f(x) \equiv f_k(x) \pmod{m_k}, \end{cases}$$

где  $f_i(x) = a_{0i} + a_{1i}x + \dots + a_{in}x^n \in \mathbb{Z}[x]$  ( $i = 1, 2, \dots, k$ ), заметим следующее.

Для многочленов  $q(x) = \sum_{j=0}^n a_j x^j$  и  $g(x) = \sum_{j=0}^n b_j x^j$  из  $\mathbb{Z}[x]$  и целого положительного числа  $m$  справедливо:

$q(x) \equiv g(x) \pmod{m}$  тогда и только тогда, когда  $a_j \equiv b_j \pmod{m}$  для всех  $j = 0, 1, 2, \dots, n$ .

Действительно,  $m \mid \{q(x) - g(x)\}$  тогда и только тогда, когда  $m \mid (a_j - b_j)$  для  $j = 0, 1, 2, \dots, n$ .



## §8. КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ ДЛЯ МНОГОЧЛЕНОВ

Подобно тому, как в кольце  $\mathbf{Z}$  можно решить систему сравнений по взаимно простым модулям, пользуясь китайской теоремой об остатках, в кольце многочленов  $K[x]$  ( $K$  – поле) можно решить систему сравнений по попарно взаимно простым многочленам – модулям. Т.е. справедливо следующее утверждение.

**Теорема.** Для заданного множества попарно взаимно простых многочленов  $m_1(x), m_2(x), \dots, m_k(x)$  из кольца  $K[x]$  ( $K$  – поле) и множества многочленов  $c_i(x)$  ( $i = 1, 2, \dots, k$ ),  $c_i(x) \in K[x]$  таких, что  $\deg c_i(x) < \deg m_i(x)$  ( $i = 1, 2, \dots, k$ ), система сравнений

$$f(x) \equiv c_i(x) \pmod{m_i(x)}, \quad i = 1, 2, \dots, k, \quad (1)$$

имеет не более одного решения  $f(x)$ , удовлетворяющего условию

$$\deg f(x) < \sum_{i=1}^k \deg m_i(x),$$

которое можно найти по формуле

$$f(x) = \sum_{i=1}^k c_i(x) M_i(x) N_i(x) \pmod{M(x)}, \quad (2)$$

где

$$M(x) = \prod_{i=1}^k m_i(x), \quad M_i(x) = \frac{M(x)}{m_i(x)} \quad (i = 1, 2, \dots, k),$$

а  $N_i(x)$  удовлетворяет условию

$$M_i(x) N_i(x) + m_i(x) n_i(x) = 1 \quad (i = 1, 2, \dots, k). \quad (3)$$

*Доказательство.* Сначала поймем, почему для каждого  $i = 1, 2, \dots, k$  можно найти многочлен  $N_i(x)$ , удовлетворяющий равенству (3). Многочлены  $M_i(x)$  и  $m_i(x)$ , очевидно, взаимно просты, поэтому с помощью расширенного алгоритма Евклида можно найти "коэффициенты" Безу, т.е. такие многочлены  $N_i(x)$  и  $n_i(x)$ , что

$$1 = \text{НОД}(M_i(x), m_i(x)) = M_i(x) N_i(x) + m_i(x) n_i(x) \quad (i = 1, 2, \dots, k).$$

Теперь покажем, что многочлен  $f(x)$ , задаваемый формулой (2), удовлетворяет всем сравнениям системы.

$$f(x) \pmod{m_l(x)} = \sum_{i=1}^n c_i(x) M_i(x) N_i(x) \pmod{m_l(x)} \equiv c_l(x) M_l(x) N_l(x) \pmod{m_l(x)},$$

так как  $m_l(x) \mid M_j(x)$  для  $j = 1, 2, \dots, l-1, l+1, \dots, k$ .

Далее, в силу

$$M_l(x) N_l(x) + m_l(x) n_l(x) = 1$$

имеем

$$M_l(x) N_l(x) \equiv 1 \pmod{m_l(x)},$$

поэтому

$$f(x) \pmod{m_l(x)} \equiv c_l(x) \quad \text{для} \quad l = 1, 2, \dots, k.$$



Таким образом, решение системы сравнений можно задать формулой (2). Из (2) также ясно, что

$$\deg f(x) < \deg M(x) = \sum_{i=1}^k \deg m_i(x).$$

Осталось доказать единственность этого решения. Предположим, что многочлен  $g(x)$  также является решением системы (1) и

$$\deg g(x) < \sum_{i=1}^k \deg m_i(x).$$

Для каждого  $i$  ( $i = 1, 2, \dots, k$ ), очевидно, справедливо

$$\begin{aligned} f(x) &= c_i(x) + m_i(x)q_i(x), \\ g(x) &= c_i(x) + m_i(x)r_i(x), \end{aligned}$$

значит,  $m_i(x)$  делит разность  $f(x) - g(x)$  для каждого  $i = 1, 2, \dots, k$ . Поскольку  $m_1(x), m_2(x), \dots, m_k(x)$  попарно взаимно просты, то многочлен  $f(x) - g(x)$  делится на их произведение, т.е. на многочлен  $\prod_{i=1}^k m_i(x) = M(x)$ . Но  $\deg \{f(x) - g(x)\} < \deg M(x)$ . Следовательно,  $f(x) - g(x) \equiv 0 \pmod{M(x)}$ , откуда  $f(x) \equiv g(x) \pmod{M(x)}$ . Теорема доказана.

**Пример.** В кольце  $\mathbb{Z}_5[x]$  решить систему сравнений

$$\begin{cases} f(x) \equiv x + 1 \pmod{x^2 + 1}, \\ f(x) \equiv 2x + 3 \pmod{x^2 + x}. \end{cases}$$

Многочлены  $m_1(x) = x^2 + 1$  и  $m_2(x) = x^2 + x$  из  $\mathbb{Z}_5[x]$  взаимно просты (корнями  $m_1(x)$  являются элементы 2 и 3 поля  $\mathbb{Z}_5$ , корнями  $m_2(x)$  — элементы 0 и 4).  $M(x) = m_1(x)m_2(x) = x^4 + x^3 + x^2 + x$ ,  $M_1(x) = x^2 + x$ ,  $M_2(x) = x^2 + 1$ .

Поскольку

$$(2x + 2)(x^2 + x) + (3x + 1)(x^2 + 1) = 1 \quad \text{в} \quad \mathbb{Z}_5[x],$$

$$N_1(x) = 2x + 2, \quad N_2(x) = 3x + 1.$$

Значит, по формуле (1) получаем

$$f(x) = (x + 1)(x^2 + x)(2x + 2) + (2x + 3)(3x + 1)(x^2 + 1) \pmod{x^4 + x^3 + x^2 + x} \equiv 4x^3 + 2x^2 + 3.$$

**Проверка:**

$$4x^3 + 2x^2 + 3 = (4x + 2)(x^2 + 1) + (x + 1) \equiv x + 1 \pmod{x^2 + 1},$$

$$4x^3 + 2x^2 + 3 = (4x - 2)(x^2 + x) + (2x + 3) \equiv 2x + 3 \pmod{x^2 + x}.$$

## §9. АЛГОРИТМ ЕВКЛИДА И ПСЕВДОДЕЛЕНИЕ

Здесь мы обсудим вопрос о том, как искать наибольший общий делитель многочленов из  $\mathbb{A}[x]$ , если старший коэффициент делителя не обратим в кольце  $\mathbb{A}$ .

**Определение 1.** Многочлен называется *примитивным*, если наибольший общий делитель его коэффициентов равен единице.

**Теорема 1.** Пусть  $\mathbb{A}$  – факториальное кольцо и  $f(x) \in \mathbb{A}[x]$  – ненулевой многочлен. Тогда  $f(x)$  может быть единственным образом представлен в виде произведения

$$f(x) = c \tilde{f}(x),$$

где  $c \in \mathbb{A}$ , а многочлен  $\tilde{f}(x)$  является примитивным. Это разложение единственно с точностью до обратимых элементов кольца  $\mathbb{A}$ , т.е. если

$$f(x) = c_1 f_1(x) = c_2 f_2(x), \quad \text{то} \quad c_1 = \varepsilon c_2 \text{ и } f_2(x) = \varepsilon f_1(x),$$

где  $\varepsilon$  – обратимый элемент кольца  $\mathbb{A}$ .

*Доказательство.* Обозначим через  $\text{cont}(f(x))$  наибольший общий делитель коэффициентов многочлена  $f(x)$ , тогда, очевидно,  $\text{cont}(f(x))$  делит все коэффициенты многочлена  $f(x)$  в  $\mathbb{A}$ , а значит, делит  $f(x)$ . Обозначим

$$\text{pp}(f(x)) = \frac{f(x)}{\text{cont}(f(x))} = \tilde{f}(x).$$

Полученный многочлен, очевидно, примитивен, т.е.

$$f(x) = c \tilde{f}(x), \tag{1}$$

где  $c \in \mathbb{A}$ , а  $\tilde{f}(x)$  – примитивный многочлен.

Представление (1) однозначно с точностью до умножения на обратимый элемент кольца  $\mathbb{A}$ .

**Лемма (Гаусс).** Пусть простой элемент  $p$  кольца  $\mathbb{A}$  делит произведение многочленов  $f(x)$  и  $g(x)$ ,  $f(x), g(x) \in \mathbb{A}[x]$ . Тогда  $p$  делит  $f(x)$  или  $g(x)$ .

*Доказательство.* Предположим противное, пусть  $p$  не делит ни  $f(x)$ , ни  $g(x)$ . Значит, в  $f(x)$  и в  $g(x)$  есть коэффициенты, не делящиеся на  $p$ .

Пусть  $f(x) = \sum_{k=0}^n a_k x^k$  и  $a_i$  – коэффициент с наименьшим номером, не делящийся на  $p$ , т.е.

$$p \mid a_0, a_1, \dots, a_{i-1}, \quad \text{но} \quad p \nmid a_i.$$

Пусть  $g(x) = \sum_{l=0}^m b_l x^l$  и  $b_j$  – коэффициент с наименьшим номером, не делящийся на  $p$ , т.е.

$$p \mid b_0, b_1, \dots, b_{j-1}, \quad \text{но} \quad p \nmid b_j.$$

Рассмотрим многочлен

$$f(x)g(x) = \sum_{i=0}^{n+m} \left( \sum_{k+l=i} a_k b_l \right) x^i.$$

По условию леммы все коэффициенты этого многочлена должны делиться на  $p$ , в том числе и коэффициент при  $x^{i+j}$ . Найдем этот коэффициент

$$\sum_{k+l=i+j} a_k b_l = a_i b_j + (a_{i-1} b_{j+1} + a_{i-2} b_{j+2} + \dots + a_s b_{i+j-s} + \dots) + (a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \dots +$$

$$a_{i+r} b_{j-r} + \dots) = a_i b_j + \sum_{\substack{k=1 \\ i-k \geq 0 \\ j+k \leq m}} a_{i-k} b_{j+k} + \sum_{\substack{l=1 \\ i+l \leq n \\ j-l \geq 0}} a_{i+l} b_{j-l}.$$

Все слагаемые первой суммы делятся на  $p$ , так как  $a_{i-k}$  ( $k = 1, 2, \dots, i$ ) все делятся на  $p$ . Все слагаемые второй суммы также делятся на  $p$ , так как  $b_{j-l}$  ( $l = 1, 2, \dots, j$ ) все делятся на  $p$ . А произведение  $a_i b_j$  не делится на  $p$ . Значит, коэффициент при  $x^{i+j}$  в произведении  $f(x)g(x)$  не делится на  $p$ . Полученное противоречие доказывает, что наше предположение неверно, т.е. либо  $f(x)$ , либо  $g(x)$  должно делиться на  $p$ .



**Следствие 1.** Произведение примитивных многочленов есть примитивный многочлен.

**Определение 2.**  $\text{cont}(f(x))$ , равный наибольшему общему делителю коэффициентов  $f(x)$ , называется содержанием многочлена  $f(x) \in \mathbf{A}[x]$  ( $\mathbf{A}$  – кольцо). Многочлен  $\text{pp}(f(x)) = \frac{f(x)}{\text{cont}(f(x))}$  называется примитивной частью многочлена  $f(x)$ .

**Следствие 2.** Содержание произведений двух многочленов ассоциировано с произведением содержаний этих многочленов.

**Следствие 3.** Пусть  $f(x)$  – примитивный многочлен с коэффициентами в факториальном поле  $\mathbf{A}$ ,  $g(x) \in \mathbf{A}[x]$ . Если  $f(x)$  делит  $g(x)$  над полем частных кольца  $\mathbf{A}$ , то он делит  $g(x)$  и в  $\mathbf{A}[x]$ . В частности, если для  $a \in \mathbf{A} \setminus \{0\}$  многочлен  $f(x)$  делит  $ag(x)$ , то  $f(x)$  делит  $g(x)$ .

**Доказательство.** Если  $g(x) = f(x)q(x)$ , то

$$\text{cont}(g(x)) = \text{cont}\{f(x)q(x)\} \sim \text{cont}(f(x)) \cdot \text{cont}(q(x))$$

в силу следствия 2. Но  $f(x)$  – примитивный многочлен, значит,  $\text{cont}(f(x)) = 1$ . В результате получаем

$$\text{cont}(g(x)) \sim \text{cont}(q(x)),$$

то  $\text{cont}(g(x)) \in \mathbf{A}$ , следовательно,  $\text{cont}(q(x))$  есть также элемент кольца  $\mathbf{A}$ . Последнее означает, что коэффициенты многочлена  $q(x)$  принадлежат кольцу  $\mathbf{A}$ , т.е.  $f(x)$  делит  $g(x)$  в  $\mathbf{A}[x]$ .

Рассмотрим в качестве кольца  $\mathbf{A}$  кольцо целых чисел  $\mathbf{Z}$ . Оно, как мы знаем, факториально. Поскольку обратимыми элементами этого кольца являются только 1 и  $-1$ , то из приведенных выше утверждений следует, что

$$\text{cont}\{\text{НОД}(f_1(x), f_2(x))\} = \text{НОД}\{\text{cont}(f_1(x)), \text{cont}(f_2(x))\}, \quad (2)$$

$$\text{pp}\{\text{НОД}(f_1(x), f_2(x))\} = \text{НОД}\{\text{pp}(f_1(x)), \text{pp}(f_2(x))\}. \quad (3)$$

Поэтому задача нахождения наибольшего общего делителя двух многочленов  $f_1(x), f_2(x)$  в кольце  $\mathbf{Z}[x]$  сводится к задаче нахождения наибольшего общего делителя примитивных многочленов.

Пусть  $f_1(x), f_2(x)$  – два примитивных ненулевых многочлена в  $\mathbf{Z}[x]$  такие, что  $\deg f_1(x) = m$ ,  $\deg f_2(x) = n$  и  $m > n$ . Мы хотим найти их наибольший общий делитель в  $\mathbf{Z}[x]$ . Обычное евклидово деление над  $\mathbf{Z}$  возможно, если старший коэффициент делителя обратим в  $\mathbf{Z}$  (т.е. равен  $\pm 1$ ). Если же старший коэффициент необратим, то прямое деление невозможно. Поэтому рассмотрим процесс псевдоделения. Если  $\text{lc}(f_2(x))$  не обратим, то домножим делимое  $f_1(x)$  на подходящую степень старшего коэффициента  $f_2(x)$  и вместо равенства

$$f_1(x) = f_2(x)q(x) + r(x)$$

получим

$$\alpha f_1(x) = f_2(x)\tilde{q}(x) + \tilde{r}(x), \quad \text{где } \tilde{q}(x), \tilde{r}(x) \in \mathbf{Z}[x].$$

В качестве  $\alpha$  берут  $\{\text{lc}(f_2(x))\}^{m-n+1}$ , т.е. деление имеет вид

$$\{\text{lc}(f_2(x))\}^{m-n+1} f_1(x) = f_2(x)\tilde{q}(x) + \tilde{r}(x), \quad \deg \tilde{r}(x) < \deg f_2(x). \quad (4)$$

Многочлены  $\tilde{q}(x)$  и  $\tilde{r}(x)$  называются соответственно псевдочастным и псевдоостатком.

Убедимся, что последовательность псевдоделений сохраняет наибольший общий делитель многочленов в определенном смысле. Если  $f_1(x)$  и  $f_2(x)$  – примитивные и выполнено псевдоделение (4), то, очевидно, любой делитель многочленов  $f_1(x)$  и  $f_2(x)$  делит и  $\tilde{r}(x)$ . Обратно, если многочлен  $d(x)$  делит  $f_2(x)$ , то  $d(x)$  – примитивный, поскольку  $f_2(x)$  – примитивный многочлен. Если, кроме того,  $d(x)$  делит и  $\tilde{r}(x)$ , то он будет делить и левую часть равенства (4), т.е.

$$\{\text{lc}(f_2(x))\}^{m-n+1} f_1(x) = \alpha f_1(x), \quad \alpha \in \mathbf{Z} \setminus \{0\}.$$



Но тогда в силу следствия 3  $d(x)$  делит  $f_1(x)$ . Таким образом, псевдоделение  $f_1(x)$  на  $f_2(x)$  сохраняет наибольший общий делитель для примитивных многочленов. Кроме того, содержание наибольшего общего делителя двух многочленов равно наибольшему общему делителю содержаний этих многочленов (см. формулу (2)).

Поэтому для вычисления наибольшего общего делителя двух многочленов с коэффициентами в  $\mathbf{Z}$  (в факториальном кольце  $\mathbf{A}$ ) получаем следующий *алгоритм*:

1. Вычислить наибольший общий делитель содержаний двух многочленов  $f_1(x)$  и  $f_2(x)$  ( пусть  $d = \text{НОД}(\text{cont}(f_1(x)), \text{cont}(f_2(x)))$ ).

2. Провести алгоритм Евклида, использующий псевдоделение, для примитивных частей исходных многочленов. На каждом шаге полученный остаток заменять его примитивной частью в целях сокращения роста коэффициентов. (Алгоритм заканчивает работу, когда на очередном шаге псевдоделения получен нулевой остаток.)

3. Наибольший общий делитель  $f_1(x)$  и  $f_2(x)$  положить равным произведению примитивной части последнего ненулевого остатка на константу  $d$ .

**Пример.** Найти наибольший общий делитель многочленов

$$f_1(x) = 6x^5 - 6x^4 - 18x^2 - 6x - 12$$

и

$$f_2(x) = 3x^4 - 15x^2 + 12$$

в  $\mathbf{Z}[x]$ .

Нетрудно видеть, что  $\text{cont}(f_1(x)) = 6$ ,  $\text{cont}(f_2(x)) = 3$ ,  $\text{НОД}(6, 3) = 3 (= d)$ . Перейдем к примитивным частям многочленов  $f_1(x)$  и  $f_2(x)$ :

$$\tilde{p}_1(x) = pp(f_1(x)) = x^5 - x^4 - 3x^2 - x - 2, \quad \tilde{p}_2(x) = pp(f_2(x)) = x^4 - 5x^2 + 4.$$

Поскольку старший коэффициент  $\tilde{p}_2(x)$  обратим, то на первом шаге алгоритма Евклида можно обойтись без псевдоделения:

$$\tilde{p}_1(x) = \tilde{p}_2(x)(x - 1) + (5x^3 - 8x^2 - 5x + 2).$$

Так как остаток от этого деления  $r_1(x) = 5x^3 - 8x^2 - 5x + 2$  является примитивным многочленом, то  $pp(r_1(x)) = r_1(x)$ .  $lc(r_1(x)) = 5$ , поэтому для следующего деления следует умножить  $\tilde{p}_2(x)$  на  $5^{4-3+1} = 5^2$ , т.е.

$$5^2 \tilde{p}_2(x) = r_1(x)(5x + 8) + (-36x^2 + 30x + 84).$$

Поскольку  $\text{cont}(r_2(x)) = \text{cont}(-36x^2 + 30x + 84) = 6$ , то перейдем к примитивной части многочлена  $r_2(x)$ :

$$\tilde{r}_2(x) = pp(r_2(x)) = -6x^2 + 5x + 14.$$

$lc(\tilde{r}_2(x)) = -6$ , поэтому для следующего деления умножим  $r_1(x)$  на  $(-6)^{3-2+1} = 6^2$  и проведем псевдоделение

$$6^2 r_1(x) = \tilde{r}_2(x)(-30x + 23) + (125x - 250).$$

Переходим к примитивной части полученного остатка:

$$\tilde{r}_3(x) = pp(r_3(x)) = x - 2 \quad (\text{cont}(r_3(x)) = 125).$$

Старший коэффициент  $\tilde{r}_3(x)$  равен 1, поэтому для следующего деления  $\tilde{r}_2(x)$  не нужно умножать на константу. Получаем

$$\tilde{r}_2(x) = \tilde{r}_3(x)(-6x - 7).$$

Итак,

$$\text{НОД}(\tilde{p}_1(x), \tilde{p}_2(x)) = \tilde{r}_3(x),$$

и

$$\text{НОД}(f_1(x), f_2(x)) = d\tilde{r}_3(x) = 3(x - 2).$$



## §10. РАЗЛОЖЕНИЕ МНОГОЧЛЕНА НА МНОЖИТЕЛИ

Напомним, что неприводимым многочленом  $f(x)$  кольца  $\mathbf{A}[x]$  (где  $\mathbf{A}$  — целостное кольцо) называется такой, для которого из  $f(x) = f_1(x) f_2(x)$  следует, что либо  $f_1(x)$ , либо  $f_2(x)$  есть константа из кольца  $\mathbf{A}$ . В теории разложения многочленов на множители неприводимые многочлены играют ту же роль, что и простые числа в теории разложения на множители целых чисел.

**Теорема 1.** Пусть  $K$  — поле и  $f_1(x), f_2(x) \in K[x]$ . Если неприводимый многочлен  $g(x) \in K[x]$  делит произведение  $f_1(x) f_2(x)$ , то  $g(x)$  делит  $f_1(x)$  или  $f_2(x)$ .

**Доказательство.** Если хотя бы один из многочленов  $f_1(x), f_2(x)$  равен нулю, то утверждение очевидно. Пусть  $f_1(x) f_2(x) \neq 0$ . Предположим, что  $g(x)$  не делит  $f_1(x)$ . Покажем, что в этом случае  $g(x)$  делит  $f_2(x)$ .

Так как  $g(x)$  не делит  $f_1(x)$  и  $g(x)$  неприводим, то  $g(x)$  и  $f_1(x)$  взаимно просты, т.е.

$$\text{НОД}(g(x), f_1(x)) = 1.$$

Значит, по теореме 1 §4 найдутся такие многочлены  $u(x), v(x) \in K[x]$ , что

$$g(x)u(x) + f_1(x)v(x) = 1.$$

Умножим обе части последнего равенства на  $f_2(x)$ , тогда получаем

$$f_2(x)g(x)u(x) + f_2(x)f_1(x)v(x) = f_2(x). \quad (1)$$

Многочлен  $g(x)$ , очевидно, делит левую часть равенства (1), поскольку он делит  $f_1(x)f_2(x)$ , значит,  $g(x)$  делит и правую часть равенства, т.е.  $g(x) \mid f_2(x)$ , что и требовалось доказать.

**Теорема 2.** Пусть  $f(x)$  — многочлен положительной степени из кольца  $K[x]$  ( $K$  — поле). Тогда  $f(x)$  можно представить в виде произведения конечного числа неприводимых многочленов из кольца  $K[x]$ .

**Доказательство.** Если  $f(x)$  — неприводим в  $K[x]$ , то утверждение очевидно. Пусть  $f(x)$  является приводимым многочленом,  $\deg f(x) = n > 0$ . Тогда его можно разложить в произведение

$$f(x) = f_1(x)f_2(x),$$

где  $0 < \deg f_1(x) < n$ ,  $0 < \deg f_2(x) < n$ . Если  $f_1(x)$  и  $f_2(x)$  оба неприводимы в  $K[x]$ , то процесс разложения завершен и теорема, очевидно, верна. В противном случае хотя бы один из многочленов  $f_1(x), f_2(x)$  приводим, пусть

$$\begin{aligned} f_1(x) &= f_{11}(x) f_{12}(x), & 0 < \deg f_{1i}(x) < \deg f_1(x) \quad (i = 1, 2), \\ f_2(x) &= f_{21}(x) f_{22}(x), & 0 < \deg f_{2i}(x) < \deg f_2(x) \quad (i = 1, 2). \end{aligned}$$

Тогда

$$f(x) = f_{11}(x) f_{12}(x) f_{21}(x) f_{22}(x). \quad (2)$$

Если среди многочленов, полученных в правой части (2), есть приводимые, то продолжим процесс разложения.

На каждом шаге степени многочленов, участвующих в разложении, уменьшаются, в то же время они ограничены снизу единицей, поэтому в силу принципа полной упорядоченности процесс разложения должен остановиться через конечное число шагов.

**Теорема 3.** Пусть  $K$  — поле и  $f(x) \in K[x]$ , причем  $\deg f(x) > 0$ . Тогда многочлен  $f(x)$  может быть разложен в произведение неприводимых унитарных многочленов из  $K[x]$ , т.е.

$$f(x) = c f_1(x) f_2(x) \dots f_k(x), \quad f_i(x) \in K[x] \quad (i = 1, 2, \dots, k),$$

где  $c \in K$ . Это разложение единственно с точностью до порядка сомножителей.



*Доказательство.* То, что многочлен  $f(x)$  можно разложить в произведение неприводимых многочленов, следует из теоремы 2. Пусть это разложение имеет вид

$$f(x) = g_1(x) g_2(x) \dots g_k(x), \quad g_i(x) \in K[x] \quad (i = 1, 2, \dots, k).$$

Обозначим  $lc(g_i(x))$  через  $c_i$ , тогда каждый многочлен  $g_i(x)$  можно представить в виде

$$g_i(x) = c_i \cdot \left( \frac{1}{c_i} g_i(x) \right) \quad (i = 1, 2, \dots, k),$$

где  $\tilde{g}_i(x) = \frac{1}{c_i} g_i(x)$  является унитарным многочленом.

Тогда

$$f(x) = (c_1 \tilde{g}_1(x)) (c_2 \tilde{g}_2(x)) \dots (c_k \tilde{g}_k(x)) = \left( \prod_{i=1}^k c_i \right) \tilde{g}_1(x) \tilde{g}_2(x) \dots \tilde{g}_k(x) = c \tilde{g}_1(x) \tilde{g}_2(x) \dots \tilde{g}_k(x),$$

где  $c = \prod_{i=1}^k c_i$ . Таким образом,  $f(x)$  представлен в виде произведения унитарных неприводимых многочленов  $\tilde{g}_i(x)$  ( $i = 1, 2, \dots, k$ ) из  $K[x]$ .

Осталось доказать единственность этого разложения. Проведем рассуждение по индукции (индукция по степени многочлена  $f(x)$ ). Если  $\deg f(x) = 1$ , то теорема, очевидно, верна, поскольку  $f(x)$  неприводим. Пусть теорема верна для многочленов, степени которых меньше  $n$ . Рассмотрим многочлен  $f(x) \in K[x]$ ,  $\deg f(x) = n$ . Предположим, что  $f(x)$  имеет два разложения на неприводимые унитарные многочлены, т.е.

$$f(x) = c g_1(x) g_2(x) \dots g_k(x)$$

и

$$f(x) = d q_1(x) q_2(x) \dots q_s(x).$$

Значит, имеем

$$c g_1(x) g_2(x) \dots g_k(x) = d q_1(x) q_2(x) \dots q_s(x). \quad (2)$$

Неприводимый многочлен  $g_1(x)$  делит произведение  $d q_1(x) q_2(x) \dots q_s(x)$ , поэтому в силу теоремы 1 он делит один из сомножителей, т.е. некоторый многочлен  $q_i(x)$ . Так как  $q_i(x)$  также неприводим, то он должен быть ассоциирован с  $g_1(x)$ , (т.е. может отличаться от  $g_1(x)$  только на обратимый множитель из  $K$ ). Но оба многочлена по условию теоремы унитарны, значит, старшие коэффициенты их равны, поэтому

$$g_1(x) = q_i(x).$$

Поделим обе части равенства (2) на  $g_1(x)$  и обозначим через  $\tilde{f}(x)$  многочлен  $\frac{f(x)}{g_1(x)}$ , тогда получим

$$\tilde{f}(x) = c g_2(x) g_3(x) \dots g_k(x) = d q_1(x) \dots q_{i-1}(x) q_{i+1}(x) \dots q_s(x).$$

Но  $\deg \tilde{f}(x) < n$ , поэтому по предположению индукции его разложение на неприводимые унитарные многочлены единственно с точностью до порядка сомножителей, следовательно,  $k-1 = s-1$  (откуда  $k = s$ ),  $c = d$  и каждый из многочленов  $g_i(x)$  ( $i = 2, \dots, k$ ) равен одному из многочленов  $q_j(x)$  ( $j = 1, 2, \dots, i-1, i+1, \dots, k$ ). А значит, и разложение  $f(x)$  на множители однозначно с точностью до порядка сомножителей.

Теорема доказана.

Из этой теоремы вытекает следующее утверждение.

**Теорема 4.** Пусть  $K$  – поле. Тогда кольцо многочленов  $K[x]$  является факториальным.

На самом деле теорема, аналогичная теореме 3, справедлива и в случае, когда вместо поля  $K$  берется факториальное кольцо  $\mathbf{A}$ .

**Теорема 5 (Гаусс).** Пусть  $\mathbf{A}$  – факториальное кольцо и  $f(x) \in \mathbf{A}[x]$ ,  $\deg f(x) > 0$ . Тогда многочлен  $f(x)$  может быть единственным образом с точностью до перестановки сомножителей разложен в произведение неприводимых нормированных многочленов из кольца  $\mathbf{A}[x]$ .

Другая формулировка этой же теоремы:

Если  $\mathbf{A}$  – факториальное кольцо, то кольцо  $\mathbf{A}[x]$  также является факториальным.

Следствием этого утверждения является, в частности, то, что поскольку  $\mathbf{Z}$  – факториальное кольцо, то кольцо  $\mathbf{Z}[x]$  также факториально. Из теоремы 4 следует, что кольца  $\mathbf{C}[x]$ ,  $\mathbf{R}[x]$  и  $\mathbf{Q}[x]$  также факториальны.



# §11. НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ НАД ПОЛЯМИ $\mathbb{C}$ , $\mathbb{R}$ , $\mathbb{Q}$ И НАД КОЛЬЦОМ $\mathbb{Z}$

Из основной теоремы алгебры:

каждый многочлен  $f(x)$  из  $\mathbb{C}[x]$ , степень которого не меньше единицы, имеет в поле  $\mathbb{C}$  хотя бы один корень

следует, что единственные, отличные от константы неприводимые многочлены в  $\mathbb{C}[x]$  — это многочлены первой степени.

**Теорема 1.** Отличный от константы многочлен  $f(x)$  из  $\mathbb{R}[x]$  неприводим тогда и только тогда, когда либо  $\deg f(x) = 1$ , либо  $f(x) = ax^2 + bx + c$  и  $b^2 - 4ac < 0$ .

*Доказательство.* Очевидно, что любой многочлен первой степени неприводим. Предположим, что  $f(x) = ax^2 + bx + c$ . В поле  $\mathbb{C}$  он имеет корни

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{и} \quad x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

значит, в  $\mathbb{C}[x]$  его можно разложить на множители

$$f(x) = a \left( x + \frac{b + \sqrt{b^2 - 4ac}}{2a} \right) \left( x + \frac{b - \sqrt{b^2 - 4ac}}{2a} \right).$$

Если  $b^2 - 4ac < 0$ , то корни  $x_1$  и  $x_2$  являются комплексными числами, поэтому в  $\mathbb{R}[x]$  многочлен  $f(x)$  неприводим.

Докажем обратное утверждение. Пусть  $f(x)$  — неприводимый многочлен из кольца  $\mathbb{R}[x]$  и  $\deg f(x) > 1$ . Так как многочлен неприводим, то у него нет корней в поле  $\mathbb{R}$ . Но согласно основной теореме алгебры у  $f(x)$  есть комплексный корень

$$\alpha = a + ib, \quad \text{где } a, b \in \mathbb{R}, \quad b \neq 0.$$

Построим многочлен второй степени

$$q(x) = (x - \alpha)(x - \bar{\alpha}), \quad \bar{\alpha} = a - ib.$$

Очевидно,  $q(x)$  есть многочлен с вещественными коэффициентами 1,  $-(\alpha + \bar{\alpha}) = -2a$ ,  $\alpha \bar{\alpha} = |\alpha|^2 = a^2 + b^2$ . Поделим  $f(x)$  на  $q(x)$ :

$$f(x) = q(x)u(x) + r(x), \quad \deg r(x) < \deg q(x), \quad (1)$$

$u(x), r(x) \in \mathbb{R}[x]$ . Многочлен  $r(x)$  имеет степень не превосходящую единицы, т.е.

$$r(x) = cx + d.$$

В равенстве (1) положим  $x = \alpha$ , тогда получим

$$f(\alpha) = q(\alpha)u(\alpha) + r(\alpha),$$

но  $\alpha$  — корень  $f(x)$ , поэтому  $f(\alpha) = 0$ ,  $q(\alpha) = 0$  по построению, значит,  $r(\alpha) = 0$ , т.е.

$$0 = r(\alpha) = c(a + ib) + d = (ca + d) + icb,$$

откуда

$$\begin{cases} ca + d = 0, \\ cb = 0. \end{cases}$$

Поскольку  $b \neq 0$ , то из последнего равенства полученной системы следует, что  $c = 0$ , но тогда из первого равенства получаем  $d = 0$ , значит,  $r(x) = 0$ . Итак,

$$f(x) = q(x)u(x),$$

т.е.  $f(x)$  приводим, если  $u(x)$  не является константой. Так как по условию  $f(x)$  неприводим, то  $u(x) = \text{const} \in \mathbb{R}$ , значит,

$$f(x) = \text{const} \cdot q(x),$$

откуда  $\deg f(x) = \deg q(x) = 2$ . Теорема доказана.

Перейдем к кольцу  $\mathbb{Q}[x]$ . Здесь мы дадим лишь некоторые достаточные критерии неприводимости. На самом деле, как мы увидим ниже, разложение на множители в  $\mathbb{Q}[x]$  – это то же самое, что разложение на множители в  $\mathbb{Z}[x]$ .

Пусть

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$$

– многочлен с рациональными коэффициентами, т.е.  $f(x) \in \mathbb{Q}[x]$ . Умножив  $f(x)$  на наименьшее общее кратное знаменателей всех его коэффициентов  $D$ , получим многочлен с целыми коэффициентами

$$g(x) = Df(x), \quad g(x) \in \mathbb{Z}[x].$$

В кольце  $\mathbb{Q}[x]$  многочлены  $g(x)$  и  $f(x)$  ассоциированы ( $D$  обратим в  $\mathbb{Q}$ ), поэтому  $g(x)$  неприводим в  $\mathbb{Q}[x]$  тогда и только тогда, когда  $f(x)$  неприводим. Поэтому, изучая многочлены в  $\mathbb{Q}[x]$ , можно всегда предполагать, что их коэффициенты являются целыми числами.

Любой многочлен из  $\mathbb{Q}[x]$  с целыми коэффициентами ассоциирован с примитивным многочленом. Действительно, если  $d$  есть наибольший общий делитель коэффициентов многочлена  $f(x)$ , то  $d^{-1}f(x)$  есть многочлен с целыми коэффициентами такой, что наибольший общий делитель его коэффициентов равен 1. Многочлены  $f(x)$  и  $d^{-1}f(x)$  ассоциированы в  $\mathbb{Q}[x]$ .

**Теорема 2 (Гаусс).** Пусть  $f(x)$  – многочлен из  $\mathbb{Q}[x]$  с целыми коэффициентами. Если  $f(x) = g(x)q(x)$  в  $\mathbb{Q}[x]$ , то  $f(x) = g_1(x)q_1(x)$ , где  $g_1(x)$ ,  $q_1(x)$  – многочлены с целыми коэффициентами, ассоциированные с  $g(x)$  и  $q(x)$  соответственно.

*Доказательство.* Без ограничения общности будем считать, что  $f(x)$  – примитивный многочлен. Пусть

$$f(x) = g(x)q(x) \quad \text{в } \mathbb{Q}[x].$$

Тогда существуют рациональные числа  $a$  и  $b$  такие, что  $ag(x)$  и  $bq(x)$  – примитивные многочлены. Произведение примитивных многочленов есть примитивный многочлен, поэтому

$$ag(x) \cdot bq(x) = (ab)f(x)$$

является примитивным многочленом. Но  $f(x)$  также примитивный. Два многочлена  $f(x)$  и  $(ab)f(x)$  примитивны тогда и только тогда, когда  $(ab)$  есть обратимое целое число, значит,  $ab = \pm 1$ . Поэтому

$$f(x) = \pm ab g(x)q(x)$$

и, положив

$$g_1(x) = \pm ag(x), \quad q_1(x) = bq(x),$$

получим

$$f(x) = g_1(x)q_1(x),$$

что и требовалось доказать.

Из этой теоремы следует

**Теорема 3.** Многочлен неприводим в  $\mathbb{Z}[x]$  тогда и только тогда, когда он неприводим как многочлен в  $\mathbb{Q}[x]$ .



**Теорема 4.** Если

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$$

— многочлен из  $\mathbb{Z}[x]$  и  $\frac{a}{b}$  — его рациональный корень такой, что  $\text{НОД}(a, b) = 1$ , то  $b \mid c_n$  и  $a \mid c_0$ .

*Доказательство.* Так как  $\frac{a}{b}$  — корень  $f(x)$ , то

$$c_n \frac{a^n}{b^n} + c_{n-1} \frac{a^{n-1}}{b^{n-1}} + \dots + c_1 \frac{a}{b} + c_0 = 0. \quad (2)$$

Умножив обе части (2) на  $b^n$ , получим

$$c_n a^n + c_{n-1} a^{n-1} b + \dots + c_1 a b^{n-1} + c_0 b^n = 0, \quad (3)$$

откуда

$$c_n a^n = -c_{n-1} a^{n-1} b - \dots - c_1 a b^{n-1} - c_0 b^n = b(-c_{n-1} a^{n-1} - \dots - c_1 a b^{n-2} - c_0 b^{n-1}) = bq, \quad \text{где } q \in \mathbb{Z}.$$

Значит,  $b \mid c_n a^n$ , но  $b$  и  $a$  взаимно простые числа, значит,

$$b \mid c_n.$$

Из (3) также следует

$$\begin{aligned} c_0 b^n &= -c_n a^n - c_{n-1} a^{n-1} b - \dots - c_1 a b^{n-1} = \\ &= a(-c_n a^{n-1} - c_{n-1} a^{n-2} b - \dots - c_1 b^{n-1}) = ar, \quad \text{где } r \in \mathbb{Z}. \end{aligned}$$

Значит,  $a \mid c_0 b^n$ , откуда в силу взаимной простоты  $a$  и  $b$  получаем

$$a \mid c_0.$$

*Замечание.* Если  $\frac{a}{b}$  — корень многочлена  $f(x)$ , то  $f(x)$  делится на  $x - \frac{a}{b}$ , а следовательно, и на  $bx - a$ .

**Теорема 5 (критерий Эйзенштейна).** Пусть

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$$

— многочлен из  $\mathbb{Z}[x]$ . Если существует простое число  $p$  такое, что

$$\begin{aligned} p &\nmid c_n, \\ p &\mid c_i \quad (i = n-1, n-2, \dots, 0), \\ \text{и } p^2 &\nmid c_0, \end{aligned}$$

то многочлен  $f(x)$  неприводим.

*Доказательство.* Предположим противное, пусть указанные условия выполняются, а  $f(x)$  — приводим, тогда

$$f(x) = (a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0)(b_s x^s + b_{s-1} x^{s-1} + \dots + b_1 x + b_0), \quad (4)$$

где  $k > 0$ ,  $s > 0$ ,  $k + s = n$ . Без ограничения общности будем считать, что  $k \geq s$ , тогда, перемножая многочлены в правой части (4) и приравнивая коэффициенты, стоящие в левой и правой частях этого равенства при одинаковых степенях  $x$ , получаем

$$\begin{aligned} c_0 &= a_0 b_0, \\ c_1 &= a_1 b_0 + a_0 b_1, \\ c_2 &= a_2 b_0 + a_1 b_1 + a_0 b_2, \\ &\dots \dots \dots \\ c_k &= a_k b_0 + a_{k-1} b_1 + \dots + a_{k-s} b_s, \\ c_{k+1} &= a_k b_1 + a_{k-1} b_2 + \dots + a_{k+1-s} b_s, \\ &\dots \dots \dots \\ c_{n-2} &= a_k b_{s-2} + a_{k-1} b_{s-1} + a_{k-2} b_s, \\ c_{n-1} &= a_k b_{s-1} + a_{k-1} b_s, \\ c_n &= a_k b_s. \end{aligned} \quad (5)$$



По условию  $p \mid c_0 = a_0 b_0$ , но  $p^2 \nmid c_0$ , поэтому так как  $p$  — простое число, то лишь одно из чисел  $a_0, b_0$  делится на  $p$ . Пусть

$$p \mid a_0 \quad \text{и} \quad p \nmid b_0.$$

Далее,  $p \mid c_1 = a_1 b_0 + a_0 b_1$ , откуда

$$p \mid (c_1 - a_0 b_1) = a_1 b_0,$$

и поскольку  $p \nmid b_0$ , то  $p \mid a_1$ .

Из третьего равенства системы (5) получаем

$$p \mid c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2,$$

значит,

$$p \mid (c_2 - a_1 b_1 - a_0 b_2) = a_2 b_0,$$

т.е.  $p \mid a_2 b_0$  и так как  $p \nmid b_0$ , то  $p \mid a_2$ .

Спускаясь по цепочке равенств (5) вниз и проводя аналогичные рассуждения, получим

$$p \mid a_3, \quad p \mid a_4, \quad \dots, \quad p \mid a_{k-1}, \quad p \mid a_k.$$

Но тогда

$$p \mid a_k b_s = c_n,$$

что противоречит условию теоремы. Значит, наше предположение о приводимости  $f(x)$  неверно.

Отметим, что критерий Эйзенштейна выполняется в любом *факториальном* кольце, а именно справедлива следующая теорема.

**Теорема 6.** Пусть  $\mathbf{A}$  — факториальное кольцо, а  $K$  — поле его дробей. Пусть

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$$

— многочлен с коэффициентами из  $\mathbf{A}$  такой, что для некоторого неприводимого элемента  $p \in \mathbf{A}$  выполнено

$$p \nmid c_n, \quad p \mid c_i \quad (i = n-1, n-2, \dots, 0), \quad p^2 \nmid c_0.$$

Тогда  $f(x)$  неприводим в  $K[x]$ , а значит, и в  $\mathbf{A}[x]$ .

Доказательство проводится аналогично доказательству теоремы 5.

**Пример 1.** Критерий неприводимости Эйзенштейна можно применить к многочлену  $x^n - 2$  ( $n \geq 1$ ). Этот многочлен неприводим в  $\mathbf{Q}[x]$  и в  $\mathbf{Z}[x]$  (в качестве простого числа берем  $p = 2$ ).

**Пример 2.** Рассмотрим многочлен

$$f_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x - 1},$$

где  $p$  — простое число. К этому многочлену непосредственно нельзя применить критерий Эйзенштейна, но можно сделать замену переменной  $x = y + 1$  и попробовать применить критерий к преобразованному многочлену. Получим

$$f(y) = (y+1)^{p-1} + (y+1)^{p-2} + \dots + (y+1) + 1 = \frac{(y+1)^p - 1}{(y+1) - 1} = \frac{1}{y} \{(y+1)^p - 1\} = \frac{1}{y} \sum_{k=1}^p C_p^k y^k =$$

$$\sum_{k=1}^p C_p^k y^{k-1} = y^{p-1} + C_p^{p-1} y^{p-2} + C_p^{p-2} y^{p-3} + \dots + C_p^1.$$

Все коэффициенты  $C_p^{p-i} = \frac{p!}{(p-i)! i!}$  ( $i = 1, 2, \dots, p-1$ ) делятся на  $p$ , так как  $p$  — простое число, старший коэффициент не делится на  $p$  (он равен 1), свободный член  $C_p^1 = p$  не делится на  $p^2$ . Значит,  $f(y)$  неприводим в  $\mathbf{Q}[x]$  и в  $\mathbf{Z}[x]$ , поэтому и  $f_p(x)$  неприводим.

**Пример 3.** Если  $n > 1$  – составное число, то многочлен

$$f_n(x) = x^{n-1} + x^{n-2} + \dots + x + 1$$

приводим. Действительно, пусть  $n = qs$ , тогда

$$f_n(x) = \frac{x^n - 1}{x - 1} = \frac{x^{qs} - 1}{x^q - 1} \cdot \frac{x^q - 1}{x - 1} = \left( x^{q(s-1)} + x^{q(s-2)} + \dots + x^q + 1 \right) (x^{q-1} + x^{q-2} + \dots + x + 1).$$

**Теорема 7.** Пусть  $f(x)$  – многочлен с целыми коэффициентами. Если  $f^{(m)}(x) \equiv f(x) \pmod{m}$  для некоторого целого  $m$ , не делящего старший коэффициент многочлена  $f(x)$ , и многочлен  $f^{(m)}(x)$  неприводим в  $\mathbb{Z}_m[x]$ , то  $f(x)$  неприводим в  $\mathbb{Q}[x]$  (и в  $\mathbb{Z}[x]$ ).

*Доказательство.* Предположим противное, пусть  $f(x)$  приводим, т.е.

$$f(x) = g(x)q(x),$$

где  $g(x)$  и  $q(x)$  – примитивные многочлены с целыми коэффициентами. Тогда для любого  $m$ , не делящего  $lc(f(x))$ , имеем

$$f^{(m)}(x) = g^{(m)}(x)q^{(m)}(x) \quad \text{в } \mathbb{Z}_m[x],$$

т.е.  $f^{(m)}(x)$  разлагается на множители, т.е. приводим. Полученное противоречие и доказывает неприводимость  $f(x)$ .

Из последней теоремы следует, что еще один способ проверки неприводимости многочлена состоит в редукции многочлена по модулю  $m$ , т.е. в переходе к  $f^{(m)}(x)$ , где

$$f^{(m)}(x) \equiv f(x) \pmod{m},$$

причем  $m \nmid lc(f(x))$ . Далее  $f^{(m)}(x)$  проверяется на неприводимость в кольце  $\mathbb{Z}_m[x]$ . Это конечная задача, поскольку в  $\mathbb{Z}_m[x]$  имеется лишь конечное число возможных делителей. Кроме того, существуют методы разложения многочлена в конечном поле, например алгоритм Берлекэмпса.

**Пример 4.** Рассмотрим многочлен

$$f(x) = x^4 + 5x^3 + 3x^2 + x + 3$$

и выясним, является ли он приводимым над полем  $\mathbb{Q}$ .

В качестве целого, не делящего старший коэффициент  $f(x)$ , возьмем  $m = 2$ . Тогда

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

В  $\mathbb{Z}_2[x]$  многочлен  $f^{(2)}(x)$  неприводим. Действительно, у него в  $\mathbb{Z}_2$  нет корней, значит, у него нет линейных сомножителей. Поэтому, если бы он был разложимым в  $\mathbb{Z}_2[x]$ , то он представлялся бы в виде произведения двух неприводимых многочленов второй степени, но в  $\mathbb{Z}_2[x]$  такой многочлен только один – это  $x^2 + x + 1$ . Очевидно, что  $f^{(2)}(x)$  не делится на  $x^2 + x + 1$ , следовательно, неприводим. Значит, по теореме 7 и  $f(x)$  неприводим в  $\mathbb{Q}[x]$  (и в  $\mathbb{Z}[x]$ ).



## §12 НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ В $\mathbb{Z}_p[x]$

**Теорема 1.** Пусть  $K$  – поле,  $m(x)$  – многочлен из кольца  $K[x]$ ,  $\deg m(x) = n$ . Тогда факторкольцо  $K[x]/(m(x))$  является коммутативным кольцом с единицей. Если  $m(x)$  – неприводимый многочлен в  $K[x]$ , то  $K[x]/(m(x))$  – поле.  $K[x]/(m(x))$  является линейным пространством размерности  $n$  над полем  $K$ . Если  $K$  – конечное поле из  $p$  элементов, то поле  $K[x]/(m(x))$  состоит из  $p^n$  элементов.

**Доказательство.** По теореме §6 факторкольцо  $K = \mathbb{Z}_p[x]/(m(x))$  есть поле в случае, когда  $m(x)$  – неприводимый многочлен. Кроме того, мы видели, что если в кольце вычетов  $K[x]/(m(x))$  выбрать классы

$$\bar{1}, \bar{x}, \bar{x}^2, \dots, \bar{x}^{n-1}, \quad (1)$$

представителями которых являются соответственно многочлены

$$1, x, x^2, \dots, x^{n-1}, \quad (2)$$

то любой элемент из  $K[x]/(m(x))$  представляется в виде

$$c_0\bar{1} + c_1\bar{x} + c_2\bar{x}^2 + \dots + c_{n-1}\bar{x}^{n-1}, \quad c_i \in K, \quad (3)$$

т.е. является линейной комбинацией классов (1).

В факторкольце  $K[x]/(m(x))$ , очевидно, выполнены все аксиомы линейного пространства относительно операций сложения элементов этого кольца и умножения их на элементы поля  $K$ , поэтому на  $K[x]/(m(x))$  можно смотреть как на линейное пространство над полем  $K$ . Система (1) является базисом этого линейного пространства. Действительно, любой элемент пространства есть линейная комбинация классов вычетов (1), и эти классы линейно независимы. Линейная независимость классов (1) следует из линейной независимости их представителей, т.е. многочленов (2). Значит, размерность  $K[x]/(m(x))$  равна  $n$ .

Пусть  $K$  – конечное поле из  $p$  элементов. Количество различных элементов в  $K[x]/(m(x))$  равно числу различных линейных комбинаций (3). В выражении (3) каждый из коэффициентов  $c_i$  может принимать любое из  $p$  значений, независимо от значения других коэффициентов. Значит, всего различных линейных комбинаций вида (3)  $p^n$ . Это и есть мощность факторкольца.

Пусть  $K = \mathbb{Z}_p$ , где  $p$  – простое число. Тогда  $K$  – поле и применима теорема 1, т.е.  $\mathbb{Z}_p[x]/(m(x))$  есть линейное пространство над полем  $\mathbb{Z}_p$ , состоящее из  $p^n$  элементов, где  $n = \deg m(x)$ . Если  $m(x)$  неприводим в  $\mathbb{Z}_p[x]$ , то  $\mathbb{Z}_p[x]/(m(x))$  – поле из  $p^n$  элементов. Таким образом, мы получили способ построения полей, состоящих из  $p^n$  элементов, если у нас имеется поле из  $p$  элементов и неприводимый над ним многочлен степени  $n$ . Поэтому займемся выяснением вопроса о существовании таких многочленов. Нам потребуется следующая лемма.

**Лемма.** В кольце характеристики  $p$ , где  $p$  – простое число, для любого целого положительного  $m$  и любого многочлена  $r(x)$  над этим кольцом справедлива формула

$$(r(x))^{p^m} = r(x^{p^m}). \quad (4)$$

**Доказательство.** Сначала покажем, что

$$(r(x))^p = r(x^p). \quad (5)$$

Рассуждения проведем индукцией по числу слагаемых в  $r(x)$ . Пусть

$$r(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}.$$

Представим этот многочлен в виде

$$r(x) = c_0 + r_1(x),$$

где  $r_1(x) = c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}$ .



Тогда имеем

$$(r(x))^p = (c_0 + r_1(x))^p = \sum_{k=0}^p C_p^k (c_0)^k (r_1(x))^{p-k} =$$

$$c_0^p + C_p^1 c_0^{p-1} r(x) + C_p^2 c_0^{p-2} r^2(x) + \dots + C_p^{p-1} c_0 r^{p-1}(x) + r_1^p(x). \quad (6)$$

Но  $p$  делит  $C_p^k$  при  $1 \leq k \leq p-1$ , так как  $p$  – число простое, а

$$C_p^k = \frac{p!}{k!(p-k)!} = pQ_k \quad - \text{целое число.}$$

(Числа в знаменателе меньше  $p$ , поэтому ни одно из них не делит простое число  $p$ .)

Значит, в кольце характеристики  $p$

$$C_p^k = 0$$

или  $C_p^k \equiv 0 \pmod{p}$  для  $1 \leq k \leq p-1$ .

Но тогда в правой части (6) остаются только два слагаемых, получающихся при  $k=0$  и  $k=p$ , т.е.

$$(r(x))^p = (c_0)^p + (r_1(x))^p.$$

Но  $c_0$  – элемент кольца  $\mathbf{Z}_p$ , поэтому по малой теореме Ферма

$$c_0^{p-1} \equiv 1 \pmod{p}$$

или

$$c_0^p \equiv c_0 \pmod{p},$$

значит,

$$(r(x))^p = c_0 + (r_1(x))^p = c_0 + (r_1(x))^p.$$

Рассмотрим  $r_1(x)$ , представив его в виде

$$r_1(x) = c_1 x + (c_2 x^2 + \dots + c_{n-1} x^{n-1}) = c_1 x + r_2(x).$$

Рассуждая так же, как и для  $r(x)$ , получим

$$(r_1(x))^p = (c_1 x + r_2(x))^p = \sum_{k=0}^p C_p^k (c_1 x)^k (r_2(x))^{p-k} \equiv (c_1 x)^p + (r_2(x))^p \pmod{p},$$

и в силу того что  $c_1$  – элемент  $\mathbf{Z}_p$ , т.е.  $c_1^p \equiv c_1 \pmod{p}$ , имеем

$$(r_1(x))^p = c_1 x^p + (r_2(x))^p.$$

Таким образом,

$$(r(x))^p = c_0 + c_1 x^p + (r_2(x))^p.$$

Далее, повторяя рассуждение для  $r_2(x)$  и т.д., получим

$$(r(x))^p = c_0 + c_1 x^p + c_2 (x^2)^p + \dots + c_{n-1} (x^{n-1})^p$$

$$= c_0 + c_1 x^p + c_2 (x^p)^2 + \dots + c_{n-1} (x^p)^{n-1} = r(x^p)$$

т.е. равенство (4) верно.

Рассмотрим

$$(r(x))^{p^2} = ((r(x))^p)^p.$$

Применяя два раза доказанное соотношение (5), получаем

$$((r(x))^p)^p = (r(x^p))^p = (r(y))^p = r(y^p) = r((x^p)^p) = r(x^{p^2})$$

(здесь  $y = x^p$ ), т.е.

$$(r(x))^{p^2} = r(x^{p^2}).$$

Применяя последнее соображение и пользуясь методом математической индукции, теперь нетрудно получить

$$(r(x))^{p^m} = r(x^{p^m})$$

для любого целого положительного  $m$ .

**Теорема 2.** Пусть  $p$  – простое целое,  $n$  – натуральное число,  $q(x)$  – неприводимый многочлен из кольца  $\mathbb{Z}_p[x]$ . Тогда

$$q(x) \mid x^{p^n} - x \quad \text{тогда и только тогда, когда} \quad \deg q(x) \mid n.$$

*Доказательство.* При  $p$  простом  $\mathbb{Z}_p$  является полем, поэтому по теореме 1 в силу неприводимости многочлена  $q(x)$  в  $\mathbb{Z}_p[x]$ , факторкольцо  $K = \mathbb{Z}_p[x]/(q(x))$  является полем из  $p^d$  элементов, где  $d = \deg q(x)$ . Тогда  $K^* = K/\{0\}$  относительно операции умножения является мультипликативной группой порядка  $p^d - 1$ . Порядок любого элемента группы должен делить порядок группы, т.е.  $p^d - 1$ , а значит, для любого элемента  $y \in K^*$  выполняется

$$y^{p^d - 1} = 1. \quad (7)$$

Пусть  $d$  делит  $n$ . Покажем, что тогда  $q(x)$  делит  $x^{p^n} - x$ . Так как  $d$  делит  $n$ , то  $p^d - 1$  делит  $p^n - 1$ . Действительно, если  $n = kd$ , то

$$p^n - 1 = p^{kd} - 1 = (p^d - 1)(p^{d(k-1)} + p^{d(k-2)} + \dots + p^d + 1).$$

Поэтому из (7) следует, что для любого  $y \in K^*$

$$y^{p^n - 1} = 1,$$

откуда

$$y^{p^n} = y. \quad (8)$$

Рассмотрим в качестве элемента  $y$  из  $K^*$  класс вычетов  $\bar{x}$ . Тогда (8) принимает вид:

$$\bar{x}^{p^n} = \bar{x}. \quad (9)$$

Переходя к представителю класса  $\bar{x}$ , (9) можно записать в виде

$$x^{p^n} \equiv x \pmod{q(x)},$$

но это означает, что  $x^{p^n} - x$  делится на  $q(x)$ .

Обратно, пусть  $q(x)$  делит  $x^{p^n} - x$ . Докажем, что  $d \mid n$ . Поскольку  $q(x)$  делит  $x^{p^n} - x$ , то справедливо сравнение

$$x^{p^n} - x \equiv 0 \pmod{q(x)}$$

или

$$x^{p^n} \equiv x \pmod{q(x)}.$$

В факторкольце вычетов  $K$  последнее сравнение можно записать в виде

$$\bar{x}^{p^n} = \bar{x}. \quad (10)$$

Всякий элемент  $y$  из кольца  $K$  по теореме 1 можно представить в виде

$$y = c_0 \cdot \bar{1} + c_1 \cdot \bar{x} + \dots + c_{d-1} \cdot \bar{x}^{d-1}, \quad c_i \in \mathbb{Z}_p \quad (i = 0, \dots, d-1),$$

т.е.

$$y = r(\bar{x}).$$

Так как поле  $K$  имеет характеристику  $p$ , то справедливо

$$y^{p^n} = (r(\bar{x}))^{p^n} = r(\bar{x}^{p^n})$$

в силу доказанной выше леммы. Из (10) получаем

$$y^{p^n} = r(\bar{x}^{p^n}) = r(\bar{x}) = y,$$

т.е. для любого  $y \in K$  выполняется

$$y^{p^n} = y,$$

а для любого  $y$  из  $K^*$  выполняется

$$y^{p^n-1} = 1.$$

Пусть  $d \nmid n$ . Тогда  $n = qd + r$ , где  $0 < r < d$  и

$$p^n - 1 = p^{qd+r} - 1 = p^{dq} p^r - 1 = p^{dq} p^r - p^r + p^r - 1 = (p^{qd} - 1)p^r + (p^r - 1).$$

Для любого  $y \in K^*$  имеем

$$1 = y^{p^n-1} = y^{(p^{qd}-1)p^r} y^{p^r-1} = y^{p^r-1}$$

так как  $y^{p^{qd}-1} = 1$  ( $p^d - 1$  делит  $p^{qd}-1$ ). Значит, для любого  $y$  из  $K^*$  выполнено

$$y^{p^r-1} = 1.$$

Так как  $K$  — поле, рассмотрим кольцо многочленов над этим полем  $K[y]$ . Очевидно, многочлен  $f(y) = y^{p^r-1} - 1$  принадлежит кольцу  $K[y]$ . Его степень  $p^r - 1 < p^d - 1$ , но любой ненулевой элемент поля  $K$  удовлетворяет уравнению

$$y^{p^r-1} = 1.$$

Значит, последнее уравнение в поле  $K$  имеет  $p^d - 1$  различных корней, но его степень меньше, чем число корней. Значит,  $y^{p^r-1} - 1$  есть нулевой многочлен, т.е.

$$y^{p^r-1} \equiv 1 \quad \text{для любого} \quad y \in K^*,$$

но это означает, что  $p^r - 1 = 0$  или  $r = 0$ . Следовательно,  $n = qd$ , т.е.  $d$  делит  $n$ , что и требовалось доказать.

Теперь с помощью теоремы 2 мы сможем найти число неприводимых многочленов степени  $n$  в кольце  $\mathbb{Z}_p[x]$  ( $p$  — простое) со старшим коэффициентом, равным единице (унитарных многочленов).

Очевидно, что любой неприводимый многочлен определен с точностью до умножения на любой ненулевой элемент поля  $\mathbb{Z}_p$ , поэтому достаточно знать набор унитарных многочленов.

**Теорема 3.** Пусть  $I_p^n$  — число неприводимых унитарных многочленов степени  $n$  в кольце  $\mathbb{Z}_p[x]$ , где  $p$  — простое число, а  $n$  — натуральное. Тогда справедливы следующие утверждения:

- $$\begin{aligned} (1) \quad p^n &= \sum_{d|n} d I_p^d; \\ (2) \quad I_p^n &\geq 1 \text{ для всякого простого числа } p \text{ и всякого натурального } n. \end{aligned} \tag{11}$$

Т.е. для любого натурального  $n$  существует неприводимый над полем  $\mathbb{Z}_p$  многочлен степени  $n$ .

**Доказательство.** Многочлен  $x^{p^n} - x$  из  $\mathbb{Z}_p[x]$  не имеет сомножителей, являющихся полными квадратами. Действительно, если предположить, что такие сомножители есть, т.е.

$$x^{p^n} - x = U^2(x) V(x), \quad U(x), V(x) \in \mathbb{Z}_p[x],$$

то, находя производную от обеих частей равенства, получаем

$$p^n x^{p^n-1} - 1 = 2U(x) U'(x) V(x) + U^2(x) V'(x)$$



и так как  $p^n \equiv 0 \pmod{p}$ , то

$$-1 = U(x) (2U'(x)V(x) + U(x)V'(x)).$$

В левой части полученного равенства стоит константа, значит, и в правой также должна стоять константа, следовательно,  $U(x)$  является константой.

Из теоремы 2 следует, что унитарные неприводимые многочлены  $Q(x)$ , степень которых делит  $n$ , являются неприводимыми унитарными делителями  $x^{p^n} - x$ . Так как  $x^{p^n} - x$  не имеет сомножителей, являющихся квадратами, то каждый из этих многочленов  $Q(x)$  появляется *ровно один раз* в разложении  $x^{p^n} - x$  на простые множители. Значит,

$$x^{p^n} - x = \prod_{d|n} \prod_{Q(x) \in \mathcal{K}_p^d} Q(x),$$

где  $\mathcal{K}_p^d$  — множество неприводимых унитарных многочленов степени  $d$  над полем  $\mathbb{Z}_p$ . Тогда степень многочлена, стоящего справа, равна

$$\sum_{d|n} d I_p^d,$$

значит,

$$p^n = \sum_{d|n} d I_p^d,$$

что доказывает (11).

Докажем второе утверждение теоремы. Очевидно, из доказанного равенства

$$p^d = \sum_{l|d} l I_p^l = d I_p^d + \sum_{\substack{l|d \\ l \neq d}} l I_p^l \geq d I_p^d. \quad (12)$$

Воспользовавшись неравенством (12), оценим  $p^n$ :

$$\begin{aligned} p^n &= \sum_{d|n} d I_p^d = n I_p^n + \sum_{\substack{d|n \\ d \neq n}} d I_p^d \leq n I_p^n + \sum_{\substack{d|n \\ d \neq n}} p^d \leq n I_p^n + \sum_{d=0}^{n-1} p^d \\ &= n I_p^n + (1 + p + p^2 + \dots + p^{n-1}) = n I_p^n + \frac{p^n - 1}{p - 1}, \end{aligned}$$

откуда

$$n I_p^n \geq p^n - \frac{p^n - 1}{p - 1} \geq 1.$$

Так как числа  $n$  и  $I_p^n$  целые, то  $I_p^n \geq 1$ . Теорема доказана.

Из этой теоремы следует, что для простого числа  $n$  имеем

$$I_p^n = \frac{p^n - p}{n} = \frac{p(p^{n-1} - 1)}{n}. \quad (13)$$

Действительно, если  $n$  — простое число, то оно делится лишь на 1 и на себя, поэтому в силу теоремы 3

$$p^n = I_p^1 + n I_p^n, \quad \text{значит,} \quad I_p^n = \frac{1}{n} (p^n - I_p^1),$$

но  $I_p^1 = p$ , откуда и следует формула (13).

В частности,

$$I_p^2 = \frac{p^2 - p}{2} = \frac{p(p-1)}{2},$$

$$I_p^3 = \frac{p^3 - p}{3} = \frac{p(p^2 - 1)}{3}.$$

Из формулы (11) получаем

$$p^n = nI_p^n + \sum_{\substack{d|n \\ d \neq n}} dI_p^d,$$

откуда

$$I_p^n = \frac{1}{n} \left( p^n - \sum_{\substack{d|n \\ d \neq n}} dI_p^d \right). \quad (14)$$

Формула (14) дает рекуррентное соотношение, позволяющее найти  $I_p^n$  для произвольного числа  $n$ .

**Пример 1.** Посчитаем число неприводимых унитарных многочленов над полем  $\mathbb{Z}_2$ , степени которых не превосходят число 7.

Для вычисления  $I_2^2$ ,  $I_2^3$ ,  $I_2^5$  и  $I_2^7$  можно воспользоваться формулой (13):

$$I_2^1 = 2, \quad I_2^2 = \frac{2^2 - 2}{2} = 1, \quad I_2^3 = \frac{2^3 - 2}{3} = 2, \quad I_2^5 = \frac{2^5 - 2}{5} = 6, \quad I_2^7 = \frac{2^7 - 2}{7} = 18.$$

Для вычисления  $I_2^4$  и  $I_2^6$  требуется формула (14):

$$I_2^4 = \frac{1}{4}(2^4 - I_2^1 - 2I_2^2) = \frac{1}{4}(16 - 2 - 2) = 3,$$

$$I_2^6 = \frac{1}{6}(2^6 - I_2^1 - 2I_2^2 - 3I_2^3) = \frac{1}{6}(64 - 2 - 2 - 3 \cdot 2) = 9.$$

**Пример 2.** Посчитаем число неприводимых унитарных многочленов степени не выше 4 над полем  $\mathbb{Z}_3$ :

$$I_3^1 = 3, \quad I_3^2 = \frac{3^2 - 3}{2} = 3, \quad I_3^3 = \frac{3^3 - 3}{3} = 8,$$

$$I_3^4 = \frac{1}{4}(3^4 - I_3^1 - 2I_3^2) = \frac{1}{4}(81 - 3 - 6) = 18.$$

Что касается нахождения самих неприводимых многочленов, то если многочлены малых степеней выписать довольно просто, то для произвольного целого  $n$  это серьезная задача, решение которой будет получено в дальнейшем.

Выпишем неприводимые многочлены малых степеней над полем  $\mathbb{Z}_2$ .

Очевидно, любой многочлен первой степени неприводим. Над  $\mathbb{Z}_2$  это многочлены

$$x, \quad x + 1. \quad (15)$$

Неприводимый многочлен второй степени в  $\mathbb{Z}_2[x]$  всего один. Это многочлен, который нельзя разложить в произведение многочленов первой степени, значит, он не имеет корней в  $\mathbb{Z}_2$ . Очевидно, это

$$x^2 + x + 1. \quad (16)$$

Неприводимых многочленов третьей степени, как мы видели, всего два. Они не должны иметь корней в  $\mathbb{Z}_2$  и не могут раскладываться в произведение одного из многочленов (15) и многочлена (16). Значит, они должны быть отличны от следующих многочленов:

$$x^3, \quad x^2(x + 1), \quad x(x + 1)^2, \quad (x + 1)^3, \quad x(x^2 + x + 1), \quad (x + 1)(x^2 + x + 1)$$

или

$$x^3, \quad x^3 + x^2, \quad x^3 + x, \quad x^3 + x^2 + x + 1, \quad x^3 + x^2 + x, \quad x^3 + 1.$$

Оставшиеся два многочлена третьей степени из  $\mathbb{Z}_2[x]$

$$x^3 + x^2 + 1, \quad x^3 + x + 1 \quad (17)$$

и являются неприводимыми.

Выписать три неприводимых многочлена четвертой степени в  $\mathbb{Z}_2[x]$  сложнее. Для этого из 16 многочленов четвертой степени надо отбросить приводимые. Будем рассуждать следующим образом: так как многочлен не должен иметь корней в  $\mathbb{Z}_2$ , то свободный член всегда равен 1 (иначе 0 – корень), и отличных от нуля коэффициентов должно быть нечетное число (иначе 1 – корень), значит, выбирать неприводимые следует из многочленов

$$x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1, \quad x^4 + x^2 + 1, \quad x^4 + x + 1,$$

только один из которых приводим в  $\mathbb{Z}_2[x]$ . Это многочлен

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

Таким образом, неприводимые многочлены:

$$x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1, \quad x^4 + x + 1.$$

Формулой (14) пользоваться не всегда удобно, так как требуется знать значения  $I_p^d$  для всех делителей  $d$  числа  $n$ . Получим еще одну формулу для вычисления  $I_p^n$ . Для этого воспользуемся формулой обращения Мебиуса (см. §13 в [4]).

Согласно доказанной теореме имеем

$$p^n = \sum_{d|n} d I_p^d. \quad (18)$$

Пусть

$$f(n) = p^n, \quad g(d) = d I_p^d, \quad (19)$$

тогда (18) принимает вид

$$f(n) = \sum_{d|n} g(d).$$

Согласно формуле обращения Мебиуса

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right),$$

т.е. в нашем случае для функций, определенных формулой (19), имеем

$$n I_p^n = \sum_{d|n} \mu(d) p^{\frac{n}{d}},$$

откуда

$$I_p^n = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}. \quad (20)$$

**Пример 3.** Вычислим  $I_2^6$  по формуле (20):

$$I_2^6 = \frac{1}{6}(\mu(1)2^6 + \mu(2)2^3 + \mu(3)2^2 + \mu(6)2).$$

Так как  $\mu(1) = 1$ ,  $\mu(2) = \mu(3) = -1$ ,  $\mu(6) = 1$ , то

$$I_2^6 = \frac{1}{6}(2^6 - 2^3 - 2^2 + 2) = 9.$$



**Пример 4.** Вычислим число неприводимых унитарных многочленов степени 4 в кольце  $\mathbb{Z}_5[x]$ , т.е.  $I_5^4$ .

По формуле (20) получаем

$$I_5^4 = \frac{1}{4}(\mu(1)5^4 + \mu(2)5^2 + \mu(4)5) = \frac{1}{4}(5^4 - 5^2) = \frac{5^2(5^2 - 1)}{4} = 5^2 \cdot 6 = 150,$$

так как  $\mu(1) = 1$ ,  $\mu(2) = -1$ ,  $\mu(4) = 0$ .

**Теорема 4 (критерий неприводимости многочлена над  $\mathbb{Z}_p$ ).** Пусть  $p$  – простое натуральное число,  $Q(x) \in \mathbb{Z}_p[x]$  – многочлен степени  $n$ . Многочлен  $Q(x)$  неприводим тогда и только тогда, когда для любого простого делителя  $q$  числа  $n$  выполнено:

$$Q(x) \text{ делит } x^{p^n} - x \quad \text{и} \quad \text{НОД}(x^{p^{\frac{n}{q}}} - x, Q(x)) = 1.$$

*Доказательство.* Пусть  $Q(x)$  – неприводимый многочлен над  $\mathbb{Z}_p$ . По теореме 2  $Q(x)$  делит  $x^{p^n} - x$  (так как  $\deg Q(x) = n$  и  $n$  делит само себя) и не делит  $x^{p^m} - x$ , если  $m$  – собственный делитель  $n$  (степень  $Q(x)$  не делит  $m$ ), т.е.  $x^{p^{\frac{n}{q}}} - x$  и  $Q(x)$  взаимно просты для любого делителя  $q$  числа  $n$ .

Обратно, пусть выполнены условия на делимость, указанные в теореме. Покажем, что тогда многочлен  $Q(x)$  неприводим. Предположим противное, т.е. что  $Q(x)$  является приводимым многочленом:

$$Q(x) = R(x)S(x),$$

где  $R(x)$  – неприводимый множитель в разложении  $Q(x)$ . Тогда  $R(x)$  делит  $x^{p^n} - x$  и не делит  $x^{p^{\frac{n}{q}}} - x$  для любого простого делителя  $q$  числа  $n$  (так как  $x^{p^{\frac{n}{q}}} - x$  и  $Q(x)$  взаимно просты). Используя теорему 2, получаем, что  $\deg R(x)$  должна делить число  $n$  и не делить числа  $\frac{n}{q}$  для любого простого делителя  $q$  числа  $n$ . Но это означает, что  $\deg R(x) = n$ , т.е.  $R(x)$  ассоциирован с  $Q(x)$  в  $\mathbb{Z}_p$ . Следовательно,  $Q(x)$  неприводим.

**Пример 5.** Выясним, является ли неприводимым над  $\mathbb{Z}_2$  многочлен  $Q(x) = x^6 + x^5 + 1$ .

В силу теоремы 4 следует проверить, что  $Q(x)$  делит  $x^{2^6} - x$  и взаимно прост с каждым из многочленов  $x^{2^3} - x$  и  $x^{2^2} - x$ . (2 и 3 – простые делители числа  $6 = \deg Q(x)$ ).

Рассмотрим многочлен  $x^{2^6} - x$  и найдем частичное разложение его на множители:

$$\begin{aligned} x^{2^6} - x &= x(x^{63} - 1) = x(x^{21} - 1)(x^{42} + x^{21} + 1) \\ &= x(x^7 - 1)(x^{14} + x^7 + 1)((x^3)^{14} + (x^3)^7 + 1) \\ &= x(x^7 - 1)(x^2 + x + 1)(x^{12} + x^{11} + x^9 + x^8 + x^6 + x^4 + x^3 + x + 1)(x^6 + x^3 + 1) \\ &\times (x^{36} + x^{33} + x^{27} + x^{24} + x^{18} + x^{12} + x^9 + x^3 + 1), \end{aligned}$$

так как

$$(x^{14} + x^7 + 1) = (x^2 + x + 1)(x^{12} + x^{11} + x^9 + x^8 + x^6 + x^4 + x^3 + x + 1).$$

В результате получаем следующее разложение многочлена  $x^{2^6} - x$

$$\begin{aligned} x^{2^6} - x &= x(x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) \\ &\times (x^{12} + x^{11} + x^9 + x^8 + x^6 + x^4 + x^3 + x + 1)(x^6 + x^3 + 1) \\ &\times (x^{36} + x^{33} + x^{27} + x^{24} + x^{18} + x^{12} + x^9 + x^3 + 1). \end{aligned}$$

Очевидно, что первые четыре сомножителя не делятся на  $Q(x)$ , и многочлен  $x^6 + x^3 + 1$  также на  $Q(x)$  не делится. Поэтому следует выяснить, делится ли на  $Q(x)$  один из оставшихся двух

многочленов, соответственно 12 и 36 степеней. Непосредственной проверкой нетрудно убедиться, что

$$x^{36} + x^{33} + x^{27} + x^{24} + x^{18} + x^{12} + x^9 + x^3 + 1 = (x^6 + x^5 + 1)(x^{30} + x^{29} + x^{28} + x^{24} + x^{22} + x^{16} + x^{15} + x^{14} + x^{13} + x^{10} + x^8 + x^6 + x^5 + x^3 + 1).$$

Итак,  $Q(x)$  делит  $x^{2^6} - x$ .

Для проверки второго условия рассмотрим многочлены  $x^{2^3} - x$  и  $x^{2^2} - x$ :

$$x^{2^3} - x = x(x^7 - 1) = x(x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = x(x - 1)(x^3 + x^2 + 1)(x^3 + x + 1),$$

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

Достаточно проверить, что  $Q(x)$  не делится ни на один из многочленов  $x$ ,  $x - 1$ ,  $x^2 + x + 1$ ,  $x^3 + x^2 + 1$ ,  $x^3 + x + 1$ . Так как каждый из них над полем  $\mathbf{Z}_2$  неприводим, то если  $Q(x)$  взаимно прост с каждым из них, он будет взаимно прост и с многочленами  $x^{2^3} - x$  и  $x^{2^2} - x$ . Очевидно, что  $x$  и  $x - 1$  не делят  $Q(x)$ . Кроме того,

$$x^6 + x^5 + 1 = (x^3 + x^2 + 1)(x^3 + 1) + x^2,$$

$$x^6 + x^5 + 1 = (x^3 + x + 1)(x^3 + x^2 + x) + (x + 1),$$

$$x^6 + x^5 + 1 = (x^2 + x + 1)(x^4 + x^2 + x) + (x + 1),$$

т.е.  $Q(x)$  не делится на  $x^3 + x^2 + 1$ ,  $x^3 + x + 1$ ,  $x^2 + x + 1$ .

Итак, условия теоремы 4 для  $Q(x)$  выполняются, следовательно,  $Q(x) = x^6 + x^5 + 1$  является неприводимым многочленом 6-й степени над полем  $\mathbf{Z}_2$ .

**Пример 6.** Выясним, является ли неприводимым над  $\mathbf{Z}_3$  многочлен  $q(x) = x^4 + x + 2$ .

Проверим, делит ли  $q(x)$  многочлен  $x^{3^4} - x$  в  $\mathbf{Z}_3[x]$ , и выясним, является ли он взаимно простым с многочленом  $x^{3^2} - x$  (2 — единственный простой делитель числа 4). Начнем с проверки второго условия. С помощью алгоритма Евклида ищем наибольший общий делитель  $q(x)$  и  $x^9 - x$  в  $\mathbf{Z}_3[x]$ :

$$x^9 - x = (x^4 + x + 2)(x^5 - x^2 - 2x) + (x^3 + x^2),$$

$$x^4 + x + 2 = (x^3 + x^2)(x - 1) + (x^2 + x + 2),$$

$$x^3 + x^2 = (x^2 + x + 2)x + x,$$

$$x^2 + x + 2 = x(x + 1) + 2,$$

значит,  $\text{НОД}(x^9 - x, q(x)) = 2 = \text{const}$ , т.е. многочлены взаимно просты.

Многочлен  $x^{3^4} - x = x^{81} - x$  в  $\mathbf{Z}_3[x]$  можно разложить в произведение многочленов меньших степеней:

$$x^{81} - x = x(x - 1)(x + 1)(x^2 + 1)(x^4 + 1)(x^8 + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1) \times$$

$$(x^8 - x^6 + x^4 - x^2 + 1)(x^{16} - x^{12} + x^8 - x^4 + 1)(x^{32} - x^{24} + x^{16} - x^8 + 1),$$

пользуясь формулами

$$x^{2k} - 1 = (x^k - 1)(x^k + 1),$$

$$x^{5k} + 1 = (x^k + 1)(x^{4k} - x^{3k} + x^{2k} - x^k + 1),$$

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1).$$

Если  $q(x)$  делит  $x^{81} - x$ , то он должен делить один из многочленов

$$x^8 + 1, \quad x^8 - x^6 + x^4 - x^2 + 1, \quad x^{16} - x^{12} + x^8 - x^4 + 1, \quad x^{32} - x^{24} + x^{16} - x^8 + 1.$$

Непосредственной проверкой убеждаемся, что

$$x^{32} - x^{24} + x^{16} - x^8 + 1 =$$

$$q(x)(x^{28} - x^{25} + x^{24} + x^{22} - 2x^{21} - x^{19} - 2x^{17} + x^{16} - x^{15} + 2x^{14} + 2x^{10} - 2x^7 + 2x^6 + x^4 - x^3 + 2x^2 - x + 2).$$

Итак,  $q(x)$  неприводим в  $\mathbf{Z}_3[x]$ .

**Пример 7.** Найти все неприводимые многочлены из  $\mathbb{Z}_3[x]$  вида  $x^3 + ax + b$ .

Так как рассматриваются многочлены третьей степени, то если такой многочлен приводим, то он раскладывается в произведение либо трех многочленов первой степени, либо в произведение многочлена первой степени и неприводимого многочлена второй степени. Но в любом случае в разложении участвует хотя бы один многочлен первой степени, следовательно, приводимый многочлен третьей степени должен иметь корень в  $\mathbb{Z}_3$ . Значит, следует найти многочлены, не имеющие корней в  $\mathbb{Z}_3$ . Чтобы 0 не являлся корнем многочлена, следует выбирать  $b \neq 0$ , т.е.  $b$  может принимать только два значения: 1 и 2.

Рассмотрим многочлены

$$x^3 + ax + 1 \quad \text{и} \quad x^3 + ax + 2, \quad a \in \mathbb{Z}_3.$$

При  $a = 0$  получаем многочлены

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

каждый из которых имеет корень в  $\mathbb{Z}_3$  ( $x = 2$  и  $x = 1$  соответственно).

При  $a = 1$  получаем многочлены

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

каждый из которых также имеет в  $\mathbb{Z}_3$  корень ( $x = 1$  и  $x = 2$  соответственно).

При  $a = 2$  получаем многочлены

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

не имеющие в  $\mathbb{Z}_3$  корней, значит, они и являются искомыми.



### §13. РЕШЕТО ЭРАТОСФЕНА ДЛЯ МНОГОЧЛЕНОВ ИЗ $\mathbb{Z}_p[x]$

Мы уже видели, что проверка критерия неприводимости многочлена из  $\mathbb{Z}_p[x]$  даже для достаточно небольших степеней  $n$  является трудоемкой задачей. Выписать же все неприводимые многочлены данной степени  $n$  (при  $n \geq 5$ ) из  $\mathbb{Z}_p[x]$  – задача еще более сложная. Один из способов ее решения – применить ту же идею, которая работает при выборе простых целых чисел, т.е. получить алгоритм для многочленов, подобный "решету Эратосфена".

Это возможно потому, что в  $\mathbb{Z}_p[x]$  количество многочленов каждой фиксированной степени  $n$  конечно, значит, можно выписать все многочлены от первой до  $n$ -й степени включительно и затем, начиная с начала списка, на каждом шаге "вычеркивать" приводимые, т.е. те, которые делятся на неприводимый, выбранный на предыдущем шаге. При этом, очевидно, следует рассматривать унитарные многочлены из  $\mathbb{Z}_p[x]$ , так как умножение на константу не влияет на приводимость многочлена.

Рассмотрим унитарные многочлены из  $\mathbb{Z}_p[x]$ , т.е. многочлены вида

$$f(x) = x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1x + a_0, \quad (1)$$

$k \geq 1$ ,  $a_i \in \mathbb{Z}_p$  ( $i = 0, 1, \dots, k-1$ ). Всего в  $\mathbb{Z}_p[x]$  многочленов вида (1) имеется ровно  $p^k$  (так как каждый из  $k$  коэффициентов  $a_0, a_1, \dots, a_{k-1}$  независимо от остальных может принимать любое значение из  $\mathbb{Z}_p$ ).

Пусть  $\mathfrak{A}_n$  – множество унитарных многочленов из  $\mathbb{Z}_p[x]$  степеней, не превосходящих  $n$ . Мощность множества  $\mathfrak{A}_n$ , очевидно, равна

$$|\mathfrak{A}_n| = p + p^2 + p^3 + \dots + p^n.$$

Рассмотрим отображение  $\varphi$ , которое каждому многочлену вида (1) ставит в соответствие пару чисел

$$(k, a_{k-1}p^{k-1} + a_{k-2}p^{k-2} + \dots + a_1p + a_0).$$

Заметим, что

$$0 \leq a_{k-1}p^{k-1} + a_{k-2}p^{k-2} + \dots + a_1p + a_0 \leq p^k - 1,$$

значит,

$$\varphi : \mathfrak{A}_n \rightarrow \mathfrak{B}_n,$$

где  $\mathfrak{B}_n = \bigcup_{k=1}^n \{k\} \times [0, p^k)$ .

Отображение  $\varphi$  биективно. Проверим это. Пусть

$$f_1(x) = x^t + a_{t-1}x^{t-1} + \dots + a_0, \quad f_2(x) = x^s + b_{s-1}x^{s-1} + \dots + b_0,$$

$a_i \in \mathbb{Z}_p$  ( $i = 0, 1, \dots, t-1$ ),  $b_j \in \mathbb{Z}_p$  ( $j = 0, 1, \dots, s-1$ ). Предположим, что

$$\varphi(f_1(x)) = \varphi(f_2(x)),$$

т.е. многочленам  $f_1(x)$  и  $f_2(x)$  отображение  $\varphi$  ставит в соответствие одинаковые пары чисел, но

$$\varphi(f_1(x)) = (t, a_{t-1}p^{t-1} + \dots + a_0), \quad \varphi(f_2(x)) = (s, b_{s-1}p^{s-1} + \dots + b_0).$$

Из равенства

$$(t, a_{t-1}p^{t-1} + \dots + a_0) = (s, b_{s-1}p^{s-1} + \dots + b_0)$$

следует, что

$$\deg f_1(x) = t = s = \deg f_2(x)$$

и

$$a_{t-1}p^{t-1} + \dots + a_1p + a_0 = b_{t-1}p^{t-1} + \dots + b_1p + b_0. \quad (2)$$

Итак, степени многочленов совпадают, а равенство (2) перепишем в виде

$$(a_{t-1} - b_{t-1})p^{t-1} + (a_{t-2} - b_{t-2})p^{t-2} + \dots + (a_1 - b_1)p + (a_0 - b_0) = 0$$

или

$$(a_{t-1} - b_{t-1})p^{t-1} + (a_{t-2} - b_{t-2})p^{t-2} + \dots + (a_1 - b_1)p = b_0 - a_0. \quad (3)$$

Левая часть равенства (3) делится на  $p$ , следовательно, и правая часть должна делиться на  $p$ , но  $a_0, b_0 \in \mathbb{Z}_p$ , поэтому  $b_0 - a_0 < p$ , значит,  $b_0 - a_0 = 0$  в  $\mathbb{Z}_p$ .

Поделим левую часть равенства (3) на  $p$ :

$$(a_{t-1} - b_{t-1})p^{t-2} + (a_{t-2} - b_{t-2})p^{t-3} + \dots + (a_1 - b_1) = 0,$$

откуда

$$(a_{t-1} - b_{t-1})p^{t-2} + (a_{t-2} - b_{t-2})p^{t-3} + \dots + (a_2 - b_2)p = b_1 - a_1. \quad (4)$$

Из того, что левая часть (4) делится на  $p$ , следует, что  $b_1 - a_1$  делится на  $p$ , но  $b_1 - a_1 < p$ , значит,  $b_1 - a_1 = 0$  в  $\mathbb{Z}_p$ .

Продолжая аналогичные рассуждения, получим

$$a_0 = b_0, \quad a_1 = b_1, \quad a_2 = b_2, \quad \dots, \quad a_{t-1} = b_{t-1},$$

откуда следует, что  $f_1(x) = f_2(x)$ . Таким образом, доказано, что отображение  $\varphi$  является инъекцией.

Покажем, что  $\varphi$  – сюръекция. Рассмотрим произвольную пару  $(k, \sigma_k)$ , где  $k \leq n$ ,  $\sigma_k \in [0, p^k)$ , и найдем многочлен  $f(x) \in \mathbb{Z}_p[x]$ , являющийся прообразом этой пары чисел при отображении  $\varphi$ . Во-первых, степень  $f(x)$  определена однозначно первым числом пары,  $\deg f(x) = k$ , значит,

$$f(x) = x^k + a_{k-1}x^{k-1} + \dots + a_1x + a_0$$

и следует определить коэффициенты  $a_0, a_1, \dots, a_{k-1}$ .

В силу определения  $\varphi$

$$\sigma_k = a_{k-1}p^{k-1} + a_{k-2}p^{k-2} + \dots + a_1p + a_0, \quad a_i \in \mathbb{Z}_p. \quad (5)$$

Из (5) следует

$$\sigma_k = p(a_{k-1}p^{k-2} + a_{k-2}p^{k-3} + \dots + a_1) + a_0 = p\sigma_k^{(1)} + a_0,$$

т.е.  $a_0$  есть остаток от деления  $\sigma_k$  на  $p$  (очевидно,  $0 \leq a_0 < p$ ).

Далее

$$\sigma_k^{(1)} = a_{k-1}p^{k-2} + a_{k-2}p^{k-3} + \dots + a_1 = p(a_{k-1}p^{k-3} + a_{k-2}p^{k-4} + \dots + a_2) + a_1 = p\sigma_k^{(2)} + a_1,$$

т.е.  $a_1$  есть остаток от деления частного  $\sigma_k^{(1)}$ , полученного выше, на  $p$  (следовательно,  $0 \leq a_1 < p$ ).

Далее,  $a_2$  есть остаток от деления  $\sigma_k^{(2)}$  на  $p$  и так далее. Поскольку  $\sigma_k < p^k$ , то процесс деления закончится после  $k$  шагов. Таким образом будут найдены все коэффициенты многочлена  $f(x)$ .

Итак, каждому многочлену из  $\mathfrak{A}_n$  отображение  $\varphi$  взаимно однозначно ставит в соответствие элемент множества  $\mathfrak{B}_n$ . Теперь отобразим множество  $\mathfrak{B}_n$  в множество целых чисел так, чтобы в результате каждому многочлену из  $\mathfrak{A}_n$  поставить в соответствие целое неотрицательное число. Для этого паре  $(k, \sigma_k) \in \{k\} \times [0, p^k)$  сопоставим число из интервала  $[p + p^2 + \dots + p^{k-1}, p + p^2 + \dots + p^k)$ , т.е.

парам из  $\{1\} \times [0, p)$  сопоставим целые числа из интервала  $[0, p)$ ;  
 парам из  $\{2\} \times [0, p^2)$  сопоставим целые числа из интервала  $[p, p + p^2)$ ;  
 парам из  $\{3\} \times [0, p^3)$  сопоставим целые числа из интервала  $[p + p^2, p + p^2 + p^3)$ ;  
 ....  
 парам из  $\{n\} \times [0, p^n)$  сопоставим целые числа из интервала  $[p + p^2 + \dots + p^{n-1}, p + p^2 + \dots + p^n)$ .

Пусть

$$\mathbf{N}_n = [0, p) \cup [p, p + p^2) \cup [p + p^2, p + p^2 + p^3) \cup \dots \cup [p + p^2 + \dots + p^{n-1}, p + p^2 + \dots + p^n),$$

т.е. множество всех целых чисел от 0 до  $p^n + p^{n-1} + \dots + p - 1$ , тогда определим отображение

$$\psi : \mathfrak{B}_n \rightarrow \mathbf{N}_n$$

равенством

$$\psi((k, \sigma_k)) = p + p^2 + p^3 + \dots + p^{k-1} + \sigma_k.$$

Отображение  $\psi$  является биекцией  $\mathfrak{B}_n$  на  $\mathbf{N}_n$ . В силу того что мощности множеств  $\mathfrak{B}_n$  и  $\mathbf{N}_n$  совпадают

$$|\mathbf{N}_n| = p^n + p^{n-1} + \dots + p^2 + p = |\mathfrak{A}_n| = |\mathfrak{B}_n|,$$

достаточно проверить, что  $\psi$  является инъекцией.

Пусть

$$\psi((k, \sigma_k)) = \psi((s, \sigma_s)),$$

т.е.

$$p + p^2 + p^3 + \dots + p^{k-1} + \sigma_k = p + p^2 + p^3 + \dots + p^{s-1} + \sigma_s, \quad (6)$$

где  $0 \leq \sigma_k < p^k$ ,  $0 \leq \sigma_s < p^s$ . При  $k \neq s$  равенство (6) невозможно. Действительно, если  $k \neq s$  пусть  $k < s$ , тогда из (6) получаем

$$\sigma_k = p^k + p^{k+1} + \dots + p^{s-1} + \sigma_s > p^k + \sigma_s > p^k \quad (\sigma_s \geq 0),$$

но  $\sigma_k < p^k$ , противоречие. Значит,  $k = s$ , но тогда  $\sigma_k = \sigma_s$ , следовательно, пары  $(k, \sigma_k)$  и  $(s, \sigma_s)$  совпадают. Итак,  $\psi$  – биективное отображение.

Тогда отображение

$$\chi = \psi(\varphi) : \mathfrak{A}_n \rightarrow \mathbf{N}_n$$

является биекцией множества  $\mathfrak{A}_n$  на  $\mathbf{N}_n$ , которая каждому унитарному многочлену степени, не большей  $n$ , из  $\mathbb{Z}_p[x]$  ставит в соответствие целое число из интервала  $[0, p + p^2 + \dots + p^n)$ . Обратное отображение

$$\chi^{-1} : \mathbf{N}_n \rightarrow \mathfrak{A}_n$$

каждому целому числу из интервала  $[0, p + p^2 + \dots + p^n)$  однозначно ставит в соответствие унитарный многочлен из множества  $\mathfrak{A}_n$ .

Отображение  $\chi$ , очевидно, определено формулой

$$\chi(x^k + a_{k-1}x^{k-1} + \dots + a_1x + a_0) = p + p^2 + p^3 + \dots + p^{k-1} + a_{k-1}p^{k-1} + \dots + a_1p + a_0. \quad (7)$$

**Пример 1.** Найдем образ многочлена  $f(x) = x^4 + x^2 + x + 1$  из  $\mathbb{Z}_2[x]$  при отображении  $\chi$ .

По формуле (7) получаем

$$\chi(x^4 + x^2 + x + 1) = 2 + 2^2 + 2^3 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1 = 21.$$

**Пример 2.** Найдем унитарный многочлен из  $\mathbb{Z}_2[x]$ , которому отображение  $\chi$  ставит в соответствие число 25.

Так как  $25 \in [0, 2 + 2^2 + 2^3 + 2^4)$ , то искомый многочлен имеет степень 4, т.е. это многочлен

$$f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0, \quad a_i \in \mathbb{Z}_2.$$

Далее, из определения  $\chi$  имеем

$$25 = 2 + 2^2 + 2^3 + a_32^3 + a_22^2 + a_12 + a_0,$$



или

$$11 = a_3 2^3 + a_2 2^2 + a_1 2 + a_0.$$

Но

$$11 = 2^3 + 2 + 1,$$

откуда

$$a_3 = 1, \quad a_2 = 0, \quad a_1 = 1, \quad a_0 = 1,$$

значит,

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

Результатом наших построений является следующий алгоритм нахождения всех унитарных неприводимых многочленов из  $\mathbb{Z}_p[x]$ , степени которых не превосходят  $n$  ("Решето Эратосфена для многочленов"):

1. вычислить  $M = p + p^2 + \dots + p^n - 1$ ;
2. цикл по  $i$  от 0 до  $M$        $a[i] := 1$ ;
3. цикл по  $i$  от 0 до  $p + p^2 + \dots + p^{n-1} - 1$
4.    если  $a[i] = 1$  (т.е. многочлен  $\chi^{-1}(i)$  неприводим), то
5.        цикл по  $j$  от  $i$  до  $p + p^2 + \dots + p^{n-1} - 1$
6.            вычислить  $s = \chi(\chi^{-1}(i) * \chi^{-1}(j))$ ;
7.            если  $s \leq M$ , то  $a[s] := 0$  (т.е. многочлен  $\chi^{-1}(s)$  объявлен приводимым), иначе закончить цикл по  $j$
8.            конец если;
9.        конец цикла по  $j$ ;
10.        конец если;
11.        конец цикла по  $i$ ;
12. цикл по  $i$  от 0 до  $M$
13.    если  $a[i] = 1$ , то выписать многочлен  $\chi^{-1}(i)$
14.    конец цикла по  $i$ .

*Замечание.* На шаге 6 в приведенном алгоритме операция  $*$  означает умножение многочленов  $\chi^{-1}(i)$  и  $\chi^{-1}(j)$  в кольце  $\mathbb{Z}_p[x]$ . Кроме того, во внутреннем цикле (по  $j$ ) предусмотрен выход из цикла, если степень многочлена, полученного в результате перемножения  $\chi^{-1}(i)$  и  $\chi^{-1}(j)$ , превышает  $n$ .

В качестве примера рассмотрим применение алгоритма к задаче нахождения всех неприводимых унитарных многочленов степени не выше 4 из кольца  $\mathbb{Z}_2[x]$ . Весь список таких многочленов

приведен в следующей таблице:

$f(x)$	$\varphi(f(x))$	$\chi(f(x))$	
$x$	(1, 0)	0	
$x + 1$	(1, 1)	1	
$x^2$	(2, 0)	2	*
$x^2 + 1$	(2, 1)	3	**
$x^2 + x$	(2, 2)	4	*
$x^2 + x + 1$	(2, 3)	5	
$x^3$	(3, 0)	6	*
$x^3 + 1$	(3, 1)	7	**
$x^3 + x$	(3, 2)	8	* (**)
$x^3 + x + 1$	(3, 3)	9	
$x^3 + x^2$	(3, 4)	10	* (**)
$x^3 + x^2 + 1$	(3, 5)	11	
$x^3 + x^2 + x$	(3, 6)	12	*
$x^3 + x^2 + x + 1$	(3, 7)	13	**
$x^4$	(4, 0)	14	*
$x^4 + 1$	(4, 1)	15	**
$x^4 + x$	(4, 2)	16	* (**)
$x^4 + x + 1$	(4, 3)	17	
$x^4 + x^2$	(4, 4)	18	* (**)
$x^4 + x^2 + 1$	(4, 5)	19	* * *
$x^4 + x^2 + x$	(4, 6)	20	*
$x^4 + x^2 + x + 1$	(4, 7)	21	**
$x^4 + x^3$	(4, 8)	22	* (**)
$x^4 + x^3 + 1$	(4, 9)	23	
$x^4 + x^3 + x$	(4, 10)	24	*
$x^4 + x^3 + x + 1$	(4, 11)	25	**
$x^4 + x^3 + x^2$	(4, 12)	26	*
$x^4 + x^3 + x^2 + 1$	(4, 13)	27	**
$x^4 + x^3 + x^2 + x$	(4, 14)	28	* (**)
$x^4 + x^3 + x^2 + x + 1$	(4, 15)	29	

Индекс  $i$  внешнего цикла на 3-м шаге алгоритма принимает значения от 0 до  $13(= 2 + 2^2 + 2^3 - 1)$ . При  $i = 0$  индекс  $j$  внутреннего цикла изменяется от 0 до 13, и в результате выполнения этого внутреннего цикла объявляются приводимыми все многочлены из таблицы, делящиеся на  $x$  (отмечены символом \*). При  $i = 1$  индекс  $j$  изменяется от 1 до 13, и приводимыми объявляются многочлены, делящиеся на  $x + 1$  (отмечены символом \*\*). При  $i = 2, 3, 4$  внутренний цикл не выполняется, так как соответствующие многочлены  $\chi^{-1}(i)$  уже объявлены приводимыми. При  $i = 5$  внутренний цикл по  $j$  начинается с  $j = 5$ , многочлен  $x^4 + x^2 + 1$  объявляется приводимым, и затем происходит выход из внутреннего цикла, поскольку далее получаются многочлены степени 5, не входящие в таблицу. При  $i = 6, \dots, 13$  внутренний цикл не выполняется, так как либо соответствующий многочлен  $\chi^{-1}(i)$  уже объявлен приводимым, либо степень получающегося при перемножении  $\chi^{-1}(i)$  и  $\chi^{-1}(j)$  многочлена больше 4. Таким образом, в результате работы нашего алгоритма получаются следующие унитарные неприводимые многочлены кольца  $\mathbb{Z}_2[x]$  степеней, не превосходящих 4:

$$x, \quad x + 1, \quad x^2 + x + 1, \quad x^3 + x + 1, \quad x^3 + x^2 + 1, \quad x^4 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1.$$

#### §14. РАЗЛОЖЕНИЕ МНОГОЧЛЕНА НА СВОБОДНЫЕ ОТ КВАДРАТОВ МНОЖИТЕЛИ

**Определение.** Многочлен  $f(x)$  называется *свободным от квадратов*, если не существует многочлена  $g(x)$  положительной степени такого, что

$$g^2(x) \mid f(x).$$

**Теорема 1.** Пусть  $\mathbf{A}$  – факториальное кольцо характеристики 0 и пусть  $f(x)$  – примитивный отличный от константы многочлен в  $\mathbf{A}[x]$ . Пусть

$$f(x) = \{p_1(x)\}^{k_1} \{p_2(x)\}^{k_2} \dots \{p_n(x)\}^{k_n}$$

однозначное разложение многочлена  $f(x)$  на неприводимые сомножители и  $f'(x)$  – его производная. Тогда

$$\text{НОД}(f(x), f'(x)) = \{p_1(x)\}^{k_1-1} \{p_2(x)\}^{k_2-1} \dots \{p_n(x)\}^{k_n-1}.$$

*Доказательство.* Пусть

$$r(x) = \text{НОД}(f(x), f'(x)), \quad g(x) = \prod_{i=2}^n \{p_i(x)\}^{k_i}.$$

Тогда

$$f(x) = \{p_1(x)\}^{k_1} g(x)$$

и

$$f'(x) = \{p_1(x)\}^{k_1} g'(x) + k_1 \{p_1(x)\}^{k_1-1} g(x) p_1'(x), \quad (1)$$

откуда следует, что

$$\{p_1(x)\}^{k_1-1} \mid r(x).$$

Покажем, что  $\{p_1(x)\}^{k_1}$  не делит  $r(x)$ . Предположим противное, пусть  $\{p_1(x)\}^{k_1} \mid r(x)$ , тогда

$$\{p_1(x)\}^{k_1} \mid f'(x).$$

Из (1) получаем, что

$$\{p_1(x)\}^{k_1} \mid k_1 \{p_1(x)\}^{k_1-1} g(x) p_1'(x). \quad (2)$$

После сокращения обоих многочленов в (2) на  $\{p_1(x)\}^{k_1-1}$  получаем

$$p_1(x) \mid k_1 g(x) p_1'(x).$$

Но  $p_1(x)$  не делит  $g(x)$ , так как он взаимно прост с  $p_2(x), \dots, p_n(x)$ , значит,

$$p_1(x) \mid k_1 p_1'(x),$$

откуда следует, что  $\deg p_1(x) \leq \deg p_1'(x)$ , что невозможно. Полученное противоречие доказывает, что  $p_1(x)$  входит сомножителем в  $r(x)$  в степени  $k_1 - 1$ . Рассуждая аналогично для  $i = 2, 3, \dots, n$ , получим, что  $p_i(x)$  входит сомножителем в  $r(x)$  ровно  $k_i - 1$  раз, откуда

$$r(x) = \{p_1(x)\}^{k_1-1} \{p_2(x)\}^{k_2-1} \dots \{p_n(x)\}^{k_n-1},$$

что и требовалось доказать.

Из этой теоремы следует, что если  $\text{НОД}(f(x), f'(x)) = 1$ , то  $f(x)$  не имеет кратных сомножителей, и наоборот.

**Следствие 1.** Простые корни многочлена не являются корнями его производной.



**Следствие 2.** Пусть  $K$  – поле и  $p(x)$  – неприводимый многочлен в  $K[x]$ , который делит  $f(x) \in K[x]$ . Тогда

$$\{p(x)\}^2 \mid f(x)$$

тогда и только тогда, когда  $p(x) \mid f'(x)$ .

*Доказательство.* Так как  $p(x) \mid f(x)$ , то  $f(x) = p(x)q(x)$ , значит,

$$f'(x) = p'(x)q(x) + p(x)q'(x). \quad (3)$$

Если  $\{p(x)\}^2$  делит  $f(x)$ , то  $p(x)$  делит  $q(x)$ , и тогда из (3) получаем, что  $p(x) \mid f'(x)$ .

Обратно, если  $p(x) \mid f'(x)$ , то из (3) следует, что  $p(x) \mid p'(x)q(x)$ . Так как  $p(x)$  – неприводимый многочлен, то он должен делить или  $p'(x)$ , или  $q(x)$ . Поскольку  $\deg p'(x) < \deg p(x)$ , то  $p(x)$  не делит  $p'(x)$ , значит,  $p(x) \mid q(x)$ , откуда следует, что

$$\{p(x)\}^2 \mid p(x)q(x) = f(x).$$

Рассмотрим алгоритм разложения многочлена на свободные от квадратов множители. (На самом деле мы представим многочлен в виде произведения степеней свободных от квадратов многочленов.)

Пусть  $\mathbb{A}$  – факториальное кольцо,  $f(x) \in \mathbb{A}[x]$  – примитивный многочлен. Предположим, что

$$f(x) = \{p_1(x)\}^{k_1} \{p_2(x)\}^{k_2} \dots \{p_n(x)\}^{k_n}$$

– разложение  $f(x)$  на неприводимые множители  $p_i(x)$  положительной степени ( $p_i(x)$  и  $p_j(x)$  взаимно просты при  $i \neq j$  и  $k_i > 0$  для каждого  $i$ ).

Пусть

$$k = \max \{k_1, k_2, \dots, k_n\}.$$

Для  $1 \leq i \leq k$  положим

$$J_i = \{j \mid k_j = i\}, \quad s_i(x) = \prod_{j \in J_i} p_j(x).$$

Тогда, очевидно,

$$f(x) = \prod_{i=1}^k \{s_i(x)\}^i. \quad (4)$$

Разложение (4) называется *разложением многочлена  $f(x)$  на свободные от квадратов множители*. Некоторые из многочленов  $s_i(x)$  могут быть равны 1 (в случае  $J_i = \emptyset$ ).  $s_1(x)$  – это произведение всех множителей, соответствующих простым корням многочлена  $f(x)$ ;  $s_2(x)$  – произведение всех сомножителей, соответствующих двойным корням многочлена  $f(x)$  и т.д. Многочлены  $s_i(x)$  ( $1 \leq i \leq k$ ) – это *свободные от квадратов сомножители многочлена  $f(x)$* . Их можно найти, используя теорему 1. Действительно,

$$r(x) = \text{НОД}(f(x), f'(x)) = \prod_{i=1}^n \{p_i(x)\}^{k_i-1} = \prod_{i=1}^k \{s_i(x)\}^{i-1}.$$

Очевидно,  $s_1(x)$  в  $r(x)$  не вошло. Тогда наибольший свободный от квадратов делитель многочлена  $f(x)$  равен

$$t(x) = \frac{f(x)}{r(x)} = \prod_{i=1}^n p_i(x) = \prod_{i=1}^k s_i(x),$$

откуда

$$v(x) = \text{НОД}(r(x), t(x)) = \prod_{i=2}^k s_i(x).$$

Таким образом,

$$s_1(x) = \frac{t(x)}{v(x)}.$$

Итак, первый свободный от квадратов сомножитель многочлена  $f(x)$  может быть вычислен с помощью следующих шагов:

1. вычисление  $f'(x)$ ;
2. нахождение НОД( $f(x)$ ,  $f'(x)$ ) =  $r(x)$ ;
3. деление  $f(x)$  на  $r(x)$   $\left(t(x) = \frac{f(x)}{r(x)}\right)$ ;
4. нахождение наибольшего общего делителя полученного частного  $t(x)$  и  $r(x)$  :  
 $v(x) = \text{НОД}(t(x), r(x))$ ;
5. деление  $t(x)$  на  $v(x)$ .

Далее, мы можем повторить этот же процесс, заменив  $f(x)$  на  $r(x)$ , т.е. вычислять  $s_2(x)$  как первый свободный от квадратов сомножитель многочлена  $r(x)$  и так далее.

На самом деле после первого шага (нахождения  $s_1(x)$ ) искать наибольший общий делитель два раза не надо. Действительно, перед отысканием  $s_2(x)$  имеем

$$f_n(x) := r(x) = \prod_{i=2}^k \{s_i(x)\}^{i-1},$$

$$r_n(x) := \prod_{i=3}^k \{s_i(x)\}^{i-2}, \quad t_n(x) := \prod_{i=2}^k s_i(x),$$

т.е.

$$r_n(x) = \frac{r(x)}{v(x)}, \quad t_n(x) = v(x).$$

**Пример.** Найдем свободные от квадратов сомножители многочлена

$$f(x) = x^5 - x^4 - 2x^3 + 2x^2 + x - 1$$

из  $\mathbb{R}[x]$ .

Найдем  $s_1(x)$  :

$$f'(x) = 5x^4 - 4x^3 - 6x^2 + 4x + 1.$$

Далее,  $r(x) = \text{НОД}(f(x), f'(x)) = x^3 - x^2 - x + 1$ , поскольку

$$f(x) = \left(\frac{1}{5}x - \frac{1}{25}\right) f'(x) + \left(-\frac{24}{25}\right) (x^3 - x^2 - x + 1),$$

$$f'(x) = (5x + 1)(x^3 - x^2 - x + 1).$$

Значит,  $t(x) = \frac{f(x)}{r(x)} = x^2 - 1$ ,  $v(x) = \text{НОД}(t(x), r(x)) = x^2 - 1$ , так как  $t(x)(x - 1) = r(x)$ . Итак,

$$s_1(x) = \frac{t(x)}{v(x)} = 1,$$

т.е. у  $f(x)$  нет простых корней.

Будем искать  $s_2(x)$ . Для этого положим

$$r(x) = \frac{x^3 - x^2 - x + 1}{x^2 - 1} = x - 1, \quad t(x) = x^2 - 1.$$

Тогда  $v(x) = \text{НОД}(r(x), t(x)) = \text{НОД}(x - 1, x^2 - 1) = x - 1$ , значит,

$$s_2(x) = \frac{t(x)}{v(x)} = \frac{x^2 - 1}{x - 1} = x + 1,$$

т.е.  $-1$  является двукратным корнем многочлена  $f(x)$ .

Найдем  $s_3(x)$ . Положим

$$r(x) = \frac{x-1}{x-1} = 1, \quad t(x) = x-1,$$

тогда  $v(x) = \text{НОД}(1, x-1) = 1$ , откуда

$$s_3(x) = \frac{x-1}{1} = x-1,$$

т.е.  $1$  является трехкратным корнем многочлена  $f(x)$ .

Поскольку  $r(x) = \text{const}$ , то процесс разложения завершен. Мы получили следующее разложение

$$f(x) = (x+1)^2 (x-1)^3.$$



## §15. Поля ГАЛУА

**Теорема 1.** *Если целостное кольцо  $\mathbb{A}$  является конечным, то оно является полем.*

*Доказательство.* Пусть  $\mathbb{A}$  – конечное целостное кольцо. Если  $a, b \in \mathbb{A}$  и  $a \neq b$ , то для любого ненулевого элемента  $c \in \mathbb{A}$  справедливо

$$ac \neq bc.$$

Действительно, если бы  $ac = bc$ , то  $c(a - b) = 0$  и в силу  $c \neq 0$  и целостности кольца  $\mathbb{A}$  мы получили бы  $a - b = 0$  или  $a = b$ .

Пусть

$$\mathbb{A} = \{a_1, a_2, \dots, a_n\},$$

т.е. кольцо  $\mathbb{A}$  состоит из  $n$  элементов. Для любого  $c \neq 0$ ,  $c \in \mathbb{A}$  элементы

$$ca_1, ca_2, \dots, ca_n$$

также принадлежат кольцу  $\mathbb{A}$  и все различны, поэтому с точностью до порядка следования совпадают с

$$a_1, a_2, \dots, a_n.$$

Среди элементов кольца есть единица, т.е. для некоторого  $a_i$

$$ca_i = 1,$$

значит, элемент  $c$  обратим в кольце  $\mathbb{A}$ . Итак, любой ненулевой элемент кольца  $\mathbb{A}$  обратим в этом кольце, значит,  $\mathbb{A}$  – поле.

**Теорема 2.** *Пусть  $F$  – поле из  $q$  элементов и  $a \in F$  – произвольный ненулевой элемент. Если  $a^n = 1$ ,  $a^k \neq 1$  при  $0 < k < n$ , то  $n \mid q - 1$ .*

*Доказательство.* Все ненулевые элементы поля  $F$  образуют мультипликативную (абелеву) группу. Порядок этой группы равен  $q - 1$ . Равенство  $a^n = 1$  и условие  $a^k \neq 1$  при  $0 < k < n$  означает, что порядок элемента  $a$  в этой группе равен  $n$ . По теореме Лагранжа порядок любого элемента группы делит порядок группы, т.е.  $n \mid q - 1$ .

**Теорема 3.** *Если  $F$  – поле из  $q$  элементов, то любой ненулевой элемент  $a$  поля  $F$  удовлетворяет уравнению*

$$a^{q-1} = 1.$$

*Доказательство.* По теореме 2 порядок элемента  $a$  делит  $q - 1$ , т.е. если  $a^n = 1$ , где  $n$  – порядок элемента  $a$ , то

$$q - 1 = nk, \quad \text{где } k \in \mathbb{Z}.$$

Тогда

$$a^{q-1} = a^{nk} = (a^n)^k = 1.$$

**Следствие.** *Если  $F$  – поле из  $q$  элементов, то любой элемент поля  $F$  удовлетворяет уравнению*

$$x^q - x = 0.$$

*Доказательство.* Из теоремы 3 имеем: все ненулевые элементы поля  $F$  удовлетворяют уравнению

$$x^{q-1} - 1 = 0.$$

Нулевой элемент поля удовлетворяет уравнению

$$x = 0.$$

Значит, все элементы поля  $F$  удовлетворяют уравнению

$$x(x^{q-1} - 1) = 0$$

или

$$x^q - x = 0.$$

Следующее утверждение нам хорошо знакомо. Но тем не менее еще раз напомним теорему, позволяющую строить конечные поля, добавив в ее формулировку еще одно утверждение.

**Теорема 4.** Пусть  $p$  — простое число и  $m(x)$  — неприводимый многочлен степени  $n > 0$  в кольце  $\mathbb{Z}_p[x]$ . Тогда факторкольцо  $\mathbb{Z}_p[x]/(m(x))$  является полем из  $p^n$  элементов, содержащим  $\mathbb{Z}_p$  и корень многочлена  $m(x)$ . Кроме того,  $\mathbb{Z}_p[x]/(m(x))$  является линейным (векторным) пространством над полем  $\mathbb{Z}_p$  размерности  $n$ .

*Доказательство.* В §6 мы доказали, что  $\mathbb{Z}_p[x]/(m(x))$  — поле в случае, когда  $m(x)$  неприводим. В §12 (теорема 1) мы показали, что это факторкольцо является линейным пространством над полем  $\mathbb{Z}_p$  размерности  $n$  и базисом этого пространства является следующая система классов вычетов:

$$\bar{1}, \bar{x}, \bar{x}^2, \dots, \bar{x}^{n-1}.$$

Там же доказано, что в  $\mathbb{Z}_p[x]/(m(x))$  будет  $p^n$  элементов.

Каждый элемент  $a$  поля  $\mathbb{Z}_p$  можно отождествить с классом вычетов  $a \pmod{m(x)}$ . Действительно, если

$$a \equiv b \pmod{m(x)} \quad \text{для } a, b \in \mathbb{Z}_p,$$

то  $m(x) \mid a - b$ , но  $\deg(a - b) < \deg m(x)$ , значит,  $a - b = 0$ , т.е.  $a = b$ . Таким образом,  $\mathbb{Z}_p \subset \mathbb{Z}_p[x]/(m(x))$ .

Каждый элемент из  $\mathbb{Z}_p[x]/(m(x))$  однозначно представляется в виде

$$c_0 + c_1\bar{x} + c_2\bar{x}^2 + \dots + c_{n-1}\bar{x}^{n-1}, \quad c_i \in \mathbb{Z}_p \quad (i = 0, 1, \dots, n-1).$$

Положим  $\bar{x} = \alpha$ . Тогда каждый элемент факторкольца имеет вид

$$c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_{n-1}\alpha^{n-1}, \quad c_i \in \mathbb{Z}_p \quad (i = 0, 1, \dots, n-1),$$

причем это представление единственно. Поэтому можно представлять элементы факторкольца как многочлены кольца  $\mathbb{Z}_p[x]$ , вычисленные в точке  $\alpha (= \bar{x})$ . При этом  $m(\alpha) = 0$ , так как  $m(\alpha) = m(x) \pmod{m(x)} = 0$ , т.е.  $\alpha$  — корень многочлена  $m(x)$ .

**Определение 1.** Поле  $\mathbb{Z}_p[x]/(m(x))$  ( $m(x)$  — неприводим в  $\mathbb{Z}_p[x]$ ) называется *простым расширением* поля  $\mathbb{Z}_p$  и обозначается  $\mathbb{Z}_p[\alpha]$ .

**Теорема 5.** Пусть  $F$  — поле из  $q$  элементов. Тогда  $q = p^r$ , где  $p$  — простое, а  $r$  — натуральное число.

*Доказательство.* Так как  $F$  — поле, оно имеет единичный элемент относительно умножения, который, как обычно, обозначаем 1. Далее,

$$1 + 1 \in F, \quad \text{обозначим } 1 + 1 = 2,$$

$$2 + 1 \in F, \quad \text{обозначим } 2 + 1 = 3 \quad \text{и т.д.}$$

Так как  $F$  — конечное поле, то после конечного числа шагов мы получим элемент, который уже был получен ранее. Пусть

$$\sum_{i=1}^{r_1} 1 = \sum_{i=1}^{r_2} 1, \quad \text{где } r_1 < r_2.$$

Следовательно,

$$0 = \sum_{i=1}^{r_2} 1 - \sum_{i=1}^{r_1} 1 = \sum_{i=1}^{r_2-r_1} 1,$$

т.е. существуют такие целые числа  $r$ , что

$$\sum_{i=1}^r 1 = 0. \tag{1}$$

Возьмем *наименьшее* целое число, удовлетворяющее свойству (1), пусть это число  $\lambda$ , т.е.

$$\lambda = \min \left\{ r > 0 \mid \sum_{i=1}^r 1 = 0 \right\}. \tag{2}$$

$\lambda$  не может быть составным числом, так как если

$$\lambda = ab, \quad 1 < a, b < \lambda,$$

то это означает, что

$$a \cdot 1 \neq 0, \quad b \cdot 1 \neq 0, \quad \text{но} \quad (a \cdot 1)(b \cdot 1) = ab \cdot 1 = \lambda \cdot 1 = 0,$$

т.е.  $a \cdot 1$  и  $b \cdot 1$  – делители нуля, но в поле их нет! Значит,  $\lambda$  – простое число  $p$ . Оно называется *характеристикой поля  $F$* .

Тогда множество целых поля  $F$

$$F_p = \{1, 1+1, 1+1+1, \dots, \underbrace{1+1+\dots+1}_{\lambda \text{ раз}}\}$$

изоморфно  $\mathbb{Z}_p = \{1, 2, 3, \dots, p-1, 0\}$ .

Будем смотреть на  $F$  как на линейное пространство над полем  $F_p$  ( $\cong \mathbb{Z}_p$ ). Тогда выберем в  $F$  базис, т.е. подмножество линейно независимых элементов с максимальным числом элементов, пусть

$$\alpha_1, \alpha_2, \dots, \alpha_r$$

образуют базис  $F$  над полем  $F_p$ . Каждый элемент  $\beta \in F$  единственным образом представляется в виде

$$\beta = c_1 \alpha_1 + c_2 \alpha_2 + \dots + c_r \alpha_r, \quad c_i \in F_p \quad (i = 1, 2, \dots, r).$$

Очевидно, (см. теорема 4) существует  $p^r$  различных линейных комбинаций такого вида, значит, в  $F$  всего  $p^r$  элементов, т.е.  $q = p^r$ .

**Следствие.** Если  $F$  – конечное поле, то оно имеет характеристику  $p$  для некоторого простого числа  $p > 0$  и, следовательно, содержит подполе, изоморфное  $\mathbb{Z}_p$ .

**Теорема 6.** Пусть  $F$  – конечное поле из  $q$  элементов. Группа ненулевых элементов поля  $F$  по умножению является циклической.

*Доказательство.* Очевидно, что это группа порядка  $q - 1$ . Если  $q - 1$  является простым числом, то теорема, очевидно, верна. Действительно, порядок любого элемента группы делит порядок группы, т.е. делит простое число  $q - 1$ , поэтому любой, отличный от 1, элемент имеет порядок  $q - 1$ , т.е. является образующей этой группы.

Докажем теорему для составного числа  $q - 1$ . Разложим  $q - 1$  в произведение простых чисел, пусть

$$q - 1 = \prod_{i=1}^s p_i^{\alpha_i}. \quad (3)$$

Над полем  $F$  рассмотрим многочлен

$$x^{\frac{q-1}{p_i}} - 1.$$

Он имеет не более  $\frac{q-1}{p_i}$  корней в поле  $F$ , поэтому среди  $q - 1$  ненулевых элементов поля  $F$  должен найтись хотя бы один, не являющийся корнем этого многочлена. Пусть

$$a_i \in F, \quad a_i \neq 0 \quad \text{и} \quad a_i^{\frac{q-1}{p_i}} \neq 1. \quad (4)$$

Для каждого  $i = 1, 2, \dots, s$  найдем в поле  $F$  элемент  $a_i$ , удовлетворяющий условию (4). Обозначим через  $b_i$  ( $i = 1, 2, \dots, s$ ) элемент

$$b_i = a_i^{\frac{q-1}{p_i \alpha_i}}, \quad b_i \in F,$$

и положим

$$b = \prod_{i=1}^s b_i.$$



Покажем, что элемент  $b$  имеет порядок  $q - 1$ .

Каждый элемент  $b_i$  имеет порядок  $p_i^{\alpha_i}$  ( $i = 1, 2, \dots, s$ ). Действительно,

$$b_i^{p_i^{\alpha_i}} = \left( a_i^{\frac{q-1}{p_i^{\alpha_i}}} \right)^{p_i^{\alpha_i}} = a_i^{q-1} = 1,$$

откуда следует, что порядок элемента  $b_i$  делит  $p_i^{\alpha_i}$ , но  $p_i$  — простое число, любой делитель  $p_i^{\alpha_i}$  имеет вид  $p_i^{n_i}$ , где  $n_i \leq \alpha_i$ . Если  $n_i < \alpha_i$ , т.е.

$$b_i^{p_i^{n_i}} = 1,$$

то

$$b_i^{p_i^{\alpha_i-1}} = 1,$$

но это невозможно, так как

$$b_i^{p_i^{\alpha_i-1}} = \left( a_i^{\frac{q-1}{p_i^{\alpha_i}}} \right)^{p_i^{\alpha_i-1}} = a_i^{\frac{q-1}{p_i}} \neq 1$$

в силу выбора  $a_i$ . Значит,  $n_i$  не может быть меньше  $\alpha_i$ , таким образом,  $\text{ord}(b_i) = p_i^{\alpha_i}$ .

Порядки элементов  $b_1, b_2, \dots, b_s$  попарно взаимно просты, а группа является абелевой, поэтому порядок элемента  $b = \prod_{i=1}^s b_i$  равен произведению порядков перемножаемых элементов, т.е.

$$\text{ord}(b) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} = \prod_{i=1}^s p_i^{\alpha_i} = q - 1.$$

Итак, элемент  $b$  является образующей нашей мультипликативной группы, следовательно, она циклическая.

**Определение 2.** Конечное поле из  $q$  элементов называется *полем Галуа* и обозначается  $GF(q)$ . *Примитивным элементом* (или *примитивным корнем*) поля Галуа  $GF(q)$  называется элемент порядка  $q - 1$  относительно умножения.

**Теорема 7.** В каждом поле Галуа имеется примитивный элемент.

Это утверждение следует из теоремы 6 и определения 2. Так как ненулевые элементы поля  $GF(q)$  образуют циклическую группу по умножению порядка  $q - 1$ , то образующая этой группы и является примитивным элементом поля.

Никаких общих формул для нахождения примитивного корня не существует. Однако можно доказать, что если  $p$  — простое число вида

$$p = 4q + 1,$$

где  $q$  — также простое, то примитивным корнем поля  $\mathbf{Z}_p$  является элемент 2. Т.е. 2 является примитивным корнем поля  $\mathbf{Z}_p$  для  $p = 5, 13, 29, 53$  и т.д.

Кроме того, для проверки того, является ли элемент поля примитивным корнем, можно использовать следующее утверждение.

**Лемма.** В конечном поле  $GF(q)$  элемент  $a$  является примитивным корнем тогда и только тогда, когда

$$a^{\frac{q-1}{p_i}} \not\equiv 1 \pmod{q}$$

для всех простых делителей  $p_1, p_2, \dots, p_s$  числа  $q - 1$ .

*Доказательство.* Если  $a \in GF(q)$  — примитивный корень, то  $\text{ord}(a) = q - 1$ , поэтому

$$a^{\frac{q-1}{p_i}} \not\equiv 1 \pmod{q} \tag{1}$$

для любого простого делителя  $p_i$  числа  $q - 1$ .

Обратно, пусть выполнены неравенства (1) для всех простых чисел  $p_i \mid q - 1$ . Пусть  $n = \text{ord}(a)$  в мультипликативной группе поля  $GF(q)$ , тогда

$$n \mid q - 1$$

и

$$n \nmid \frac{q-1}{p_i}$$

для всех простых делителей  $p_i$  числа  $q - 1$ . Значит,  $n = q - 1$ , т.е.  $a$  — образующая мультипликативной группы поля  $GF(q)$ .

**Пример 1.** Найдём примитивный элемент в поле  $GF(31)$ .

Порядок мультипликативной группы поля  $GF(31)$  равен  $31 - 1 = 30$ . Он имеет простые делители 2, 3 и 5. Значит, если  $a \in GF(31)$  – примитивный корень, то должно выполняться

$$a^{\frac{30}{2}} = a^{15} \not\equiv 1 \pmod{31},$$

$$a^{\frac{30}{3}} = a^{10} \not\equiv 1 \pmod{31},$$

$$a^{\frac{30}{5}} = a^6 \not\equiv 1 \pmod{31}.$$

Элемент 2 не подходит, так как  $2^5 = 32 \equiv 1 \pmod{31}$ , значит,  $\text{ord}(2) = 5$ . Попробуем взять  $a = 3$ . Имеем

$$3^6 = 3^4 \cdot 3^2 = 81 \cdot 9 \equiv 19 \cdot 9 \pmod{31} \equiv 171 \equiv 16 \pmod{31},$$

$$3^{10} = 3^6 \cdot 3^4 \equiv 16 \cdot 81 \pmod{31} \equiv 16 \cdot 19 \pmod{31} \equiv 304 \pmod{31} \equiv 25 \pmod{31},$$

$$\begin{aligned} 3^{15} &= 3^{10} \cdot 3^4 \cdot 3 \equiv 25 \cdot 81 \cdot 3 \pmod{31} \equiv 25 \cdot 19 \cdot 3 \pmod{31} \equiv 75 \cdot 19 \pmod{31} \equiv 13 \cdot 19 \pmod{31} \\ &\equiv 247 \pmod{31} \equiv -1 \pmod{31}, \end{aligned}$$

значит, 3 – примитивный корень в  $GF(31)$ .

**Теорема 8.** Пусть  $F$  – поле и  $f(x)$  – унитарный многочлен из  $F[x]$ ,  $\deg f(x) \geq 1$ . Тогда существует поле  $K$ , содержащее  $F$ , такое, что многочлен  $f(x)$  в  $K[x]$  разлагается в произведение линейных сомножителей.

*Доказательство.* Проведем индукцию по степени многочлена  $f(x)$ . Пусть  $\deg f(x) = 1$ . В этом случае  $f(x) = x - \alpha$ ,  $\alpha \in F$ , поэтому  $K = F$ . Пусть  $\deg f(x) = 2$ . Если  $f(x)$  приводим, то он раскладывается в  $F[x]$  в произведение линейных сомножителей, значит, его корни принадлежат  $F$ , следовательно,  $K = F$ .

Если  $f(x)$  неприводим, то построим факторкольцо  $F[x]/(f(x))$ . В силу теоремы 4 это факторкольцо является полем, содержащим поле  $F$  и корень  $\alpha$  многочлена  $f(x)$ , т.е.  $F[x]/(f(x)) = F[\alpha] = F_1$ . В  $F_1$

$$f(x) = (x - \alpha) f_1(x),$$

где  $\deg f_1(x) = 1$ , а следовательно,  $f_1(x) = x - \beta$ . Поэтому в  $F_1$  имеем

$$f(x) = (x - \alpha)(x - \beta),$$

т.е. оба корня  $f(x)$  принадлежат  $F_1$ , значит,  $K = F_1$ .

Предположим, что теорема верна для многочленов, степени которых меньше  $n$ , т.е. для многочлена степени, меньшей  $n$ , существует поле  $K$ , содержащее  $F$ , в котором многочлен раскладывается на линейные множители.

Рассмотрим многочлен  $f(x)$  степени  $n$ . Пусть

$$f(x) = \prod_{i=1}^s (p_i(x))^{k_i}$$

-- разложение  $f(x)$  в произведение неприводимых унитарных многочленов над полем  $F$ .

Факторкольцо  $F[x]/(p_1(x)) = F[\alpha_1] = F_1$  по теореме 4 является полем, содержащим  $F$  и корень  $\alpha_1$  многочлена  $p_1(x)$ . Значит, в  $F_1$

$$f(x) = (x - \alpha_1)^{k_1} q(x),$$

где  $\deg q(x) < n$ . По предположению индукции существует поле  $K$ , содержащее  $F_1$ , в котором  $q(x)$  раскладывается на линейные множители. Тогда в поле  $K$  многочлен  $f(x)$  также раскладывается на линейные множители. Кроме того,  $F \subset F_1 \subset K$ . Теорема доказана.

**Определение 3.** Поле  $K$  (определенное в теореме 8), в котором многочлен  $f(x)$  раскладывается на линейные множители, называется *полем разложения* этого многочлена.

**Пример 2.** В  $\mathbb{Q}[x]$  многочлен  $x^2 + 1$  неприводим. Его полем разложения является поле  $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ .

**Пример 3.** В  $\mathbb{Q}[x]$  многочлен  $x^3 - 2$  неприводим. В поле  $\mathbb{R}$  он имеет корень  $\sqrt[3]{2}$ , но  $\mathbb{R}$  не является его полем разложения, так как

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$$

и второй сомножитель неприводим над  $\mathbb{R}$ , поскольку имеем комплексные корни.

Из основной теоремы алгебры следует, что поле  $\mathbb{C}$  является полем разложения любого многочлена из  $\mathbb{Q}[x]$ .

**Определение 4.** Пусть  $F$  – поле и  $K$  – поле, содержащее  $F$ . Элемент  $\alpha \in K$ , являющийся корнем некоторого ненулевого многочлена  $f(x) \in F[x]$ , называется *алгебраическим над полем  $F$* .

Числа, не являющиеся алгебраическими, называются *трансцендентными*.

Примерами трансцендентных над полем  $\mathbb{Q}$  чисел являются числа  $e$  и  $\pi$ . (В теории чисел доказывается, что ни  $e$ , ни  $\pi$  не являются корнями уравнения с рациональными коэффициентами.)

**Теорема 9.** Пусть элемент  $\alpha \in K$  является алгебраическим над полем  $F$  ( $K \supset F$ ). Тогда существует единственный унитарный неприводимый многочлен  $m(x) \in F[x]$  такой, что  $\alpha$  является его корнем, и каждый многочлен  $p(x) \in F[x]$  с корнем  $\alpha$  делится на  $m(x)$ .

*Доказательство.* Рассмотрим все ненулевые многочлены из  $F[x]$  с корнем  $\alpha$ . Используя принцип полного упорядочения множества степеней многочленов из  $F[x]$ , найдем унитарный многочлен наименьшей степени среди всех ненулевых многочленов с корнем  $\alpha$ , пусть это многочлен  $m(x)$ . Этот многочлен неприводим. Если бы это было не так, т.е.

$$m(x) = m_1(x)m_2(x), \quad \text{где } 0 < \deg m_1(x) < \deg m(x), \quad 0 < \deg m_2(x) < \deg m(x),$$

то

$$0 = m(\alpha) = m_1(\alpha)m_2(\alpha).$$

Но  $m_1(\alpha), m_2(\alpha) \in K$  и так как  $K$  – поле, то оно не содержит делителей нуля, значит, либо  $m_1(\alpha) = 0$ , либо  $m_2(\alpha) = 0$ , т.е. найдется многочлен с корнем  $\alpha$  степени, меньшей чем  $\deg m(x)$ , но это противоречит выбору многочлена  $m(x)$ . Итак,  $m(x)$  неприводим.

Покажем, что  $m(x)$  – единственный многочлен с указанными свойствами. Предположим, что это не так, тогда существует еще хотя бы один многочлен  $\tilde{m}(x)$  с такими же свойствами. Заметим, что  $\deg m(x) = \deg \tilde{m}(x)$ , иначе опять приходим к противоречию с выбором  $m(x)$ . Если  $m(x) \neq \tilde{m}(x)$ , то многочлен

$$d(x) = m(x) - \tilde{m}(x) \neq 0,$$

причем  $\deg d(x) < \deg m(x)$ . (Так как  $lc(m(x)) = lc(\tilde{m}(x)) = 1$ , то старшие члены сокращаются.) Но

$$d(\alpha) = m(\alpha) - \tilde{m}(\alpha) = 0,$$

значит, нашелся многочлен  $d(x) \in F[x]$ ,  $d(x) \neq 0$  с корнем  $\alpha$  степени меньшей, чем  $\deg m(x)$ . Противоречие с выбором  $m(x)$ .

Пусть  $p(x)$  – произвольный многочлен из  $F[x]$  и  $p(\alpha) = 0$ . Поделим  $p(x)$  на  $m(x)$ :

$$p(x) = m(x)q(x) + r(x), \quad \text{где } \deg r(x) < \deg m(x).$$

Так как  $p(\alpha) = 0$ , то

$$0 = m(\alpha)q(\alpha) + r(\alpha),$$

откуда в силу  $m(\alpha) = 0$  следует, что  $r(\alpha) = 0$ . Так как  $\deg r(x) < \deg m(x)$ , то  $r(x) = 0$ , значит,

$$p(x) = m(x)q(x),$$

т.е.  $m(x) \mid p(x)$ , что и требовалось доказать.



**Определение 5.** Ненулевой многочлен наименьшей степени из  $F[x]$  такой, что алгебраический над полем  $F$  элемент  $\alpha$  является его корнем, называется *минимальным многочленом элемента  $\alpha$  над полем  $F$* .

**Теорема 10.** Пусть  $K = F[\alpha]$  – простое расширение поля  $F$ , и минимальный многочлен  $m(x)$  элемента  $\alpha$  над  $F$  имеет степень  $r$ . Тогда если  $\beta$  – произвольный элемент поля  $K$ , то  $\beta$  является алгебраическим над полем  $F$ , и минимальный многочлен элемента  $\beta$  над полем  $F$  имеет степень, не превосходящую  $r$ .

*Доказательство.* По условию теоремы  $K = F[\alpha] = F[x]/(m(x))$ . Из теоремы 4 следует, что  $K$  – линейное пространство над полем  $F$  размерности  $r$  и в качестве базиса этого пространства можно взять систему элементов

$$1, \alpha, \alpha^2, \dots, \alpha^{r-1}.$$

Тогда каждый элемент  $\beta \in K$  можно единственным образом представить в виде линейной комбинации базисных элементов

$$\beta = c_0 \cdot 1 + c_1 \alpha + c_2 \alpha^2 + \dots + c_{r-1} \alpha^{r-1}, \quad c_i \in F \quad (i = 0, 1, \dots, r-1),$$

т.е. в виде многочлена от  $\alpha$  степени, не превосходящей  $r-1$ , с коэффициентами из  $F$ . То же верно и для любой степени элемента  $\beta$ , так как  $\beta^s \in K$  для любого натурального  $s$ .

В линейном пространстве  $K$  размерности  $r$  любые  $r+1$  элементов линейно зависимы, поэтому

$$1, \beta, \beta^2, \dots, \beta^{r-1}, \beta^r$$

линейно зависимы. Тогда существуют такие коэффициенты  $d_0, d_1, \dots, d_r$  из  $F$ , не все равные нулю такие, что

$$d_0 \cdot 1 + d_1 \beta + d_2 \beta^2 + \dots + d_{r-1} \beta^{r-1} + d_r \beta^r = 0. \quad (5)$$

Равенство (5) означает, что  $\beta$  является корнем многочлена

$$f(x) = d_0 + d_1 x + d_2 x^2 + \dots + d_r x^r$$

с коэффициентами из поля  $F$ ,  $f(x) \neq 0$  (среди чисел  $d_i$  хотя бы одно ненулевое),  $\deg f(x) \leq r$ . Значит,  $\beta$  – алгебраическое над полем  $F$  число. И так как нашелся ненулевой многочлен степени, не превосходящей  $r$  из  $F[x]$  с корнем  $\beta$ , то минимальный многочлен элемента  $\beta$  над полем  $F$  будет иметь степень, не превосходящую  $r$ . Теорема доказана.

Из теоремы 10 видно, как можно искать минимальный многочлен элемента  $\beta$ . Для этого следует найти ненулевое решение уравнения (5), заменив  $\beta$  и все его степени многочленами от  $\alpha$ .

Пусть

$$\beta^s = \sum_{i=0}^{r-1} a_{si} \alpha^i, \quad (s = 1, 2, \dots, r). \quad (6)$$

Подставляя выражения  $\beta^s$  из (6) в равенство (5), получим

$$\sum_{s=0}^r d_s \left( \sum_{i=0}^{r-1} a_{si} \alpha^i \right) = 0.$$

Перегруппируем слагаемые в левой части полученного равенства, собирая коэффициенты при одинаковых степенях  $\alpha$ :

$$\sum_{i=0}^{r-1} \alpha^i \left( \sum_{s=0}^r a_{si} d_s \right) = 0. \quad (7)$$

Так как  $1, \alpha, \alpha^2, \dots, \alpha^{r-1}$  – базис  $K$  над полем  $F$ , то равенство (7) возможно лишь в случае, когда

$$\sum_{s=0}^r a_{si} d_s = 0, \quad (i = 0, 1, \dots, r-1). \quad (8)$$

Соотношения (8) представляют собой систему линейных однородных уравнений, содержащую  $r$  уравнений и  $r+1$  неизвестное  $d_0, d_1, \dots, d_r$ . Так как ранг системы меньше числа неизвестных, то она всегда имеет ненулевые решения. В результате найдем ненулевой многочлен  $f(x) = d_0 + d_1 x + d_2 x^2 + \dots + d_r x^r$  из  $F[x]$  с корнем  $\beta$ .

**Пример 4.** Пусть  $F = \mathbb{Z}_2$  и  $m(x) = x^3 + x + 1$  – неприводимый многочлен из  $\mathbb{Z}_2[x]$ . Пусть  $K = \mathbb{Z}_2[x]/(m(x)) = \mathbb{Z}_2[\alpha] \cong GF(2^3)$ , т.е.  $\alpha$  – корень  $m(x)$ . Найдем минимальный многочлен элемента  $\beta = \alpha + 1$ .

Так как  $\alpha$  – корень  $m(x)$ , то  $\alpha^3 + \alpha + 1 = 0$ , откуда  $\alpha^3 = \alpha + 1$ . Рассмотрим элементы  $1, \beta, \beta^2, \beta^3$ . Очевидно,

$$\beta^2 = \alpha^2 + 1,$$

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

(вычисления проводятся в  $\mathbb{Z}_2$ ). Тогда равенство (5)

$$d_0 + d_1\beta + d_2\beta^2 + d_3\beta^3 = 0$$

можно записать в виде

$$d_0 + d_1(\alpha + 1) + d_2(\alpha^2 + 1) + d_3\alpha^2 = 0$$

или

$$(d_0 + d_1 + d_2) + d_1\alpha + (d_2 + d_3)\alpha^2 = 0,$$

откуда получаем систему

$$\begin{cases} d_0 + d_1 + d_2 = 0 \\ d_1 = 0 \\ d_2 + d_3 = 0, \end{cases}$$

решение которой над  $\mathbb{Z}_2$  есть:

$$\begin{cases} d_3 = d_2 \\ d_0 = d_2 \\ d_1 = 0, \end{cases} \quad d_2 \in \mathbb{Z}_2.$$

В качестве ненулевого решения этой системы выбираем набор  $d_3 = d_2 = d_0 = 1, d_1 = 0$ , значит, многочлен  $x^3 + x^2 + 1$  имеет корнем элемент  $\beta$ . Этот многочлен неприводим в  $\mathbb{Z}_2[x]$  и является минимальным многочленом элемента  $\beta$  над  $\mathbb{Z}_2$ .

**Теорема 11.** Для простого числа  $p$  и натурального числа  $r$  все конечные поля из  $q = p^r$  элементов изоморфны.

*Доказательство.* Пусть  $F$  – конечное поле из  $q$  элементов, тогда  $F \setminus \{0\} = F^*$  – мультипликативная группа порядка  $q - 1$ . Порядок произвольного ненулевого элемента  $\alpha \in F$  ( $\alpha \in F^*$ ) делит  $q - 1$ , т.е.  $\alpha^{q-1} = 1$ . Умножая последнее равенство на  $\alpha$ , получаем

$$\alpha^q - \alpha = 0, \tag{9}$$

что выполняется и для  $\alpha = 0$ . Поэтому все элементы  $\alpha_1, \alpha_2, \dots, \alpha_q$  поля  $F$  являются корнями уравнения (9), т.е. корнями многочлена  $x^q - x$ . Если  $\alpha_i$  – корень  $x^q - x$ , то  $x^q - x$  делится на  $x - \alpha_i$  для  $1 \leq i \leq q$ , значит,  $x^q - x$  делится на  $\prod_{i=1}^q (x - \alpha_i)$ . Имеем два многочлена степени  $q$ , у которых старшие коэффициенты равны (и корни одного являются корнями другого), значит,

$$x^q - x = \prod_{i=1}^q (x - \alpha_i).$$

Из следствия из теоремы 5 получаем, что поле  $F$  получается из  $\mathbb{Z}_p$  присоединением всех корней многочлена  $x^q - x$  и потому определено однозначно с точностью до изоморфизма.

Например, поле  $\mathbb{Z}_2[x] \setminus (x^3 + x^2 + 1) \cong GF(2^3)$  изоморфно полю  $\mathbb{Z}_2[x] \setminus (x^3 + x + 1) \cong GF(2^3)$ .

**Следствие 1.** Любое конечное поле изоморфно простому расширению поля  $\mathbb{Z}_p$  для некоторого простого числа  $p$ .

**Следствие 2.** Если  $q$  не является степенью простого числа  $p$ , то не существует конечного поля из  $q$  элементов.

*Доказательство.* Если  $F$  – конечное поле, то оно изоморфно  $\mathbb{Z}_p[x] \setminus (m(x))$  для некоторого неприводимого многочлена  $m(x)$  степени  $r$ . Тогда  $\mathbb{Z}_p[x] \setminus (m(x))$  содержит ровно  $p^r$  элементов, то же верно и для  $F$ .

**Теорема 12.** В любом поле характеристики  $p$  справедливо

$$(x - a)^p = x^p - a^p.$$

*Доказательство.* Используем бином Ньютона:

$$(x - a)^p = \sum_{k=0}^p C_p^k x^{p-k} (-a)^k = x^p + \sum_{k=1}^{p-1} C_p^k x^{p-k} (-a)^k + (-a)^p, \quad (10)$$

где

$$C_p^k = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\dots(p-k+1)}{k!} \quad (1 \leq k \leq p-1).$$

Так как  $p$  – характеристика поля, то  $p$  – простое число, значит, оно не делится на  $2, 3, \dots, k$  ( $k < p$ ), но  $C_p^k$  – целое число, значит,  $p \mid C_p^k$ , т.е.  $C_p^k = pQ_k$  ( $1 \leq k \leq p-1$ ). В поле характеристики  $p$   $C_p^k = pQ_k = 0$ . Значит,  $C_p^k = 0$  ( $k = 1, 2, \dots, p-1$ ) и (10) принимает вид

$$(x - a)^p = x^p + (-a)^p.$$

Если  $p = 2$ , то

$$(-a)^2 \equiv a^2 \equiv -a^2 \pmod{2},$$

поэтому

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

Если  $p$  – нечетное простое, то  $(-a)^p = -a^p$ , поэтому и в этом случае верно

$$(x - a)^p = x^p - a^p.$$

**Следствие.** В поле характеристики  $p$  ни у одного элемента порядок не является кратным  $p$ .

*Доказательство.* Предположим противное, пусть нашелся элемент  $a$  такой, что его порядок равен  $kp$  ( $k > 0$  – целое), т.е.

$$a^{kp} = 1$$

или  $a^{kp} - 1 = 0$ .

Но в поле характеристики  $p$ , согласно теореме 12, имеем

$$(a^k - 1)^p = a^{kp} - 1 = 0,$$

откуда следует, что  $a^k - 1 = 0$  или  $a^k = 1$ . Полученное равенство противоречит тому, что порядок элемента  $a$  равен  $kp$ .

**Теорема 13.** Пусть  $F$  – поле характеристики  $p$ . Тогда для любого натурального  $r$  и  $a_1, a_2, \dots, a_k \in F$  справедливо

$$\left( \sum_{i=1}^k a_i \right)^{p^r} = \sum_{i=1}^k a_i^{p^r}. \quad (11)$$

*Доказательство.* Проведем индукцию по числу слагаемых в формуле (11).



Пусть  $k = 2$ . Докажем, что

$$(a_1 + a_2)^{p^r} = a_1^{p^r} + a_2^{p^r}. \quad (12)$$

для любого натурального  $r$ , проводя индукцию по  $r$ .

Для  $r = 1$  результат следует из теоремы 12:

$$(a_1 + a_2)^p = a_1^p + a_2^p.$$

Пусть формула (12) верна для  $r = s - 1$ , т.е.

$$(a_1 + a_2)^{p^{s-1}} = a_1^{p^{s-1}} + a_2^{p^{s-1}}.$$

Возьмем  $r = s$ . Тогда, используя теорему 12 и предположение индукции, получаем

$$(a_1 + a_2)^{p^s} = ((a_1 + a_2)^{p^{s-1}})^p = (a_1^{p^{s-1}} + a_2^{p^{s-1}})^p = (a_1^p)^{p^{s-1}} + (a_2^p)^{p^{s-1}} = a_1^{p^s} + a_2^{p^s},$$

что и завершает доказательство формулы (12).

Предположим, что формула (11) верна для  $k = n - 1$ , т.е.

$$\left( \sum_{i=1}^{n-1} a_i \right)^{p^r} = \sum_{i=1}^{n-1} a_i^{p^r}$$

для любого натурального  $r$ .

Возьмем  $k = n$ . Тогда

$$\left( \sum_{i=1}^n a_i \right)^{p^r} = \left( \sum_{i=1}^{n-1} a_i + a_n \right)^{p^r} = \left( \sum_{i=1}^{n-1} a_i \right)^{p^r} + a_n^{p^r} = \sum_{i=1}^{n-1} a_i^{p^r} + a_n^{p^r} = \sum_{i=1}^n a_i^{p^r}$$

для любого натурального числа  $r$ .

**Следствие.** Пусть  $g(x)$  - произвольный многочлен из  $\mathbb{Z}_p[x]$  ( $p$  - простое число), и  $\alpha$  - один из его корней. Тогда  $\alpha^p$  также является корнем многочлена  $g(x)$ .

**Доказательство.** Пусть

$$g(x) = \sum_{i=0}^n c_i x^i, \quad c_i \in \mathbb{Z}_p, \quad (i = 0, 1, \dots, n).$$

Так как  $\alpha$  - корень  $g(x)$ , то справедливо равенство

$$\sum_{i=0}^n c_i \alpha^i = 0. \quad (13)$$

Возведем обе части равенства (13) в степень  $p$ . Пользуясь теоремой 13, получаем

$$0 = \left( \sum_{i=0}^n c_i \alpha^i \right)^p = \sum_{i=0}^n (c_i \alpha^i)^p = \sum_{i=0}^n c_i^p \alpha^{ip} = \sum_{i=0}^n c_i^p (\alpha^p)^i.$$

Но  $c_i \in \mathbb{Z}_p$ ,  $p$  - простое число, поэтому если  $c_i \neq 0$  ( $0 < c_i < p$ ), то согласно малой теореме Ферма

$$c_i^{p-1} \equiv 1 \pmod{p},$$

откуда  $c_i^p \equiv c_i \pmod{p}$ . Последнее верно и для  $c_i = 0$ . Значит,

$$0 = \sum_{i=0}^n c_i^p (\alpha^p)^i = \sum_{i=0}^n c_i (\alpha^p)^i = g(\alpha^p),$$

т.е.  $\alpha^p$  - корень многочлена  $g(x)$ .

**Теорема 14.** Пусть  $m(x)$  – унитарный неприводимый многочлен из  $\mathbb{Z}_p[x]$  ( $p$  – простое) степени  $r$  и пусть  $K$  – поле, содержащее  $\mathbb{Z}_p$ . Если  $\alpha \in K$  является корнем многочлена  $m(x)$ , то все корни этого многочлена есть

$$\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{r-1}}.$$

*Доказательство.* По следствию из теоремы 13 если  $\alpha$  – корень многочлена  $m(x) \in \mathbb{Z}_p[x]$ , то  $\alpha^p$  – тоже корень. Применяя это следствие к  $\alpha^p$  и т.д., получаем, что

$$\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^k}, \dots \quad (14)$$

тоже корни  $m(x)$ . Так как число корней у  $m(x)$  конечно, то, начиная с некоторого момента, последовательность (14) начинает повторяться. Пусть  $n$  – наименьшее натуральное число такое, что

$$\alpha^{p^n} = \alpha.$$

Тогда

$$\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{n-1}} \quad (15)$$

– различные корни многочлена  $m(x)$ . Действительно, если предположить, что в последовательности (15) есть два одинаковых элемента, пусть  $\alpha^{p^i} = \alpha^{p^j}$  ( $i < j$ ), то

$$(\alpha^{p^i})^{p^{n-j}} = (\alpha^{p^j})^{p^{n-j}} = \alpha^{p^n} = \alpha,$$

или

$$\alpha^{p^{n-(j-i)}} = \alpha,$$

но  $j - i > 0$ , значит,  $n - (j - i) < n$ , а это противоречит выбору числа  $n$ . Поэтому  $m(x)$  имеет по крайней мере  $n$  различных корней, следовательно,  $r = \deg m(x) \geq n$ .

Пусть

$$m_1(x) = (x - \alpha)(x - \alpha^p) \dots (x - \alpha^{p^{n-1}}).$$

Очевидно,  $\deg m_1(x) = n$  и его корнями являются элементы ряда (15).

В  $\mathbb{Z}_p[x]$  возведем  $m_1(x)$  в степень  $p$ :

$$\begin{aligned} \{m_1(x)\}^p &= \{(x - \alpha)(x - \alpha^p) \dots (x - \alpha^{p^{n-1}})\}^p = (x - \alpha)^p (x - \alpha^p)^p \dots (x - \alpha^{p^{n-1}})^p = \\ &= (x^p - \alpha^p)(x^p - \alpha^{p^2}) \dots (x^p - \alpha^{p^n}) = (x^p - \alpha)(x^p - \alpha^p)(x^p - \alpha^{p^2}) \dots (x^p - \alpha^{p^{n-1}}) \end{aligned}$$

в силу  $\alpha^{p^n} = \alpha$  и теоремы 13. Таким образом,

$$\{m_1(x)\}^p = m_1(x^p),$$

но отсюда следует, что коэффициенты многочлена  $m_1(x)$  не изменились при возведении в степень  $p$ , т.е. если

$$m_1(x) = \sum_{i=0}^n c_i x^i, \quad \text{то} \quad c_i^p \equiv c_i \pmod{p},$$

а это означает, что  $c_i \in \mathbb{Z}_p$  ( $i = 0, 1, \dots, n$ ). Значит,  $m_1(x) \in \mathbb{Z}_p[x]$ .

Многочлены  $m(x)$  и  $m_1(x)$  из кольца  $\mathbb{Z}_p[x]$  имеют общий корень (даже не один!) и  $m(x)$  неприводим в  $\mathbb{Z}_p[x]$ . По теореме 9  $m_1(x)$  должен делиться на  $m(x)$ , но тогда

$$n = \deg m_1(x) \geq \deg m(x) = r,$$

или  $n \geq r$ .

Мы получили, что, с одной стороны,  $r \geq n$ , а с другой –  $n \geq r$ , откуда заключаем, что  $n = r$ , т.е.  $m(x) = m_1(x)$ . Теорема доказана.

Из этой теоремы следует, что у неприводимого многочлена  $m(x) \in \mathbb{Z}_p[x]$  нет кратных корней ни в каком расширении поля  $\mathbb{Z}_p$ . Кроме того, зная один корень  $\alpha$  этого многочлена, мы можем получить и все остальные, выписав последовательность

$$\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{r-1}},$$

где  $r = \deg m(x)$ .

Докажем теперь утверждение, обратное теореме 5.

**Теорема 15.** Для числа  $q = p^r$ , где  $p$  – простое число, а  $r > 0$  – целое, существует одно, с точностью до изоморфизма, конечное поле из  $q$  элементов. Эти элементы – корни многочлена  $x^q - x$ .

*Доказательство.* Рассмотрим многочлен  $f(x) = x^q - x \in \mathbb{Z}_p[x]$ . По теореме 8 существует поле разложения  $K$  этого многочлена, т.е. в  $K[x]$   $f(x)$  можно разложить в произведение линейных сомножителей.

Пусть  $F \subset K$  – подмножество поля  $K$ , состоящее из всех корней многочлена  $f(x)$ , т.е.

$$F = \{ a \in K \mid a^q - a = 0 \}.$$

Покажем, что  $F$  и есть искомое поле. Для этого требуется показать, что  $F$  содержит  $q = p^r$  элементов и является полем.

Найдем НОД( $f(x)$ ,  $f'(x)$ ) в  $K[x]$ . Так как

$$f'(x) = qx^{q-1} - 1 = p^r x^{p^r-1} - 1 \equiv -1 \pmod{p},$$

то НОД( $f(x)$ ,  $f'(x)$ ) = 1 в  $K[x]$  ( $\mathbb{Z}_p \subset K$ ), значит, у  $f(x)$  в  $K$  нет кратных корней. Поэтому в  $K$  имеется ровно  $q = p^r$  различных корней многочлена  $f(x)$ , т.е.  $F$  содержит  $q = p^r$  элементов.

Чтобы показать, что  $F$  – поле, достаточно проверить, что если  $a, b \in F$ , то  $a + b$ ,  $a \cdot b$ ,  $-a$ ,  $a^{-1}$  ( $a \neq 0$ ) тоже принадлежат  $F$ . Действительно, из замкнутости этих операций и того, что  $F$  – подмножество поля  $K$ , будет следовать, что все аксиомы, выполняющиеся в  $K$ , выполняются и в  $F$ .

Итак, пусть  $a, b \in F$  ( $a \neq 0$ ). Из определения  $F$  имеем

$$a^{p^r} = a \quad \text{и} \quad b^{p^r} = b.$$

Рассмотрим  $a + b$ . По теореме 13 имеем

$$(a + b)^{p^r} = a^{p^r} + b^{p^r} = a + b,$$

значит,  $a + b$  – корень  $f(x)$ , т.е.  $a + b \in F$ .

Далее,

$$(ab)^{p^r} = a^{p^r} b^{p^r} = ab,$$

следовательно,  $ab \in F$ .

Для элемента  $-a \in K$  имеем

$$(-a)^{p^r} = ((-1)a)^{p^r} = (-1)^{p^r} a^{p^r} = (-1)^{p^r} a$$

и так как если  $p = 2$ , то  $(-1)^{2^r} = 1 \equiv -1 \pmod{2}$ , если  $p$  – нечетно, то  $(-1)^{p^r} = -1$ , то получаем

$$(-a)^{p^r} = (-1)^{p^r} a = (-1)a = -a,$$

значит,  $-a \in F$ .

Наконец, если  $a \neq 0$ , то  $a^{-1} \in K$ . Рассмотрим равенство

$$aa^{-1} = 1$$

и возведем обе части его в степень  $q = p^r$ . Получим

$$(aa^{-1})^{p^r} = 1 \quad \text{или} \quad a^{p^r} (a^{-1})^{p^r} = 1$$

и так как  $a \in F$ , то  $a^{p^r} = a$ , значит,

$$a(a^{-1})^{p^r} = 1,$$

поэтому  $(a^{-1})^{p^r} = a^{-1}$ , следовательно,  $a^{-1} \in F$ .

Итак,  $F$  – поле из  $q = p^r$  элементов. Теорема доказана.



**Теорема 16.** Для любого натурального  $r$  и простого  $p$  в кольце  $\mathbb{Z}_p[x]$  существует неприводимый многочлен степени  $r$ .

Это утверждение уже было доказано в теореме 3 §12. Однако теперь мы можем дать более простое доказательство.

**Доказательство.** Пусть  $F$  – конечное поле из  $p^r$  элементов. Тогда  $F$  изоморфно фактор-кольцу  $\mathbb{Z}_p[x]/(m(x))$  для некоторого неприводимого многочлена  $m(x) \in \mathbb{Z}_p[x]$ . Причем  $\mathbb{Z}_p[x]/(m(x))$  является полем и также содержит  $p^r$  элементов, следовательно,  $\deg m(x) = r$ .

**Теорема 17.** Многочлен  $f(x) = x^{p^n} - x$  равен произведению всех неприводимых унитарных многочленов из  $\mathbb{Z}_p[x]$ , степени которых делят  $n$ .

Это утверждение следует из теорем 2 и 3 §12.

**Пример 5.** Рассмотрим поле Галуа  $GF(2^4) \cong \mathbb{Z}_2[x]/(m(x))$ , где  $m(x) = x^4 - x - 1$ . Требуется разложить многочлен  $f(x) = x^{2^4} - x$  в произведение неприводимых многочленов из  $\mathbb{Z}_2[x]$ .

Очевидно, что  $m(x) = x^4 - x - 1$  – один из сомножителей. Пусть  $\alpha$  – его корень, тогда по теореме 14  $\alpha^2, \alpha^{2^2}, \alpha^{2^3}$  также являются его корнями, т.е. все корни  $m(x)$  – это  $\alpha, \alpha^2, \alpha^4, \alpha^8$  и

$$x^4 - x - 1 = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8).$$

Еще два очевидных сомножителя  $f(x)$  – это  $x$  и  $x - 1 \equiv x + 1$  из  $\mathbb{Z}_2[x]$ .

Возьмем степень  $\alpha$ , которая еще не встречалась, например  $\alpha^3$ .  $\alpha^3 \in GF(2^4)$ , значит, является корнем  $f(x)$ , следовательно, корнем одного из неприводимых сомножителей этого многочлена. Другими корнями этого неприводимого сомножителя многочлена  $f(x)$  будут  $(\alpha^3)^2, (\alpha^3)^{2^2}, (\alpha^3)^{2^3}$ . И так как  $\alpha^{15} = 1$  ( $\alpha$  – корень  $f(x)$ , т.е.  $\alpha^{16} - \alpha = 0$ ), то корнями являются

$$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9,$$

т.е.

$$m_2(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9).$$

Опять выберем степень  $\alpha$ , которая еще не встречалась. Наименьшая такая степень равна 5. Тогда  $\alpha^5, (\alpha^5)^2$  будут корнями еще одного неприводимого сомножителя многочлена  $f(x)$ . Здесь мы получили всего два корня, так как далее следуют  $(\alpha^5)^{2^2} = \alpha^{20} = \alpha^5$  и  $(\alpha^5)^{2^3} = \alpha^{40} = \alpha^{10}$ , т.е. степени  $\alpha$  повторяются. Этот неприводимый сомножитель – многочлен второй степени

$$m_3(x) = (x - \alpha^5)(x - \alpha^{10}).$$

Берём следующую степень  $\alpha$ , которая еще не встречалась, а именно  $\alpha^7$ . Тогда

$$\alpha^7, (\alpha^7)^2 = \alpha^{14}, (\alpha^7)^{2^2} = \alpha^{28} = \alpha^{13}, (\alpha^7)^{2^3} = \alpha^{56} = \alpha^{11}$$

являются корнями неприводимого сомножителя многочлена  $f(x)$ , т.е.

$$m_4(x) = (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11}).$$

Все степени  $\alpha$ , меньшие 15, исчерпаны. Мы получили три неприводимых сомножителя  $m(x), m_2(x), m_4(x)$  четвертой степени, один – второй степени  $m_3(x)$  и два многочлена  $x$  и  $x - 1$  первой степени.

Осталось вычислить коэффициенты многочленов  $m_2(x), m_3(x)$  и  $m_4(x)$ . При вычислениях нам придется рассматривать степени элемента  $\alpha$ , учитывая, что  $\alpha$  – корень  $m(x) = x^4 - x - 1$ , т.е.  $\alpha^4 = \alpha + 1$ , и кроме того,  $\alpha^{15} = 1$ .

Начнем с более простого многочлена  $m_3(x)$ :

$$m_3(x) = (x - \alpha^5)(x - \alpha^{10}) = x^2 - (\alpha^5 + \alpha^{10})x + \alpha^{15} = x^2 - (\alpha^5 + \alpha^{10})x + 1.$$

Поскольку

$$\alpha^5 = \alpha^4 \cdot \alpha = (\alpha + 1)\alpha = \alpha^2 + \alpha,$$

$$\alpha^{10} = (\alpha^5)^2 = (\alpha^2 + \alpha)^2 = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1,$$

то

$$m_3(x) = x^2 - (\alpha^2 + \alpha + \alpha^2 + \alpha + 1)x + 1 = x^2 - x + 1 = x^2 + x + 1$$

(все операции проводятся в  $\mathbb{Z}_2$ ).

Вычислим коэффициенты  $m_2(x)$  :

$$m_2(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) = \{(x - \alpha^3)(x - \alpha^{12})\} \{(x - \alpha^6)(x - \alpha^9)\} =$$

$$\{x^2 - (\alpha^3 + \alpha^{12})x + \alpha^{15}\} \{x^2 - (\alpha^6 + \alpha^9)x + \alpha^{15}\} = (x^2 - (\alpha^3 + \alpha^{12})x + 1)(x^2 - (\alpha^6 + \alpha^9)x + 1).$$

Так как

$$\alpha^6 = \alpha^5 \cdot \alpha = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2,$$

$$\alpha^9 = \alpha^3 \alpha^6 = \alpha^3(\alpha^3 + \alpha^2) = \alpha^6 + \alpha^5 = \alpha^3 + \alpha^2 + \alpha^2 + \alpha = \alpha^3 + \alpha,$$

$$\alpha^{12} = (\alpha^6)^2 = (\alpha^3 + \alpha^2)^2 = \alpha^6 + \alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1,$$

то

$$\alpha^3 + \alpha^{12} = \alpha^2 + \alpha + 1 = \alpha^{10},$$

$$\alpha^6 + \alpha^9 = \alpha^2 + \alpha = \alpha^5,$$

значит,

$$m_2(x) = (x^2 - (\alpha^2 + \alpha + 1)x + 1)(x^2 - (\alpha^2 + \alpha)x + 1) = (x^2 - \alpha^{10}x + 1)(x^2 - \alpha^5x + 1) =$$

$$x^4 - (\alpha^{10} + \alpha^5)x^3 + (1 + \alpha^{15} + 1)x^2 - (\alpha^{10} + \alpha^5)x + 1 = x^4 - x^3 + x^2 - x + 1 = x^4 + x^3 + x^2 + x + 1.$$

Наконец, найдем коэффициенты  $m_4(x)$  :

$$m_4(x) = (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11}) = \{(x - \alpha^7)(x - \alpha^{13})\} \{(x - \alpha^{14})(x - \alpha^{11})\} =$$

$$\{x^2 - (\alpha^7 + \alpha^{13})x + \alpha^{20}\} \{x^2 - (\alpha^{11} + \alpha^{14})x + \alpha^{25}\}$$

Но

$$\alpha^{20} = \alpha^5, \quad \alpha^{25} = \alpha^{10},$$

$$\alpha^7 = \alpha^6 \cdot \alpha = (\alpha^3 + \alpha^2)\alpha = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1,$$

$$\alpha^{13} = \alpha\alpha^{12} = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + \alpha + 1 = \alpha^3 + \alpha^2 + 1,$$

$$\alpha^{11} = \alpha\alpha^{10} = \alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha,$$

$$\alpha^{14} = \alpha\alpha^{13} = \alpha(\alpha^3 + \alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha + \alpha + 1 = \alpha^3 + 1,$$

откуда

$$\alpha^7 + \alpha^{13} = \alpha^2 + \alpha = \alpha^5,$$

$$\alpha^{11} + \alpha^{14} = \alpha^3 + \alpha^2 + \alpha + \alpha^3 + 1 = \alpha^2 + \alpha + 1 = \alpha^{10},$$

значит, получаем

$$m_4(x) = (x^2 - \alpha^5x + \alpha^5)(x^2 - \alpha^{10}x + \alpha^{10}) = x^4 - (\alpha^{10} + \alpha^5)x^3 + (\alpha^5 + \alpha^{15} + \alpha^{10})x^2 - (\alpha^{15} + \alpha^{15})x + \alpha^{15} =$$

$$x^4 - x^3 + 1 = x^4 + x^3 + 1$$

Итак,

$$x^{2^4} - x = x^{16} - x = x(x + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x^4 + x^3 + 1).$$

## §16. ПОСТРОЕНИЕ ПОЛЕЙ ГАЛУА $GF(2^n)$

В качестве *основного* поля при построении  $GF(2^n)$  берется поле характеристики 2, арифметика в котором совпадает с арифметикой в поле  $\mathbb{Z}_2$ , обозначим его  $GF(2)$ .

**Определение.** Неприводимый многочлен  $p(x)$  степени  $n$  назовем *c-примитивным* над  $\mathbb{Z}_2$ , если наименьшее целое число  $N$ , для которого  $p(x)$  делит  $x^N - 1$ , есть  $N = 2^n - 1$ .

Например, многочлены  $x^4 + x + 1$  и  $x^4 + x^3 + 1$  являются *c-примитивными* многочленами четвертой степени, а  $x^4 + x^3 + x^2 + x + 1$  — нет, поскольку последний является делителем многочлена  $x^5 - 1$ .

Возьмем элементы 0, 1 из нашего основного поля характеристики 2 и добавим к ним символ  $\alpha$ . Определим естественное умножение:

$$\begin{aligned} 0 \cdot \alpha &= \alpha \cdot 0 = 0, \\ 1 \cdot \alpha &= \alpha \cdot 1 = \alpha, \\ \alpha \cdot \alpha &= \alpha^2, \\ \alpha^2 \cdot \alpha &= \alpha^3 \end{aligned}$$

и т.д.

В результате получаем бесконечное множество

$$0, 1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^k, \dots, \quad (1)$$

на элементах которого введена операция умножения.

Наложим на  $\alpha$  такое условие, чтобы в (1) осталось только  $2^n$  элементов и операция умножения была замкнута.

Пусть  $p(x)$  есть *c-примитивный* многочлен степени  $n$  над нашим полем  $GF(2)$  и пусть  $\alpha$  — корень этого многочлена, т.е.  $p(\alpha) = 0$ . По определению  $p(x) \mid x^{2^n-1} - 1$ , т.е.

$$x^{2^n-1} - 1 = p(x)q(x),$$

но тогда

$$\alpha^{2^n-1} - 1 = p(\alpha)q(\alpha) = 0,$$

откуда

$$\alpha^{2^n-1} = 1. \quad (2)$$

Условие (2) превращает множество (1) в конечное множество  $F$ , состоящее из элементов

$$F = \{0, 1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{2^n-2}\}.$$

Нетрудно видеть, что  $F \setminus \{0\} = F^*$  — мультипликативная группа. Действительно, в силу условия (2) умножение в  $F^*$  замкнуто

$$\alpha^i \cdot \alpha^j = \begin{cases} \alpha^{i+j}, & \text{если } i+j < 2^n - 1, \\ \alpha^{(i+j)-(2^n-1)}, & \text{если } i+j \geq 2^n - 1. \end{cases}$$

1 является нейтральным элементом относительно умножения, операция умножения, очевидно, ассоциативна и коммутативна. Наконец, каждый элемент  $\alpha^i \in F^*$  имеет обратный, равный  $\alpha^{(2^n-1)-i}$ .

Теперь определим в множестве  $F$  сложение так, чтобы относительно этой операции  $F$  также было абелевой группой.

Разделим  $x^i$  на  $p(x)$ ,  $0 \leq i < 2^n - 1$ :

$$x^i = p(x)q_i(x) + r_i(x), \quad \deg r_i(x) < n \quad (3)$$

над полем  $GF(2)$ , т.е.

$$r_i(x) = r_{in-1}x^{n-1} + r_{in-2}x^{n-2} + \dots + r_{i1}x + r_{i0}.$$

Поскольку  $p(x)$  – неприводимый многочлен над  $GF(2)$ , то  $\text{НОД}(x^i, p(x)) = 1$  и  $p(x)$  не делит  $x^i$ , поэтому для любого  $i$   $r_i(x) \neq 0$ . Кроме того, при  $i \neq j$   $r_i(x) \neq r_j(x)$ .

Действительно, предположим противное, пусть  $i \neq j$  и

$$\begin{aligned} x^i &= p(x)q_i(x) + r_i(x), \\ x^j &= p(x)q_j(x) + r_j(x), \quad \text{причем} \quad r_i(x) = r_j(x). \end{aligned}$$

Тогда (будем считать, что  $j > i$ )

$$x^j - x^i = p(x)(q_j(x) - q_i(x)),$$

откуда

$$p(x) \mid x^j - x^i = x^i(x^{j-i} - 1).$$

Но  $p(x)$  не делит  $x^i$ , значит,  $p(x) \mid x^{j-i} - 1$ , но  $\deg x^{j-i} < 2^n - 1$ , это противоречит  $s$ -примитивности  $p(x)$ .

Таким образом, для  $i = 0, 1, 2, \dots, 2^n - 2$  мы получаем  $2^n - 1$  различных ненулевых многочленов  $r_i(x)$  степени  $\leq n - 1$ .

Заменяя  $x$  на  $\alpha$  в формуле (3), получаем

$$\alpha^i = p(\alpha)q_i(\alpha) + r_i(\alpha) = r_i(\alpha), \quad (p(\alpha) = 0)$$

или

$$\alpha^i = r_{in-1}\alpha^{n-1} + r_{in-2}\alpha^{n-2} + \dots + r_{i1}\alpha + r_{i0}.$$

Отсюда видно, что каждый элемент из  $F^*$  единственным способом представляется в виде многочлена от  $\alpha$  над полем  $GF(2)$  степени  $\leq n - 1$ . Нулевой элемент представляется нулевым многочленом. Поэтому сложение в  $F$  можно рассматривать как сложение многочленов над полем  $GF(2)$ . Легко видеть, что  $F$  – абелева группа по сложению.

Таким образом,  $F$  является полем, состоящим из  $2^n$  элементов. Мы получили два представления элементов этого поля: во-первых, как степени элемента  $\alpha$  и, во-вторых, в виде многочленов от  $\alpha$  степени  $\leq n - 1$ . Существует также третье представление, получаемое, если представить многочлен вектором его коэффициентов. В этом случае на  $GF(2^n)$  мы смотрим как на  $n$ -мерное векторное пространство над полем  $GF(2)$  и ставим в соответствие элементу  $\alpha^i \in GF(2^n)$  вектор

$$(r_{in-1}, r_{in-2}, \dots, r_{i1}, r_{i0}), \quad (0 \leq i < 2^n - 1).$$

При этом сложение векторов выполняется покомпонентно, умножение на скаляр из поля  $GF(2)$  – также покомпонентно.

**Пример 1.** Пользуясь  $s$ -примитивным многочленом  $p(x) = x^4 + x + 1$ , построим поле  $GF(2^4)$ .

Так как  $\alpha$  – корень  $p(x)$ , то  $\alpha^4 + \alpha + 1 = 0$  или  $\alpha^4 = \alpha + 1$  в  $\mathbb{Z}_2$ . Повторно применяя это равенство, получаем представление  $\alpha^i$  ( $i = 5, \dots, 14$ ) в виде многочлена от  $\alpha$  степени  $\leq 3$ . Три различных представления элементов поля  $GF(2^4)$  показаны в следующей таблице:



Представление в виде $\alpha^i$	Представление в виде многочлена от $\alpha$	Векторное представление
0	0	(0, 0, 0, 0)
1	1	(0, 0, 0, 1)
$\alpha$	$\alpha$	(0, 0, 1, 0)
$\alpha^2$	$\alpha^2$	(0, 1, 0, 0)
$\alpha^3$	$\alpha^3$	(1, 0, 0, 0)
$\alpha^4$	$\alpha + 1$	(0, 0, 1, 1)
$\alpha^5$	$\alpha^2 + \alpha$	(0, 1, 1, 0)
$\alpha^6$	$\alpha^3 + \alpha^2$	(1, 1, 0, 0)
$\alpha^7$	$\alpha^3 + \alpha + 1$	(1, 0, 1, 1)
$\alpha^8$	$\alpha^2 + 1$	(0, 1, 0, 1)
$\alpha^9$	$\alpha^3 + \alpha$	(1, 0, 1, 0)
$\alpha^{10}$	$\alpha^2 + \alpha + 1$	(0, 1, 1, 1)
$\alpha^{11}$	$\alpha^3 + \alpha^2 + \alpha$	(1, 1, 1, 0)
$\alpha^{12}$	$\alpha^3 + \alpha^2 + \alpha + 1$	(1, 1, 1, 1)
$\alpha^{13}$	$\alpha^3 + \alpha^2 + 1$	(1, 1, 0, 1)
$\alpha^{14}$	$\alpha^3 + 1$	(1, 0, 0, 1)

*Замечание.* На самом деле, чтобы построить поле  $GF(p^n)$  для любого простого  $p$ , достаточно найти примитивный элемент  $\alpha$  этого поля. Порядок элемента  $\alpha$  равен  $p^n - 1$ , поэтому все ненулевые элементы поля  $GF(p^n)$  являются степенями элемента  $\alpha$ , т.е.

$$GF(p^n) \setminus \{0\} = \{ \alpha, \alpha^2, \alpha^3, \dots, \alpha^{p^n-2}, \alpha^{p^n-1} = 1 \}.$$

Добавляя к этому множеству нуль, получаем поле из  $p^n$  элементов. Трудность заключается в том, чтобы найти неприводимый многочлен степени  $n$  из  $\mathbb{Z}_p[x]$ , корень которого  $\alpha$  имеет порядок  $p^n - 1$ . Для этого нужно выбрать такой неприводимый многочлен из  $\mathbb{Z}_p[x]$ , который делит  $x^{p^n-1} - 1$  и не делит многочлены вида  $x^s - 1$  при  $s < p^n - 1$ . Этот многочлен выше и назван *c*-примитивным.

Исходя из этих соображений, можно строить поле Галуа  $GF(p^n)$  для любого простого  $p$  и натурального  $n$ .

**Пример 2.** Построим поле  $GF(3^2)$ .

Рассмотрим многочлен  $x^3 - x = x^9 - x = x(x^8 - 1)$ . Требуется найти такой неприводимый многочлен второй степени из  $\mathbb{Z}_3[x]$ , который делит  $x^8 - 1$  и не делит  $x^s - 1$  при  $s < 8$ . Так как

$$x^8 - 1 = (x^4 + 1)(x^4 - 1) = (x^4 + 1)(x^2 + 1)(x + 1)(x - 1),$$

то следует взять неприводимый делитель многочлена  $x^4 + 1$  второй степени. В  $\mathbb{Z}_3[x]$

$$x^4 + 1 = x^4 - 2x^2 + 1 + 2x^2 = (x^2 - 1)^2 - x^2 = (x^2 - x - 1)(x^2 + x - 1) = (x^2 + 2x + 2)(x^2 + x + 2),$$

значит, нам подходит любой из полученных сомножителей.

Пусть  $\alpha$  – корень многочлена  $x^2 + 2x + 2 = p_1(x)$ , тогда  $GF(3^2) \cong \mathbb{Z}_3[x]/((p_1(x)))$ . Используя соотношение  $\alpha^2 + 2\alpha + 2 = 0$  или  $\alpha^2 = -2\alpha - 2 = \alpha + 1$ , построим три представления элементов поля  $GF(3^2)$  :

Представление в виде $\alpha^i$	Представление в виде многочлена от $\alpha$	Векторное представление
0	0	(0, 0)
1	1	(0, 1)
$\alpha$	$\alpha$	(1, 0)
$\alpha^2$	$\alpha + 1$	(1, 1)
$\alpha^3$	$2\alpha + 1$	(2, 1)
$\alpha^4$	2	(0, 2)
$\alpha^5$	$2\alpha$	(2, 0)
$\alpha^6$	$2\alpha + 2$	(2, 2)
$\alpha^7$	$\alpha + 2$	(1, 2)

Если  $\alpha$  – корень многочлена  $p_2(x) = x^2 + x + 2$ , то  $\alpha^2 + \alpha + 2 = 0$ , откуда  $\alpha^2 = -\alpha - 2 = 2\alpha + 1$  и получится поле  $GF(3^2) \cong \mathbb{Z}_3[x]/(p_2(x))$ , три представления элементов которого записаны в следующей таблице:

Представление в виде $\alpha^i$	Представление в виде многочлена от $\alpha$	Векторное представление
0	0	(0, 0)
1	1	(0, 1)
$\alpha$	$\alpha$	(1, 0)
$\alpha^2$	$2\alpha + 1$	(2, 1)
$\alpha^3$	$2\alpha + 2$	(2, 2)
$\alpha^4$	2	(0, 2)
$\alpha^5$	$2\alpha$	(2, 0)
$\alpha^6$	$\alpha + 2$	(1, 2)
$\alpha^7$	$\alpha + 1$	(1, 1)

## §17. КРУГОВЫЕ МНОГОЧЛЕНЫ

**Определение 1.** Пусть  $K$  – поле характеристики  $p$ ,  $n$  – натуральное число, не делящееся на  $p$ ,  $\zeta$  – первообразный корень  $n$ -й степени из 1 над полем  $K$ . Тогда многочлен

$$Q_n(x) = \prod_{\substack{s=1 \\ \text{НОД}(s,n)=1}}^n (x - \zeta^s)$$

называется  $n$ -круговым (или  $n$ -циклотомическим) многочленом над полем  $K$ .

Степень многочлена  $Q_n(x)$  равна, очевидно,  $\varphi(n)$  (количество натуральных чисел, меньших  $n$  и взаимно простых с  $n$ ). Корнями  $Q_n(x)$  являются все первообразные корни  $n$ -й степени из 1. Очевидно, что  $Q_n(x)$  не зависит от выбора  $\zeta$ .

**Определение 2.** Поле, не содержащее собственных подполей, называется *простым полем*.

Простое поле можно получить, пересекая все подполя данного поля. Примерами простых полей являются поле  $\mathbb{Z}_p$  ( $p$  – простое), поле рациональных чисел  $\mathbb{Q}$ . Поле Галуа  $GF(p^n)$  при  $n > 1$  не является простым, так как содержит, например, подполе  $GF(p) \cong \mathbb{Z}_p$ . Поля  $\mathbb{R}$  и  $\mathbb{C}$  также не являются простыми, поскольку содержат подполе рациональных чисел  $\mathbb{Q}$ .

**Теорема 1.** Пусть  $K$  – поле характеристики  $p$  и  $n$  – натуральное число, не делящееся на  $p$ . Тогда:

(1)

$$x^n - 1 = \prod_{d|n} Q_d(x);$$

(2) коэффициенты  $n$ -кругового многочлена  $Q_n(x)$  принадлежат простому подполю поля  $K$ , если  $p$  – простое число, или кольцу целых чисел  $\mathbb{Z}$ , если  $p = 0$ .

**Доказательство.** Корнями многочлена  $x^n - 1$  являются все корни  $n$ -й степени из 1. Если  $\zeta$  – первообразный корень  $n$ -й степени из 1, то все корни  $x^n - 1$  есть

$$1 = \zeta^0, \zeta, \zeta^2, \dots, \zeta^{n-1}. \quad (1)$$

Рассмотрим подмножества всех корней (1), вводя

$$E_t^{(n)} = \{ \zeta^s \mid \text{НОД}(s, n) = t \}$$

для любого делителя  $t$  числа  $n$ .

В частности,

$$E_1^{(n)} = \{ \zeta^s \mid \text{НОД}(s, n) = 1 \},$$

т.е. это множество состоит из всех первообразных корней  $n$ -й степени из 1.

Покажем, что множество  $E_t^{(n)}$  состоит из всех первообразных корней степени  $d = \frac{n}{t}$  из 1 для любого делителя  $t$  числа  $n$ . Пусть  $\zeta^s \in E_t^{(n)}$ , тогда

$$(\zeta^s)^d = (\zeta^s)^{\frac{n}{t}} = (\zeta^n)^{\frac{s}{t}} = 1$$

( $t = \text{НОД}(s, n)$ , значит,  $t \mid s$ ).

Пусть  $(\zeta^s)^{d'} = 1$ . Покажем, что  $d' \geq d$ . Предположим, что это не так, т.е.  $d' < d$ . Тогда поделим  $d$  на  $d'$ :

$$d = kd' + r, \quad \text{где } r < d' < d.$$

Из равенства

$$1 = (\zeta^s)^d = (\zeta^s)^{kd' + r} = (\zeta^s)^{kd'} (\zeta^s)^r = (\zeta^s)^{d'k} \zeta^{sr} = \zeta^{sr}$$

следует, что

$$\zeta^{sr} = 1,$$

значит,  $n \mid sr$ .

Из  $n \mid sr$  следует, что  $\frac{n}{t} \mid \frac{s}{t}r$ , но  $\text{НОД}(\frac{n}{t}, \frac{s}{t}) = 1$ , поэтому  $\frac{n}{t} \mid r$ , значит,  $d = \frac{n}{t} \mid r$ , т.е.  $r \geq d$ , но это противоречит тому, что  $r < d' < d$ . Итак,  $\zeta^s \in E_t^{(n)}$  является корнем уравнения  $x^d - 1$  и не является корнем  $x^{d'} - 1$  при  $d' < d$ , т.е. это первообразный корень степени  $d$  из единицы.

Тогда

$$\prod_{\zeta^s \in E_t^{(n)}} (x - \zeta^s) = \prod_{\text{НОД}(s, n)=t} (x - \zeta^s) = Q_d(x), \quad (d = \frac{n}{t})$$

очевидно,  $\deg Q_d(x) = \varphi(d)$ .

Множества  $E_t^{(n)}$ , очевидно, не пересекаются, и каждый элемент последовательности (1) попадает в одно из множеств  $E_t^{(n)}$ , поэтому

$$x^n - 1 = \prod_{d \mid n} Q_d(x),$$

так как  $n = \sum_{d \mid n} \varphi(d)$  (теорема 2 §12 в [4]).

Утверждение (1) теоремы доказано.

Утверждение (2) докажем индукцией по  $n$ . Заметим, что для любого  $n > 0$   $Q_n(x)$  — унитарный многочлен.

При  $n = 1$  имеем  $Q_1(x) = x - 1$ , и утверждение верно.

При  $n = 2$  имеем  $Q_2(x) = (x - 1)(x + 1) = x^2 - 1$ , т.е. опять утверждение (2) справедливо.

Предположим, что утверждение справедливо для всех многочленов  $Q_d(x)$ ,  $1 \leq d < n$ . Покажем, что оно справедливо и для  $Q_n(x)$ . Из доказанного выше утверждения (1) следует

$$x^n - 1 = \prod_{d \mid n} Q_d(x) = Q_n(x) \prod_{\substack{d \mid n \\ 1 \leq d < n}} Q_d(x) = Q_n(x)f(x), \quad \text{где} \quad f(x) = \prod_{\substack{d \mid n \\ 1 \leq d < n}} Q_d(x),$$

откуда

$$Q_n(x) = \frac{x^n - 1}{f(x)}.$$

По предположению индукции  $f(x)$  — многочлен с коэффициентами из простого подполя поля  $K$  (если  $p$  — простое число). В результате деления  $x^n - 1$  на  $f(x)$  получаем многочлен с коэффициентами из того же подполя.

Для кольца  $\mathbb{Z}$  рассмотрим равенство

$$x^n - 1 = Q_n(x)f(x). \quad (2)$$

Пусть

$$f(x) = x^{n-k} + b_{n-k-1}x^{n-k-1} + b_{n-k-2}x^{n-k-2} + \dots + b_1x + b_0, \quad b_i \in \mathbb{Z}, \quad (0 \leq i \leq n-k),$$

$$Q_n(x) = x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1x + a_0, \quad k > n-k,$$

тогда

$$x^n - 1 = (x^k + a_{k-1}x^{k-1} + \dots + a_1x + a_0)(x^{n-k} + b_{n-k-1}x^{n-k-1} + \dots + b_1x + b_0),$$



откуда, приравнявая коэффициенты при одинаковых степенях  $x$ , получаем

[illegible]

Поскольку  $b_{n-k-1}$  – целое, то  $a_{k-1} = -b_{n-k-1}$  – тоже целое. Далее,  $a_{k-2} = -b_{n-k-2} - b_{n-k-1}a_{k-1}$  – целое. Спускаемся вниз по равенствам (3) и получаем, что  $a_{k-3}, \dots, a_0$  – все целые.

Теорема доказана.

**Пример 1.** Если  $p$  – простое число, а  $r$  – натуральное, то

$$Q_{p^r}(x) = \frac{x^{p^r} - 1}{\prod_{\substack{d|p^r \\ 1 \leq d < p^r}} Q_d(x)} = \frac{x^{p^r} - 1}{Q_1(x)Q_p(x) \dots Q_{p^{r-1}}(x)} = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \dots + x^{(p-1)p^{r-1}},$$

ТАК КАК

$$Q_{p^{r-1}}(x) = \frac{x^{p^{r-1}} - 1}{Q_1(x)Q_p(x)\dots Q_{p^{r-2}}(x)}.$$

**Теорема 2 (Мультипликативная формула обращения Мебиуса).** Пусть  $f, g$  – функции, определенные на множестве натуральных чисел со значениями в некоторой абелевой группе. Тогда

$$f(n) = \prod_{d|n} g(d) \quad \text{тогда и только тогда, когда} \quad g(n) = \prod_{d|n} f\left(\frac{n}{d}\right)^{\mu(d)}.$$

*Доказательство.* Пусть

$$f(n) = \prod_{d \mid n} g(d).$$

Докажем правую формулу. Рассмотрим

$$\prod_{d|n} f \left( \frac{n}{d} \right)^{\mu(d)}$$

и заменим  $f\left(\frac{n}{d}\right)$  на его выражение через  $g$ , т.е.

$$\prod_{d \mid n} f\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d \mid n} \left( \prod_{k \mid \frac{n}{d}} g(k) \right)^{\mu(d)} = \prod_{k \mid n} \left( \prod_{d \mid \frac{n}{k}} g(k) \right)^{\mu(d)} = \prod_{k \mid n} g(k)^{\sum_{d \mid \frac{n}{k}} \mu(d)}.$$

### По свойству функции Мебиуса

$$\sum_{d \mid \frac{n}{k}} \mu(d) = 0, \quad \text{если} \quad \frac{n}{k} > 1,$$

и

$$\sum_{d \mid \frac{n}{k}} \mu(d) = 1, \quad \text{если} \quad \frac{n}{k} = 1, \quad \text{т.е.} \quad k = n,$$

поэтому

$$\prod_{k \mid n} g(k)^{\sum_{d \mid \frac{n}{k}} \mu(d)} = g(n).$$

Обратно, пусть выполнено

$$g(n) = \prod_{d \mid n} f\left(\frac{n}{d}\right)^{\mu(d)}.$$

Докажем левую формулу:

$$\begin{aligned} \prod_{d \mid n} g(d) &= \prod_{d \mid n} \left( \prod_{k \mid d} f\left(\frac{d}{k}\right)^{\mu(k)} \right) = \prod_{d \mid n} \left( \prod_{k \mid d} f(k)^{\mu(\frac{d}{k})} \right) = \prod_{k \mid n} \prod_{\substack{d \mid n \\ \frac{d}{k} \mid \frac{n}{k}}} f(k)^{\mu(\frac{d}{k})} = \\ &= \prod_{k \mid n} f(k)^{\sum_{\substack{d \mid n \\ \frac{d}{k} \mid \frac{n}{k}}} \mu(\frac{d}{k})} = f(n), \end{aligned}$$

так как

$$\sum_{\substack{d \mid n \\ \frac{d}{k} \mid \frac{n}{k}}} \mu\left(\frac{d}{k}\right) = \begin{cases} 0 & \text{при} \quad \frac{n}{k} > 1, \\ 1 & \text{при} \quad k = n. \end{cases}$$

Доказанным утверждением мы воспользуемся для получения следующего результата.

**Теорема 3.** Пусть  $K$  — поле характеристики  $p$ ,  $n$  — натуральное число, не делящееся на  $p$ . Тогда  $n$ -круговой многочлен  $Q_n(x)$  над полем  $K$  задается формулой

$$Q_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(\frac{n}{d})} = \prod_{d \mid n} (x^{\frac{n}{d}} - 1)^{\mu(d)}. \quad (4)$$

*Доказательство.* По теореме 1 имеем

$$x^n - 1 = \prod_{d \mid n} Q_d(x).$$

Пусть  $f(n) = x^n - 1$ ,  $g(d) = Q_d(x)$ . Тогда по теореме 2 из

$$f(n) = \prod_{d \mid n} g(d) \quad \text{следует, что} \quad g(n) = \prod_{d \mid n} f(d)^{\mu(\frac{n}{d})}$$

или

$$Q_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(\frac{n}{d})}.$$

(Мы применили формулу обращения Мебиуса к мультипликативной группе ненулевых рациональных функций над полем  $K$ .)

**Пример 2.**

$$Q_{12}(x) = \prod_{d \mid 12} (x^{\frac{12}{d}} - 1)^{\mu(d)} = (x^{12} - 1)^{\mu(1)} (x^6 - 1)^{\mu(2)} (x^4 - 1)^{\mu(3)} (x^3 - 1)^{\mu(4)} (x^2 - 1)^{\mu(6)} \times$$

$$(x - 1)^{\mu(12)} = \frac{(x^{12} - 1)(x^2 - 1)}{(x^6 - 1)(x^4 - 1)} = \frac{x^6 + 1}{x^2 + 1} = x^4 - x^2 + 1,$$

так как  $\mu(1) = 1$ ,  $\mu(2) = \mu(3) = -1$ ,  $\mu(6) = 1$ ,  $\mu(4) = \mu(12) = 0$ .

**Пример 3.**

$$x^{63} - 1 = \prod_{d \mid 63} Q_d(x) = Q_1(x) Q_3(x) Q_7(x) Q_9(x) Q_{21}(x) Q_{63}(x).$$

Поскольку

$$Q_1(x) = x - 1,$$

$$Q_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1,$$

$$Q_7(x) = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

$$Q_9(x) = \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1,$$

$$Q_{21} = \frac{(x^{21} - 1)(x - 1)}{(x^7 - 1)(x^3 - 1)} = \frac{x^{14} + x^7 + 1}{x^2 + x + 1} = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1,$$

$$Q_{63} = \frac{(x^{63} - 1)(x^3 - 1)}{(x^{21} - 1)(x^9 - 1)} = \frac{x^{42} + x^{21} + 1}{x^6 + x^3 + 1} = x^{36} - x^{33} + x^{27} - x^{24} + x^{18} - x^{12} + x^9 - x^3 + 1,$$

то

$$x^{63} - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x^6 + x^3 + 1)(x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1) \times \\ (x^{36} - x^{33} + x^{27} - x^{24} + x^{18} - x^{12} + x^9 - x^3 + 1).$$

В §12 мы посчитали число унитарных неприводимых многочленов степени  $n$  в кольце  $\mathbb{Z}_p[x]$ . Теперь мы можем получить формулу для *произведения* всех унитарных неприводимых многочленов данной степени  $n$  из кольца  $\mathbb{Z}_p[x]$ .

**Теорема 4.** *Произведение  $I(p, n; x)$  всех унитарных неприводимых многочленов степени  $n$  из кольца  $\mathbb{Z}_p[x]$  задается формулой*

$$I(p, n; x) = \prod_{d \mid n} (x^{p^d} - x)^{\mu(\frac{n}{d})} = \prod_{d \mid n} (x^{p^{\frac{n}{d}}} - x)^{\mu(d)}. \quad (5)$$

*Доказательство.* В §12 было доказано, что многочлен  $x^{p^n} - x$  равен произведению всех унитарных неприводимых многочленов кольца  $\mathbb{Z}_p[x]$ , степени которых делят  $n$ , значит,

$$x^{p^n} - x = \prod_{d \mid n} I(p, d; x).$$

Положим

$$g(d) = I(p, d; x),$$

$$f(n) = x^{p^n} - x \quad \text{для } n \in \mathbb{N}$$

и применим мультипликативную формулу обращения Мебиуса (теорема 2):

$$g(n) = \prod_{d \mid n} f(d)^{\mu(\frac{n}{d})}.$$

или

$$I(p, n; x) = \prod_{d \mid n} (x^{p^d} - x)^{\mu(\frac{n}{d})}.$$

**Пример 4.** Найдем произведение всех неприводимых унитарных многочленов четвертой степени из кольца  $\mathbb{Z}_2[x]$ .

По формуле (5)

$$I(2, 4; x) = \prod_{d|4} (x^{2^d} - x)^{\mu(\frac{4}{d})} = \prod_{d|4} (x^{2^{\frac{4}{d}}} - x)^{\mu(d)} = (x^{2^4} - x)^{\mu(1)} (x^{2^2} - x)^{\mu(2)} (x^2 - x)^{\mu(4)} =$$

$$\frac{x^{16} - x}{x^4 - x} = \frac{x^{15} - 1}{x^3 - 1} = x^{12} + x^9 + x^6 + x^3 + 1.$$

Если же требуется найти сами неприводимые многочлены, то дальше придется разложить полученный многочлен на множители. Это разложение требует некоторых усилий, поэтому было бы полезно представить многочлен  $I(p, n; x)$  хотя бы в частично разложенном виде. Это достигается с помощью следующей теоремы.

**Теорема 5.** Пусть  $I(p, n; x)$  – произведение всех унитарных неприводимых многочленов степени  $n$  из кольца  $\mathbb{Z}_p[x]$ . Тогда для натурального числа  $n > 1$  справедлива формула

$$I(p, n; x) = \prod_m Q_m(x), \quad (6)$$

где  $Q_m(x)$  есть  $m$ -круговой многочлен над  $\mathbb{Z}_p$ , а произведение берется по всем натуральным делителям  $m$  числа  $p^n - 1$ , для которых  $p \equiv 1 \pmod{m}$ , причем  $n$  – наименьшее целое, удовлетворяющее этому условию.

*Доказательство.* Рассмотрим поле Галуа  $GF(p^n)$ . Множество  $GF(p^n) \setminus \{0\} = GF(p^n)^*$  является мультипликативной группой порядка  $p^n - 1$ , поэтому порядок любого элемента  $\alpha$  этой группы делит число  $p^n - 1$ .  $\mathbb{Z}_p \cong GF(p)$  является собственным подполем поля  $GF(p^n)$ . Для любого натурального  $n > 1$  обозначим через  $S$  множество всех элементов из  $GF(p^n)^*$ , которые являются корнями неприводимых унитарных многочленов с коэффициентами из  $\mathbb{Z}_p$  степени  $n$ , а значит, корнями многочлена  $I(p, n; x)$ . Обратно, если  $\beta$  – корень многочлена  $I(p, n; x)$ , то он является корнем одного из многочленов, входящих в это произведение, т.е. унитарного неприводимого многочлена степени  $n$  из  $\mathbb{Z}_p[x]$ , значит, принадлежит множеству  $S$ . Поэтому

$$I(p, n; x) = \prod_{\alpha \in S} (x - \alpha),$$

причем  $\text{ord}(\alpha) = m$  делит  $p^n - 1$ , т.е.  $p^n \equiv 1 \pmod{m}$ .

Покажем, что  $n$  – наименьшее натуральное число, для которого  $p^n \equiv 1 \pmod{m}$ . Предположим, что это не так, т.е.

$$p^d \equiv 1 \pmod{m}, \quad \text{причем } d < n. \quad (7)$$

Сравнение (7) означает, что

$$p^d = mQ + 1, \quad Q \in \mathbb{Z},$$

поэтому

$$\alpha^{p^d} = \alpha^{mQ+1} = \alpha^{mQ} \cdot \alpha = \alpha,$$

т.е.  $\alpha$  – корень многочлена  $x^{p^d} - x \in \mathbb{Z}_p[x]$ . С другой стороны,  $\alpha$  – корень неприводимого унитарного многочлена степени  $n$  из  $\mathbb{Z}_p[x]$ , пусть этот многочлен  $q(x)$ . Многочлены  $x^{p^d} - x$  и  $q(x)$  из  $\mathbb{Z}_p[x]$  имеют общий корень  $\alpha$ , следовательно, не взаимно просты. Так как  $q(x)$  – неприводим, то он делит  $x^{p^d} - x$ . Но мы знаем (теорема 2 §12), что унитарный неприводимый многочлен из  $\mathbb{Z}_p[x]$  делит многочлен  $x^{p^d} - x$  тогда и только тогда, когда его степень делит  $d$ , значит,  $n = \deg q(x) | d$ , что невозможно, так как  $d < n$ . Полученное противоречие доказывает, что  $n$  – наименьшее целое положительное число такое, что  $p^n \equiv 1 \pmod{m}$ .



Обозначим через  $S_m$  множество элементов порядка  $m$  из  $S$ , где  $m$  – положительный делитель  $p^n - 1$  такой, что  $n$  – наименьшее натуральное число такое, что  $p^n \equiv 1 \pmod{m}$ . Тогда

$$S = \bigcup_m S_m,$$

причем  $S_{m_1} \cap S_{m_2} = \emptyset$  при  $m_1 \neq m_2$ , т.е. множества  $S_m$  не пересекаются. Тогда

$$I(p, n; x) = \prod_m \prod_{\alpha \in S_m} (x - \alpha).$$

Множество  $S_m$  состоит из всех элементов мультипликативной группы  $GF(p^n)^*$ , имеющих порядок  $m$ , т.е.  $S_m$  – множество первообразных корней  $m$ -й степени из 1 над  $\mathbb{Z}_p$ . Но тогда по определению круговых многочленов

$$\prod_{\alpha \in S_m} (x - \alpha) = Q_m(x) \in \mathbb{Z}_p[x],$$

откуда получаем

$$I(p, n; x) = \prod_m Q_m(x).$$

**Пример 5.** Найдем все унитарные неприводимые многочлены степени 4 из  $\mathbb{Z}_2[x]$ .

Мы уже видели выше, что  $I(2, 4; x) = x^{12} + x^9 + x^6 + x^3 + 1$ . Формула (6) позволяет получить частичное разложение этого многочлена. Делители числа  $2^4 - 1 = 15$  есть: 1, 3, 5, 15. Выберем из чисел 3, 5, 15 те, для которых 4 является наименьшей степенью такой, что  $2^4 \equiv 1 \pmod{m}$ . Очевидно, 3 не подходит, так как  $2^2 \equiv 1 \pmod{3}$ .

Числа 5 и 15 подходят:

$$\begin{aligned} 2^2 &\not\equiv 1 \pmod{5}, & 2^3 &\not\equiv 1 \pmod{5}, \\ 2^2 &\not\equiv 1 \pmod{15}, & 2^3 &\not\equiv 1 \pmod{15}, \end{aligned}$$

поэтому

$$I(2, 4; x) = Q_5(x) Q_{15}(x).$$

Так как

$$\begin{aligned} Q_5(x) &= \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1, \\ Q_{15}(x) &= \frac{(x^{15} - 1)(x - 1)}{(x^5 - 1)(x^3 - 1)} = \frac{x^{10} + x^5 + 1}{x^2 + x + 1} = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1, \end{aligned}$$

то один неприводимый многочлен 4-й степени равен  $Q_5(x)$ , произведение двух других равно  $Q_{15}(x)$ .

Сделаем замену  $x$  на  $x + 1$  в многочлене  $Q_5(x)$ ; полученный в результате многочлен также будет неприводимым. Имеем

$$(x + 1)^4 + (x + 1)^3 + (x + 1)^2 + (x + 1) + 1 = (x^4 + 1) + (x^3 + x^2 + x + 1) + (x^2 + 1) + (x + 1) + 1 = x^4 + x^3 + 1,$$

т.е. получен новый неприводимый многочлен 4-й степени. Так как он является сомножителем в разложении  $Q_{15}(x)$ , то последний многочлен получаем делением  $Q_{15}(x)$  на  $x^4 + x^3 + 1$ :

$$\frac{Q_{15}(x)}{x^4 + x^3 + 1} = x^4 + x + 1.$$

Таким образом,

$$I(2, 4; x) = (x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x + 1).$$

**Пример 6.** Получим частичное разложение многочлена  $I(2, 6; x)$  в  $\mathbb{Z}_2[x]$ .

Так как  $2^6 - 1 = 63$ , то рассмотрим следующие делители  $63 : 3, 7, 9, 21, 63$ . Выше мы уже видели, что 3 не подходит, число 7 нам также не подходит, так как  $2^3 \equiv 1 \pmod{7}$ . Остальные делители удовлетворяют теореме 5, поэтому

$$I(2, 6; x) = Q_9(x) Q_{21}(x) Q_{63}(x),$$

где

$$\begin{aligned} Q_9(x) &= \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1, \\ Q_{21}(x) &= \frac{(x^{21} - 1)(x - 1)}{(x^7 - 1)(x^3 - 1)} = \frac{x^{14} + x^7 + 1}{x^2 + x + 1} = x^{12} + x^{11} + x^9 + x^8 + x^6 + x^4 + x^3 + x + 1, \\ Q_{63}(x) &= \frac{(x^{63} - 1)(x^3 - 1)}{(x^{21} - 1)(x^9 - 1)} = \frac{x^{42} + x^{21} + 1}{x^6 + x^3 + 1} = x^{36} + x^{33} + x^{27} + x^{24} + x^{18} + x^{12} + x^9 + x^3 + 1. \end{aligned}$$

Имея неприводимый многочлен 6-й степени  $x^6 + x^3 + 1 \in \mathbb{Z}_2[x]$ , попробуем получить другой с помощью замены  $x$  на  $x + 1$ :

$$(x + 1)^6 + (x + 1)^3 + 1 = (x^6 + x^4 + x^2 + 1) + (x^3 + x^2 + x + 1) + 1 = x^6 + x^4 + x^3 + x + 1.$$

Можно проверить, что полученный многочлен является делителем  $Q_{63}(x)$ :

$$Q_{63}(x) = (x^6 + x^4 + x^3 + x + 1)(x^{30} + x^{28} + x^{26} + x^{22} + x^{19} + x^{18} + x^{16} + x^{15} + x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

Попробуем найти неприводимый многочлен 6-й степени из  $\mathbb{Z}_2[x]$ . Нетрудно проверить, что многочлен  $x^6 + x^5 + 1$  не имеет в  $\mathbb{Z}_2$  корней (значит, в частности, не представляется в виде произведения неприводимого многочлена 5-й степени на многочлен первой степени), не делится на неприводимый многочлен  $x^2 + x + 1$  (значит, не представляется в виде произведения неприводимого многочлена 4-й степени на многочлен второй степени), не делится на неприводимые многочлены 3-й степени  $x^3 + x^2 + 1$ ,  $x^3 + x + 1$ . Значит, это неприводимый многочлен. То же относится и к многочлену  $x^6 + x + 1$ .

Делая замену  $x$  на  $x + 1$  в каждом из этих двух многочленов, получим еще два неприводимых многочлена:

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

Последний многочлен является делителем многочлена  $Q_{21}(x)$ :

$$Q_{21}(x) = (x^6 + x^4 + x^2 + x + 1)(x^6 + x^5 + x^4 + x^2 + 1).$$

В результате деления получен еще один неприводимый многочлен 6-й степени  $x^6 + x^5 + x^4 + x^2 + 1$ . Делая в нем замену  $x$  на  $x + 1$ , получаем

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

т.е. еще один неприводимый многочлен 6-й степени.

Многочлены  $x^6 + x^5 + 1$ ,  $x^6 + x + 1$ ,  $x^6 + x^5 + x^2 + x + 1$ ,  $x^6 + x^5 + x^4 + x + 1$  должны быть делителями многочлена  $Q_{63}(x)$ , т.е.

$$Q_{63}(x) = (x^6 + x^4 + x^3 + x + 1)(x^6 + x^5 + 1)(x^6 + x + 1)(x^6 + x^5 + x^2 + x + 1)(x^6 + x^5 + x^4 + x + 1)q(x),$$

где  $q(x)$  – многочлен 6-й степени, т.е. последний неприводимый многочлен 6-й степени из  $\mathbb{Z}_2[x]$ . Чтобы его найти, придется поделить  $Q_{63}(x)$  на его найденные сомножители:

$$\frac{x^{30} + x^{28} + x^{26} + x^{22} + x^{19} + x^{18} + x^{16} + x^{15} + x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^5 + x^4 + x^3 + x^2 + x + 1}{(x^6 + x^4 + x^3 + x + 1)(x^6 + x^5 + 1)(x^6 + x + 1)(x^6 + x^5 + x^2 + x + 1)(x^6 + x^5 + x^4 + x + 1)}$$

$$= x^6 + x^5 + x^3 + x^2 + 1 = q(x)$$

В результате нам удалось разложить  $I(2, 6; x)$  в произведение неприводимых унитарных многочленов, а значит, получить все неприводимые унитарные многочлены 6-й степени из кольца  $\mathbb{Z}_2[x]$ :

$$\begin{array}{llll} x^6 + x^3 + 1, & x^6 + x^4 + x^3 + x + 1, & x^6 + x^5 + x^4 + x^2 + 1, & \\ x^6 + x^5 + 1, & x^6 + x^5 + x^2 + x + 1, & x^6 + x^5 + x^3 + x^2 + 1, & x^6 + x^5 + x^4 + x + 1. \\ x^6 + x + 1, & x^6 + x^4 + x^2 + x + 1, & & \end{array}$$

## ПРИЛОЖЕНИЕ

### §1. Модулярный алгоритм для нахождения наибольшего общего делителя двух многочленов

Мы видели, что в кольце  $\mathbb{Z}[x]$  для отыскания наибольшего общего делителя двух многочленов приходится пользоваться псевдоделением. При этом коэффициенты многочленов растут и, если не переходить на каждом шаге к примитивной части остатка от деления, этот рост коэффициентов будет экспоненциальным. Но для перехода к примитивной части остатка приходится каждый раз искать наибольший общий делитель его коэффициентов, что делает алгоритм весьма неэффективным.

Вычисление наибольшего общего делителя двух многочленов над конечным полем не приводит к экспоненциальному росту коэффициентов, поскольку они не могут превосходить размер модуля. Поэтому можно преобразовать задачу нахождения наибольшего общего делителя двух многочленов над  $\mathbb{Z}$  к нескольким задачам нахождения наибольшего общего делителя над некоторыми конечными полями. Ответы к этим задачам затем интерполировать, используя китайскую теорему об остатках, чтобы получить наибольший общий делитель над  $\mathbb{Z}$ . Это и есть идея *модулярного алгоритма* нахождения наибольшего общего делителя.

Пусть

$$g(x) = \sum_{i=0}^n c_i x^i$$

— многочлен из кольца  $\mathbb{Z}[x]$ ,  $p > 1$  — целое число. Через  $g^{(p)}(x)$  обозначим многочлен

$$g^{(p)}(x) = \sum_{i=0}^n c_i \pmod{p} x^i.$$

Очевидно,  $g^{(p)}(x)$  принадлежит кольцу  $\mathbb{Z}_p[x]$ .

**Лемма.** Если простое число  $p$  не делит старший коэффициент многочлена  $d(x)$ , где  $d(x) = \text{НОД}(f(x), g(x))$ ,  $f(x), g(x) \in \mathbb{Z}[x]$ , а

$$t(x) = \text{НОД}(f^{(p)}(x), g^{(p)}(x))$$

в  $\mathbb{Z}_p[x]$ , то

$$\deg t(x) \geq \deg d(x).$$

**Доказательство.** Поскольку  $d(x)$ , являясь наибольшим общим делителем многочленов  $f(x)$  и  $g(x)$ , делит каждый из них, то  $d^{(p)}(x)$  делит  $f^{(p)}(x)$  и  $g^{(p)}(x)$ . Действительно, из

$$f(x) = d(x)q(x),$$

$$g(x) = d(x)r(x),$$

очевидно, следует

$$f^{(p)}(x) = d^{(p)}(x)q^{(p)}(x),$$

$$g^{(p)}(x) = d^{(p)}(x)r^{(p)}(x)$$

в  $\mathbb{Z}_p[x]$ .

Значит,  $d^{(p)}(x)$  делит  $t(x)$ , поэтому  $\deg d^{(p)}(x) \leq \deg t(x)$ . Но  $\deg d^{(p)}(x) = \deg d(x)$ , так как старший коэффициент  $d(x)$  по условию леммы не делится на  $p$ . Значит,

$$\deg t(x) \geq \deg d(x),$$

что и требовалось доказать.



**Теорема 1.** Пусть  $f(x), g(x) \in \mathbb{Z}[x]$ ,  $d(x) = \text{НОД}(f(x), g(x)) \in \mathbb{Z}[x]$ ,  $t(x) = \text{НОД}(f^{(p)}(x), g^{(p)}(x))$  в  $\mathbb{Z}_p[x]$ . Для всех простых чисел  $p$  таких, что  $p$  не делит  $lc(f(x)) \cdot lc(g(x))$ , справедливо неравенство

$$\deg t(x) \geq \deg d(x). \quad (1)$$

Существует только конечное число таких чисел  $p$ , для которых это неравенство строгое.

*Доказательство.* Первое утверждение теоремы следует из леммы и того, что  $lc(d(x))$  должен делить старшие коэффициенты  $f(x)$  и  $g(x)$ , а значит, и  $lc(f(x)) \cdot lc(g(x))$ .

Докажем второе утверждение.  $\deg t(x) > \deg d(x)$  только в случае, когда в кольце  $\mathbb{Z}_p[x]$  алгоритм Евклида заканчивается за меньшее число шагов, чем в  $\mathbb{Z}[x]$ . Т.е. если в  $\mathbb{Z}[x]$  требуется  $n$  шагов, то в  $\mathbb{Z}_p[x]$  наибольший общий делитель отыскивается за  $i < n$  шагов, т.е. на  $i$ -м шаге остаток  $r_i(x)$  по модулю  $p$  обращается в нуль, следовательно, все его коэффициенты делятся на  $p$ , в том числе и старший  $lc(r_i(x))$ . Так как число шагов алгоритма Евклида конечно, то существует лишь конечное число простых чисел, делящих старшие коэффициенты остатков от деления.

Простые числа  $p$ , для которых неравенство (1) строгое, будем называть "несчастливыми". В алгоритме, который будет приведен ниже, такие числа отбрасываются.

Вспомним еще одну теорему, доказанную ранее.

**Теорема 2.** Если многочлен  $f(x)$  с целыми коэффициентами неприводим над  $\mathbb{Z}_m$ , где  $m \nmid lc(f(x))$ , то  $f(x)$  неприводим над  $\mathbb{Z}$ .

*Доказательство.* Без ограничения общности будем считать, что  $f(x)$  – примитивный многочлен. (НОД его коэффициентов всегда можно выделить в качестве числового множителя:  $f(x) = \text{cont}(f(x)) \cdot \text{pp}(f(x))$ ).

Предположим противное, пусть  $f(x)$  приводим над  $\mathbb{Z}$ , т.е.

$$f(x) = q(x)r(x),$$

где  $q(x), r(x)$  – примитивные многочлены из  $\mathbb{Z}[x]$ . Имеем

$$lc(f(x)) = lc(q(x))lc(r(x)),$$

и если  $m \nmid lc(f(x))$ , (т.е.  $\deg f(x) = \deg f^{(m)}(x)$ ), то

$$f^{(m)}(x) = q^{(m)}(x)r^{(m)}(x)$$

есть разложение над  $\mathbb{Z}_m$ , т.е.  $f(x)$  приводим над  $\mathbb{Z}_m$ . Полученное противоречие и доказывает утверждение теоремы.

**Теорема 3.** Если многочлены с целыми коэффициентами  $f(x)$  и  $g(x)$  взаимно просты над  $\mathbb{Z}_m$ , где  $m \nmid lc(f(x))$  и  $m \nmid lc(g(x))$ , то  $f(x)$  и  $g(x)$  взаимно просты над  $\mathbb{Z}$ .

Это утверждение следует из теоремы 1.

### Модулярный алгоритм нахождения НОД двух многочленов

Пусть даны два примитивных многочлена  $f(x)$  и  $g(x)$  из  $\mathbb{Z}[x]$ .

1. Найти  $c = \text{НОД}\{lc(f(x)), lc(g(x))\}$ . Выбрать простое число  $p$ , которое не делит  $lc(f(x)) \cdot lc(g(x))$  и найти нормированный многочлен  $t(x) = \text{НОД}(f^{(p)}(x), g^{(p)}(x))$  в  $\mathbb{Z}_p[x]$ . Пусть  $d = \deg t(x)$ . Если  $d = 0$ , то  $t(x) = 1$  и многочлены  $f(x)$  и  $g(x)$  взаимно просты в  $\mathbb{Z}[x]$ . В этом случае алгоритм заканчивает работу.

2. Положить  $d^{(p)}(x) = ct(x) \pmod{p}$  и взять его примитивную часть  $\text{pp}(d^{(p)}(x))$ .

Если  $\text{pp}(d^{(p)}(x)) \mid f(x)$  и  $\text{pp}(d^{(p)}(x)) \mid g(x)$  над  $\mathbb{Z}$ , то  $\text{pp}(d^{(p)}(x))$  и есть НОД( $f(x), g(x)$ ) в  $\mathbb{Z}$ . Алгоритм заканчивает работу.

3. Выбрать новое простое число  $p_1$ , которое не делит  $lc(f(x)) \cdot lc(g(x))$  и найти нормированный многочлен

$$t_1(x) = \text{НОД}(f^{(p_1)}(x), g^{(p_1)}(x)) \quad \text{в } \mathbb{Z}_{p_1}[x].$$

Если  $t_1(x) = 0$ , то  $f(x)$  и  $g(x)$  взаимно просты в  $\mathbb{Z}$ . Алгоритм заканчивает работу.

4. Если  $\deg t_1(x) > d$ , то  $p_1$  – "несчастливое простое", отбросить его и перейти к шагу 3.

Если  $\deg t_1(x) < d$ , то  $p$  – "несчастливое простое"; положить  $t(x)$  равным  $t_1(x)$ ,  $d$  – равным  $\deg t_1(x)$ ,  $p := p_1$  и перейти к шагу 2.

5. (Случай  $\deg t(x) = \deg t_1(x)$ .) Пусть

$$t(x) = \sum_{i=0}^d a_i x^i \quad \text{из } \mathbb{Z}_p[x],$$

$$t_1(x) = \sum_{i=0}^d b_i x^i \quad \text{из } \mathbb{Z}_{p_1}[x].$$

Используя китайскую теорему об остатках, найти многочлен

$$t_2(x) = \sum_{i=0}^d c_i x^i \quad \text{из } \mathbb{Z}_{pp_1}[x]$$

такой, что

$$\begin{cases} c_i \equiv a_i \pmod{p} \\ c_i \equiv b_i \pmod{p_1}, \end{cases} \quad (i = 0, 1, \dots, d).$$

6. Положить  $p = p \cdot p_1$ ,  $t(x) := t_2(x)$  и перейти к шагу 2.

**Пример 1.** Найдем наибольший общий делитель многочленов

$$\begin{aligned} f(x) &= 9x^5 + 6x^4 + 3x^3 + 3x^2 + 2x + 1, \\ g(x) &= 3x^4 + 5x^3 + 6x^2 + 3x + 1 \end{aligned}$$

в  $\mathbb{Z}[x]$ .

Очевидно,  $c = \text{НОД}(9, 3) = 3$ . В качестве первого простого числа выберем  $p = 5$  ( $5 \nmid 9 \cdot 3$ ). В кольце  $\mathbb{Z}_5[x]$  найдем  $\text{НОД}(f^{(5)}(x), g^{(5)}(x))$ :

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

Имеем

$$\begin{aligned} f^{(5)}(x) &= g^{(5)}(x)(3x + 2) + (2x^2 + 3x + 4), \\ g^{(5)}(x) &= (2x^2 + 3x + 4)(4x^2 + 4x + 4), \end{aligned}$$

поэтому  $\text{НОД}(f^{(5)}(x), g^{(5)}(x)) = 2x^2 + 3x + 4$ .

Перейдем к нормированному в  $\mathbb{Z}_5[x]$  многочлену, для чего умножим его на 3 в  $\mathbb{Z}_5[x]$ , тогда получим

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

Положим  $d^{(5)}(x) = 3t(x) \pmod{5} \equiv 3x^2 + 2x + 1$ . Этот многочлен примитивен и поскольку

$$\begin{aligned} f(x) &= (3x^2 + 2x + 1)(3x^3 + 1) \\ g(x) &= (3x^2 + 2x + 1)(x^2 + x + 1), \end{aligned}$$

то  $d^{(5)}(x) \mid f(x)$  и  $d^{(5)}(x) \mid g(x)$  в  $\mathbb{Z}[x]$ , значит,  $3x^2 + 2x + 1$  и есть  $\text{НОД}(f(x), g(x))$  в  $\mathbb{Z}[x]$ .

**Пример 2.** Найдем в  $\mathbb{Z}[x]$  наибольший общий делитель многочленов

$$f(x) = 3x^5 + 8x^4 + 14x^3 + 18x^2 + 11x + 10$$

$$\text{и } g(x) = 6x^4 + 13x^3 + 2x^2 - 11x - 10.$$

$c = \text{НОД}(3, 6) = 3$ . В качестве простого числа  $p$  берем  $p = 5$  ( $5 \nmid 3 \cdot 6$ ) и ищем  $\text{НОД}(f^{(5)}(x), g^{(5)}(x))$  в кольце  $\mathbb{Z}_5[x]$ :

$$f^{(5)} = 3x^5 + 3x^4 + 4x^3 + 3x^2 + x,$$

$$g^{(5)} = x^4 + 3x^3 + 2x^2 - x.$$

Поскольку

$$\begin{aligned} f^{(5)}(x) &= g^{(5)}(x)(3x - 1) + r_1(x), & r_1(x) &= x^3 + 3x^2, \\ g^{(5)}(x) &= r_1(x)(x + 2) + r_2(x), & r_2(x) &= 2x^2 - x, \\ r_1(x) &= r_2(x)(3x + 3) + r_3(x), & r_3(x) &= 3x, \\ r_2(x) &= r_3(x)(4x - 2), \end{aligned}$$

то  $\text{НОД}(f^{(5)}(x), g^{(5)}(x)) = r_3(x) = 3x$ . Нормируем этот многочлен, получаем  $2r_3(x) \pmod{5} \equiv x$ . Так как, очевидно,  $d^{(5)}(x) = 3x$  не делит  $f(x)$  и  $g(x)$  в  $\mathbb{Z}[x]$ , то следует выбрать следующее простое число  $p_1$ . Пусть  $p_1 = 7$  ( $7 \nmid 3 \cdot 6$ ). Найдем  $\text{НОД}(f^{(7)}(x), g^{(7)}(x))$  в кольце  $\mathbb{Z}_7[x]$ , где

$$f^{(7)} = 3x^5 + x^4 + 4x^2 + 4x + 3,$$

$$g^{(7)} = 6x^4 + 6x^3 + 2x^2 - 4x - 3.$$

Применяя алгоритм Евклида, получаем

$$\begin{aligned} f^{(7)}(x) &= g^{(7)}(x)(4x - 5) + r_1(x), & r_1(x) &= x^3 + 2x^2 + 3x + 2, \\ g^{(7)}(x) &= r_1(x)(6x + 1) + r_2(x), & r_2(x) &= 3x^2 + 2x + 2, \\ r_1(x) &= r_2(x)(5x - 5) + r_3(x), & r_3(x) &= 3x + 5, \\ r_2(x) &= r_3(x)(x - 1), \end{aligned}$$

откуда  $\text{НОД}(f^{(7)}(x), g^{(7)}(x)) = r_3(x) = 3x + 5$ . Нормируем этот многочлен:  $5r_3(x) \pmod{7} \equiv x + 4$ .

Итак, мы получили два многочлена, имеющих одинаковую степень, значит, следует выполнить пятый шаг алгоритма. Имеем

$$\begin{aligned} t(x) &= x & \text{в } \mathbb{Z}_5[x], \\ t_1(x) &= x + 4 & \text{в } \mathbb{Z}_7[x]. \end{aligned}$$

Ищем  $t_2(x) = ax + b$  в  $\mathbb{Z}_{35}[x]$ , используя китайскую теорему об остатках для нахождения коэффициентов  $a$  и  $b$ . Следует решить следующие две системы сравнений:

$$\begin{cases} a \equiv 1 \pmod{5} \\ a \equiv 1 \pmod{7} \end{cases} \quad \text{и} \quad \begin{cases} b \equiv 0 \pmod{5} \\ b \equiv 4 \pmod{7}. \end{cases}$$

В результате получаем  $a \equiv 1 \pmod{35}$ ,  $b \equiv 25 \pmod{35}$ , значит,  $t_2(x) = x + 25$  в  $\mathbb{Z}_{35}[x]$ .

Возьмем многочлен  $ct_2(x) = 3x + 75 \pmod{35} \equiv 3x + 5$  и проверим, не делит ли он  $f(x)$  и  $g(x)$  в  $\mathbb{Z}[x]$ ? Получаем

$$f(x) = (3x + 5)(x^4 + x^3 + 3x^2 + x + 2),$$

$$g(x) = (3x + 5)(2x^3 + x^2 - x - 2),$$

значит,  $3x + 5$  и есть  $\text{НОД}(f(x), g(x))$  в  $\mathbb{Z}[x]$ .

## §2. ДЕЛЕНИЕ МНОГОЧЛЕНОВ И МЕТОД ГАУССА

Рассмотрим многочлены

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, & a_n \neq 0, \quad n > 0, \\ g(x) &= b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0, & b_m \neq 0, \quad m > 0 \end{aligned}$$

над кольцом  $\mathbb{Z}$  и пусть  $n \geq m$ . Мы хотим поделить многочлен  $f(x)$  на  $g(x)$  в  $\mathbb{Z}[x]$  и найти остаток от этого деления. На самом деле, если  $b_m \neq \pm 1$ , то мы должны применить процесс псевдоделения и найти псевдоостаток:

$$\alpha f(x) = g(x)q(x) + r(x), \quad \deg r(x) < \deg g(x), \quad (1)$$

где  $r(x) = c_{m-1}x^{m-1} + \dots + c_1x + c_0$ .

Утверждается, что

*деление многочленов эквивалентно гауссову исключению.*

Чтобы убедиться в этом, рассмотрим матрицу размера  $(n - m + 2) \times (n + 1)$ , составленную из коэффициентов многочленов  $f(x)$  и  $g(x)$ :

$$M = \begin{pmatrix} b_m & b_{m-1} & b_{m-1} & \dots & b_0 & 0 & 0 & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_1 & b_0 & 0 & 0 & \dots & 0 \\ 0 & 0 & b_m & \dots & b_2 & b_1 & b_0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & b_m & b_{m-1} & \dots & \dots & \dots & \dots & b_0 \\ a_n & a_{n-1} & a_{n-2} & \dots & \dots & \dots & \dots & \dots & \dots & a_0 \end{pmatrix}.$$

Можно считать, что первые  $(n - m + 1)$  строки этой матрицы составлены из коэффициентов многочленов

$$x^{n-m}g(x), x^{n-m-1}g(x), \dots, xg(x), g(x)$$

соответственно, а последняя строка – из коэффициентов многочлена  $f(x)$ .

Пока для простоты будем считать, что  $b_m$  обратим. Применим процесс гауссова исключения для приведения матрицы  $M$  к треугольному виду. Сначала из последней строки вычтем первую, умноженную на  $\frac{a_n}{b_m} = a_n b_m^{-1}$ , что эквивалентно

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = r_1(x),$$

где  $r_1(x)$  – многочлен степени, не превосходящей  $n - 1$ , коэффициенты которого стоят теперь в последней строке матрицы. Если  $\deg r_1(x) = n - 1$ , то из последней строки вычтем вторую, умноженную на  $lc(r_1(x))b_m^{-1}$ , что эквивалентно

$$r_1(x) - lc(r_1(x))b_m^{-1}x^{n-m-1}g(x) = r_2(x),$$

где  $\deg r_2(x) \leq n - 2$ , и его коэффициенты опять стоят в последней строке нашей матрицы и т.д. Очевидно, что процесс эквивалентен описанному в теореме о делении многочленов. Исключая последовательно степени  $x^n, x^{n-1}, \dots, x^m$  из последней строки (т.е. из  $f(x)$ ), получаем

$$f(x) - g(x)q(x) = r(x) = c_{m-1}x^{m-1} + \dots + c_1x + c_0,$$

т.е. коэффициенты  $r(x)$  стоят в последней строке матрицы  $M$ , приведенной к треугольному виду:

$$\begin{pmatrix} b_m & b_{m-1} & \dots & b_0 & 0 & \dots & 0 \\ 0 & b_m & \dots & b_1 & b_0 & \dots & 0 \\ \dots & \dots & \ddots & b_m & \dots & \dots & b_0 \\ 0 & 0 & \dots & 0 & c_{m-1} & \dots & c_0 \end{pmatrix}.$$



Если  $b_m$  не обратим, то в процессе исключения придется домножать последнюю строку (т.е.  $f(x)$ ) на  $b_m$  каждый раз, когда исключаемый из этой строки коэффициент при наибольшей оставшейся степени  $x$  не кратен  $b_m$ . Очевидно, число таких умножений не превышает  $n - m + 1$ , т.е. в (1)  $\alpha = b_m^k$ , где  $k \leq n - m + 1$ . Если в результате такого исключения последняя строка матрицы становится нулевой, то

$$\alpha f(x) = g(x)q(x),$$

т.е.  $\alpha f(x)$  делится на  $g(x)$ .

Такой процесс деления можно использовать при отыскании наибольшего общего делителя двух многочленов, повторно применяя эту схему вычисления для последовательных псевдоделений в алгоритме Евклида.

**Пример.** Вычислить в  $\mathbb{Z}[x]$  наибольший общий делитель многочленов

$$f(x) = x^4 + 2x^3 - 7x^2 - 8x + 12$$

и

$$g(x) = x^3 - 13x + 12.$$

Проведем первое деление  $f(x)$  на  $g(x)$ . Имеем  $n = 4$ ,  $m = 3$ ,  $n - m + 1 = 2$ , значит,

$$M = \begin{pmatrix} 1 & 0 & -13 & 12 & 0 \\ 0 & 1 & 0 & -13 & 12 \\ 1 & 2 & -7 & -8 & 12 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & -13 & 12 & 0 \\ 0 & 1 & 0 & -13 & 12 \\ 0 & 2 & 6 & -20 & 12 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & -13 & 12 & 0 \\ 0 & 1 & 0 & -13 & 12 \\ 0 & 0 & 6 & 6 & -12 \end{pmatrix},$$

т.е.

$$f(x) = g(x)q(x) + r_1(x), \quad \text{где} \quad r_1(x) = 6x^2 + 6x - 12.$$

В данном случае домножать последнюю строку не пришлось, так как  $lc(g(x)) = 1$  — обратим в  $\mathbb{Z}$ .

Продолжим процесс деления. Следует делить  $g(x)$  на  $r_1(x)$ . Имеем  $n = 3$ ,  $m = 2$ ,  $n - m + 1 = 2$ , значит,

$$M_1 = \begin{pmatrix} 6 & 6 & -12 & 0 \\ 0 & 6 & 6 & -12 \\ 1 & 0 & -13 & 12 \end{pmatrix} \rightarrow \begin{pmatrix} 6 & 6 & -12 & 0 \\ 0 & 6 & 6 & -12 \\ 0 & -6 & -66 & 72 \end{pmatrix} \rightarrow \begin{pmatrix} 6 & 6 & -12 & 0 \\ 0 & 6 & 6 & -12 \\ 0 & 0 & -60 & 60 \end{pmatrix},$$

т.е.

$$6g(x) = r_1(x)q_1(x) + r_2(x), \quad \text{где} \quad r_2(x) = -60x + 60.$$

(В процессе исключения пришлось один раз домножить последнюю строку на 6.)

На самом деле, при получении промежуточных остатков, можно сокращать их на наибольший общий делитель коэффициентов, т.е. переходить к примитивным многочленам. Поэтому можно взять  $\tilde{r}_1(x) = x^2 + x - 2$ ,  $\tilde{r}_2(x) = -x + 1$ . Тогда следующее деление  $\tilde{r}_1(x)$  на  $\tilde{r}_2(x)$  имеет вид:

$$M_2 = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 1 & -2 \end{pmatrix} \rightarrow \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 2 & -2 \end{pmatrix} \rightarrow \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

т.е.  $\tilde{r}_2(x) \mid \tilde{r}_1(x)$ . Значит,  $\tilde{r}_2(x) = -x + 1$  и есть наибольший общий делитель  $f(x)$  и  $g(x)$ .

### §3. МЕТОД КРОНЕКЕРА – ШУБЕРТА РАЗЛОЖЕНИЯ МНОГОЧЛЕНА НА МНОЖИТЕЛИ НАД КОЛЬЦОМ $\mathbb{Z}$

Пусть  $f(x)$  – многочлен с целыми коэффициентами степени  $n$ . Если многочлен  $f(x)$  приводим, т.е. разлагается в произведение многочленов, то один из его сомножителей должен иметь степень не выше  $\frac{n}{2}$ . Пусть

$$m = \left\lfloor \frac{n}{2} \right\rfloor$$

– наибольшее целое, не превосходящее  $\frac{n}{2}$ . Выясним, имеет ли  $f(x)$  множитель  $g(x)$  степени, не превосходящей  $m$ . Для этого выберем  $m + 1$  различных целых чисел

$$a_0, a_1, a_2, \dots, a_m$$

и вычислим значения многочлена  $f(x)$  в этих точках

$$f(a_0), f(a_1), f(a_2), \dots, f(a_m).$$

Если  $g(x)$  делит  $f(x)$ , то

$$\begin{aligned} g(a_0) &| f(a_0), \\ g(a_1) &| f(a_1), \\ &\dots\dots\dots \\ g(a_m) &| f(a_m). \end{aligned}$$

Обозначим через  $f_i$  конечное множество всех целых делителей числа  $f(a_i)$ ,  $i = 0, 1, \dots, m$ .

Теперь для  $k = 2, 3, \dots, m + 1$  выполним следующие операции:

выбираем  $k$  элементов  $b_i$  из различных множеств  $f_i$  (по одному из множества);

находим интерполяционный многочлен (по формуле Лагранжа)  $g(x)$  степени  $k - 1$  такой, что  $g(a_i) = b_i$  для всех  $i$ .

Если построенный многочлен  $g(x)$  делит  $f(x)$ , то множитель многочлена  $f(x)$  найден, можно рассмотреть частное  $q(x) = \frac{f(x)}{g(x)}$  и применить к  $q(x)$  тот же метод. Если же  $g(x)$  не делит  $f(x)$ , то выбираем другое множество  $k$  элементов  $b_i$  из множеств  $f_i$  (не совпадающее с выбранными ранее при предыдущих попытках) и снова интерполируем. Когда мы испытаем все возможные комбинации из  $k$  элементов, то увеличим  $k$  и начнем процедуру заново. Если мы испытали все возможные комбинации из  $2 \leq k \leq m + 1$  целых значений из  $f_i$  и не нашли ни одного делителя многочлена  $f(x)$ , то можно утверждать, что  $f(x)$  в  $\mathbb{Z}[x]$  неприводим.

Этот метод, конечно, очень неэффективен, время вычислений экспоненциально, поэтому при небольших значениях  $n$  еще имеет смысл его применять, при  $n \geq 5$  он работает очень медленно.

**Пример.** Разложить на множители многочлен  $f(x) = x^4 + 3x^3 + 5x^2 + 4x + 2$ .

Так как  $n = \deg f(x) = 4$ , то  $m = 2$ . Нетрудно проверить, что у данного многочлена нет целых корней, а значит, нет сомножителей первой степени. Будем искать сомножитель второй степени. Для этого выберем три целых числа, например,

$$a_0 = 0, \quad a_1 = 1, \quad a_2 = -1.$$

Так как

$$\begin{aligned} f(0) &= 2, & f_0 &= \{1, -1, 2, -2\}, \\ f(1) &= 15, & \text{то} & & f_1 &= \{1, -1, 3, -3, 5, -5, 15, -15\}, \\ f(-1) &= 1, & & & f_2 &= \{1, -1\}. \end{aligned}$$

Видно, что в худшем случае придется перебрать все возможные комбинации, число которых равно  $4 \cdot 8 \cdot 2 = 64$ .

Выберем, например,  $b_0 = 1 \in f_0$ ,  $b_1 = -1 \in f_1$ ,  $b_2 = 1 \in f_2$  и построим интерполяционный многочлен  $g(x)$  такой, что

$$g(0) = 1, \quad g(1) = -1, \quad g(-1) = 1.$$

По формуле Лагранжа получаем

$$g(x) = 1 \cdot \frac{(x-1)(x+1)}{(0-1)(0+1)} + (-1) \cdot \frac{x(x+1)}{(1-0)(1+1)} + 1 \cdot \frac{x(x-1)}{(-1)(-1-1)} = 1 - x^2 - \frac{x^2+x}{2} + \frac{x^2-x}{2} = -x^2 - x + 1.$$

Проверим, не является ли построенный многочлен делителем  $f(x)$  :

$$f(x) = g(x)(-x^2 - 2x - 4) + (2x + 6),$$

значит,  $g(x) \nmid f(x)$ .

Выберем другое множество чисел  $b_i$ . Пусть  $b_0 = 1 \in f_0$ ,  $b_1 = 3 \in f_1$ ,  $b_2 = 1 \in f_2$ . Построим  $g(x)$  такой, что  $g(0) = 1$ ,  $g(1) = 3$ ,  $g(-1) = 1$ , пользуясь формулой Лагранжа:

$$g(x) = 1 \cdot (1 - x^2) + 3 \cdot \frac{x^2 + x}{2} + 1 \cdot \frac{x^2 - x}{2} = 1 - x^2 + 2x^2 + x = x^2 + x + 1.$$

Имеем

$$f(x) = (x^2 + x + 1)(x^2 + 2x + 2),$$

т.е. найденный многочлен является множителем  $f(x)$ . Нам удалось представить  $f(x)$  в виде произведения двух многочленов. Очевидно также, что это полное разложение  $f(x)$ , так как оба полученных сомножителя неприводимы в  $\mathbb{Z}[x]$ .

#### §4. РАЗЛОЖЕНИЕ НА СВОБОДНЫЕ ОТ КВАДРАТОВ МНОЖИТЕЛИ НАД КОНЕЧНЫМИ ПОЛЯМИ

Начнем со следующего несложного утверждения.

**Лемма.** Пусть  $\mathbf{A}$  – кольцо характеристики  $p$  и  $f(x) \in \mathbf{A}[x]$ ,  $\deg f(x) > 0$ ,  $f(x) \neq 0$ . Производная многочлена  $f(x)$  равна нулю тогда и только тогда, когда  $f(x)$  есть многочлен от  $x^p$ .

*Доказательство.* Пусть  $f'(x) = 0$ . Если

$$f(x) = \sum_{i=0}^n a_i x^i,$$

то

$$f'(x) = \sum_{i=1}^n i a_i x^{i-1},$$

и, значит,  $i a_i = 0$  для  $i = 1, 2, \dots, n$ . Поэтому  $p \mid i$  или  $a_i = 0$  для каждого  $i$ , но все  $a_i$  не могут обращаться в нуль, это означало бы, что  $f(x) = 0$  или является константой, но тогда  $\deg f(x) = 0$ . Значит,  $p \mid i$  для всех  $i$ , т.е. все степени  $x$  в многочлене  $f(x)$  кратны  $p$ .

Обратное утверждение очевидно, так как если

$$f(x) = \sum_{i=0}^n a_i x^{ip},$$

то

$$f'(x) = \sum_{i=1}^n i p a_i x^{ip-1}$$

и в кольце характеристики  $p$  все коэффициенты  $i p a_i$  обращаются в 0.

**Теорема 1.** Пусть  $\mathbf{A}$  – факториальное кольцо характеристики  $p$  и  $f(x)$  – не являющийся константой примитивный многочлен над  $\mathbf{A}$ . Пусть

$$f(x) = \{f_1(x)\}^{k_1} \{f_2(x)\}^{k_2} \dots \{f_n(x)\}^{k_n} \quad (1)$$

– однозначное разложение  $f(x)$  на неприводимые множители и пусть  $\delta_i = 0$ , если  $k_i f'_i(x) = 0$ , в противном случае пусть  $\delta_i = 1$  ( $i = 1, 2, \dots, n$ ). Тогда

$$\text{НОД}(f(x), f'(x)) = \{f_1(x)\}^{k_1 - \delta_1} \{f_2(x)\}^{k_2 - \delta_2} \dots \{f_n(x)\}^{k_n - \delta_n}. \quad (2)$$

Эта теорема обобщает аналогичную теорему для кольца характеристики нуль.

*Доказательство.* Обозначим

$$r(x) = \text{НОД}(f(x), f'(x)),$$

$$g(x) = \prod_{i=2}^n \{f_i(x)\}^{k_i},$$

тогда  $f(x)$  можно представить в виде

$$f(x) = \{f_1(x)\}^{k_1} g(x),$$

значит,

$$f'(x) = \{f_1(x)\}^{k_1} g'(x) + k_1 \{f_1(x)\}^{k_1 - 1} g(x) f'_1(x). \quad (3)$$



В случае  $k_1 f'_1(x) = 0$  получаем

$$f'(x) = \{f_1(x)\}^{k_1} g'(x),$$

следовательно,  $\{f_1(x)\}^{k_1}$  делит  $r(x)$ .

В случае  $k_1 f'_1(x) \neq 0$  получаем, что  $\{f_1(x)\}^{k_1-1}$  делит  $r(x)$ . В этом случае  $\{f_1(x)\}^{k_1}$  не делит  $r(x)$ . Действительно, если предположить противное, то  $\{f_1(x)\}^{k_1}$  должно делить  $f'(x)$ , из формулы (3) следует, что  $\{f_1(x)\}^{k_1}$  должно делить  $k_1 \{f_1(x)\}^{k_1-1} g(x) f'_1(x)$ , откуда

$$f_1(x) \mid k_1 f'_1(x) g(x).$$

Поскольку  $\text{НОД}(f_1(x), g(x)) = 1$ , то  $f_1(x) \mid k_1 f'_1(x)$ , откуда  $\deg f_1(x) \leq \deg f'_1(x)$ . Полученное противоречие показывает, что наше предположение неверно.

Итак, получаем

$$\{f_1(x)\}^{k_1-\delta_1} \mid r(x),$$

причем  $\delta_1 = 0$ , если  $k_1 f'_1(x) = 0$  и  $\delta_1 = 1$  в противном случае.

Проводя аналогичные рассуждения для каждого  $i = 1, 2, \dots, n$  и учитывая, что многочлены  $f_1(x), f_2(x), \dots, f_n(x)$  попарно взаимно просты, получаем

$$\prod_{i=1}^n \{f_i(x)\}^{k_i-\delta_i} \mid r(x).$$

Если  $d(x)$  – общий делитель  $f(x)$  и  $f'(x)$ , то поскольку  $d(x) \mid f(x)$ , то из (1) получаем

$$d(x) = \prod_{i=1}^n \{f_i(x)\}^{s_i},$$

где  $0 \leq s_i \leq k_i$ ,  $i = 1, 2, \dots, n$ .

С другой стороны,  $d(x) \mid f'(x)$ , поэтому в силу изложенных выше соображений,  $0 \leq s_i \leq k_i - \delta_i$  для всех  $i$ . Значит,

$$d(x) \mid \prod_{i=1}^n \{f_i(x)\}^{k_i-\delta_i},$$

откуда по определению наибольшего общего делителя получаем

$$r(x) = \prod_{i=1}^n \{f_i(x)\}^{k_i-\delta_i}.$$

Полезными оказываются и следующие два утверждения.

**Теорема 2.** Пусть  $f(x)$  – многочлен из кольца  $\mathbb{Z}_p[x]$ ,  $p$  – простое число. Тогда

$$\{f(x)\}^p = f(x^p).$$

*Доказательство.* Пусть  $f_1(x), f_2(x) \in \mathbb{Z}_p[x]$ , тогда

$$\{f_1(x) + f_2(x)\}^p = \sum_{k=0}^p C_p^k \{f_1(x)\}^{p-k} \{f_2(x)\}^k = \{f_1(x)\}^p + \sum_{k=1}^{p-1} C_p^k \{f_1(x)\}^{p-k} \{f_2(x)\}^k + \{f_2(x)\}^p.$$

Так как  $p$  – простое число, то  $p \mid C_p^k$  для всех  $1 \leq k \leq p-1$ , поэтому  $C_p^k \equiv 0 \pmod{p}$ , значит,

$$\{f_1(x) + f_2(x)\}^p = \{f_1(x)\}^p + \{f_2(x)\}^p \quad (4)$$

в  $\mathbb{Z}_p[x]$ .

Пусть

$$f(x) = \sum_{i=0}^n a_i x^i$$

– произвольный многочлен из кольца  $\mathbb{Z}_p[x]$ . Применяя формулу (4) к его членам  $a_i x^i$  и рассуждая по индукции, получим

$$\{f(x)\}^p = \left\{ \sum_{i=0}^n a_i x^i \right\}^p = \{a_n x^n\}^p + \{a_{n-1} x^{n-1}\}^p + \cdots + \{a_1 x\}^p + a_0^p. \quad (5)$$

Так как  $p$  – простое число, а  $a_i \in \mathbb{Z}_p$ , то в силу малой теоремы Ферма имеем

$$a_i^{p-1} \equiv 1 \pmod{p}$$

или

$$a_i^p \equiv a_i \pmod{p}.$$

Тогда (5) переписывается в виде

$$\{f(x)\}^p = a_n x^{np} + a_{n-1} x^{(n-1)p} + \cdots + a_1 x^p + a_0 = f(x^p),$$

что и требовалось доказать.

**Теорема 3.** Пусть  $f(x) \in \mathbb{Z}_p[x]$ . Тогда его производная  $f'(x)$  обращается в нуль тогда и только тогда, когда  $f(x)$  есть  $p$ -я степень некоторого многочлена  $q(x)$  из  $\mathbb{Z}_p[x]$ .

*Доказательство.* Если  $f(x) = \{q(x)\}^p$ , то

$$f'(x) = p \{q(x)\}^{p-1} q'(x) = 0.$$

Обратно, пусть  $f'(x) = 0$ , тогда, используя лемму, можно утверждать, что  $f(x)$  есть многочлен от  $x^p$ , т.е.

$$f(x) = a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_n x^{np},$$

где  $a_i \in \mathbb{Z}_p$ .

Каждый коэффициент многочлена  $f(x)$  является элементом поля  $\mathbb{Z}_p$ , а значит, и элементом некоторого простого расширения  $GF(p^k)$  этого поля. Но все элементы поля  $GF(p^k)$  являются корнями уравнения  $x^{p^k} - x = 0$ . Значит,  $a_i^{p^k} \equiv a_i \pmod{p^k}$ , откуда  $a_i^{p^{k-1}} \equiv a_i^{\frac{1}{p}} \pmod{p^k}$ , ( $i = 0, 1, \dots, n$ ) – также элемент поля  $\mathbb{Z}_p$ .

Рассмотрим многочлен

$$q(x) = a_0^{\frac{1}{p}} + a_1^{\frac{1}{p}} x + a_2^{\frac{1}{p}} x^2 + \cdots + a_n^{\frac{1}{p}} x^n$$

из кольца  $\mathbb{Z}_p[x]$ . По теореме 2 имеем

$$\{q(x)\}^p = a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_n x^{np} = f(x),$$

т.е.  $q(x) \in \mathbb{Z}_p[x]$  и есть искомый многочлен.

Теперь рассмотрим алгоритм разложения многочлена на свободные от квадратов множители в кольце  $\mathbb{Z}_p[x]$ . Пусть

$$f(x) = \prod_{i=1}^n \{f_i(x)\}^{k_i},$$

где  $f_1(x), f_2(x), \dots, f_n(x)$  – попарно различные неприводимые многочлены из  $\mathbb{Z}_p[x]$ .

Пусть  $k = \max\{k_1, k_2, \dots, k_n\}$ . Для  $1 \leq i \leq k$  положим

$$s_i(x) = \begin{cases} \prod_{\substack{j \mid k_j=i \\ \{f'_j(x) \neq 0\}}} f_j(x), & \text{если } p \nmid i, \\ 1, & \text{в противном случае} \end{cases}$$

и

$$s(x) = \prod_{\substack{j \mid p \text{ делит } k_j \\ \text{или } \{f'_j(x)=0\}}} \{f_j(x)\}^{k_j}.$$

Тогда

$$f(x) = s_1(x) \{s_2(x)\}^2 \dots \{s_k(x)\}^k s(x).$$

По теореме 1 имеем  $\text{НОД}(s_i(x), s'_i(x)) = 1$  ( $i = 1, 2, \dots, k$ ) и  $s'(x) = 0$ . Кроме того, из этой же теоремы следует, что

$$r(x) = \text{НОД}(f(x), f'(x)) = s_2(x) \{s_3(x)\}^2 \dots \{s_k(x)\}^{k-1} s(x),$$

а потому

$$t(x) = \frac{f(x)}{r(x)} = \frac{f(x)}{\text{НОД}(f(x), f'(x))} = s_1(x) s_2(x) \dots s_k(x).$$

Далее,

$$v(x) = \text{НОД}(r(x), t(x)) = s_2(x) s_3(x) \dots s_k(x)$$

и значит,

$$s_1(x) = \frac{t(x)}{v(x)},$$

таким образом, первый свободный от квадратов множитель  $f(x)$  найден.

Теперь положим  $r(x)$  равным  $\frac{r(x)}{v(x)}$ , т.е.

$$r(x) = s_3(x) \{s_4(x)\}^2 \dots \{s_k(x)\}^{k-2} s(x),$$

а

$$t(x) := v(x) = s_2(x) s_3(x) \dots s_k(x).$$

Тогда

$$v(x) = \text{НОД}(r(x), t(x)) = s_3(x) s_4(x) \dots s_k(x),$$

значит,

$$s_2(x) = \frac{t(x)}{v(x)}.$$

Продолжаем этот процесс, пока не найдем все многочлены  $s_i(x)$  ( $i = 1, 2, \dots, k$ ).

Что же касается оставшегося многочлена  $s(x)$ , то так как  $s'(x) = 0$ , то по теореме 3

$$s(x) = \{q(x)\}^p,$$

где  $q(x) = \{s(x)\}^{\frac{1}{p}}$ . Далее, к многочлену  $q(x)$  можно применить тот же алгоритм.

**Пример 1.** Разложим на свободные от квадратов множители многочлен  $f(x) = x^{14} + x^{13} + x^{12} + x^{10} + x^8 + x^7 + x^6 + x^4$  из  $\mathbb{Z}_2[x]$ .

Сначала найдем  $f'(x)$ , проводя вычисления в  $\mathbb{Z}_2$ :

$$f'(x) = x^{12} + x^6,$$

$$r(x) = \text{НОД}(f(x), f'(x)) = x^{10} + x^4.$$

Действительно,

$$\begin{aligned} f(x) &= x^4 (x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + 1) \\ f'(x) &= x^6 (x^6 + 1) \end{aligned}$$

и многочлен  $x^6 + 1$  делит  $x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + 1$ .

Тогда

$$t(x) = \frac{f(x)}{r(x)} = x^4 + x^3 + x^2 + 1.$$

Найдем наибольший общий делитель  $r(x)$  и  $t(x)$  :

$$\begin{aligned} x^{10} + x^4 &= t(x) (x^6 + x^5 + x^3 + 1) + (x^2 + 1), \\ x^4 + x^3 + x^2 + 1 &= (x^2 + 1) (x^2 + x) + (x + 1), \\ x^2 + 1 &= (x + 1)^2, \end{aligned}$$

откуда  $v(x) = x + 1$ ,  
значит,

$$s_1(x) = \frac{t(x)}{v(x)} = x^3 + x + 1.$$

Положим

$$\begin{aligned} r(x) &= \frac{x^{10} + x^4}{x + 1} = x^9 + x^8 + x^7 + x^6 + x^5 + x^4, \\ t(x) &= x + 1 \end{aligned}$$

и найдем  $v(x) = \text{НОД}(r(x), t(x))$ . Очевидно,  $v(x) = x + 1$  (единица является корнем  $t(x)$  и  $r(x)$  в  $\mathbb{Z}_2$ ), откуда

$$s_2(x) = \frac{t(x)}{v(x)} = 1.$$

Далее, положим

$$\begin{aligned} r(x) &= \frac{x^9 + x^8 + x^7 + x^6 + x^5 + x^4}{x + 1} = x^8 + x^6 + x^4, \\ t(x) &= x + 1 \end{aligned}$$

и найдем  $v(x) = \text{НОД}(r(x), t(x))$ . Единица является корнем  $t(x)$  и не является корнем  $r(x)$ , значит,  $r(x)$  и  $t(x)$  взаимно просты, т.е.  $v(x) = 1$ , откуда

$$s_3(x) = \frac{x + 1}{1} = x + 1.$$

На следующем шаге

$$\begin{aligned} r(x) &= \frac{r(x)}{1} = x^8 + x^6 + x^4, \\ t(x) &= 1, \end{aligned}$$

тогда, очевидно,  $v(x) = \text{НОД}(r(x), t(x)) = 1$  и  $s_4(x) = 1$ , и далее этот шаг будет повторяться с тем же результатом, следовательно,

$$f(x) = s_1(x) s_2(x)^2 s_3(x)^3 s(x) = (x^3 + x^2 + 1) (x + 1)^3 s(x),$$

где  $s(x) = x^8 + x^6 + x^4$ .

Так как  $s'(x) = 0$  в  $\mathbb{Z}_2[x]$ , то

$$s(x) = \{q(x)\}^2.$$

Очевидно,  $q(x) = x^4 + x^3 + x^2$  (по теореме 2). Теперь мы должны применить тот же алгоритм разложения на свободные от квадратов множители к многочлену  $q(x) = x^4 + x^3 + x^2$  в  $\mathbb{Z}_2[x]$ . Хотя разложение  $q(x)$  на множители в  $\mathbb{Z}_2[x]$  очевидно, проиллюстрируем, как будет работать наш алгоритм.



Ищем  $q'(x)$  в  $\mathbb{Z}_2[x]$  :

$$q'(x) = x^2.$$

Тогда

$$r(x) = \text{НОД}(q(x), q'(x)) = q'(x) = x^2 \quad (\text{так как } x^2 \mid x^4 + x^3 + x^2),$$

$$t(x) = \frac{q(x)}{r(x)} = x^2 + x + 1,$$

$$v(x) = \text{НОД}(r(x), t(x)) = 1,$$

откуда  $s_1(x) = x^2 + x + 1$ .

Положим

$$r(x) = \frac{x^2}{1} = x^2,$$

$$t(x) = 1,$$

тогда  $v(x) = \text{НОД}(r(x), t(x)) = 1$  и  $s_2(x) = 1$ . Далее, последний шаг будет повторяться с тем же результатом, следовательно,

$$q(x) = (x^2 + x + 1)s(x),$$

где  $s(x) = x^2 = (x)^2 = \{q_1(x)\}^2$ .

Таким образом,

$$q(x) = (x^2 + x + 1)x^2$$

и

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

**Пример 2.** Разложим на свободные от квадратов множители многочлен  $f(x) = x^{11} + x^9 + x^8 + x^6 + 2x^5 + 2x^3 + 2x^2 + 2$  из  $\mathbb{Z}_3[x]$ .

Найдем производную  $f(x)$  в  $\mathbb{Z}_3[x]$  :

$$f'(x) = 2x^{10} + 2x^7 + x^4 + x.$$

Далее, из равенств

$$f(x) = f'(x)2x + (x^9 + x^6 + 2x^3 + 2),$$

$$f'(x) = 2x(x^9 + x^6 + 2x^3 + 2)$$

следует, что  $r(x) = \text{НОД}(f(x), f'(x)) = x^9 + x^6 + 2x^3 + 2$ . Тогда

$$t(x) = \frac{f(x)}{r(x)} = x^2 + 1.$$

Найдем наибольший общий делитель  $t(x)$  и  $r(x)$  :

$$x^9 + x^6 + 2x^3 + 2 = (x^2 + 1)(x^7 - x^5 + x^4 + x^3 - x^2 + x + 1) + (-x + 1),$$

$$x^2 + 1 = (-x + 1)(-x - 1) + 2,$$

$$-x + 1 = 2(-2x - 1),$$

значит,

$$v(x) = \text{НОД}(t(x), r(x)) = \text{const},$$

поэтому

$$s_1(x) = x^2 + 1.$$

Положим

$$r(x) = x^9 + x^6 + 2x^3 + 2,$$

$$t(x) = 1,$$

тогда  $v(x) = 1$  и  $s_2(x) = 1$ , и далее этот шаг будет повторяться, значит,

$$f(x) = s_1(x) s(x) = (x^2 + 1) (x^9 + x^6 + 2x^3 + 2).$$

Рассмотрим  $s(x)$ , он должен быть степенью многочлена  $q(x)$  :

$$s(x) = \{q(x)\}^3.$$

Так как  $2^3 \equiv 2 \pmod{3}$ , то, очевидно, в силу теоремы 2

$$q(x) = x^3 + x^2 + 2x + 2.$$

Теперь применим наш алгоритм к многочлену  $q(x)$ . Имеем

$$q'(x) = 2x + 2 = 2(x + 1),$$

тогда

$$r(x) = \text{НОД}(q(x), q'(x)) = x + 1,$$

$$t(x) = \frac{q(x)}{r(x)} = x^2 + 2$$

и

$$v(x) = \text{НОД}(t(x), r(x)) = x + 1,$$

откуда

$$s_1(x) = \frac{t(x)}{v(x)} = x + 2.$$

Далее, полагаем

$$\begin{aligned} r(x) &= \frac{x + 1}{x + 1} = 1, \\ t(x) &= x + 1, \end{aligned}$$

тогда  $v(x) = \text{НОД}(t(x), r(x)) = 1$  и  $s_2(x) = x + 1$ .

На следующем шаге  $r(x) = t(x) = v(x) = 1$  и  $s_3(x) = 1$ , значит,

$$q(x) = (x + 2) (x + 1)^2,$$

откуда

$$s(x) = (x + 2)^3 (x + 1)^6$$

и

$$f(x) = (x^2 + 1) (x + 2)^3 (x + 1)^6.$$

## §5. РАЗЛОЖЕНИЕ МНОГОЧЛЕНА НА МНОЖИТЕЛИ РАЗНЫХ СТЕПЕНЕЙ НАД КОНЕЧНЫМИ ПОЛЯМИ

Мы знаем, что многочлен

$$x^{p^n} - x$$

равен произведению всех неприводимых многочленов в  $\mathbb{Z}_p[x]$ , степени которых делят  $n$  (см. §12). Причем если многочлен  $g(x)$  степени  $d$  неприводим, то он делит  $x^{p^d} - x$ , но не делит  $x^{p^k} - x$  для  $k < d$ . Поэтому если  $f(x)$  — многочлен степени  $n$  свободен от квадратов, можно выделить его неприводимые множители каждой степени отдельно, включив в алгоритм разложения соотношения

$$f_i(x) = \text{НОД} \left\{ x^{p^i} - x, \frac{f(x)}{\prod_{j=1}^{i-1} f_j(x)} \right\}$$

для  $i = 1, 2, \dots, n$ .

Здесь  $f_j(x)$  — произведение всех нормированных неприводимых сомножителей степени  $j$  многочлена  $f(x)$ .

Т.е. для разложения свободного от квадратов многочлена  $f(x)$  на множители, каждый из которых равен произведению нормированных неприводимых многочленов одной степени, следует выполнить следующий алгоритм:

1.  $q(x) := f(x)$ ;  $r(x) := x$ ;  $d := 0$ ;
2. Если  $d + 1 > \frac{1}{2} \deg q(x)$ , то алгоритм заканчивает работу (в этом случае либо  $q(x) = 1$ , либо  $q(x)$  неприводим), иначе увеличить  $d$  на 1 ( $d := d + 1$ ) и  $r(x) := \{r(x)\}^p \pmod{q(x)}$ .
3. Найти  $f_d(x) = \text{НОД}\{r(x) - x, q(x)\}$ .
4. Если  $f_d(x) \neq 1$ , то положить  $q(x) = \frac{q(x)}{f_d(x)}$ ,  $r(x) \equiv r(x) \pmod{q(x)}$ ; перейти к шагу 2.

**Пример.** В  $\mathbb{Z}_2[x]$  рассмотрим многочлен  $f(x) = x^{15} - 1$  и разложим его в произведение сомножителей, каждый из которых равен произведению его неприводимых множителей одинаковой степени.

Сначала ищем

$$f_1(x) = \text{НОД}\{x^{15} - x, x^2 - 1\} = x - 1.$$

Далее делим  $f(x)$  на  $f_1(x)$  и берем

$$q(x) = \frac{x^{15} - x}{x - 1} = x^{14} + x^{13} + x^{12} + \dots + x + 1.$$

На следующем проходе алгоритма ищем

$$f_2(x) = \text{НОД}\{x^{14} + x^{13} + x^{12} + \dots + x + 1, x^4 - x\} = x^2 + x + 1.$$

Делим  $q(x)$  на  $f_2(x)$ , получаем

$$q(x) = \frac{x^{14} + x^{13} + x^{12} + \dots + x + 1}{x^2 + x + 1} = x^{12} + x^9 + x^6 + x^3 + 1.$$

На следующем проходе получаем

$$f_3(x) = \text{НОД}\{x^{12} + x^9 + x^6 + x^3 + 1, x^8 - x\} = 1,$$

следовательно,  $q(x)$  не меняется. Теперь

$$r(x) = x^{16} - x \pmod{x^{12} + x^9 + x^6 + x^3 + 1} \equiv x,$$

поэтому на следующем шаге

$$f_4(x) = \text{НОД}\{x^{12} + x^9 + x^6 + x^3 + 1, x - x\} = x^{12} + x^9 + x^6 + x^3 + 1$$

и  $q(x)$  становится равным 1, т.е. алгоритм заканчивает работу.

Таким образом,

$$f(x) = x^{15} - x = f_1(x) f_2(x) f_4(x) = (x - 1)(x^2 + x + 1)(x^{12} + x^9 + x^6 + x^3 + 1),$$

причем  $f_4(x)$  есть произведение трех неприводимых над  $\mathbb{Z}_2$  многочленов четвертой степени.

В рассмотренном алгоритме требуется вычислять  $x^p \pmod{f(x)}$  и

$$x^{p^i} \pmod{f(x)} = \{x^{p^{i-1}} \pmod{f(x)}\}^p \pmod{f(x)}$$

для  $i = 2, 3, \dots, \left\lfloor \frac{n}{2} \right\rfloor$ .

Пусть в  $i$ -й строке матрицы  $Q$  размера  $n \times n$  находятся коэффициенты многочлена  $x^{ip} \pmod{f(x)}$  для  $i = 0, 1, 2, \dots, n-1$ . отождествим многочлены степени меньшей  $n$  с вектор-строкой его коэффициентов. Тогда справедливо следующее утверждение.

**Теорема.** Для любого многочлена

$$g(x) = \sum_{i=0}^{n-1} g_i x^i$$

в  $\mathbb{Z}_p[x]$ , рассматриваемого как вектор  $\mathbf{g} = (g_0, g_1, \dots, g_{n-1})$  своих коэффициентов, справедливо

$$\mathbf{g} Q = \mathbf{g}^p \pmod{f(x)}.$$

*Доказательство.* Пусть  $Q = (q_{ij})$ ,  $i, j = 0, 1, 2, \dots, n-1$ . Тогда

$$\begin{aligned} \{g(x)\}^p \pmod{f(x)} &= g(x^p) \pmod{f(x)} = \sum_{i=0}^{n-1} g_i x^{ip} \pmod{f(x)} = \sum_{i=0}^{n-1} g_i \sum_{k=0}^{n-1} q_{ik} x^k \pmod{f(x)} \\ &= \sum_{k=0}^{n-1} \left( \sum_{i=0}^{n-1} g_i q_{ik} \right) x^k \pmod{f(x)}, \end{aligned}$$

где

$$x^{ip} = \sum_{k=0}^{n-1} q_{ik} x^k \quad (i = 0, 1, 2, \dots, n-1).$$

Значит, многочлену  $\{g(x)\}^p \pmod{f(x)}$  отвечает строка коэффициентов

$$\left( \sum_{i=0}^{n-1} g_i q_{i0}, \sum_{i=0}^{n-1} g_i q_{i1}, \dots, \sum_{i=0}^{n-1} g_i q_{in-1} \right),$$

т.е.

$$\mathbf{g}^p \pmod{f(x)} = \mathbf{g} Q.$$

Из этой теоремы, очевидно, следует, что

$$\{x^{p^{i-1}} \pmod{f(x)}\} Q = x^{p^i} \pmod{f(x)}.$$



**Пример.** Пусть  $f(x) = x^4 + x^3 + x + 1$  из  $\mathbf{Z}_2[x]$ . Построим матрицу  $Q$  и найдем  $x^{2^i} \pmod{f(x)}$  для  $i = 3, 4, 5$ .

Строки матрицы  $Q$  составим из коэффициентов многочленов

$$x^0 = 1, \quad x^2, \quad x^4 \equiv x^3 + x + 1 \pmod{f(x)}, \quad x^6 \pmod{f(x)}.$$

Так как

$$\begin{aligned} x^6 &= x^2 x^4 \equiv x^2 (x^3 + x + 1) \equiv x^5 + x^3 + x^2 \equiv x x^4 + x^3 + x^2 \equiv x (x^3 + x + 1) + x^3 + x^2 = \\ &= x^4 + x^2 + x + x^3 + x^2 \equiv x^3 + x + 1 + x^3 + x \equiv 1 \pmod{f(x)}, \end{aligned}$$

то получаем

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Чтобы вычислить  $x^{2^3} = x^8 \pmod{f(x)}$ , следует взять строку коэффициентов многочлена  $x^{2^2} = x^4 \pmod{f(x)}$ , т.е.  $(1 \ 1 \ 0 \ 1)$  и умножить ее на матрицу  $Q$

$$(1 \ 1 \ 0 \ 1) Q = (0 \ 0 \ 1 \ 0),$$

т.е.  $x^8 \equiv x^2 \pmod{f(x)}$ . Далее  $x^{2^4} = x^{16} \pmod{f(x)}$  получается таким же образом, если взять строку коэффициентов  $x^8 \pmod{f(x)}$ :

$$(0 \ 0 \ 1 \ 0) Q = (1 \ 1 \ 0 \ 1),$$

т.е.  $x^{16} \equiv x^3 + x + 1 \pmod{f(x)}$ . Наконец,  $x^{2^5} = x^{32} \pmod{f(x)}$  получаем, используя строку коэффициентов  $x^{16}$ :

$$(1 \ 1 \ 0 \ 1) Q = (0 \ 0 \ 1 \ 0),$$

т.е.  $x^{32} \equiv x^2 \pmod{f(x)}$ .

Действительно, непосредственные вычисления дают

$$\begin{aligned} x^8 &= x^6 \cdot x^2 \equiv 1 \cdot x^2 \equiv x^2 \pmod{f(x)}, \\ x^{16} &= (x^8)^2 \equiv (x^2)^2 \equiv x^4 \equiv x^3 + x + 1 \pmod{f(x)}, \\ x^{32} &= (x^{16})^2 \equiv (x^3 + x + 1)^2 \equiv x^6 + x^2 + 1 \equiv 1 + x^2 + 1 \equiv x^2 \pmod{f(x)}. \end{aligned}$$

## §6. АЛГОРИТМ БЕРЛЕКЭМПА РАЗЛОЖЕНИЯ МНОГОЧЛЕНА НА МНОЖИТЕЛИ НАД КОНЕЧНЫМ ПОЛЕМ

Китайская теорема об остатках для многочленов из кольца  $\mathbb{Z}_p[x]$  утверждает, что если  $p_1(x), p_2(x), \dots, p_r(x)$  — многочлены из кольца  $\mathbb{Z}_p[x]$ , причем  $\text{НОД}(p_j(x), p_k(x)) = 1$  для всех  $j \neq k$ , и  $s_1(x), s_2(x), \dots, s_r(x)$  — произвольные многочлены из  $\mathbb{Z}_p[x]$ , то существует единственный многочлен  $t(x) \in \mathbb{Z}_p[x]$  такой, что

$$\deg t(x) < \sum_{i=1}^r \deg p_i(x) \quad \text{и} \quad t(x) \equiv s_i(x) \pmod{p_i(x)} \quad (i = 1, 2, \dots, r).$$

Эта теорема, в частности, утверждает, что для произвольного вектора  $(s_1, s_2, \dots, s_r)$  целых чисел по  $\text{mod } p$  существует единственный многочлен  $t(x)$  такой, что

$$\begin{aligned} t(x) &\equiv s_1 \pmod{p_1(x)}, \quad t(x) \equiv s_2 \pmod{p_2(x)}, \quad \dots, \quad t(x) \equiv s_r \pmod{p_r(x)}, \\ \deg t(x) &< \sum_{i=1}^r \deg p_i(x) = \deg p(x) = n \quad \left( p(x) = \prod_{i=1}^r p_i(x) \right). \end{aligned} \quad (1)$$

Многочлен  $t(x)$ , определенный формулой (1), позволяет получить информацию о сомножителях многочлена  $p(x)$ , поскольку если  $r \geq 2$  и  $s_1 \neq s_2$ , то  $\text{НОД}(p(x), t(x) - s_1)$  делится на  $p_1(x)$  и не делится на  $p_2(x)$ .

Обсудим этот вопрос подробнее. По теореме 2 §4 многочлен  $t(x)$  удовлетворяет условию

$$\{t(x)\}^p \equiv s_i^p \equiv s_i \equiv t(x) \pmod{p_i(x)} \quad \text{для} \quad 1 \leq i \leq r$$

и потому

$$\{t(x)\}^p \equiv t(x) \pmod{p(x)}, \quad \deg t(x) < \deg p(x). \quad (2)$$

Более того, справедливо следующее утверждение.

**Теорема 1.** В конечном поле  $GF(p)$  имеет место разложение

$$x^p - x = \prod_{s \in GF(p)} (x - s).$$

Это утверждение мы доказали в §15 (следствие из теоремы 3).

**Следствие.** Для любого многочлена  $t(x)$  над полем  $GF(p)$  справедливо

$$\{t(x)\}^p - t(x) = \prod_{s \in GF(p)} \{t(x) - s\}. \quad (3)$$

Если многочлен  $t(x)$  удовлетворяет условию (2), то  $p(x)$  делит левую часть соотношения (3), так что каждый неприводимый сомножитель многочлена  $p(x)$  должен делить один из  $p$  взаимно простых сомножителей в правой части (3). Поэтому все решения сравнения (2) должны иметь вид (1):

$$t(x) \equiv s_1 \pmod{p_1(x)}, \quad t(x) \equiv s_2 \pmod{p_2(x)}, \quad \dots, \quad t(x) \equiv s_r \pmod{p_r(x)}$$

для некоторых  $s_1, s_2, \dots, s_r$ . Поскольку мы можем  $p^r$  способами выбрать элементы  $s_i$ , существует в точности  $p^r$  решений сравнения (2). Когда мы найдем все решения этого сравнения, мы сможем разложить на множители многочлен  $p(x)$  в  $\mathbb{Z}_p[x]$ . Действительно, справедлива следующая теорема.

**Теорема 2.** Пусть  $p(x)$  и  $t(x)$  – два унитарных многочлена над  $GF(p)$  такие, что

$$\{t(x)\}^p \equiv t(x) \pmod{p(x)}, \quad \deg t(x) < \deg p(x).$$

Тогда

$$p(x) = \prod_{s \in GF(p)} \text{НОД}(p(x), t(x) - s). \quad (4)$$

*Доказательство.* Поскольку

$$\{t(x)\}^p \equiv t(x) \pmod{p(x)},$$

то

$$p(x) \mid \{(t(x))^p - t(x)\},$$

поэтому

$$p(x) = \text{НОД}\{p(x), \{(t(x))^p - t(x)\}\} = \text{НОД}\{p(x), \prod_{s \in GF(p)} (t(x) - s)\}$$

по следствию из теоремы 1. Кроме того,

$$\text{НОД}(t(x) - s, t(x) - l) = 1 \quad \text{для } s \neq l,$$

значит, многочлены  $\text{НОД}(p(x), t(x) - s)$  и  $\text{НОД}(p(x), t(x) - l)$  также взаимно просты.

Поэтому

$$\text{НОД}\{p(x), \prod_{s \in GF(p)} (t(x) - s)\} = \prod_{s \in GF(p)} \text{НОД}\{p(x), t(x) - s\}.$$

Степень каждого сомножителя в правой части (4) не больше степени многочлена  $t(x)$ , которая, в свою очередь, меньше степени  $p(x)$ . Таким образом, в правой части (4) должно быть не менее двух нетривиальных делителей многочлена  $p(x)$ , и (4) представляет собой *нетривиальное разложение* многочлена  $p(x)$ .

Если  $t(x)$  – скаляр, т.е.  $\deg t(x) = 0$ , то

$$p(x) = \text{НОД}(p(x), 0) \cdot \prod_{\substack{s \neq 0 \\ s \in GF(p)}} \text{НОД}(p(x), s) = p(x) \cdot \prod_{s \neq 0} 1.$$

Поэтому формула (4) является формулой полного разложения. Это основная формула, используемая в алгоритме Берлекэмпа.

Чтобы воспользоваться формулой (4), требуется найти многочлен  $t(x)$ , удовлетворяющий условиям (2). Будем искать  $t(x)$ , исходя из следующих соображений. Пусть

$$t(x) = t_0 + t_1x + t_2x^2 + \cdots + t_{n-1}x^{n-1},$$

где  $t_i$ ,  $i = 0, 1, \dots, n-1$  – неизвестные коэффициенты многочлена  $t(x)$ .

Вычислим  $(t(x))^p$ . Так как в  $\mathbb{Z}_p[x]$  справедливо  $(f(x))^p = f(x^p)$ , то получаем

$$(t(x))^p = t_0 + t_1x^p + t_2x^{2p} + \cdots + t_{n-1}x^{(n-1)p}. \quad (5)$$

Поделим  $x^{ip}$  на  $p(x)$  ( $i = 0, 1, \dots, n-1$ ):

$$x^{ip} = p(x)q_i(x) + r_i(x), \quad (6)$$

где

$$r_i(x) = r_{i0} + r_{i1}x + r_{i2}x^2 + \cdots + r_{in-1}x^{n-1}. \quad (7)$$

Теперь заменим  $x^{ip}$  в (5) соответствующим выражением из (6), тогда имеем

$$(t(x))^p = t_0 r_0(x) + t_1 r_1(x) + \dots + t_{n-1} r_{n-1}(x) + p(x)Q(x).$$

Значит,  $p(x)$  делит  $\{t(x)\}^p - t(x)$  тогда и только тогда, когда  $p(x)$  делит многочлен

$$\begin{aligned} t_0 r_0(x) + t_1 r_1(x) + \dots + t_{n-1} r_{n-1}(x) - (t_0 + t_1 x + t_2 x^2 + \dots + t_{n-1} x^{n-1}) = \\ t_0(r_0(x) - 1) + t_1(r_1(x) - x) + \dots + t_{n-1}(r_{n-1}(x) - x^{n-1}), \end{aligned} \quad (8)$$

степень которого  $\leq n - 1$ . Многочлен  $p(x)$  степени  $n$  делит многочлен (8) степени  $\leq n - 1$  тогда и только тогда, когда последний равен нулю. Поэтому

$$t_0(r_0(x) - 1) + t_1(r_1(x) - x) + \dots + t_{n-1}(r_{n-1}(x) - x^{n-1}) = 0. \quad (9)$$

Перепишем (9) в виде

$$t_0 r_0(x) + t_1 r_1(x) + \dots + t_{n-1} r_{n-1}(x) = t_0 + t_1 x + t_2 x^2 + \dots + t_{n-1} x^{n-1}$$

и подставим вместо  $r_i(x)$  их выражения из (7):

$$\begin{aligned} t_0 \sum_{k=0}^{n-1} r_{0k} x^k + t_1 \sum_{k=0}^{n-1} r_{1k} x^k + \dots + t_{n-1} \sum_{k=0}^{n-1} r_{n-1k} x^k = \\ t_0 + t_1 x + t_2 x^2 + \dots + t_{n-1} x^{n-1}. \end{aligned}$$

В левой части полученного равенства соберем коэффициенты при одинаковых степенях  $x$ :

$$\begin{aligned} \left( \sum_{i=0}^{n-1} t_i r_{i0} \right) \cdot 1 + \left( \sum_{i=0}^{n-1} t_i r_{i1} \right) \cdot x + \left( \sum_{i=0}^{n-1} t_i r_{i2} \right) \cdot x^2 + \dots + \left( \sum_{i=0}^{n-1} t_i r_{in-1} \right) \cdot x^{n-1} = \\ t_0 + t_1 x + t_2 x^2 + \dots + t_{n-1} x^{n-1}. \end{aligned} \quad (10)$$

Приравнивая коэффициенты при одинаковых степенях  $x$  в правой и левой частях равенства (10), получаем систему линейных уравнений

$$\left\{ \begin{array}{l} \sum_{i=0}^{n-1} t_i r_{i0} = t_0, \\ \sum_{i=0}^{n-1} t_i r_{i1} = t_1, \\ \dots\dots\dots \\ \sum_{i=0}^{n-1} t_i r_{in-1} = t_{n-1}. \end{array} \right. \quad (11)$$

Пусть

$$Q = \begin{pmatrix} r_{00} & r_{01} & \dots & r_{0n-1} \\ r_{10} & r_{11} & \dots & r_{1n-1} \\ r_{20} & r_{21} & \dots & r_{2n-1} \\ \dots & \dots & \dots & \dots \\ r_{n-10} & r_{n-11} & \dots & r_{n-1n-1} \end{pmatrix},$$

тогда систему (11) можно записать в виде:

$$(t_0 \ t_1 \ \dots \ t_{n-1}) Q = (t_0 \ t_1 \ \dots \ t_{n-1}) \quad (12)$$

или

$$(t_0 \ t_1 \ \dots \ t_{n-1}) (Q - E) = (0 \ 0 \ \dots \ 0). \quad (13)$$

Таким образом, получена следующая теорема.



**Теорема 3.** Многочлен  $t(x) = t_0 + t_1x + t_2x^2 + \dots + t_{n-1}x^{n-1}$  является решением сравнения  $\{t(x)\}^p \equiv t(x) \pmod{p(x)}$  тогда и только тогда, когда

$$(t_0 \ t_1 \ \dots \ t_{n-1})Q = (t_0 \ t_1 \ \dots \ t_{n-1})$$

или

$$(t_0 \ t_1 \ \dots \ t_{n-1})(Q - E) = (0 \ 0 \ \dots \ 0).$$

Пусть  $L$  – пространство решений однородной системы линейных уравнений (13).  $L$  называют также нуль – пространством матрицы  $Q - E$  или ядром. Если  $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_r$  – базис этого пространства, то для любого решения  $\mathbf{a}$  системы (13) в  $\mathbb{Z}_p$  найдутся такие числа  $\alpha_1, \dots, \alpha_r$ , что

$$\mathbf{a} = \alpha_1\mathbf{b}_1 + \alpha_2\mathbf{b}_2 + \dots + \alpha_r\mathbf{b}_r.$$

Ядро матрицы  $Q - E$  легко вычислить, а следовательно, найти многочлены  $t(x)$ , удовлетворяющие условию (2). Далее мы можем применить теорему 2 и найти сомножители многочлена  $p(x)$ .

Ответ на вопрос – найдено ли полное разложение  $p(x)$ ? – дает следующая теорема.

**Теорема 4.** Число различных неприводимых сомножителей  $p_i(x)$  многочлена  $p(x)$  в  $\mathbb{Z}_p[x]$  равно размерности ядра матрицы  $Q - E$ .

*Доказательство.* Многочлен

$$p(x) = \prod_{i=1}^r p_i(x)$$

делит

$$\prod_{s \in \mathbb{Z}_p} \text{НОД}(p(x), t(x) - s)$$

тогда и только тогда, когда каждый многочлен  $p_i(x)$  делит  $t(x) - s_i$  для некоторого  $s_i \in \mathbb{Z}_p$ . Из китайской теоремы об остатках следует существование для данных  $s_1, \dots, s_r \in \mathbb{Z}_p$  единственного многочлена  $t(x) \pmod{p(x)}$  такого, что  $t(x) \equiv s_i \pmod{p_i(x)}$ . Мы можем  $p^r$  способами выбрать элементы  $s_i$ , и, как мы видели, существует в точности  $p^r$  решений сравнения  $\{t(x)\}^p \equiv t(x) \pmod{p(x)}$ . Из теоремы 3 известно, что  $t(x)$  является решением (2) тогда и только тогда, когда выполнено (13). Значит, система (13) имеет  $p^r$  решений, поэтому базис ядра матрицы  $Q - E$  должен содержать  $r$  векторов, т.е. размерность ядра матрицы  $Q - E$  равна  $r$ , т.е. числу различных унитарных неприводимых сомножителей многочлена  $p(x)$ .

Из этой теоремы получаем критерий неприводимости многочлена  $p(x) \in \mathbb{Z}_p[x]$ .

**Теорема 5.** Многочлен  $p(x)$  неприводим в  $\mathbb{Z}_p[x]$  тогда и только тогда, когда ядро матрицы  $Q - E$  одномерно и  $\text{НОД}(p(x), p'(x)) = 1$ .

*Доказательство.* По теореме 4 ядро матрицы  $Q - E$  одномерно тогда и только тогда, когда  $p(x) = (p_1(x))^k$ , т.е.  $p(x)$  является степенью неприводимого многочлена. Значит,  $r = 1$  и  $p(x)$  неприводим тогда и только тогда, когда он взаимно прост со своей производной, т.е.  $\text{НОД}(p(x), p'(x)) = 1$ .

**Теорема 6.** Пусть  $p(x) = p_1(x)p_2(x)\dots p_r(x)$  в  $\mathbb{Z}_p[x]$  и  $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_r$  – базис ядра матрицы  $Q - E$ . Тогда для каждого  $j \neq j', 1 \leq j < j' \leq r$  существуют целое  $k$  ( $1 \leq k \leq r$ ) и  $s \in \mathbb{Z}_p$  такие, что  $p_j(x)$  делит, а  $p_{j'}(x)$  не делит  $\text{НОД}(p(x), b_k(x) - s)$ .

*Доказательство.* (Под  $b_k(x)$  понимаем многочлен, соответствующий вектору  $\mathbf{b}_k$ , т.е. многочлен, коэффициентами которого являются соответствующие компоненты вектора.)

Покажем, что в ядре матрицы  $Q - E$  найдется вектор,  $j$ -я компонента которого отличается от его  $j'$ -й компоненты. Из этого следует, что существует  $k$  ( $1 \leq k \leq r$ ) такое, что

$$b_k(x) \pmod{p_j(x)} \neq b_k(x) \pmod{p_{j'}(x)}. \quad (14)$$

Предположим противное. Пусть для всех  $k$  ( $1 \leq k \leq r$ ) имеет место равенство

$$b_k(x) \pmod{p_j(x)} = b_k(x) \pmod{p_{j'}(x)}.$$

Так как любое **решение уравнения** (2) является линейной комбинацией векторов  $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_r$  с коэффициентами из  $\mathbb{Z}_p$ , для любого такого решения  $\mathbf{b}$  существует элемент  $s \in \mathbb{Z}_p$  такой, что

$$\mathbf{b}(x) \equiv s \pmod{p_j(x)} \quad \text{и} \quad b(x) \equiv s \pmod{p_{j'}(x)}.$$

Однако существует **решение (2)** такое, что  $b(x) \equiv 0 \pmod{p_j(x)}$  и  $b(x) \equiv 1 \pmod{p_{j'}(x)}$ . Полученное противоречие **показывает, что (14)** справедливо. Полагая

$$b(x) \pmod{p_j(x)} = s \in \mathbb{Z}_p,$$

получаем, что

$$p_j(x) \mid \{b_k(x) - s\} \quad \text{и} \quad p_{j'}(x) \nmid \{b_k(x) - s\}.$$

Объединяя **полученные** результаты, можно сформулировать следующий алгоритм разложения многочлена  $p(x) \in \mathbb{Z}_p[x]$  на неприводимые сомножители, который носит имя Берлекэмпа.

#### АЛГОРИТМ БЕРЛЕКЭМПА

Пусть  $p(x)$  — **свободный** от квадратов многочлен из  $\mathbb{Z}_p[x]$  степени  $n$ .

1. (Построение матрицы  $Q - E$ .) Построить  $n \times n$  матрицу  $Q$ , в строках которой стоят коэффициенты многочленов  $r_i(x)$  ( $i = 0, 1, \dots, n-1$ ) в порядке возрастания степеней  $x$ , где  $r_i(x)$  есть остаток от деления  $x^{i^2}$  на  $p(x)$ .

2. (Триангуляризация  $Q - E$ .) Привести матрицу  $Q - E$  к треугольному виду, действуя с ее столбцами, и вычислить ее ранг  $n - r$ . Найти ядро этой матрицы, т.е.  $r$  линейно независимых векторов  $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_r$  таких, что

$$\mathbf{b}_j(Q - E) = \mathbf{0} \quad \text{для} \quad 1 \leq j \leq r.$$

Первый вектор  $\mathbf{b}_1$  всегда может быть выбран в виде  $(1, 0, \dots, 0)$ , что представляет тривиальное решение  $b_1(x) = 1$  уравнения (2).

$r$  — это число неприводимых сомножителей многочлена  $p(x)$ .

Если  $r = 1$ , то  $p(x)$  неприводим, и алгоритм заканчивает работу.

3. (Нахождение сомножителей многочлена  $p(x)$ .) Пусть  $b_2(x)$  — многочлен, соответствующий вектору  $\mathbf{b}_2$ . Вычислить НОД( $p(x), b_2(x) - s$ ) для всех  $s \in \mathbb{Z}_p$ . В результате по теореме 2 получим нетривиальное разложение многочлена  $p(x)$ . Если с использованием  $b_2(x)$  получено менее  $r$  сомножителей, то вычислим

$$\text{НОД}(\omega(x), b_k(x) - s) \quad \text{для всех} \quad s \in \mathbb{Z}_p$$

и всех сомножителей  $\omega(x)$ , найденных к данному моменту времени, для  $k = 3, 4, \dots, r$ , пока не будет найдено  $r$  сомножителей. Теорема 6 гарантирует, что таким образом мы найдем все сомножители многочлена  $p(x)$ .

Заметим, что если  $p$  — мало, то вычисления на данном шаге достаточно эффективны.

Для работы алгоритма Берлекэмпа требуется построить матрицу  $Q$ . Рассмотрим этот процесс.

Пусть

$$p(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \dots + c_1x + c_0.$$

Предположим, что известно  $x^k \pmod{p(x)}$ , т.е.

$$x^k \equiv r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \dots + r_1x + r_0 \pmod{p(x)}.$$

Вычислим  $x^{k+1} \pmod{p(x)}$ :

$$\begin{aligned} x^{k+1} &\equiv r_{n-1}x^n + r_{n-2}x^{n-1} + \dots + r_1x^2 + r_0x \equiv r_{n-1}(-c_{n-1}x^{n-1} - c_{n-2}x^{n-2} - \dots - c_1x - c_0) + \\ &+ r_{n-2}x^{n-1} + \dots + r_1x^2 + r_0x \equiv (r_{n-2} - c_{n-1}r_{n-1})x^{n-1} + (r_{n-3} - c_{n-2}r_{n-1})x^{n-2} + (r_{n-4} - c_{n-3}r_{n-1})x^{n-3} + \\ &+ \dots + (r_1 - c_2r_{n-1})x^2 + (r_0 - c_1r_{n-1})x - c_0r_{n-1} \pmod{p(x)}. \end{aligned}$$

Т.е. вычисление коэффициентов многочлена  $x^{k+1} \pmod{p(x)}$  можно проводить, используя рекуррентную формулу:

$$\begin{aligned}\tilde{r}_j &\equiv r_{j-1} - r_{n-1}c_j \pmod{p} \quad (j = 1, 2, \dots, n-1), \\ \tilde{r}_0 &\equiv -c_0r_{n-1} \pmod{p},\end{aligned}\tag{15}$$

где  $x^{k+1} \equiv \tilde{r}_{n-1}x^{n-1} + \tilde{r}_{n-2}x^{n-2} + \dots + \tilde{r}_1x + \tilde{r}_0 \pmod{p(x)}$ .

Если  $p$  – большое число, то более эффективно вычислять  $x^k \pmod{p(x)}$  следующим образом. Будем возводить на каждом шаге в квадрат по  $\pmod{p(x)}$ , т.е. от  $x^k \pmod{p(x)}$  переходим к  $x^{2k} \pmod{p(x)}$ . Операцию возведения в квадрат легко выполнить, если предварительно составить дополнительную таблицу значений  $x^i \pmod{p(x)}$  для  $i = n, n+1, \dots, 2n-2$ . Таким образом, если

$$x^k \pmod{p(x)} \equiv r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \dots + r_1x + r_0,$$

то

$$\begin{aligned}x^{2k} \pmod{p(x)} &\equiv r_{n-1}^2x^{2n-2} + r_{n-2}^2x^{2n-4} + \dots + r_1^2x^2 + r_0^2 + 2r_{n-1}r_{n-2}x^{2n-3} + \\ &2r_{n-1}r_{n-3}x^{2n-4} + \dots + 2r_1r_0x \pmod{p(x)},\end{aligned}$$

где степени  $x^{2n-2}, x^{2n-3}, \dots, x^n$  могут быть заменены многочленами из дополнительной таблицы.

В  $\mathbb{Z}_p$  для вычисления второй строки матрицы  $Q$  надо вычислить  $x^p \pmod{p(x)}$ , для вычисления третьей строки –  $x^{2p} \pmod{p(x)}$ , затем  $x^{3p} \pmod{p(x)}$  и т.д. Это можно сделать, последовательно умножая на  $x^p \pmod{p(x)}$  и пользуясь дополнительной таблицей, аналогично тому, как при возведении в квадрат.

**Пример.** В  $\mathbb{Z}_{13}$  разложить на множители свободный от квадратов многочлен  $p(x) = 5x^4 + 5x^3 + 11x^2 + 9$ .

Сначала перейдем к нормированному многочлену, для чего домножим  $p(x)$  на  $5^{-1} \equiv 8 \pmod{13}$ . В результате получим

$$p(x) = x^4 + x^3 + 10x^2 + 7.$$

Нам потребуются обратные элементы к ненулевым элементам поля  $\mathbb{Z}_{13}$ , поэтому вычислим их заранее:

$$\begin{aligned}1^{-1} &\equiv 1, \quad 2^{-1} \equiv 7, \quad 3^{-1} \equiv 9, \quad 4^{-1} \equiv 10, \quad 5^{-1} \equiv 8, \quad 6^{-1} \equiv 11, \\ 7^{-1} &\equiv 2, \quad 8^{-1} \equiv 5, \quad 9^{-1} \equiv 3, \quad 10^{-1} \equiv 4, \quad 11^{-1} \equiv 6, \quad 12^{-1} \equiv 12 \pmod{13}.\end{aligned}$$

Найдем  $4 \times 4$  матрицу  $Q$ , первая строка которой имеет вид  $(1 \ 0 \ 0 \ 0)$ , представляя многочлен  $x^0 \pmod{p(x)} \equiv 1$ . Во второй строке должны стоять коэффициенты многочлена  $x^{13} \pmod{p(x)}$ , в третьей –  $x^{26} \pmod{p(x)}$ , в четвертой – коэффициенты  $x^{39} \pmod{p(x)}$ .

Построим таблицу для  $x^k \pmod{p(x)}$ ,  $0 \leq k \leq 13$ , используя формулы (15) для  $k \geq 5$  и сравнение

$$x^4 \equiv -x^3 - 10x^2 - 7 \equiv 12x^3 + 3x^2 + 6 \pmod{p(x)} \quad \text{в } \mathbb{Z}_{13}[x].$$

$x^k$	$r_0$	$r_1$	$r_2$	$r_3$
$x^0$	1	0	0	0
$x^1$	0	1	0	0
$x^2$	0	0	1	0
$x^3$	0	0	0	1
$x^4$	6	0	3	12
$x^5$	7	6	10	4
$x^6$	11	7	5	6
$x^7$	10	11	12	12
$x^8$	7	10	8	0
$x^9$	0	7	10	8
$x^{10}$	9	0	5	2
$x^{11}$	12	9	6	3
$x^{12}$	5	12	5	3
$x^{13}$	5	5	8	2

Действительно,

$$\begin{aligned}
x^5 &= 12(12x^3 + 3x^2 + 6) + 3x^3 + 6x = 147x^3 + 36x^2 + 6x + 72 \equiv 4x^3 + 10x^2 + 6x + 7, \\
x^6 &= 4(12x^3 + 3x^2 + 6) + 10x^3 + 6x^2 + 7x = 58x^3 + 18x^2 + 7x + 24 \equiv 6x^3 + 5x^2 + 7x + 11, \\
x^7 &= 6(12x^3 + 3x^2 + 6) + 5x^3 + 7x^2 + 11x = 77x^3 + 25x^2 + 11x + 36 \equiv 12x^3 + 12x^2 + 11x + 10, \\
x^8 &= 12(12x^3 + 3x^2 + 6) + 12x^3 + 11x^2 + 10x = 156x^3 + 47x^2 + 10x + 72 \equiv 8x^2 + 10x + 7, \\
x^9 &= 8x^3 + 10x^2 + 7x, \\
x^{10} &= 8(12x^3 + 3x^2 + 6) + 10x^3 + 7x^2 = 106x^3 + 31x^2 + 48 \equiv 2x^3 + 5x^2 + 9, \\
x^{11} &= 2(12x^3 + 3x^2 + 6) + 5x^3 + 9x = 29x^3 + 6x^2 + 9x + 12 \equiv 3x^3 + 6x^2 + 9x + 12, \\
x^{12} &= 3(12x^3 + 3x^2 + 6) + 6x^3 + 9x^2 + 12x = 42x^3 + 18x^2 + 12x + 18 \equiv 3x^3 + 5x^2 + 12x + 5, \\
x^{13} &= 3(12x^3 + 3x^2 + 6) + 5x^3 + 12x^2 + 5x = 41x^3 + 21x^2 + 5x + 18 \equiv 2x^3 + 8x^2 + 5x + 5.
\end{aligned}$$

Итак, вторая строка матрицы  $Q$  есть  $(5 \ 5 \ 8 \ 2)$ .

Чтобы найти  $x^{26} \pmod{p(x)}$ , возведем  $x^{13} \pmod{p(x)}$  в квадрат и воспользуемся нашей таблицей:

$$\begin{aligned}
x^{26} &= (x^{13})^2 \equiv (2x^3 + 8x^2 + 5x + 5)^2 = 4x^6 + 6x^5 + 6x^4 + 9x^3 + x^2 + 11x + 12 = \\
&= 4(6x^3 + 5x^2 + 7x + 11) + 6(4x^3 + 10x^2 + 6x + 7) + 6(12x^3 + 3x^2 + 6) + 9x^3 + x^2 + 11x + 12 = \\
&= (11x^3 + 7x^2 + 2x + 5) + (11x^3 + 8x^2 + 10x + 3) + (7x^3 + 5x^2 + 10) + 9x^3 + x^2 + 11x + 12 \equiv \\
&\equiv 12x^3 + 8x^2 + 10x + 4 \pmod{p(x)}.
\end{aligned}$$

Наконец,

$$\begin{aligned}
x^{39} &= x^{26} \cdot x^{13} = (12x^3 + 8x^2 + 10x + 4)(2x^3 + 8x^2 + 5x + 5) \equiv 11x^6 + 8x^5 + x^4 + 6x^3 + 5x^2 + 5x + 7 \equiv \\
&\equiv 11(6x^3 + 5x^2 + 7x + 11) + 8(4x^3 + 10x^2 + 6x + 7) + (12x^3 + 3x^2 + 6) + 6x^3 + 5x^2 + 5x + 7 \equiv (x^3 + 3x^2 + 12x + 4) + \\
&\quad + (6x^3 + 2x^2 + 9x + 4) + (12x^3 + 3x^2 + 6) + 6x^3 + 5x^2 + 5x + 7 \equiv 12x^3 + 8.
\end{aligned}$$

В результате получаем матрицу  $Q$ :

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 5 & 5 & 8 & 2 \\ 4 & 10 & 8 & 12 \\ 8 & 0 & 0 & 12 \end{pmatrix}.$$

Рассмотрим  $Q - E$  и приведем ее к треугольному виду, действуя со столбцами:

$$Q - E = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 5 & 4 & 8 & 2 \\ 4 & 10 & 7 & 12 \\ 8 & 0 & 0 & 11 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 \\ 4 & 12 & 11 & 0 \\ 8 & 4 & 8 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 \\ 4 & 12 & 0 & 0 \\ 8 & 4 & 0 & 0 \end{pmatrix}.$$

(Из второго столбца вычитаем первый, умноженный на  $4 \cdot 5^{-1} \equiv 6 \pmod{13}$ , из третьего столбца вычитаем первый, умноженный на  $8 \cdot 5^{-1} \equiv 12 \pmod{13}$ , из четвертого столбца вычитаем первый, умноженный на  $2 \cdot 5^{-1} \equiv 3 \pmod{13}$ , затем из третьего столбца вычитаем второй, умноженный на  $11 \cdot 12^{-1} \equiv 2 \pmod{13}$ .)

Если теперь дополнительно вычесть из первого столбца второй, умноженный на 2, то получим матрицу

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 \\ 6 & 12 & 0 & 0 \\ 0 & 4 & 0 & 0 \end{pmatrix},$$



откуда видно, что ранг матрицы  $Q - E$  равен 2, значит, ядро имеет размерность  $4 - 2 = 2$ . Найдем два линейно независимых решения системы

$$(x_1 \ x_2 \ x_3 \ x_4) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 \\ 6 & 12 & 0 & 0 \\ 0 & 4 & 0 & 0 \end{pmatrix} = (0 \ 0 \ 0 \ 0),$$

которая может быть записана в виде:

$$\begin{cases} 5x_2 + 6x_3 \equiv 0 \\ 12x_3 + 4x_4 \equiv 0 \end{cases} \pmod{13} \quad (16)$$

Одно решение —  $\mathbf{b}_1 = (1 \ 0 \ 0 \ 0)$ . Второе найдем, решив систему. Очевидно, из первого уравнения системы (16) получим

$$x_2 \equiv (-6) 5^{-1} x_3 \equiv 4x_3,$$

а из второго —

$$x_4 \equiv (-12) 4^{-1} x_3 \equiv 10x_3.$$

Если положить  $x_3 \equiv 4 \pmod{13}$ , то  $x_2 \equiv 3 \pmod{13}$ , и  $x_4 \equiv 1 \pmod{13}$ , поэтому в качестве  $\mathbf{b}_2$  можно взять следующий вектор  $(0 \ 3 \ 4 \ 1)$ .

Так как ядро матрицы  $Q - E$  имеет размерность 2, то многочлен  $p(x)$  должен раскладываться в произведение ровно двух неприводимых сомножителей над полем  $\mathbb{Z}_{13}$ .

Будем вычислять НОД( $p(x)$ ,  $b_2(x) - s$ ) для  $s \in \mathbb{Z}_{13}$ , где  $b_2(x) = x^3 + 4x^2 + 3x$ . Пусть  $s = 0$ , тогда

$$\begin{aligned} x^4 + x^3 + 10x^2 + 7 &= (x^3 + 4x^2 + 3x)(x - 3) + (6x^2 + 9x + 7), \\ x^3 + 4x^2 + 3x &= (6x^2 + 9x + 7)(11x - 5) + (-3x + 9), \\ 6x^2 + 9x + 7 &= (-3x + 9)(-2x + 4) - 3, \end{aligned}$$

значит,  $\text{НОД}(p(x), b_2(x)) = 1$ .

При  $s = 1, 2, \dots, 5$  также получим  $\text{НОД}(p(x), b_2(x) - s) = 1$ .

При  $s = 6$  имеем

$$\begin{aligned} x^4 + x^3 + 10x^2 + 7 &= (x^3 + 4x^2 + 3x - 6)(x - 3) + (6x^2 + 2x + 2), \\ x^3 + 4x^2 + 3x - 6 &= (6x^2 + 2x + 2)(11x - 3), \end{aligned}$$

откуда  $\text{НОД}(p(x), b_2(x) - 6) = 6x^2 + 2x + 2$ .

Умножая полученный многочлен на  $6^{-1} \equiv 11 \pmod{13}$ , получаем унитарный многочлен

$$p_1(x) = 11(6x^2 + 2x + 2) \equiv x^2 + 9x + 9$$

в  $\mathbb{Z}_{13}[x]$ . Значит,

$$p(x) = (x^2 + 9x + 9) p_2(x).$$

Теперь  $p_2(x)$  можно найти, поделив  $p(x)$  на  $p_1(x) = x^2 + 9x + 9$ .

Если же действовать согласно алгоритму Берлекэмпа, то надо брать другие значения  $s \in \mathbb{Z}_{13}$  и искать НОД( $p(x)$ ,  $b_2(x) - s$ ). Отличный от 1 наибольший общий делитель получится в данном случае при  $s = 8$ :

$$b_2(x) - 8 = x^3 + 4x^2 + 3x - 8 \equiv x^3 + 4x^2 + 3x + 5.$$

Далее,

$$\begin{aligned} x^4 + x^3 + 10x^2 + 7 &= (x^3 + 4x^2 + 3x + 5)(x - 3) + (6x^2 + 4x - 4), \\ x^3 + 4x^2 + 3x + 5 &= (6x^2 + 4x - 4)(11x + 2), \end{aligned}$$

откуда  $\text{НОД}(p(x), b_2(x) - 8) = 6x^2 + 4x - 4$ .

В приведенном виде

$$p_2(x) = 11(6x^2 + 4x - 4) \equiv x^2 + 5x + 8.$$

Таким образом, окончательно получаем

$$p(x) = x^4 + x^3 + 10x^2 + 7 = (x^2 + 9x + 9)(x^2 + 5x + 8)$$

в  $\mathbb{Z}_{13}[x]$ .

## ЛИТЕРАТУРА

1. Ноден П., Китте К. Алгебраическая алгоритмика. М.: Мир, 1999.
2. Акритас А. Основы компьютерной алгебры с приложениями. М.: Мир, 1994.
3. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1. М.: Мир, 1988.
4. Яблокова С.И. Основы алгебраической алгоритмики. Часть 1. Ярославль: ЯрГУ, 2008.

## СОДЕРЖАНИЕ

Предисловие	3
§1. Основные сведения о многочленах. Наибольший общий делитель многочленов	4
§2. Метод Горнера и его применение	9
§3. Евклидовы кольца и делимость многочленов. Наибольший общий делитель многочленов	12
§4. Расширенный алгоритм Евклида для многочленов над полем	14
§5. Интерполяция над полем	22
§6. Факторкольцо $K[x]/(m(x))$	26
§7. Вычислительные схемы, использующие интерполяцию	31
§8. Китайская теорема об остатках для многочленов	34
§9. Алгоритм Евклида и псевдоделение	36
§10. Разложение многочлена на множители	39
§11. Неприводимые многочлены над полями $\mathbb{C}$ , $\mathbb{R}$ , $\mathbb{Q}$ и над кольцом $\mathbb{Z}$	42
§12. Неприводимые многочлены в $\mathbb{Z}_p[x]$	47
§13. Решето Эратосфена для многочленов из $\mathbb{Z}_p[x]$	57
§14. Разложение многочлена на свободные от квадратов множители	62
§15. Поля Галуа	66
§16. Построение полей Галуа $GF(2^n)$	80
§17. Круговые многочлены	84
ПРИЛОЖЕНИЕ	
§1. Модулярный алгоритм для нахождения наибольшего общего делителя двух многочленов	93
§2. Деление многочленов и метод Гаусса	97
§3. Метод Кронекера – Шуберта разложения многочлена на множители над кольцом $\mathbb{Z}$	99
§4. Разложение на свободные от квадратов множители над конечными полями	101
§5. Разложение многочлена на множители разных степеней над конечными полями	108
§6. Алгоритм Берлекэмпа разложения многочлена на множители над конечным полем	111
ЛИТЕРАТУРА	119