

Министерство образования и науки Российской Федерации  
Ярославский государственный университет  
им. П. Г. Демидова  
Кафедра алгебры и математической логики

С. И. Яблокова

# Задачи по алгебраической алгоритмике

*Часть 2*

*Практикум*

Ярославль  
ЯрГУ  
2018

УДК 512+519.6  
ББК В14я73+В18я73  
Я82

*Рекомендовано  
Редакционно-издательским советом университета  
в качестве учебного издания. План 2018 года*

Рецензент

кафедра алгебры и математической логики ЯрГУ

**Яблокова, Светлана Ивановна.**

Задачи по алгебраической алгоритмике. Часть 2 : практикум  
Я82 / С. И. Яблокова ; Яросл. гос. ун-т им. П. Г. Демидова. —  
Ярославль : ЯрГУ, 2018. — 56 с.

Предназначен для студентов, обучающихся по дисциплинам "Алгебраическая алгоритмика", "Теория чисел".

УДК 512+519.6  
ББК В14я73+В18я73

© ЯрГУ, 2018

В практикуме содержатся задачи по алгебраической алгоритмике по темам, изучаемым в пятом семестре студентами специальности "Компьютерная безопасность" в курсе "Алгебраическая алгоритмика". Для решения предлагаемых задач требуется знать основные алгебраические и числовые алгоритмы и связанные с ними определения и понятия курса, такие как: алгоритм Евклида для нахождения наибольшего общего делителя многочленов над полем (кольцом); расширенный алгоритм Евклида для многочленов; интерполяционные формулы; определение и свойства сравнений по модулю многочлена, методы решения сравнений; китайскую теорему об остатках для многочленов; определение и свойства факторкольца по модулю многочлена; основные утверждения и понятия теории конечных полей. Требуется умение применять эти знания для решения задач. Наибольшие трудности, как правило, представляют задания, связанные со строением факторколец по модулю многочлена. Обычно это вычислительные проблемы. Особое внимание надо уделить пониманию того, что такое кольцо вычетов по данному модулю, что представляют из себя элементы этого кольца.

Практикум начинается с напоминания основных понятий, формул и алгоритмов, используемых при решении задач. Эти понятия и алгоритмы иллюстрируются примерами. Далее предлагаются задачи по курсу для решения на практических занятиях. Они снабжены указаниями и ответами для контроля правильности решения. В заключение предлагаются задачи для самостоятельного решения, которые могут быть использованы для контрольных и расчетно-графических работ.

## Схема Горнера

Поделим многочлен  $f(x) = a_n x^n + \dots + a_1 x + a_0$  из кольца  $\mathbb{A}[x]$  на  $x - \alpha$ ,  $\alpha \in \mathbb{A}$  ( $\mathbb{A}$  – кольцо или поле), т. е. ищем представление в виде

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

где  $r \in \mathbb{A}$ ,  $\deg q(x) = n - 1$ , т. е.  $q(x) = b_{n-1}x^{n-1} + \dots + b_1x + b_0$ .

Подставляя  $q(x)$  в (1) и приравнявая коэффициенты при одинаковых степенях  $x$ , получаем формулы

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

**Пример 1.** Вычислить значение многочлена  $f(x) = x^5 + 2x^4 - 3x^2 + 2x - 1$  из  $\mathbb{Z}_7[x]$  при  $x = 3$ . Формулы (2) удобно записать в таблицу :

$$\begin{array}{c|c|c|c|c|c|c} & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \\ \hline \alpha & b_{n-1} & b_{n-2} & b_{n-3} & \dots & b_0 & r \end{array}.$$

В нашем случае имеем

$$\begin{array}{c|c|c|c|c|c|c} & 1 & 2 & 0 & -3 & 2 & -1 \\ \hline 3 & 1 & 5 & 1 & 0 & 2 & 5 \end{array},$$

т. е.  $f(x) = (x - 3)(x^4 + 5x^3 + x^2 + 2) + 5$  и  $f(3) = 5$ .

Сделаем замену аргумента в  $f(x)$  :  $x = y + \alpha$ . Чтобы найти коэффициенты  $f(y) = \sum_{i=0}^n b_i y^i$ , запишем равенство

$$f(x) = \sum_{i=0}^n a_i x^i = \sum_{i=0}^n b_i (x - \alpha)^i,$$

откуда

$$f(x) = (x - \alpha) \sum_{i=1}^n b_i (x - \alpha)^{i-1} + b_0 = (x - \alpha)f_1(x) + b_0,$$

т. е.  $b_0$  есть остаток от деления  $f(x)$  на  $x - \alpha$ . Далее, повторяем рассуждение для  $f_1(x)$

$$f_1(x) = (x - \alpha) \sum_{i=2}^n b_i (x - \alpha)^{i-2} + b_1 = (x - \alpha)f_2(x) + b_1,$$

т. е.  $b_1$  есть остаток от деления  $f_1(x)$  на  $x - \alpha$  и т. д. Получаем последовательно  $b_2, \dots, b_n$ : берем частное, полученное на предыдущем шаге, делим его на  $x - \alpha$ , используя схему Горнера, получаем остаток от деления, равный очередному коэффициенту  $b_i$  и новое частное, которое используем на следующем шаге.

**Пример 2.** Пусть  $f(x) = x^5 = 2x^4 - x^3 + 3x^2 + 2$  из  $\mathbb{Z}_{11}[x]$ . Найдем  $f(y)$ , где  $y = x - 2$ .

Все шаги деления запишем в одну таблицу:

		1		2		-1		3		0		2
2		1		4		7		4		8		7
2		1		6		8		9		4		
2		1		8		2		2				
2		1		10		0						
2		1		1								
2		1										

Таким образом, получена следующая цепочка равенств:

$$\begin{aligned}
 f(x) &= (x - 2)(x^4 + 4x^3 + 7x^2 + 4x + 8) + 7 = (x - 2)f_1(x) + 7, \\
 f_1(x) &= (x - 2)(x^3 + 6x^2 + 8x + 9) + 4 = (x - 2)f_2(x) + 4, \\
 f_2(x) &= (x - 2)(x^2 + 8x + 2) + 2 = (x - 2)f_3(x) + 2, \\
 f_3(x) &= (x - 2)(x + 10) = (x - 2)f_4(x), \\
 f_4(x) &= (x - 2) + 1, \\
 f_5(x) &= 1,
 \end{aligned}$$

откуда  $f(y) = y^5 + y^4 + 2y^2 + 4y + 7$ .

## Интерполяция

Пусть  $K$  – поле. Рассмотрим множество  $n + 1$  наборов пар  $(a_i, b_i) \in K \times K$ ,  $i = 0, 1, \dots, n$ , где  $a_i$  все различны. Задача интерполяции состоит в построении многочлена  $f(x) \in K[x]$  такого, что

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

Ее можно решить, пользуясь интерполяционной формулой Лагранжа:

$$f(x) = \sum_{i=0}^n b_i \prod_{j=0, j \neq i}^n \frac{x - a_j}{a_i - a_j} = \sum_{i=0}^n b_i L_i(x). \quad (3)$$

**Пример 3.** Найти  $f(x) \in \mathbb{Z}_{13}[x]$  такой, что

$$f(1) = 3, \quad f(3) = 11, \quad f(5) = 1, \quad f(7) = 8.$$

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

$$\begin{aligned}
L_0(x) &= \frac{(x-3)(x-5)(x-7)}{(1-3)(1-5)(1-7)} = 4^{-1}(x-3)(x-5)(x-7) \\
&= 10(x^3 - 2x^2 + 6x - 1), \\
L_1(x) &= \frac{(x-1)(x-5)(x-7)}{(3-1)(3-5)(3-7)} = 3^{-1}(x-1)(x-5)(x-7) \\
&= -4(x^3 + 8x + 4), \\
L_2(x) &= \frac{(x-1)(x-3)(x-7)}{(5-1)(5-3)(5-7)} = (-3)^{-1}(x-1)(x-3)(x-7) \\
&= 4(x^3 + 2x^2 + 5x + 5), \\
L_3(x) &= \frac{(x-1)(x-3)(x-5)}{(7-1)(7-3)(7-5)} = 9^{-1}(x-1)(x-3)(x-5) \\
&= 3(x^3 - 9x^2 - 3x - 2).
\end{aligned}$$

Значит,

$$\begin{aligned}
f(x) &= 3L_0(x) + 11L_1(x) + L_2(x) + 8L_3(x) = 4(x^3 - 2x^2 + 6x - 1) \\
&\quad - 5(x^3 + 8x + 4) + 4(x^3 + 2x^2 + 5x + 5) - 2(x^3 - 9x^2 - 3x - 2) \\
&= x^3 + 5x^2 - 3x.
\end{aligned}$$

Задачу интерполяции можно также решать, используя китайскую теорему об остатках для многочленов. В этом случае

$$f(x) = q_0 m_0(x) + q_1 m_1(x) + \dots + q_n m_n(x),$$

где

$$m_0(x) = 1, \quad m_i(x) = (x - a_0)(x - a_1) \dots (x - a_{i-1}) \quad (1 \leq i \leq n),$$

$$q_0 = b_0, \quad q_i = \{b_i - f_{i-1}(a_i)\} \{m_i(a_i)\}^{-1}, \quad (1 \leq i \leq n).$$

Если

$$f_0(x) = b_0, \quad f_i(x) = f_{i-1}(x) + q_i m_i(x), \quad (1 \leq i \leq n)$$

таковы, что  $f_i(a_j) = b_j$ ,  $0 \leq j \leq i$ , то  $f_n(x) = f(x)$ . Поэтому будем последовательно строить многочлены  $f_i(x)$  ( $i = 0, 1, \dots, n$ ).

**Пример 4.** Найти  $f(x) \in \mathbb{Z}_7[x]$  такой, что

$$f(1) = 2, \quad f(2) = 1, \quad f(3) = 6, \quad f(4) = 3, \quad f(5) = 2.$$

Все вычисления запишем в таблицу, вводя обозначения  $d_i = b_i - f_{i-1}(a_i)$ ,  $c_i = \{m_i(a_i)\}^{-1}$ ,  $q_i = d_i c_i$  :

$a_i \mid b_i \mid$	$m_i(x)$	$d_i \mid c_i \mid q_i \mid$	$f_i(x)$
1   2	1	-   -   -	2
2   1	$x - 1$	-1   1   -1	$3 - x$
3   6	$(x - 1)(x - 2)$	6   4   3	$3x^2 - 10x + 9$
4   3	$(x - 1)(x - 2)(x - 3)$	0   -1   0	$3x^2 - 10x + 9$
5   2	$(x - 1)(x - 2)(x - 3)(x - 4)$	3   5   1	$f_4(x)$

$f_1(x) = 2 - (x - 1) = 3 - x,$   
 $f_2(x) = 3 - x + 3(x - 1)(x - 2) = 3x^2 - 10x + 9,$   
 $f_3(x) = 3x^2 - 10x + 9,$   
 $f_4(x) = 3x^2 - 10x + 9 + (x - 1)(x - 2)(x - 3)(x - 4) = x^4 - 3x^3 + 3x^2 - 4x + 5.$

### Расширенный алгоритм Евклида и псевдоделение

Для многочленов  $f_1(x), f_2(x) \in \mathbb{K}[x]$ , где  $\mathbb{K}$  – поле,  $f_2(x) \neq 0$ , можно найти в  $\mathbb{K}[x]$  наибольший общий делитель, пользуясь алгоритмом Евклида для многочленов.

Пусть

$$\begin{aligned}
 r_0(x) &= f_1(x), \\
 r_1(x) &= f_2(x), \\
 r_{i-1}(x) &= r_i(x)q_i(x) + r_{i+1}(x), \quad \deg r_{i+1}(x) < \deg r_i(x), \\
 &\quad (1 \leq i \leq n), \\
 r_{n+1}(x) &= 0,
 \end{aligned}$$

тогда  $r_n(x) = (f_1(x), f_2(x))$ .

Если требуется представить наибольший общий делитель двух многочленов в виде

$$\text{НОД}(f_1(x), f_2(x)) = f_1(x)u(x) + f_2(x)v(x), \quad (5)$$

то используется расширенный алгоритм Евклида, в котором на каждом шаге, кроме очередного остатка от деления  $r_i(x)$ , строятся многочлены  $u_i(x), v_i(x)$  такие, что

$$r_i(x) = f_1(x)u_i(x) + f_2(x)v_i(x), \quad (0 \leq i \leq n).$$

Тогда при  $i = n$  получаем равенство (5), т. е.  $u(x) = u_n(x), v(x) = v_n(x)$ . Многочлены  $u_i(x), v_i(x)$  ищутся по рекуррентным формулам :

$$\begin{aligned}
 u_0(x) &= 1, \quad u_1(x) = 0, \\
 u_{i+1}(x) &= u_{i-1}(x) - q_i(x)u_i(x), \quad (1 \leq i \leq n), \\
 v_0(x) &= 0, \quad v_1(x) = 1, \\
 v_{i+1}(x) &= v_{i-1}(x) - q_i(x)v_i(x), \quad (1 \leq i \leq n).
 \end{aligned}$$

Если рассматриваются многочлены над кольцом  $\mathbb{A}$ , то алгоритм Евклида можно провести только в случае, когда на каждом шаге алгоритма коэффициент при старшей степени делителя обратим в кольце  $\mathbb{A}$ . Для многочленов над кольцом  $\mathbb{Z}$  при нахождении наибольшего общего делителя применяются алгоритм Евклида с псевдоделением, который сохраняет наибольший общий делитель для примитивных частей многочленов  $f_1(x)$ ,  $f_2(x)$ .

Примитивной частью  $pp(f(x))$  многочлена  $f(x)$  называется многочлен  $\frac{f(x)}{\text{cont}(f(x))}$ , где  $\text{cont}(f(x))$  – содержание многочлена  $f(x)$ , т. е. наибольший общий делитель всех коэффициентов многочлена  $f(x)$  в кольце  $\mathbb{A}$ .

Каждый шаг деления в этом случае имеет вид:

$$\begin{aligned}\alpha r_{i-1}(x) &= r_i(x)\tilde{q}_i(x) + \tilde{r}_{i+1}(x), \quad (1 \leq i \leq n), \\ r_{i+1}(x) &= pp(\tilde{r}_{i+1}(x)), \\ r_{n+1} &= 0,\end{aligned}$$

где  $\alpha = \{lc(r_i(x))\}^{m-n+1}$ ,  $m = \deg r_{i-1}(x)$ ,  $n = \deg r_i(x)$ .

При этом сначала вычисляется наибольший общий делитель содержаний многочленов  $f_1(x)$  и  $f_2(x)$ , пусть это элемент  $d \in \mathbb{A}$ . Затем проводится алгоритм Евклида с псевдоделениями, на каждом шаге которого следует переходить к примитивной части полученного остатка. Наибольший общий делитель  $f_1(x)$  и  $f_2(x)$  равен произведению  $d$  на примитивную часть последнего ненулевого остатка  $r_n(x)$ .

**Пример 5.** Найти обратный к элементу  $f(x) = x^3 + x + 1$  в факторкольце  $\mathbb{Z}_2[x]/(x^4 + x^3 + x^2 + x + 1)$ .

Так как  $m(x) = x^4 + x^3 + x^2 + x + 1$  в  $\mathbb{Z}_2[x]$  неприводим, то он взаимно прост с  $f(x)$ , значит,  $\text{НОД}(m(x), f(x)) = 1$ . Используя расширенный алгоритм Евклида, получим представление

$$1 = m(x)u(x) + f(x)v(x),$$

откуда  $f(x)v(x) \equiv 1 \pmod{m(x)}$ , т. е.  $v(x) = f(x)^{-1}$ .

Проведем алгоритм Евклида

$$\begin{aligned}x^4 + x^3 + x^2 + x + 1 &= (x^3 + x + 1)(x + 1) + x (= r_2(x)), \\ x^3 + x + 1 &= x(x^2 + 1) + 1 (= r_3(x)),\end{aligned}$$

тогда  $(q_1(x) = x + 1, \quad q_2(x) = x^2 + 1)$ ,

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



откуда  $1 = xm(x) + (x^3 + x^2 + x)f(x)$ , т. е.  $f(x)^{-1} = x^3 + x^2 + x$ .

**Пример 6.** Найти наибольший общий делитель многочленов  $f(x) = 3x^4 - 6x^3 + 12x - 9$ ,  $g(x) = 6x^4 + 18x^3 - 12x^2 - 6x - 6$  в кольце  $\mathbb{Z}[x]$ .

Так как  $\mathbb{Z}$  – кольцо, то воспользуемся алгоритмом Евклида с псевдоделением. Найдем содержание каждого многочлена. Очевидно,  $\text{cont}(f(x)) = 3$ ,  $\text{cont}(g(x)) = 6$  и  $d = \text{НОД}(3, 6) = 3$ . Переходим к примитивным частям многочленов  $f(x)$  и  $g(x)$  :

$$\begin{aligned} r_0(x) &= pp(f(x)) = x^4 - 2x^2 + 4x - 3, \\ r_1(x) &= pp(g(x)) = x^4 + 3x^3 - 2x^2 - x - 1. \end{aligned}$$

Первый шаг алгоритма Евклида:

$$r_0(x) = r_1(x) + (-5x^3 + 2x^2 + 5x - 2).$$

Полученный остаток  $\tilde{r}_2(x)$  примитивен, т. е.  $r_2(x) = pp(\tilde{r}_2(x)) = \tilde{r}_2(x)$ . Далее надо делить  $r_1(x)$  на  $r_2(x)$ , и, так как  $lc(r_2(x)) = -5$  необратим в  $\mathbb{Z}$ , то используем псевдоделение :

$$(-5)^{4-3+1}r_1(x) = r_2(x)(-5x - 17) + (9x^2 + 50x - 59).$$

Полученный остаток  $\tilde{r}_3(x)$  примитивен, т. е.  $r_3(x) = pp(r_3(x)) = \tilde{r}_3(x)$ . Чтобы поделить  $r_2(x)$  на  $r_3(x)$  следует опять воспользоваться псевдоделением, т. е. предварительно умножить  $r_2(x)$  на  $9^{3-2+1} = 9^2$  :

$$9^2r_2(x) = r_3(x)(-45x + 268) + (-15650x + 15650).$$

Полученный остаток  $\tilde{r}_4(x)$  непримитивен. Переходим к его примитивной части  $r_4(x) = pp(\tilde{r}_4(x)) = -x + 1$ . Наконец,

$$r_3(x) = r_4(x)(-9x - 1).$$

Значит,  $dr_4(x) = 3(-x + 1) = 3 - 3x$  и есть наибольший общий делитель  $f(x)$  и  $g(x)$ .

### Китайская теорема об остатках для многочленов

Теорема дает способ решения системы сравнений по взаимно простым модулям для многочлена из кольца  $\mathbb{K}[x]$ , где  $\mathbb{K}$  – поле, а именно:

*если  $m_1(x), m_2(x), \dots, m_s(x) \in \mathbb{K}[x]$  попарно взаимно просты,  $c_1(x), c_2(x), \dots, c_s(x) \in \mathbb{K}[x]$  таковы, что  $\deg c_i(x) < \deg m_i(x)$  ( $1 \leq i \leq s$ ), то система сравнений*

$$f(x) \equiv c_i(x) \pmod{m_i(x)}, \quad 1 \leq i \leq s$$

имеет не более одного решения  $f(x)$  такого, что  $\deg f(x) < \sum_{i=1}^s \deg m_i(x)$ , которое можно найти по формуле

$$f(x) = \sum_{i=1}^s c_i(x) M_i(x) N_i(x) \pmod{m(x)},$$

где  $m(x) = \prod_{i=1}^s m_i(x)$ ,  $M_i(x) = \frac{m(x)}{m_i(x)}$ ,  
 $M_i(x) N_i(x) + m_i(x) n_i(x) = 1$ , ( $i \leq i \leq s$ ).

**Пример 7.** В кольце  $\mathbb{Z}_{11}[x]$  решим систему сравнений :

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

Очевидно, многочлены  $m_2(x) = x - 1$ ,  $m_3(x) = x + 1$ ,  $m_4(x) = x - 4$  попарно взаимно просты. Каждый из них взаимно прост с  $m_1(x) = x^2 + 1$ , так как ни один из корней многочленов  $m_i(x)$  ( $i = 2, 3, 4$ ) не является корнем  $m_1(x)$ .

Результаты вычислений удобно записать в таблицу:

$m_i(x)$	$M_i(x)$	$N_i(x)$
$x^2 + 1$	$x^3 - 4x^2 - x + 4$	$x - 7$
$x - 1$	$x^4 - 3x^3 - 3x^2 - 3x - 4$	$-1$
$x + 1$	$x^4 - 5x^3 + 5x^2 - 5x + 4$	$5$
$x - 4$	$x^4 - 1$	$6$

$m(x) = (x^2 + 1)(x - 1)(x + 1)(x - 4) = x^5 - 4x^4 - x + 4$ . Многочлены  $N_i(x)$  ( $i = 1, \dots, 4$ ) найдены из соотношений

$$\begin{aligned} (x - 7)M_1(x) + (2x^2 - x - 4)m_1(x) &= 1, \\ (-1)M_2(x) + (x^3 - 2x^2 - 5x - 8)m_2(x) &= 1, \\ 5M_3(x) + (-5x^3 - 3x^2 + 3)m_3(x) &= 1, \\ 6M_4(x) + (6x^3 + 2x^2 + 8x - 1)m_4(x) &= 1, \end{aligned}$$

полученных с помощью расширенного алгоритма Евклида, примененного к парам многочленов  $M_i(x)$ ,  $m_i(x)$  ( $1 \leq i \leq 4$ ).

$$\begin{aligned} \text{Значит, } f(x) &= (-x + 2)(x - 7)(x^3 - 4x^2 - x + 4) - \\ &5(x^4 - 3x^3 - 3x^2 - 3x - 4) + 7 \cdot 5(x^4 - 5x^3 + 5x^2 - 5x + 4) + \\ &6(x^4 - 1) \pmod{x^5 - 4x^4 - x + 4} = \\ &= -x^5 + 5x^4 + 2x^2 - 1 \pmod{x^5 - 4x^4 - x + 4} \equiv x^4 + 2x^2 - x + 3. \end{aligned}$$

## Неприводимые многочлены над полями $\mathbb{C}$ , $\mathbb{R}$ , $\mathbb{Q}$ , $\mathbb{Z}_p$ и кольцом $\mathbb{Z}$

Неприводимым многочленом  $f(x) \in \mathbb{A}[x]$  ( $\mathbb{A}$  – целостное кольцо) называется такой, для которого из  $f(x) = f_1(x)f_2(x)$  следует, что один из многочленов  $f_1(x), f_2(x)$  есть константа из кольца  $\mathbb{A}$ .

Из основной теоремы алгебры следует, что отличный от константы неприводимый многочлен из  $\mathbb{C}[x]$  есть многочлен первой степени. В кольце  $\mathbb{R}[x]$  неприводимыми многочленами положительной степени являются многочлены первой степени и квадратные трехчлены, не имеющие вещественных корней (т. е. с отрицательным дискриминантом).

Справедливо утверждение, что многочлен из  $\mathbb{Z}[x]$  неприводим тогда и только тогда, когда он неприводим в  $\mathbb{Q}[x]$ . Достаточным условием неприводимости многочлена в  $\mathbb{Q}[x]$  ( $\mathbb{Z}[x]$ ) является **критерий Эйзенштейна**:

*если  $f(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0 \in \mathbb{Z}[x]$  и существует простое число  $p$  такое, что*

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

*то  $f(x)$  неприводим в  $\mathbb{Q}[x]$  (и в  $\mathbb{Z}[x]$ ).*

Кроме того, для многочленов из  $\mathbb{Z}[x]$  можно пользоваться следующим утверждением.

**Теорема.** Пусть  $f(x) \in \mathbb{Z}[x]$ . Если  $f_{(m)}(x) \equiv f(x) \pmod{m}$  для некоторого целого  $m$ , не делящего старший коэффициент многочлена  $f(x)$ , и  $f_{(m)}(x)$  неприводим в  $\mathbb{Z}_m[x]$ , то  $f(x)$  неприводим в  $\mathbb{Q}[x]$  (и в  $\mathbb{Z}[x]$ ).

Для многочленов из  $\mathbb{Z}_p[x]$  ( $p$  – простое) имеется **необходимое и достаточное условие неприводимости**:

*пусть  $p$  – простое. Многочлен  $f(x) \in \mathbb{Z}_p[x]$ ,  $\deg f(x) = n$ , неприводим тогда и только тогда, когда для любого простого делителя  $q$  числа  $n$  выполнено*

$$f(x) \mid x^{p^n} - x \quad \text{и} \quad \text{НОД}(x^{p^{\frac{n}{q}}} - x, f(x)) = 1.$$

$I_p^n$  – число неприводимых унитарных многочленов степени  $n$  в кольце  $\mathbb{Z}_p[x]$ , где  $p$  – простое,  $n$  – натуральное, — можно вычислить по одной из следующих формул:

$$I_p^n = \frac{1}{n} \left( p^n - \sum_{d \mid n, d \neq n} d I_p^d \right),$$

$$I_p^n = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}},$$

где  $\mu(*)$  – функция Мёбиуса.

В случае простого числа  $n$  первая из этих формул принимает вид:

$$I_p^n = \frac{p^n - p}{n} = \frac{p(p^{n-1} - 1)}{n}.$$

**Пример 8.** Выясним вопрос о приводимости многочлена  $x^4 - 2$  в кольцах  $\mathbb{C}[x]$ ,  $\mathbb{R}[x]$ ,  $\mathbb{Z}_7[x]$ ,  $\mathbb{Q}[x]$  ( $\mathbb{Z}[x]$ ).

$$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) - \text{разложение в } \mathbb{R}[x],$$

$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}) - \text{разложение в } \mathbb{C}[x],$$

$$x^4 - 2 = (x - 2)(x + 2)(x^2 + 4) - \text{разложение в } \mathbb{Z}_7[x].$$

Для кольца  $\mathbb{Q}[x]$  воспользуемся критерием Эйзенштейна. Очевидно, что в качестве простого числа  $p$  можно взять число 2. Действительно,  $2 \nmid 1$ ,  $2 \mid (-2)$  и  $2^2 \nmid (-2)$ . Следовательно,  $x^4 - 2$  неприводим в  $\mathbb{Q}[x]$  (и в  $\mathbb{Z}[x]$ ).

**Пример 9.** Является ли приводимым многочлен  $f(x) = x^4 + x^3 + 1$  в кольце  $\mathbb{Z}_2[x]$  ?

Воспользуемся критерием неприводимости многочлена в кольце  $\mathbb{Z}_p[x]$ .  $f(x)$  неприводим в  $\mathbb{Z}_2[x]$ , если он делит многочлен  $x^{2^4} - x = x^{16} - x$  и взаимно прост с многочленом  $x^{2^2} - x$ . (У числа 4 только один простой делитель – 2 и  $\frac{4}{2} = 2$ ). Применим алгоритм Евклида к многочленам  $x^4 - x = x^4 + x \in \mathbb{Z}_2[x]$  и  $f(x)$  :

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

$$x^4 + x = (x^3 + x + 1) \cdot x + x^2,$$

$$x^3 + x + 1 = x^2 \cdot x + (x + 1),$$

$$x^2 = (x + 1)(x + 1) + 1,$$

откуда следует, что  $x^4 - x$  и  $f(x)$  взаимно просты. Кроме того,

$$x^{16} - x = (x^4 + x^3 + 1)(x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^5 + x^4 + x).$$

Значит,  $f(x) = x^4 + x^3 + 1$  неприводим в кольце  $\mathbb{Z}_2[x]$ .

### Разложение на свободные от квадратов сомножители

Пусть  $f(x) \in \mathbb{A}[x]$  – примитивный многочлен ( $\mathbb{A}$  – факториальное кольцо) разложен в произведение неприводимых многочленов

$$f(x) = \prod_{i=1}^s \{p_i(x)\}^{k_i}.$$

Пусть  $k = \max \{k_1, k_2, \dots, k_s\}$  и  $J_i = \{j \mid k_j = i\}$ ,

$$s_i(x) = \prod_{j \in J_i} p_j(x).$$

Тогда

$$f(x) = \prod_{i=1}^k \{s_i(x)\}^i$$

есть разложение  $f(x)$  на свободные от квадратов сомножители  $s_i(x)$  ( $i = 1, \dots, k$ ).

Алгоритм нахождения этих сомножителей состоит из следующих шагов, которые следует повторять до тех пор, пока не получим  $r(x) = \text{const} \in \mathbb{A}$ :

1. Найти  $f'(x)$ ;
2. Вычислить  $r(x) = \text{НОД}(f(x), f'(x))$ ;
3. Найти  $t(x) = \frac{f(x)}{r(x)}$ ;
4. Вычислить  $v(x) = \text{НОД}(t(x), r(x))$ ;
5. Найти  $s_i(x) = \frac{t(x)}{v(x)}$ .

При первом проходе получим  $s_1(x)$ , затем заменяем  $f(x)$  на  $r(x)$  и снова применяем алгоритм. При втором проходе получаем  $s_2(x)$  и т. д. На самом деле, первые три шага алгоритма придется провести только при первом проходе, а далее их можно заменить на шаги:

- 1'. Положить  $f(x) = f_n(x) := r(x)$ ;
- 2'. Положить  $r(x) = r_n(x) := \frac{r(x)}{v(x)}$ ;
- 3'. Положить  $t(x) = t_n(x) := v(x)$ .

**Пример 10.** Разложить на свободные от квадратов сомножители многочлен

$$f(x) = x^7 - x^6 - 3x^5 + 3x^4 + 3x^3 - 3x^2 - x + 1.$$

Так как  $f'(x) = 7x^6 - 6x^5 - 15x^4 + 12x^3 + 9x^2 - 6x - 1$  и

$r(x) = \text{НОД}(f(x), f'(x)) = x^5 - x^4 - 2x^3 + 2x^2 + x - 1$ , то

$t(x) = x^2 - 1$  и  $v(x) = \text{НОД}(x^2 - 1, x^5 - x^4 - 2x^3 + 2x^2 + x - 1) = x^2 - 1$ .

Значит,

$$s_1(x) = \frac{x^2 - 1}{x^2 - 1} = 1.$$

Полагаем :

$$f_n(x) = x^5 - x^4 - 2x^3 + 2x^2 + x - 1, \quad t_n(x) = x^2 - 1,$$

$$r_n(x) = \frac{x^5 - x^4 - 2x^3 + 2x^2 + x - 1}{x^2 - 1} = x^3 - x^2 - x + 1.$$

$$\text{Тогда } v_n(x) = \text{НОД}(x^2 - 1, x^3 - x^2 - x + 1) = x^2 - 1,$$

$$s_2(x) = \frac{x^2 - 1}{x^2 - 1} = 1.$$

Полагаем :

$$f_{nn}(x) = x^3 - x^2 - x + 1, t_{nn} = x^2 - 1,$$

$$r_{nn} = \frac{x^3 - x^2 - x + 1}{x^2 - 1} = x - 1.$$

Так как  $v_{nn}(x) = \text{НОД}(x - 1, x^2 - 1) = x - 1$ , то

$$s_3(x) = \frac{x^2 - 1}{x - 1} = x + 1.$$

Полагаем :  $f_{nnn}(x) = x - 1, t_{nnn}(x) = x - 1, r_{nnn}(x) = \frac{x - 1}{x - 1} = 1$ , тогда  $v_{nnn}(x) = \text{НОД}(x - 1, 1) = 1$  и

$$s_4(x) = \frac{x - 1}{1} = x - 1.$$

Поскольку  $r_{nnn}(x) = 1$ , то алгоритм завершает свою работу. Мы получили

$$f(x) = \{s_3(x)\}^3 \{s_4(x)\}^4 = (x + 1)^3 (x - 1)^4.$$

На самом деле, если можно подобрать корень многочлена  $f(x)$ , то лучше снизить степень раскладываемого многочлена, выделив все возможные сомножители. Тогда алгоритм будет применяться к многочлену меньшей степени, следовательно, можно ожидать, что он потребует меньшего объема вычислений. Для нашего примера алгоритм не потребовался бы совсем, если мы заметим, что корнем данного многочлена является 1. Делим  $f(x)$  на  $x - 1$  до тех пор, пока деление происходит нацело :

$$\begin{array}{r|rrrrrrrrrr} & 1 & -1 & -3 & 3 & 3 & -3 & -1 & 1 \\ \hline 1 & 1 & 0 & -3 & 0 & 3 & 0 & -1 & 0 \\ 1 & 1 & 1 & -2 & -2 & 1 & 1 & 0 \\ 1 & 1 & 2 & 0 & -2 & -1 & 0 \\ 1 & 1 & 3 & 3 & 1 & 0 \end{array}$$

В итоге получаем тот же результат :

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

## Поля Галуа

Конечное поле из  $q$  элементов называется *полем Галуа* и обозначается  $GF(q)$ .

*Примитивным элементом (примитивным корнем)* поля Галуа  $GF(q)$  называется элемент порядка  $q - 1$  относительно умножения.

Справедливо утверждение о том, что в каждом поле Галуа есть примитивный элемент.

Общих формул для отыскания примитивного элемента нет, но полезно следующее утверждение.

**Лемма.** *В поле  $GF(q)$  элемент  $a$  является примитивным корнем тогда и только тогда, когда*

$$a^{\frac{q-1}{p_i}} \neq 1 \pmod{q}$$

*для всех простых делителей  $p_1, p_2, \dots, p_s$  числа  $q - 1$ .*

Поле Галуа можно построить, имея конечное поле  $\mathbb{Z}_p$  ( $p$  – простое) следующим образом:

*найти неприводимый унитарный многочлен  $m(x) \in \mathbb{Z}_p[x]$  и построить факторкольцо  $\mathbb{Z}_p[x]/(m(x))$ . В результате получим поле, содержащее  $\mathbb{Z}_p$  и корень  $\alpha$  многочлена  $m(x)$ . Это поле состоит из  $p^r$  элементов, где  $r = \deg m(x)$ , и является линейным пространством размерности  $r$  над полем  $\mathbb{Z}_p$ .*

Элементы поля  $GF(p^r)$  можно представлять различными способами: как степени элемента  $\alpha$  (корня  $m(x)$ ); как многочлены из кольца  $\mathbb{Z}_p[x]$  степени меньшей  $r$ , вычисленные в точке  $\alpha$ ; как векторы линейного пространства, координаты которых даны в базисе  $1, \alpha, \alpha^2, \dots, \alpha^{r-1}$ .

Если  $\alpha$  – алгебраическое над полем  $F$  число, то оно по определению является корнем многочлена положительной степени из кольца  $F[x]$ . Сам элемент  $\alpha$  может не принадлежать  $F$ , тогда он содержится в некотором расширении  $K$  поля  $F$ .

*Минимальным многочленом* алгебраического числа  $\alpha$  над полем  $F$  называется многочлен наименьшей положительной степени из кольца  $F[x]$  с корнем  $\alpha$ . Этот многочлен, очевидно, неприводим в  $F[x]$ , если рассматривать унитарный минимальный многочлен, то он определен однозначно для данного элемента  $\alpha$ . Справедливо утверждение.

**Теорема.** *Пусть  $K = F[\alpha] = F[x]/(m(x))$  – простое расширение поля  $F$ , минимальный многочлен  $m(x)$  элемента  $\alpha$  над  $F$  имеет степень  $r$ . Тогда любой элемент поля  $F[\alpha]$  является алгебраическим над полем  $F$ ,*

и минимальный многочлен этого элемента над полем  $F$  имеет степень, не превосходящую  $r$ .

Для того чтобы найти минимальный многочлен элемента  $\beta \in F[\alpha]$  над полем  $F$ , будем смотреть на факторкольцо  $F[\alpha] = F[x]/(m(x))$  как на линейное пространство размерности  $r$  над полем  $F$ . В качестве базиса этого линейного пространства можно взять

$$1, \alpha, \alpha^2, \dots, \alpha^{r-1}.$$

Тогда любые  $r + 1$  элементов этого линейного пространства линейно зависимы. Значит,

$$1, \beta, \beta^2, \dots, \beta^r$$

линейно зависимы, т. е. существуют коэффициенты  $d_0, d_1, \dots, d_r \in F$ , среди которых хотя бы один отличен от нуля, такие что

$$d_0 + d_1\beta + d_2\beta^2 + \dots + d_r\beta^r = 0. \quad (6)$$

Каждый элемент линейного пространства раскладывается по базису, следовательно,

$$\beta^s = \sum_{i=0}^{r-1} c_{si} \alpha^i \quad (s = 1, 2, \dots, r). \quad (7)$$

Подставляя (7) в (6), получаем

$$0 = \sum_{s=0}^r d_s \beta^s = \sum_{s=0}^r d_s \left( \sum_{i=0}^{r-1} c_{si} \alpha^i \right) = \sum_{i=0}^{r-1} \alpha^i \left( \sum_{s=0}^r c_{si} d_s \right),$$

и, так как  $1, \alpha, \alpha^2, \dots, \alpha^{r-1}$  — линейно независимы, отсюда следует :

$$\sum_{s=0}^r c_{si} d_s = 0 \quad (i = 0, 1, \dots, r-1).$$

Получили однородную систему линейных уравнений из  $r$  уравнений с  $r+1$  неизвестными. Она всегда имеет ненулевые решения. Решая ее, найдем ненулевой многочлен  $f(x) = d_0 + d_1x + \dots + d_rx^r \in F[x]$  с корнем  $\beta$ .

**Пример 11.** Найти минимальный многочлен элемента  $\beta = \alpha^3$  поля  $\mathbb{Z}_2[x]/(m(x))$  в кольце  $\mathbb{Z}_2[x]$ , если  $\alpha$  — корень многочлена  $m(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ .

Поскольку  $\alpha$  корень  $m(x)$ , то  $m(\alpha) = \alpha^4 + \alpha + 1 = 0$ , откуда  $\alpha^4 = \alpha + 1$ . Разложим степени элемента  $\beta$  по базису линейного пространства



$\mathbb{Z}_2[x]/(m(x) : 1, \alpha, \alpha^2, \alpha^3)$ . Имеем

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

Тогда из соотношения

$$d_0 + d_1\alpha^3 + d_2(\alpha^3 + \alpha^2) + d_3(\alpha^3 + \alpha) + d_4(\alpha^3 + \alpha^2 + \alpha + 1) = 0$$

получаем систему уравнений :

$$\begin{cases} d_0 + d_4 = 0 \\ d_1 + d_4 = 0 \\ d_2 + d_4 = 0 \\ d_1 + d_2 + d_3 + d_4 = 0. \end{cases}$$

Решая эту систему, получаем  $d_3 = d_2 = d_0 = d_1 = d_4$ . Значит, минимальный многочлен элемента  $\beta$  – это многочлен  $x^4 + x^3 + x^2 + x + 1$ .

**Пример 12.** Найти примитивный элемент в поле  $\mathbb{Z}_{53}$ .

Согласно приведенной выше теореме элемент  $a \in \mathbb{Z}_{53}$  является примитивным тогда и только тогда, когда

$$a^{\frac{53-1}{p}} \neq 1 \pmod{53}$$

для всех простых делителей  $p$  числа 52. Таких делителей всего два: 2 и 13. В качестве  $a$  попробуем взять элемент 2:

$$\begin{aligned}2^{\frac{52}{13}} &= 2^4 = 16 \neq 1 \pmod{53}, \\ 2^{\frac{52}{2}} &= 2^{26} = (2^{10})^2 \cdot 2^6 = (1024)^2 \cdot 64 \equiv 17^2 \cdot 11 \equiv 289 \cdot 11 \\ &\equiv 24 \cdot 11 \equiv 264 \equiv -1 \neq 1 \pmod{53}.\end{aligned}$$

Значит,  $a = 2$  является примитивным элементом поля  $\mathbb{Z}_{53}$ .

**Пример 13.** Построить поле Галуа  $GF(3^3) \cong \mathbb{Z}_3[x]/(x^3 + 2x + 1)$ .

Многочлен  $x^3 + 2x + 1$  является  $s$  - примитивным. Действительно, он неприводим и является делителем многочлена  $x^{3^3-1} - 1 = x^{26} - 1 = (x^{13} - 1)(x^{13} + 1)$  в  $\mathbb{Z}_3[x]$ . В то же время он не делит  $x^{13} - 1$ .

Если  $\alpha$  – корень  $x^3 + 2x + 1$ , то  $\alpha^3 + 2\alpha + 1 = 0$ , откуда  $\alpha^3 = -2\alpha - 1 = \alpha + 2$ .

Элементы поля  $\mathbb{Z}_3[x]/(x^3 + 2x + 1)$  представим в следующей таблице тремя различными способами:

<i>I</i>	<i>II</i>	<i>III</i>
0	0	(0, 1, 0)
1	1	(0, 1, 0)
$\alpha$	$\alpha$	(0, 1, 0)
$\alpha^2$	$\alpha^2$	(1, 0, 0)
$\alpha^3$	$\alpha + 2$	(0, 1, 2)
$\alpha^4$	$\alpha^2 + 2\alpha$	(1, 2, 0)
$\alpha^5$	$2\alpha^2 + \alpha + 2$	(2, 1, 2)
$\alpha^6$	$\alpha^2 + \alpha + 1$	(1, 1, 1)
$\alpha^7$	$\alpha^2 + 2\alpha + 2$	(1, 2, 2)
$\alpha^8$	$2\alpha^2 + 2$	(2, 0, 2)
$\alpha^9$	$\alpha + 1$	(0, 1, 1)
$\alpha^{10}$	$\alpha^2 + \alpha$	(1, 1, 0)
$\alpha^{11}$	$\alpha^2 + \alpha + 2$	(1, 1, 2)
$\alpha^{12}$	$\alpha^2 + 2$	(1, 0, 2)
$\alpha^{13}$	2	(0, 0, 2)
$\alpha^{14}$	$2\alpha$	(0, 2, 0)
$\alpha^{15}$	$2\alpha^2$	(2, 0, 0)
$\alpha^{16}$	$2\alpha + 1$	(0, 2, 1)
$\alpha^{17}$	$2\alpha^2 + \alpha$	(2, 1, 0)
$\alpha^{18}$	$\alpha^2 + 2\alpha + 1$	(1, 2, 1)
$\alpha^{19}$	$2\alpha^2 + 2\alpha + 2$	(2, 2, 2)
$\alpha^{20}$	$2\alpha^2 + \alpha + 1$	(2, 1, 1)
$\alpha^{21}$	$\alpha^2 + 1$	(1, 0, 1)
$\alpha^{22}$	$2\alpha + 2$	(0, 2, 2)
$\alpha^{23}$	$2\alpha^2 + 2\alpha$	(2, 2, 0)
$\alpha^{24}$	$2\alpha^2 + 2\alpha + 1$	(2, 2, 1)
$\alpha^{25}$	$2\alpha^2 + 1$	(2, 0, 1)

## Задачи

### Задание № 1

Используя схему Горнера, вычислить  $f(x_0)$ . Вычисления проводятся в кольце  $K[x]$  :

- 1).  $f(x) = x^5 - 2x^4 + 3x^3 - 4x + 6, \quad x_0 = -2, \quad K = \mathbb{Z};$
- 2).  $f(x) = x^6 + 4x^4 - 3x^3 + 2x^2 + 3x - 6, \quad x_0 = 3, \quad K = \mathbb{Z}_7;$
- 3).  $f(x) = x^5 + 3x^3 - 4x^2 + 2x - 1, \quad x_0 = 4, \quad K = \mathbb{Z}_{11};$
- 4).  $f(x) = x^6 + 5x^5 - 3x^4 + 2x^2 + 3, \quad x_0 = 2, \quad K = \mathbb{Z}_{19};$
- 5).  $f(x) = x^6 - 3x^4 + 5x^3 - 2x^2 + 10x - 5, \quad x_0 = -3, \quad K = \mathbb{Z}_{17}.$

### Задание № 2

Используя схему Горнера, найти  $f(y + y_0)$  в кольце  $K[x]$  :

- 1).  $f(x) = x^4 - 3x^2 + 2x + 5, \quad y_0 = 2, \quad K = \mathbb{Z};$
- 2).  $f(x) = x^3 - x^2 + 2x + 1, \quad y_0 = 2, \quad K = \mathbb{Z}_3;$
- 3).  $f(x) = x^5 + 3x^3 + 2x^2 + x + 4, \quad y_0 = 3, \quad K = \mathbb{Z}_5;$
- 4).  $f(x) = x^4 + 10x^3 + 7x^2 + 5x + 3, \quad y_0 = -2, \quad K = \mathbb{Z}_{11};$
- 5).  $f(x) = x^5 - 2x^4 + 3x^2 + 5x - 2, \quad y_0 = -3, \quad K = \mathbb{Z}_{13};$
- 6).  $f(x) = x^4 + 2x^2 - 3x + 6, \quad y_0 = 1, \quad K = \mathbb{Z};$
- 7).  $f(x) = x^5 + 3x^3 - 2x^2 + 4x - 1, \quad y_0 = -2, \quad K = \mathbb{Z}.$

### Задание № 3

Используя расширенный алгоритм Евклида, найти наибольший общий делитель многочленов  $f(x)$  и  $g(x)$  в кольце  $K[x]$  и многочлены  $u(x), v(x) \in K[x]$  такие, что  $\text{НОД}(f(x), g(x)) = f(x)u(x) + g(x)v(x)$  :

- 1).  $f(x) = x^4 - x^3 - 5x^2 - x - 6, \quad g(x) = x^4 - 1, \quad K = \mathbb{R};$
- 2).  $f(x) = x^4 + 4x^3 + 6x^2 + 5x + 2, \quad g(x) = x^3 + 5x^2 + 2x + 6,$   
 $K = \mathbb{Z}_7;$
- 3).  $f(x) = x^4 + 2x^3 + 3x^2 - 2x + 1,$   
 $g(x) = x^4 + 2x^3 + 4x^2 + 3x, \quad K = \mathbb{Z}_5;$
- 4).  $f(x) = x^5 + 2x^4 - 4x^3 - 4x^2 - 5x + 5,$   
 $g(x) = x^4 + 3x^3 + 3x^2 - 5x + 2, \quad K = \mathbb{Z}_{11};$
- 5).  $f(x) = x^4 - x^3 + x - 1, \quad g(x) = x^3 + 2x^2 + 2x + 1, \quad K = \mathbb{Z}_7;$
- 6).  $f(x) = x^5 + 4x^4 + 5x^3 + 7x^2 + 4x + 3,$   
 $g(x) = x^5 + 2x^4 - x - 2, \quad K = \mathbb{R};$
- 7).  $f(x) = x^5 - x^4 - 2x^3 - x^2 + x + 2,$   
 $g(x) = x^4 - 6x^3 - 5x^2 - 6x + 1, \quad K = \mathbb{Z}_{11};$

- 8).  $f(x) = x^4 + 2, \quad g(x) = x^3 + x + 2, \quad K = \mathbb{Z}_3;$   
 9).  $f(x) = x^5 - 4x^4 - 3x^3 - 6x^2 - 2x + 1,$   
 $g(x) = x^4 - 5x^3 + 3x^2 + 7x - 2, \quad K = \mathbb{Z}_{13}.$

#### Задание № 4

Пользуясь интерполяционной формулой Лагранжа, восстановить многочлен  $f(x)$  в кольце  $K[x]$  по таблице его значений  $f(a_i) = b_i$  ( $i = 0, 1, \dots, n$ ):

- 1).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 1 & 2 & 4 & 6 \\ \hline b_i & -5 & -2 & 5 & 151 & 913 \end{array} \quad K = \mathbb{Q};$   
 2).  $\begin{array}{c|c|c|c|c} a_i & 0 & 1 & 2 & 4 \\ \hline b_i & 1 & 2 & 3 & 4 \end{array} \quad K = \mathbb{Z}_5;$   
 3).  $\begin{array}{c|c|c|c|c} a_i & 2 & 3 & 5 & 7 \\ \hline b_i & 2 & 2 & 10 & 10 \end{array} \quad K = \mathbb{Z}_{11};$   
 4).  $\begin{array}{c|c|c|c|c|c} a_i & -1 & 0 & 1 & 2 & 3 \\ \hline b_i & 5 & 1 & 1 & 5 & 37 \end{array} \quad K = \mathbb{Q};$   
 5).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 1 & 3 & 5 & 7 \\ \hline b_i & 5 & 9 & 5 & 9 & 2 \end{array} \quad K = \mathbb{Z}_{13};$   
 6).  $\begin{array}{c|c|c|c|c|c} a_i & 1 & 3 & 4 & 5 & 8 \\ \hline b_i & 1 & 1 & 3 & 15 & 1 \end{array} \quad K = \mathbb{Z}_{17};$   
 7).  $\begin{array}{c|c|c|c|c|c|c} a_i & 2 & 5 & 6 & 8 & 10 & 11 \\ \hline b_i & 5 & 1 & 17 & 10 & 12 & 5 \end{array} \quad K = \mathbb{Z}_{19};$   
 8).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 1 & 3 & 4 & 5 \\ \hline b_i & 5 & 5 & 2 & 0 & 1 \end{array} \quad K = \mathbb{Z}_7;$   
 9).  $\begin{array}{c|c|c|c|c|c|c} a_i & 1 & 3 & 4 & 6 & 8 & 11 \\ \hline b_i & 8 & 11 & 10 & 12 & 2 & 3 \end{array} \quad K = \mathbb{Z}_{17};$   
 10).  $\begin{array}{c|c|c|c|c|c|c|c} a_i & -1 & 0 & 1 & 2 & 3 & 4 \\ \hline b_i & -28 & -11 & -10 & -19 & 16 & 317 \end{array} \quad K = \mathbb{Q}.$

#### Задание № 5

Решить задачу интерполяции в кольце  $K[x]$ , используя алгоритм, основанный на китайской теореме об остатках:

- 1).  $\begin{array}{c|c|c|c|c|c} a_i & 1 & 3 & 4 & 5 & 8 \\ \hline b_i & 1 & 1 & 3 & 15 & 1 \end{array} \quad K = \mathbb{Z}_{17};$

- 2).  $\frac{a_i \mid 2 \mid 5 \mid 6 \mid 8 \mid 10 \mid 11}{b_i \mid 5 \mid 1 \mid 17 \mid 10 \mid 12 \mid 5} \quad K = \mathbb{Z}_{19};$
- 3).  $\frac{a_i \mid 0 \mid 1 \mid 3 \mid 4 \mid 5}{b_i \mid 5 \mid 5 \mid 2 \mid 0 \mid 1} \quad K = \mathbb{Z}_7;$
- 4).  $\frac{a_i \mid 1 \mid 3 \mid 4 \mid 6 \mid 8 \mid 11}{b_i \mid 8 \mid 11 \mid 10 \mid 12 \mid 2 \mid 3} \quad K = \mathbb{Z}_{17};$
- 5).  $\frac{a_i \mid -1 \mid 0 \mid 1 \mid 2 \mid 3 \mid 4}{b_i \mid -28 \mid -11 \mid -10 \mid -19 \mid 16 \mid 317} \quad K = \mathbb{Q};$
- 6).  $\frac{a_i \mid 0 \mid 1 \mid 2 \mid 4 \mid 6}{b_i \mid -5 \mid -2 \mid 5 \mid 151 \mid 913} \quad K = \mathbb{Q};$
- 7).  $\frac{a_i \mid 0 \mid 1 \mid 2 \mid 4}{b_i \mid 1 \mid 2 \mid 3 \mid 4} \quad K = \mathbb{Z}_5;$
- 8).  $\frac{a_i \mid 2 \mid 3 \mid 5 \mid 7}{b_i \mid 2 \mid 2 \mid 10 \mid 10} \quad K = \mathbb{Z}_{11};$
- 9).  $\frac{a_i \mid -1 \mid 0 \mid 1 \mid 2 \mid 3}{b_i \mid 5 \mid 1 \mid 1 \mid 5 \mid 37} \quad K = \mathbb{Q};$
- 10).  $\frac{a_i \mid 0 \mid 1 \mid 3 \mid 5 \mid 7}{b_i \mid 5 \mid 9 \mid 5 \mid 9 \mid 2} \quad K = \mathbb{Z}_{13}.$

### Задание № 6

Вычислить выражение  $f(x) = F(g_1(x), g_2(x), \dots, g_n(x))$  над  $K[x]$ , работая над полями  $K[x]/(m_s(x))$  для различных  $s$ , где  $m_s(x) = x - a_s$ ,  $a_s \in K$ , и пользуясь алгоритмом интерполяции, основанным на китайской теореме об остатках:

- 1).  $f_1(f_2(x)), \quad f_1(x) = 3x^2 + 2x + 1, \quad f_2(x) = x^2 + 2x - 1,$   
 $K = \mathbb{Z}_5;$
- 2).  $f_1(f_2(f_3(x))), \quad f_1(x) = 2x^2 + x + 3,$   
 $f_2(x) = x^2 + 4x + 1, \quad f_3(x) = 3x^2 + 2x + 4, \quad K = \mathbb{Z}_7;$
- 3).  $(f_1 + f_2)(f_3(x)), \quad f_1(x) = x^3 + x + 2,$   
 $f_2(x) = 6x^2 + 5x + 3, \quad f_3(x) = x^2 + 5x + 1, \quad K = \mathbb{Z}_{11};$
- 4).  $f_1(f_2 + f_3)(x), \quad f_1(x) = x^2 + 3x + 5,$   
 $f_2(x) = x^3 + 7x^2 + 1, \quad f_3(x) = 5x^2 + 4x + 3, \quad K = \mathbb{Z}_{19}.$

## Задание № 7

Вычислить выражение  $f(x) = F(g_1(x), g_2(x), \dots, g_n(x))$  над  $\mathbb{Z}[x]$ , работая над полями  $\mathbb{Z}_{m_s}$  для различных взаимно простых модулей  $m_s$  и пользуясь китайской теоремой об остатках:

- 1).  $(f_1(x) + f_2(x)) \cdot f_3(x)$ ,  $f_1(x) = 3x^2 + 5x - 1$ ,  
 $f_2(x) = 4x^3 - 2x + 3$ ,  $f_3(x) = 7x^2 + 6x + 5$ ;
- 2).  $(f_1(x) + 2f_2(x)) \cdot f_3^2(x)$ ,  $f_1(x) = x^2 + 2x + 3$ ,  
 $f_2(x) = 3x^2 + 2x - 1$ ,  $f_3(x) = 4x^2 + 3x + 5$ ;
- 3).  $(2f_1(x) - f_2(x)) \cdot (f_2(x) + f_3(x))$ ,  $f_1(x) = 3x^2 + 2x + 1$ ,  
 $f_2(x) = 4x^2 + x + 3$ ,  $f_3(x) = x^2 + 1$ ;
- 4).  $f_1(x) \cdot f_2(x) \cdot f_3(x)$ ,  $f_1(x) = 2x^2 + 3x + 3$ ,  
 $f_2(x) = x^3 + 2x + 5$ ,  $f_3(x) = x^2 + 2x + 7$ .

## Задание № 8

Решить систему сравнений в кольце  $K[x]$  :

- 1). 
$$\begin{cases} f(x) \equiv 3 \pmod{x+1} \\ f(x) \equiv 1 \pmod{x^2+1} \\ f(x) \equiv 4x+3 \pmod{x^2-x} \end{cases} \quad K = \mathbb{R};$$
- 2). 
$$\begin{cases} f(x) \equiv 2 \pmod{x-1} \\ f(x) \equiv -1 \pmod{x-2} \\ f(x) \equiv 7x+3 \pmod{x^2+x} \end{cases} \quad K = \mathbb{R};$$
- 3). 
$$\begin{cases} f(x) \equiv 4 \pmod{x} \\ f(x) \equiv 0 \pmod{x-1} \\ f(x) \equiv 4 \pmod{x+2} \\ f(x) \equiv 3 \pmod{x-2} \end{cases} \quad K = \mathbb{Z}_5;$$
- 4). 
$$\begin{cases} f(x) \equiv 3 \pmod{x} \\ f(x) \equiv 4 \pmod{x-1} \\ f(x) \equiv 3x+1 \pmod{x^2+x+1} \\ f(x) \equiv 0 \pmod{x-2} \end{cases} \quad K = \mathbb{Z}_7;$$
- 5). 
$$\begin{cases} f(x) \equiv 9 \pmod{x} \\ f(x) \equiv 4 \pmod{x-1} \\ f(x) \equiv 7 \pmod{x+1} \\ f(x) \equiv 9 \pmod{x-2} \end{cases} \quad K = \mathbb{Z}_{11};$$
- 6). 
$$\begin{cases} f(x) \equiv 3 \pmod{x-1} \\ f(x) \equiv -9 \pmod{x+1} \\ f(x) \equiv 2x-13 \pmod{x^2+1} \end{cases} \quad K = \mathbb{R}.$$

### Задание № 9

Найти наибольший общий делитель двух многочленов в кольце  $\mathbb{Z}[x]$ , используя псевдоделение:

- 1).  $f_1(x) = 6x^5 - 6x^4 - 18x^2 - 6x - 12$ ,  $f_2(x) = 3x^4 - 15x^2 + 12$ ;
- 2).  $f_1(x) = 2x^5 + 8x^4 + 8x^3 + 10x^2 + 14x + 6$ ,  
 $f_2(x) = 6x^4 + 18x^3 - 6x - 18$ ;
- 3).  $f_1(x) = 3x^5 - 6x^4 - 12x^3 + 12x^2 - 15x + 18$ ,  
 $f_2(x) = 6x^4 + 6x^3 - 42x^2 - 6x + 36$ ;
- 4).  $f_1(x) = 8x^5 + 8x^4 + 8x^3 - 8x^2 - 16$ ,  
 $f_2(x) = 36x^4 + 6x^3 + 24x^2 + 6x - 12$ ;
- 5).  $f_1(x) = 6x^5 + 16x^4 + 22x^3 + 26x^2 + 16x + 10$ ,  
 $f_2(x) = 14x^5 + 22x^4 + 8x^3 - 14x^2 - 22x - 8$ .

### Задание № 10

Разложить многочлен на неприводимые множители над полем  $K$  :

- 1).  $x^4 + 4$ ,  $K = \mathbb{C}$ ;
- 2).  $x^4 + 4x^3 + 4x^2 + 1$ ,  $K = \mathbb{C}$ ;
- 3).  $x^4 + 4x^3 + 4x^2 + 1$ ,  $K = \mathbb{R}$ ;
- 4).  $x^4 - 10x^2 + 1$ ,  $K = \mathbb{C}$ ;
- 5).  $x^4 + 4$ ,  $K = \mathbb{R}$ ;
- 6).  $x^6 + 27$ ,  $K = \mathbb{R}$ ;
- 7).  $x^4 + 4x^2 + 2x + 5$ ,  $K = \mathbb{Z}_7$ ;
- 8).  $x^4 + 4x^2 + 5x + 5$ ,  $K = \mathbb{Z}_7$ ;
- 9).  $x^4 + 3x^3 + 2x^2 + 2x + 1$ ,  $K = \mathbb{Z}_5$ ;
- 10).  $x^4 + 2x + 2$ ,  $K = \mathbb{Z}_3$ ;
- 11).  $x^4 + 1$ ,  $K = \mathbb{Z}_2$ ;
- 12).  $x^4 + 1$ ,  $K = \mathbb{Z}_3$ ;
- 13).  $x^4 + 1$ ,  $K = \mathbb{Z}_5$ ;
- 14).  $x^4 + 1$ ,  $K = \mathbb{Z}_{17}$ .

### Задание № 11

Является ли многочлен приводимым в кольце  $A[x]$ ?

- 1).  $x^3 + 4x^2 - 3x + 7$ ,  $A = \mathbb{Z}$ ;
- 2).  $x^3 + 3x^2 + 4x - 5$ ,  $A = \mathbb{Z}$ ;
- 3).  $x^6 + x^5 + 1$ ,  $A = \mathbb{Z}_2$ ;
- 4).  $x^6 + x + 1$ ,  $A = \mathbb{Z}_2$ ;
- 5).  $x^3 + 2x + 2$ ,  $A = \mathbb{Z}_3$ ;
- 6).  $x^3 + 2x^2 + x + 1$ ,  $A = \mathbb{Z}_3$ .

### Задание № 12

Найти число неприводимых многочленов степени  $\leq n$  над полем  $\mathbb{Z}_p$  :

- 1).  $n = 6, p = 2$ ;
- 2).  $n = 7, p = 2$ ;
- 3).  $n = 8, p = 2$ ;
- 4).  $n = 4, p = 3$ ;
- 5).  $n = 5, p = 3$ ;
- 6).  $n = 6, p = 3$ ;
- 7).  $n = 4, p = 5$ ;
- 8).  $n = 6, p = 5$ .

### Задание № 13

Выписать все унитарные неприводимые многочлены степени  $\leq n$  из кольца  $\mathbb{Z}_p[x]$  :

- 1).  $n = 5, p = 2$ ;
- 2).  $n = 3, p = 3$ ;
- 3).  $n = 2, p = 5$ .

### Задание № 14

В  $\mathbb{Z}_p[x]/(m(x))$  найти обратный к многочлену  $f(x)$  :

- 1).  $p = 2, m(x) = x^3 + x + 1, f(x) = x^2 + x + 1$ ;
- 2).  $p = 3, m(x) = x^4 + 2x^3 + x + 1, f(x) = x^3 + x^2 + 2x + 1$ ;
- 3).  $p = 3, m(x) = x^5 + 2x^3 + x^2 + x + 2, f(x) = x^3 + 2x^2 + 2x + 1$ ;
- 4).  $p = 3, m(x) = x^5 + 2x^3 + x^2 + x + 2, f(x) = 2x^4 + x^3 + 2x + 1$ ;
- 5).  $p = 2, m(x) = x^5 + x^3 + 1, f(x) = x^4 + x^2 + x + 1$ .

### Задание № 15

Найти все унитарные неприводимые многочлены из кольца  $\mathbb{Z}_p[x]$  третьей степени вида:

- 1).  $x^3 + ax^2 + bx + 1, p = 5$ ;
- 2).  $x^3 + ax^2 + b, p = 5$ ;
- 3).  $x^3 + ax + b, p = 5$ ;
- 4).  $x^3 + ax^2 + bx + 1, p = 7$ ;
- 5).  $x^3 + ax^2 + b, p = 7$ .



Задание № 16

Построить поле  $\mathbb{Z}_p[x]/(m(x))$  :

- 1).  $\mathbb{Z}_2[x]/(x^3 + x + 1)$ ;
- 2).  $\mathbb{Z}_3[x]/(x^2 + 2x + 2)$ ;
- 3).  $\mathbb{Z}_2[x]/(x^3 + x^2 + 1)$ ;
- 4).  $\mathbb{Z}_3[x]/(x^3 + 2x^2 + x + 1)$ ;
- 5).  $\mathbb{Z}_3[x]/(x^3 + 2x^2 + 1)$ .

Задание № 17

Разложить на свободные от квадратов множители в кольце  $\mathbb{Q}[x]$  :

- 1).  $x^5 - x^4 - 2x^3 + 2x^2 + x - 1$ ;
- 2).  $x^8 + 3x^7 - 7x^6 - 27x^5 + 6x^4 + 72x^3 + 32x^2 - 48x - 32$ ;
- 3).  $x^5 - x^3 - x^2 + 1$ ;
- 4).  $x^6 + 3x^5 - 6x^3 - 3x^2 + 3x + 2$ ;
- 5).  $x^8 - 11x^6 + 4x^5 + 31x^4 - 8x^3 - 33x^2 + 4x + 12$ .

Задание № 18

В поле Галуа  $GF(q)$  найти примитивный элемент:

- 1).  $q = 31$ ;
- 2).  $q = 37$ ;
- 3).  $q = 67$ ;
- 4).  $q = 83$ ;
- 5).  $q = 41$ .

Задание № 19

Найти минимальный многочлен элемента  $\beta$  в  $\mathbb{Z}_p[x]$ , если  $\alpha$  – корень неприводимого многочлена  $m(x)$  из кольца  $\mathbb{Z}_p[x]$  :

- 1).  $\beta = \alpha + 1, \quad m(x) = x^3 + x + 1, \quad p = 2$ ;
- 2).  $\beta = \alpha^2 + 1, \quad m(x) = x^3 + x + 1, \quad p = 2$ ;
- 3).  $\beta = \alpha^2 + \alpha, \quad m(x) = x^3 + x + 1, \quad p = 2$ ;
- 4).  $\beta = \alpha + 1, \quad m(x) = x^3 + 2x + 1, \quad p = 3$ ;
- 5).  $\beta = \alpha^2 + 1, \quad m(x) = x^3 + 2x + 1, \quad p = 3$ ;
- 6).  $\beta = \alpha + 2, \quad m(x) = x^3 + 2x + 1, \quad p = 3$ ;
- 7).  $\beta = \alpha^2 + \alpha, \quad m(x) = x^3 + 2x + 1, \quad p = 3$ .

## Задание № 20

Разложить в кольце  $\mathbb{Z}_p[x]$  многочлен на неприводимые множители:

- 1).  $x^{2^4} - x$ ,  $p = 2$ ,  $GF(2^4) \equiv \mathbb{Z}_2[x]/(x^4 + x + 1)$ ;
- 2).  $x^{3^3} - x$ ,  $p = 3$ ,  $GF(3^3) \equiv \mathbb{Z}_3[x]/(x^3 + 2x + 1)$ ;
- 3).  $x^{2^5} - x$ ,  $p = 2$ ,  $GF(2^5) \equiv \mathbb{Z}_2[x]/(x^5 + x^3 + 1)$ ;
- 4).  $x^{2^6} - x$ ,  $p = 2$ ,  $GF(2^6) \equiv \mathbb{Z}_2[x]/(x^6 + x^5 + 1)$ ;
- 5).  $x^{5^2} - x$ ,  $p = 5$ ,  $GF(5^2) \equiv \mathbb{Z}_5[x]/(x^2 + x + 2)$ ;
- 6).  $x^{3^4} - x$ ,  $p = 3$ ,  $GF(3^4) \equiv \mathbb{Z}_3[x]/(x^4 + 2x^3 + x + 1)$ .

### Ответы и указания

1. 1). -74; 2). 6; 3). 4; 4). 16; 5). 9.
2. 1).  $y^4 + 8y^3 + 21y^2 + 22y + 13$ ; 2).  $y^3 + 2y^2 + y$ ; 3).  $y^5 + 3y^3 + 4y^2 + 4y + 4$ ;  
4).  $y^4 + 2y^3 + 4y^2 - y + 1$ ; 5).  $y^5 - 4y^4 + 10y^3 + 2y^2 + 10y - 5$ ; 6).  $y^4 + 4y^3 + 8y^2 + 5y + 6$ ;  
7).  $y^5 - 10y^4 + 43y^3 - 100y^2 + 128y - 73$ .
3. 1).  $24x^2 + 24 = (x - 5)f(x) + (6 - x)g(x)$ ; 2).  $x + 2 = (3x + 3)f(x) + (4x^2 + 4)g(x)$ ; 3).  $-x^2 + 1 = f(x) - g(x)$ ; 4).  $4x^2 + 4x + 9 = (3x + 1)f(x) + (-3x^2 + 2x + 2)g(x)$ ; 5).  $-x - 1 = (-1 - 2x)f(x) + (2x^2 - 5x - 2)g(x)$ ;  
6).  $\frac{32}{9}x + \frac{32}{9} = (-\frac{4}{9}x^2 - \frac{20}{27}x + \frac{40}{27})f(x) + (\frac{4}{9}x^2 + \frac{44}{27}x + \frac{12}{27})g(x)$ ;  
7).  $8x^2 + 8x - 3 = f(x) + (-x - 5)g(x)$ ; 8).  $x - 2 = (x - 2)f(x) + (-x^2 + 2x + 1)g(x)$ ; 9).  $-5x + 3 = (2x^2 - x - 2)f(x) + (-2x^3 - x^2 + 5x + 4)g(x)$ .
4. 1).  $x^4 - 2x^3 + x^2 + 3x - 5$ ; 2).  $x^3 + 2x^2 + 3x + 1$ ; 3).  $x^3 - 5x^2 + 6x + 2$ ;  
4).  $x^4 - 2x^3 + x^2 + 1$ ; 5).  $7x^4 - 2x^2 - x + 5$ ; 6).  $x^4 - 2x^3 + 3x - 1$ ;  
7).  $x^5 + 2x^4 - x^2 + 2$ ; 8).  $x^4 - 5x^3 + 3x^2 + x + 5$ ; 9).  $x^5 - 3x^4 + 2x^2 + x + 7$ ;  
10).  $x^5 - 3x^4 + 2x^3 - 5x^2 + 6x - 11$ .
5. 1).  $x^4 - 2x^3 + 3x - 1$ ; 2).  $x^5 + 2x^4 - x^2 + 2$ ; 3).  $x^4 - 5x^3 + 3x^2 + x + 5$ ;  
4).  $x^5 - 3x^4 + 2x^2 + x + 7$ ; 5).  $x^5 - 3x^4 + 2x^3 - 5x^2 + 6x - 11$ ; 6).  $x^4 - 2x^3 + x^2 + 3x - 5$ ;  
7).  $x^3 + 2x^2 + 3x + 1$ ; 8).  $x^3 - 5x^2 + 6x + 2$ ; 9).  $x^4 - 2x^3 + x^2 + 1$ ; 10).  $7x^4 - 2x^2 - x + 5$ .
6. 1).  $3x^4 + 2x^3 + 3x^2 - 3x + 2$ ; 2).  $6x^8 + 3x^7 - x^6 + 2x^5 - 2x^4 + 2x^3 - 2x^2 - 6x + 4$ ;  
3).  $x^6 + 4x^5 + 7x^4 - 5x^3 + 4x^2 + 6x + 7$ ; 4).  $x^6 + 5x^5 + 12x^3 + 15x^2 + 6x + 14$ .
7. 1).  $28x^5 + 45x^4 + 59x^3 + 47x^2 + 27x + 10$ ; 2).  $112x^6 + 264x^5 + 503x^4 + 528x^3 + 404x^2 + 180x + 25$ ; 3).  $10x^4 + 17x^3 + 6x^2 + 11x - 4$ ; 4).  $2x^7 + 7x^6 + 27x^5 + 51x^4 + 102x^3 + 169x^2 + 177x + 105$ .
8. 1).  $x^3 + 2x^2 + x + 3$ ; 2).  $x^3 - 4x^2 + 2x + 3$ ; 3).  $x^3 + 3x^2 + 2x + 4$ ;  
4).  $x^4 + 5x^3 + 2x + 3$ ; 5).  $x^3 + 2x^2 + 3x - 2$ ; 6).  $2x^3 + 5x^2 + 4x - 8$ .
9. 1).  $3(x - 2)$ ; 2).  $2(x + 3)$ ; 3).  $3(x - 1)$ ; 4).  $2(x^2 + 1)$ ; 5).  $2(x^2 + x + 1)$ .
10. 1).  $(x - 1 - i)(x - 1 + i)(x + 1 + i)(x + 1 - i)$ ;  
2).  $\left(x + 1 - \sqrt{\frac{\sqrt{2}+1}{2}} - i\sqrt{\frac{\sqrt{2}-1}{2}}\right) \left(x + 1 - \sqrt{\frac{\sqrt{2}+1}{2}} + i\sqrt{\frac{\sqrt{2}-1}{2}}\right)$ .

- $\left(x + 1 + \sqrt{\frac{\sqrt{2}+1}{2}} + i\sqrt{\frac{\sqrt{2}-1}{2}}\right) \left(x + 1 + \sqrt{\frac{\sqrt{2}+1}{2}} - i\sqrt{\frac{\sqrt{2}-1}{2}}\right);$   
 3).  $\left(x^2 + 2x + 1 + \sqrt{2} - 2(x+1)\sqrt{\frac{\sqrt{2}+1}{2}}\right) \left(x^2 + 2x + 1 + \sqrt{2} + 2(x+1)\sqrt{\frac{\sqrt{2}+1}{2}}\right);$   
 4).  $(x - \sqrt{3} - \sqrt{2})(x + \sqrt{3} + \sqrt{2})(x - \sqrt{3} + \sqrt{2})(x + \sqrt{3} - \sqrt{2});$   
 5).  $(x^2 + 2x + 2)(x^2 - 2x + 2);$  6).  $(x^2 + 3)(x^2 + 3x + 3)(x^2 - 3x + 3);$   
 7).  $(x^2 + 3x + 5)(x^2 + 4x + 1);$  8).  $(x^2 + 3x + 1)(x^2 + 4x + 5);$   
 9).  $(x^2 + 2x + 3)(x^2 + x + 2);$  10). неприводим; 11).  $(x + 1)^4;$   
 12).  $(x^2 + 2x + 2)(x^2 - 2x + 2);$  13).  $(x^2 + 2)(x^2 + 3);$  14).  $(x - 2)(x + 2)(x - 8)(x + 8).$

11. 1) неприводим; 2) неприводим; 3) неприводим; 4) неприводим;  
 5) неприводим; 6) неприводим.

12. 1). 9; 2). 18; 3). 30; 4). 18; 5). 48; 6). 116; 7). 150; 8). 2580.

13. 1).  $x^5 + x^3 + 1; x^5 + x^2 + 1; x^5 + x^4 + x^3 + x^2 + 1; x^5 + x^4 + x^3 + x + 1;$   
 $x^5 + x^4 + x^2 + x + 1; x^5 + x^3 + x^2 + x + 1;$   
 2).  $x^3 + 2x^2 + 1; x^3 + x^2 + 2; x^3 + 2x + 1; x^3 + 2x + 2; x^3 + 2x^2 + 2x + 2;$   
 $x^3 + 2x^2 + x + 1; x^3 + x^2 + 2x + 1; x^3 + x^2 + x + 2;$   
 3).  $x^2 - x + 1; x^2 + x + 1; x^2 - 2; x^2 + 2; x^2 + x + 2; x^2 + 3x + 4; x^2 + 2x + 3;$   
 $x^2 + 4x + 2; x^2 + 2x + 4; x^2 + 3x + 3.$

14. 1).  $x^2;$  2).  $x^3 + 2x^2;$  3).  $-x^3 + 2x^2 - x + 1;$  4).  $x^4 - x^2 + x - 1;$   
 5).  $x^4 + x + 1.$

15. 1).  $x^3 + x + 1; x^3 + 2x + 1; x^3 + x^2 + 1; x^3 + x^2 + 3x + 1; x^3 + x^2 + 4x + 1;$   
 $x^3 + 2x^2 + 1; x^3 + 3x^2 + x + 1; x^3 + 3x^2 + 4x + 1; x^3 + 4x^2 + x + 1; x^3 + 4x^2 + 3x + 1;$   
 2).  $x^3 + x^2 + 1; x^3 + x^2 + 2; x^3 + 2x^2 + 1; x^3 + 2x^2 + 3; x^3 + 3x^2 + 2; x^3 + 3x^2 + 4;$   
 $x^3 + 4x^2 + 3; x^3 + 4x^2 + 4;$   
 3).  $x^3 + x + 1; x^3 + x + 4; x^3 + 2x + 1; x^3 + 2x + 4; x^3 + 3x + 2; x^3 + 3x + 3;$   
 $x^3 + 4x + 2; x^3 + 4x + 3;$   
 4).  $x^3 + x + 1; x^3 + 2x + 1; x^3 + 4x + 1; x^3 + x^2 + 1; x^3 + x^2 + 3x + 1; x^3 + x^2 + 5x + 1;$   
 $x^3 + 2x^2 + 1; x^3 + 2x^2 + 5x + 1; x^3 + 2x^2 + 6x + 1; x^3 + 3x^2 + x + 1; x^3 + 3x^2 + 4x + 1;$   
 $x^3 + 4x^2 + 1; x^3 + 4x^2 + 3x + 1; x^3 + 4x^2 + 6x + 1; x^3 + 5x^2 + x + 1; x^3 + 6x^2 + 2x + 1;$   
 $x^3 + 6x^2 + 4x + 1;$   
 5).  $x^3 + 2; x^3 + 3; x^3 + 4; x^3 + 5; x^3 + x^2 + 1; x^3 + x^2 + 3; x^3 + 2x^2 + 1;$   
 $x^3 + 2x^2 + 3; x^3 + 3x^2 + 4; x^3 + 3x^2 + 6; x^3 + 4x^2 + 1; x^3 + 4x^2 + 3; x^3 + 5x^2 + 4;$   
 $x^3 + 5x^2 + 6; x^3 + 6x^2 + 4; x^3 + 6x^2 + 6.$

16.

1).	0		0		(0, 0, 0)	$\alpha^3$		$\alpha + 1$		(0, 1, 1)
	1		1		(0, 0, 1)	$\alpha^4$		$\alpha^2 + \alpha$		(1, 1, 0)
	$\alpha$		$\alpha$		(0, 1, 0)	$\alpha^5$		$\alpha^2 + \alpha + 1$		(1, 1, 1)
	$\alpha^2$		$\alpha^2$		(1, 0, 0)	$\alpha^6$		$\alpha^2 + 1$		(1, 0, 1)

$$\begin{array}{llll}
2). & 0 & | & 0 & | & (0,0) & \alpha^2 & | & \alpha + 1 & | & (1,1) & \alpha^5 & | & 2\alpha & | & (2,0) \\
& 1 & | & 1 & | & (0,1) & \alpha^3 & | & 2\alpha + 1 & | & (2,1) & \alpha^6 & | & 2\alpha + 2 & | & (2,2) \\
& \alpha & | & \alpha & | & (1,0) & \alpha^4 & | & 2 & | & (0,2) & \alpha^7 & | & \alpha + 2 & | & (1,2)
\end{array}$$

$$\begin{array}{llll}
3). & 0 & | & 0 & | & (0,0,0) & \alpha^2 & | & \alpha^2 & | & (1,0,0) & \alpha^5 & | & \alpha + 1 & | & (0,1,1) \\
& 1 & | & 1 & | & (0,0,1) & \alpha^3 & | & \alpha^2 + 1 & | & (1,0,1) & \alpha^6 & | & \alpha^2 + \alpha & | & (1,1,0) \\
& \alpha & | & \alpha & | & (0,1,0) & \alpha^4 & | & \alpha^2 + \alpha + 1 & | & (1,1,1)
\end{array}$$

$$\begin{array}{llll}
4). & 0 & | & 0 & | & (0,0,0) & \alpha^{13} & | & 2 & | & (0,0,2) \\
& 1 & | & 1 & | & (0,0,1) & \alpha^{14} & | & 2\alpha & | & (0,2,0) \\
& \alpha & | & \alpha & | & (0,1,0) & \alpha^{15} & | & 2\alpha^2 & | & (2,0,0) \\
& \alpha^2 & | & \alpha^2 & | & (1,0,0) & \alpha^{16} & | & 2\alpha^2 + \alpha + 1 & | & (2,1,1) \\
& \alpha^3 & | & \alpha^2 + 2\alpha + 2 & | & (1,2,2) & \alpha^{17} & | & 2\alpha + 1 & | & (0,2,1) \\
& \alpha^4 & | & \alpha + 2 & | & (0,1,2) & \alpha^{18} & | & 2\alpha^2 + \alpha & | & (2,1,0) \\
& \alpha^5 & | & \alpha^2 + 2\alpha & | & (1,2,0) & \alpha^{19} & | & \alpha + 1 & | & (0,1,1) \\
& \alpha^6 & | & 2\alpha + 2 & | & (0,2,2) & \alpha^{20} & | & \alpha^2 + \alpha & | & (1,1,0) \\
& \alpha^7 & | & 2\alpha^2 + 2\alpha & | & (2,2,0) & \alpha^{21} & | & 2\alpha^2 + 2\alpha + 2 & | & (2,2,2) \\
& \alpha^8 & | & \alpha^2 + \alpha + 1 & | & (1,1,1) & \alpha^{22} & | & \alpha^2 + 1 & | & (1,0,1) \\
& \alpha^9 & | & 2\alpha^2 + 2 & | & (2,0,2) & \alpha^{23} & | & \alpha^2 + 2 & | & (1,0,2) \\
& \alpha^{10} & | & 2\alpha^2 + 1 & | & (2,0,1) & \alpha^{24} & | & \alpha^2 + \alpha + 2 & | & (1,1,2) \\
& \alpha^{11} & | & 2\alpha^2 + 2\alpha + 1 & | & (2,2,1) & \alpha^{25} & | & 2\alpha^2 + \alpha + 2 & | & (2,1,2) \\
& \alpha^{12} & | & \alpha^2 + 2\alpha + 1 & | & (1,2,1)
\end{array}$$

$$\begin{array}{llll}
5). & 0 & | & 0 & | & (0,0,0) & \alpha^8 & | & \alpha^2 + \alpha + 2 & | & (1,1,2) \\
& 1 & | & 1 & | & (0,0,1) & \alpha^9 & | & 2\alpha^2 + 2\alpha + 2 & | & (2,2,2) \\
& \alpha & | & \alpha & | & (0,1,0) & \alpha^{10} & | & \alpha^2 + 2\alpha + 1 & | & (1,2,1) \\
& \alpha^2 & | & \alpha^2 & | & (1,0,0) & \alpha^{11} & | & \alpha + 2 & | & (0,1,2) \\
& \alpha^3 & | & \alpha^2 + 2 & | & (1,0,2) & \alpha^{12} & | & \alpha^2 + 2\alpha & | & (1,2,0) \\
& \alpha^4 & | & \alpha^2 + 2\alpha + 2 & | & (1,2,2) & \alpha^{13} & | & 2 & | & (0,0,2) \\
& \alpha^5 & | & 2\alpha + 2 & | & (0,2,2) & \alpha^{14} & | & 2\alpha & | & (0,2,0) \\
& \alpha^6 & | & 2\alpha^2 + 2\alpha & | & (2,2,0) & \alpha^{15} & | & 2\alpha^2 & | & (2,0,0) \\
& \alpha^7 & | & \alpha^2 + 1 & | & (1,0,1) & \alpha^{16} & | & 2\alpha^2 + 1 & | & (2,0,1)
\end{array}$$

$\alpha^{17} \mid 2\alpha^2 + \alpha + 1$	$\mid (2, 1, 1)$	$\alpha^{22} \mid \alpha^2 + \alpha + 1$	$\mid (1, 1, 1)$
$\alpha^{18} \mid \alpha + 1$	$\mid (0, 1, 1)$	$\alpha^{23} \mid 2\alpha^2 + \alpha + 2$	$\mid (2, 1, 2)$
$\alpha^{19} \mid \alpha^2 + \alpha$	$\mid (1, 1, 0)$	$\alpha^{24} \mid 2\alpha + 1$	$\mid (0, 2, 1)$
$\alpha^{20} \mid 2\alpha^2 + 2$	$\mid (2, 0, 2)$	$\alpha^{25} \mid 2\alpha^2 + \alpha$	$\mid (2, 1, 0)$
$\alpha^{21} \mid 2\alpha^2 + 2\alpha + 1$	$\mid (2, 2, 1)$		

- 17.** 1).  $s_1(x) = 1$ ,  $s_2(x) = x + 1$ ,  $s_3(x) = x - 1$ ;  
 2).  $s_1(x) = x - 1$ ,  $s_2(x) = (x + 1)(x - 2)$ ,  $s_3(x) = x + 2$ ;  
 3).  $s_1(x) = (x + 1)(x^2 + x + 1)$ ,  $s_2(x) = x - 1$ ;  
 4).  $s_1(x) = x + 2$ ,  $s_2(x) = x - 1$ ,  $s_3(x) = x + 1$ ;  
 5).  $s_1(x) = x + 3$ ,  $s_2(x) = (x - 1)(x - 2)$ ,  $s_3(x) = x + 1$ .

**18.** 1). 3; 2). 2; 3). 2; 4). 2; 5). 7.

- 19.** 1).  $x^3 + x^2 + 1$ ; 2).  $x^3 + x^2 + 1$ ; 3).  $x^3 + x + 1$ ; 4).  $x^3 + 2x + 1$ ;  
 5).  $x^3 + x^2 + 2x + 1$ ; 6).  $x^3 + 2x + 1$ ; 7).  $x^3 + x^2 + 2$ .

- 20.** 1).  $x(x - 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$ ;  
 2).  $x(x + 1)(x - 1)(x^3 + 2x + 1)(x^3 + x^2 + x - 1)(x^3 + x^2 - 1)(x^3 - x^2 + 1)(x^3 - x^2 + x + 1)(x^3 - x^2 + 2x - 1)(x^3 + x^2 + 2x + 1)(x^3 + 2x - 1)$ ;  
 3).  $x(x - 1)(x^5 + x^3 + 1)(x^5 + x^2 + 1)(x^5 + x^3 + x^2 + x + 1)(x^5 + x^4 + x^3 + x + 1)(x^5 + x^4 + x^3 + x^2 + 1)(x^5 + x^4 + x^2 + x + 1)$ ;  
 4).  $x(x + 1)(x^2 + x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)(x^6 + x^5 + 1)(x^6 + x^3 + 1)(x^6 + x^5 + x^4 + x^2 + 1)(x^6 + x^5 + x^4 + x + 1)(x^6 + x^4 + x^3 + x + 1)(x^6 + x^4 + x^2 + x + 1)(x^6 + x^5 + x^2 + x + 1)(x^6 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1)$ ;  
 5).  $x(x + 1)(x - 1)(x + 2)(x - 2)(x^2 - x + 1)(x^2 + x + 1)(x^2 - 2)(x^2 + 2)(x^2 + x + 2)(x^2 + 3x + 4)(x^2 + 2x + 3)(x^2 + 4x + 2)(x^2 + 2x + 4)(x^2 + 3x + 3)$ ;  
 6).  $x(x - 1)(x - 2)(x^2 - 2x - 1)(x^2 - x + 1)(x^2 - x + 2)(x^4 + x + 2)(x^4 + x^2 + 2x + 1)(x^4 + 2x^3 + x + 1)(x^4 + x^2 + 2)(x^4 + x^3 + 2x^2 + 2x + 2)(x^4 + 2x^3 + x^2 + 2x + 1)(x^4 + 2x^3 + x^2 + x + 2)(x^4 + x^3 + 2)(x^4 + x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + x^2 + 2x + 2)(x^4 + x^3 + x^2 + 1)(x^4 + 2x^3 + 2x^2 + x + 2)(x^4 + 2x^2 + 2)(x^4 + 2x^3 + x^2 + 1)(x^4 + 2x + 2)(x^4 + x^3 + 2x + 1)(x^4 + 2x^3 + 2)$ .

# Задачи для самостоятельного решения

## Задание № 1

Используя схему Горнера, вычислить  $f(x_0)$ . Вычисления проводятся в кольце  $K[x]$  :

- 1).  $f(x) = x^6 + 3x^5 + 9x^3 + 8x^2 + 10x - 6$ ,  $x_0 = 4$ ,  $K = \mathbb{Z}_{11}$ ;
- 2).  $f(x) = x^5 + 2x^4 + x^3 + 2x^2 + 2x + 1$ ,  $x_0 = 2$ ,  $K = \mathbb{Z}_3$ ;
- 3).  $f(x) = x^6 + 10x^5 + 7x^3 + 6x^2 + 5x + 4$ ,  $x_0 = 9$ ,  $K = \mathbb{Z}_{17}$ ;
- 4).  $f(x) = x^6 + 11x^5 + 4x^4 + 8x^3 + 2x + 12$ ,  $x_0 = 3$ ,  $K = \mathbb{Z}_{13}$ ;
- 5).  $f(x) = x^5 + 11x^4 + 5x^3 + 9x^2 + 7x + 18$ ,  $x_0 = 3$ ,  $K = \mathbb{Z}_{19}$ ;
- 6).  $f(x) = x^6 + 3x^5 + 12x^4 + 15x^3 + 8x + 12$ ,  $x_0 = 5$ ,  $K = \mathbb{Z}_{23}$ ;
- 7).  $f(x) = x^5 + 5x^4 + 4x^3 + 2x^2 + 3x + 4$ ,  $x_0 = -2$ ,  $K = \mathbb{Z}_7$ ;
- 8).  $f(x) = x^5 + 7x^4 - 3x^2 + 11x - 5$ ,  $x_0 = 4$ ,  $K = \mathbb{Z}$ ;
- 9).  $f(x) = x^5 + 10x^4 + 4x^3 + 5x^2 + 9x + 8$ ,  $x_0 = 7$ ,  $K = \mathbb{Z}_{13}$ ;
- 10).  $f(x) = x^7 + 2x^5 + x^4 + 2x^3 + x + 2$ ,  $x_0 = 2$ ,  $K = \mathbb{Z}_3$ ;
- 11).  $f(x) = x^5 + 9x^4 + 10x^3 + 5x^2 + 6x + 8$ ,  $x_0 = 7$ ,  $K = \mathbb{Z}_{11}$ ;
- 12).  $f(x) = x^5 + 8x^4 + 13x^3 + 11x^2 + 6x + 7$ ,  $x_0 = 6$ ,  $K = \mathbb{Z}_{17}$ ;
- 13).  $f(x) = x^6 - 11x^5 + 13x^4 - 5x^3 + 4x^2 - 3x + 12$ ,  
 $x_0 = 1$ ,  $K = \mathbb{Z}$ ;
- 14).  $f(x) = x^6 + 7x^5 + 15x^4 + 6x^3 + 8x^2 + 11x + 7$ ,  
 $x_0 = 8$ ,  $K = \mathbb{Z}_{19}$ ;
- 15).  $f(x) = x^5 + 4x^4 + 2x^3 + 4x^2 + 3x + 1$ ,  $x_0 = 4$ ,  $K = \mathbb{Z}_5$ ;
- 16).  $f(x) = x^5 - 8x^4 + 14x^3 - 11x^2 - 2x + 9$ ,  $x_0 = 2$ ,  $K = \mathbb{Z}$ ;
- 17).  $f(x) = x^6 - 2x^5 + 4x^4 + 3x^2 + 4x + 2$ ,  $x_0 = 3$ ,  $K = \mathbb{Z}_7$ ;
- 18).  $f(x) = x^6 + 12x^5 + 9x^4 + 6x^3 + 5x^2 + 11x + 2$ ,  
 $x_0 = 4$ ,  $K = \mathbb{Z}_{13}$ ;
- 19).  $f(x) = x^5 + 13x^4 + 9x^3 + 21x^2 + 3x + 19$ ,  $x_0 = 13$ ,  
 $K = \mathbb{Z}_{23}$ ;
- 20).  $f(x) = x^6 + 13x^4 - 10x^3 + 7x^2 - 8x + 6$ ,  $x_0 = -1$ ,  $K = \mathbb{Z}$ ;
- 21).  $f(x) = x^5 + 2x^4 - 3x^3 + 2x^2 - 10$ ,  $x_0 = -2$ ,  $K = \mathbb{Z}$ ;
- 22).  $f(x) = x^5 + 3x^4 + 2x^3 + 3x^2 + 4x + 1$ ,  $x_0 = 2$ ,  $K = \mathbb{Z}_5$ ;
- 23).  $f(x) = x^5 + 8x^4 - 9x^3 + 10x^2 - 7$ ,  $x_0 = 5$ ,  $K = \mathbb{Z}_{11}$ ;
- 24).  $f(x) = x^6 + 2x^5 + x^4 + 2x^3 + x^2 + 2x + 1$ ,  $x_0 = 1$ ,  $K = \mathbb{Z}_3$ ;
- 25).  $f(x) = x^5 + 15x^4 + 11x^3 + 4x^2 + 8x + 16$ ,  $x_0 = 2$ ,  $K = \mathbb{Z}_{17}$ ;
- 26).  $f(x) = x^6 + 8x^5 + 17x^4 + 4x^3 + 9x + 3$ ,  $x_0 = 11$ ,  $K = \mathbb{Z}_{19}$ ;
- 27).  $f(x) = x^5 + 18x^4 + 11x^3 + 8x^2 + 5x + 21$ ,  $x_0 = 7$ ,  $K = \mathbb{Z}_{23}$ ;
- 28).  $f(x) = x^6 + 6x^5 - 3x^3 + 5x^2 - 2x + 5$ ,  $x_0 = -1$ ,  $K = \mathbb{Z}_7$ ;
- 29).  $f(x) = x^6 - 3x^4 + 5x^3 + 10x^2 - 12x + 3$ ,  $x_0 = 3$ ,  $K = \mathbb{Z}$ ;
- 30).  $f(x) = x^6 + 4x^5 + x^3 + 2x^2 + 3x + 4$ ,  $x_0 = 3$ ,  $K = \mathbb{Z}_5$ .

## Задание № 2

Используя схему Горнера, найти  $f(y + y_0)$  в кольце  $K[x]$  :

- 1).  $f(x) = x^5 + 2x^4 - 3x^3 + 2x^2 - 10, \quad y_0 = -2, \quad K = \mathbb{Z};$
- 2).  $f(x) = x^5 + 3x^4 + 2x^3 + 3x^2 + 4x + 1, \quad y_0 = 2, \quad K = \mathbb{Z}_5;$
- 3).  $f(x) = x^5 + 8x^4 - 9x^3 + 10x^2 - 7, \quad y_0 = 5, \quad K = \mathbb{Z}_{11};$
- 4).  $f(x) = x^6 + 2x^5 + x^4 + 2x^3 + x^2 + 2x + 1, \quad y_0 = 1, \quad K = \mathbb{Z}_3;$
- 5).  $f(x) = x^5 + 15x^4 + 11x^3 + 4x^2 + 8x + 16, \quad y_0 = 2, \quad K = \mathbb{Z}_{17};$
- 6).  $f(x) = x^6 + 8x^5 + 17x^4 + 4x^3 + 9x + 3, \quad y_0 = 11, \quad K = \mathbb{Z}_{19};$
- 7).  $f(x) = x^5 + 18x^4 + 11x^3 + 8x^2 + 5x + 21, \quad y_0 = 7, \quad K = \mathbb{Z}_{23};$
- 8).  $f(x) = x^6 + 6x^5 - 3x^3 + 4x^2 - 2x + 5, \quad y_0 = -1, \quad K = \mathbb{Z}_7;$
- 9).  $f(x) = x^6 - 3x^4 + 5x^3 + 10x^2 - 12x + 3, \quad y_0 = 3, \quad K = \mathbb{Z};$
- 10).  $f(x) = x^6 + 4x^5 + x^3 + 2x^2 + 3x + 4, \quad y_0 = 3, \quad K = \mathbb{Z}_5;$
- 11).  $f(x) = x^6 + 3x^5 + 9x^3 + 8x^2 + 10x - 6, \quad y_0 = 4, \quad K = \mathbb{Z}_{11};$
- 12).  $f(x) = x^5 + 2x^4 + x^3 + 2x^2 + 2x + 1, \quad y_0 = 2, \quad K = \mathbb{Z}_3;$
- 13).  $f(x) = x^6 + 10x^5 + 7x^3 + 6x^2 + 5x + 4, \quad y_0 = 9, \quad K = \mathbb{Z}_{17};$
- 14).  $f(x) = x^6 + 11x^5 + 4x^4 + 8x^3 + 2x + 12, \quad y_0 = 3, \quad K = \mathbb{Z}_{13};$
- 15).  $f(x) = x^5 + 11x^4 + 5x^3 + 9x^2 + 7x + 18, \quad y_0 = 3, \quad K = \mathbb{Z}_{19};$
- 16).  $f(x) = x^6 + 3x^5 + 12x^4 + 15x^3 + 8x + 12, \quad y_0 = 5, \quad K = \mathbb{Z}_{23};$
- 17).  $f(x) = x^5 + 5x^4 + 4x^3 + 2x^2 + 3x + 4, \quad y_0 = -2, \quad K = \mathbb{Z}_7;$
- 18).  $f(x) = x^5 + 7x^4 - 3x^2 + 11x - 5, \quad y_0 = 4, \quad K = \mathbb{Z};$
- 19).  $f(x) = x^5 + 10x^4 + 4x^3 + 5x^2 + 9x + 8, \quad y_0 = 7, \quad K = \mathbb{Z}_{13};$
- 20).  $f(x) = x^7 + 2x^5 + x^4 + 2x^3 + x + 2, \quad y_0 = 2, \quad K = \mathbb{Z}_3;$
- 21).  $f(x) = x^5 + 9x^4 + 10x^3 + 5x^2 + 6x + 8, \quad y_0 = 7, \quad K = \mathbb{Z}_{11};$
- 22).  $f(x) = x^5 + 8x^4 + 13x^3 + 11x^2 + 6x + 7, \quad y_0 = 6, \quad K = \mathbb{Z}_{17};$
- 23).  $f(x) = x^6 - 11x^5 + 13x^4 - 5x^3 + 4x^2 - 3x + 12,$   
 $y_0 = 1, \quad K = \mathbb{Z};$
- 24).  $f(x) = x^6 + 7x^5 + 15x^4 + 6x^3 + 8x^2 + 11x + 7,$   
 $y_0 = 8, \quad K = \mathbb{Z}_{19};$
- 25).  $f(x) = x^5 + 4x^4 + 2x^3 + 4x^2 + 3x + 1, \quad y_0 = 4, \quad K = \mathbb{Z}_5;$
- 26).  $f(x) = x^5 - 8x^4 + 14x^3 - 11x^2 - 2x + 9, \quad y_0 = 2, \quad K = \mathbb{Z};$
- 27).  $f(x) = x^6 - 2x^5 + 4x^4 + 3x^2 + 4x + 2, \quad y_0 = 3, \quad K = \mathbb{Z}_7;$
- 28).  $f(x) = x^6 + 12x^5 + 9x^4 + 6x^3 + 5x^2 + 11x + 2,$   
 $y_0 = 4, \quad K = \mathbb{Z}_{13};$
- 29).  $f(x) = x^5 + 13x^4 + 9x^3 + 21x^2 + 3x + 19, \quad y_0 = 13,$   
 $K = \mathbb{Z}_{23};$
- 30).  $f(x) = x^6 + 13x^4 - 10x^3 + 7x^2 - 8x + 6, \quad y_0 = -1, \quad K = \mathbb{Z}.$

### Задание № 3

Пользуясь интерполяционной формулой Лагранжа, восстановить многочлен  $f(x)$  в кольце  $K[x]$  по таблице его значений  $f(a_i) = b_i$  ( $i = 0, 1, \dots, n$ ):

- 1).  $\begin{array}{c|c|c|c|c|c} a_i & 1 & 3 & 5 & 7 & 9 \\ \hline b_i & 3 & 0 & 16 & 8 & 13 \end{array} \quad K = \mathbb{Z}_{19};$
- 2).  $\begin{array}{c|c|c|c|c|c} a_i & -3 & -2 & -1 & 2 & 3 \\ \hline b_i & -11 & -19 & -7 & 29 & 121 \end{array} \quad K = \mathbb{Q};$
- 3).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 1 & 2 & 3 & 4 \\ \hline b_i & 7 & 9 & 10 & 10 & 16 \end{array} \quad K = \mathbb{Z}_{17};$
- 4).  $\begin{array}{c|c|c|c|c|c} a_i & 1 & 2 & 3 & 5 & 6 \\ \hline b_i & 5 & 6 & 2 & 6 & 0 \end{array} \quad K = \mathbb{Z}_7;$
- 5).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 1 & 2 & 3 & 4 \\ \hline b_i & 1 & 2 & 1 & 1 & 4 \end{array} \quad K = \mathbb{Z}_5;$
- 6).  $\begin{array}{c|c|c|c|c|c} a_i & -3 & -2 & -1 & 2 & 3 \\ \hline b_i & -47 & -28 & -5 & 28 & 127 \end{array} \quad K = \mathbb{Q};$
- 7).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 1 & 2 & 4 & 7 \\ \hline b_i & 2 & 4 & 2 & 6 & 0 \end{array} \quad K = \mathbb{Z}_{11};$
- 8).  $\begin{array}{c|c|c|c|c|c} a_i & 1 & 2 & 3 & 5 & 7 \\ \hline b_i & 0 & 9 & 11 & 6 & 2 \end{array} \quad K = \mathbb{Z}_{13};$
- 9).  $\begin{array}{c|c|c|c|c|c} a_i & 2 & 3 & 6 & 7 & 10 \\ \hline b_i & 17 & 10 & 0 & 14 & 9 \end{array} \quad K = \mathbb{Z}_{19};$
- 10).  $\begin{array}{c|c|c|c|c|c} a_i & 1 & 3 & 5 & 6 & 8 \\ \hline b_i & 16 & 10 & 0 & 13 & 1 \end{array} \quad K = \mathbb{Z}_{17};$
- 11).  $\begin{array}{c|c|c|c|c|c} a_i & -3 & -1 & 1 & 2 & 4 \\ \hline b_i & 118 & -6 & -2 & 3 & 139 \end{array} \quad K = \mathbb{Q};$
- 12).  $\begin{array}{c|c|c|c|c|c} a_i & 1 & 3 & 5 & 6 & 8 \\ \hline b_i & 5 & 8 & 7 & 10 & 1 \end{array} \quad K = \mathbb{Z}_{11};$
- 13).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 1 & 2 & 3 & 4 \\ \hline b_i & 2 & 2 & 1 & 1 & 3 \end{array} \quad K = \mathbb{Z}_5;$
- 14).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 2 & 3 & 4 & 5 \\ \hline b_i & 4 & 6 & 4 & 5 & 6 \end{array} \quad K = \mathbb{Z}_7;$
- 15).  $\begin{array}{c|c|c|c|c|c} a_i & 2 & 4 & 6 & 7 & 8 \\ \hline b_i & 1 & 5 & 0 & 2 & 2 \end{array} \quad K = \mathbb{Z}_{13};$



- 16).  $\frac{a_i \mid -5 \mid -3 \mid -1 \mid 1 \mid 4}{b_i \mid 337 \mid -9 \mid -11 \mid -5 \mid 229} \quad K = \mathbb{Q};$
- 17).  $\frac{a_i \mid 2 \mid 4 \mid 6 \mid 8 \mid 11}{b_i \mid 7 \mid 3 \mid 7 \mid 1 \mid 16} \quad K = \mathbb{Z}_{17};$
- 18).  $\frac{a_i \mid 1 \mid 4 \mid 6 \mid 9 \mid 12}{b_i \mid 11 \mid 16 \mid 17 \mid 9 \mid 16} \quad K = \mathbb{Z}_{19};$
- 19).  $\frac{a_i \mid 2 \mid 4 \mid 6 \mid 7 \mid 9}{b_i \mid 1 \mid 10 \mid 9 \mid 9 \mid 4} \quad K = \mathbb{Z}_{11};$
- 20).  $\frac{a_i \mid 1 \mid 2 \mid 3 \mid 4 \mid 6}{b_i \mid 4 \mid 4 \mid 4 \mid 4 \mid 6} \quad K = \mathbb{Z}_7;$
- 21).  $\frac{a_i \mid -2 \mid -1 \mid 0 \mid 2 \mid 3}{b_i \mid 19 \mid 6 \mid 3 \mid 51 \mid 234} \quad K = \mathbb{Q};$
- 22).  $\frac{a_i \mid 0 \mid 1 \mid 2 \mid 3 \mid 4}{b_i \mid 1 \mid 2 \mid 4 \mid 0 \mid 1} \quad K = \mathbb{Z}_5;$
- 23).  $\frac{a_i \mid 1 \mid 3 \mid 5 \mid 9 \mid 11}{b_i \mid 8 \mid 10 \mid 9 \mid 9 \mid 7} \quad K = \mathbb{Z}_{13};$
- 24).  $\frac{a_i \mid 0 \mid 2 \mid 4 \mid 5 \mid 6}{b_i \mid 4 \mid 4 \mid 0 \mid 1 \mid 3} \quad K = \mathbb{Z}_7;$
- 25).  $\frac{a_i \mid 2 \mid 3 \mid 8 \mid 10 \mid 13}{b_i \mid 0 \mid 12 \mid 7 \mid 11 \mid 7} \quad K = \mathbb{Z}_{19};$
- 26).  $\frac{a_i \mid 0 \mid 1 \mid 2 \mid 3 \mid 4}{b_i \mid 2 \mid 4 \mid 4 \mid 0 \mid 3} \quad K = \mathbb{Z}_5;$
- 27).  $\frac{a_i \mid -3 \mid -1 \mid 1 \mid 2 \mid 4}{b_i \mid 227 \mid -1 \mid 3 \mid 17 \mid 339} \quad K = \mathbb{Q};$
- 28).  $\frac{a_i \mid 1 \mid 3 \mid 6 \mid 9 \mid 12}{b_i \mid 0 \mid 15 \mid 10 \mid 2 \mid 11} \quad K = \mathbb{Z}_{17};$
- 29).  $\frac{a_i \mid 2 \mid 4 \mid 7 \mid 9 \mid 12}{b_i \mid 10 \mid 3 \mid 3 \mid 5 \mid 12} \quad K = \mathbb{Z}_{13};$
- 30).  $\frac{a_i \mid 1 \mid 3 \mid 5 \mid 9 \mid 10}{b_i \mid 4 \mid 6 \mid 6 \mid 0 \mid 7} \quad K = \mathbb{Z}_{11}.$

## Задание № 4

Решить задачу интерполяции в кольце  $K[x]$ , используя алгоритм, основанный на китайской теореме об остатках:

- 1).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 1 & 2 & 3 & 4 \\ \hline b_i & 1 & 2 & 1 & 1 & 4 \end{array} \quad K = \mathbb{Z}_5;$
- 2).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 1 & 2 & 3 & 4 \\ \hline b_i & 7 & 9 & 10 & 10 & 16 \end{array} \quad K = \mathbb{Z}_{17};$
- 3).  $\begin{array}{c|c|c|c|c|c} a_i & 1 & 2 & 3 & 5 & 7 \\ \hline b_i & 0 & 9 & 11 & 6 & 2 \end{array} \quad K = \mathbb{Z}_{13};$
- 4).  $\begin{array}{c|c|c|c|c|c} a_i & -3 & -2 & -1 & 2 & 3 \\ \hline b_i & -11 & -19 & -7 & 29 & 121 \end{array} \quad K = \mathbb{Q};$
- 5).  $\begin{array}{c|c|c|c|c|c} a_i & 1 & 2 & 3 & 5 & 6 \\ \hline b_i & 5 & 6 & 2 & 6 & 0 \end{array} \quad K = \mathbb{Z}_7;$
- 6).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 1 & 2 & 4 & 7 \\ \hline b_i & 2 & 4 & 2 & 6 & 0 \end{array} \quad K = \mathbb{Z}_{11};$
- 7).  $\begin{array}{c|c|c|c|c|c} a_i & 1 & 3 & 5 & 7 & 9 \\ \hline b_i & 3 & 0 & 16 & 8 & 13 \end{array} \quad K = \mathbb{Z}_{19};$
- 8).  $\begin{array}{c|c|c|c|c|c} a_i & -3 & -2 & -1 & 2 & 3 \\ \hline b_i & -47 & -28 & -5 & 28 & 127 \end{array} \quad K = \mathbb{Q};$
- 9).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 1 & 2 & 3 & 4 \\ \hline b_i & 2 & 2 & 1 & 1 & 3 \end{array} \quad K = \mathbb{Z}_5;$
- 10).  $\begin{array}{c|c|c|c|c|c} a_i & 2 & 4 & 6 & 7 & 8 \\ \hline b_i & 1 & 5 & 0 & 2 & 2 \end{array} \quad K = \mathbb{Z}_{13};$
- 11).  $\begin{array}{c|c|c|c|c|c} a_i & 0 & 2 & 3 & 4 & 5 \\ \hline b_i & 4 & 6 & 4 & 5 & 6 \end{array} \quad K = \mathbb{Z}_7;$
- 12).  $\begin{array}{c|c|c|c|c|c} a_i & 1 & 3 & 5 & 6 & 8 \\ \hline b_i & 16 & 10 & 0 & 13 & 1 \end{array} \quad K = \mathbb{Z}_{17};$
- 13).  $\begin{array}{c|c|c|c|c|c} a_i & -3 & -1 & 1 & 2 & 4 \\ \hline b_i & 118 & -6 & -2 & 3 & 139 \end{array} \quad K = \mathbb{Q};$
- 14).  $\begin{array}{c|c|c|c|c|c} a_i & 2 & 3 & 6 & 7 & 10 \\ \hline b_i & 17 & 10 & 0 & 14 & 9 \end{array} \quad K = \mathbb{Z}_{19};$
- 15).  $\begin{array}{c|c|c|c|c|c} a_i & 1 & 3 & 5 & 6 & 8 \\ \hline b_i & 5 & 8 & 7 & 10 & 1 \end{array} \quad K = \mathbb{Z}_{11};$

- 16).  $\frac{a_i}{b_i} \mid \frac{0}{1} \mid \frac{1}{2} \mid \frac{2}{4} \mid \frac{3}{0} \mid \frac{4}{1}$   $K = \mathbb{Z}_5;$
- 17).  $\frac{a_i}{b_i} \mid \frac{2}{1} \mid \frac{4}{10} \mid \frac{6}{9} \mid \frac{7}{9} \mid \frac{9}{4}$   $K = \mathbb{Z}_{11};$
- 18).  $\frac{a_i}{b_i} \mid \frac{1}{4} \mid \frac{2}{4} \mid \frac{3}{4} \mid \frac{4}{4} \mid \frac{6}{6}$   $K = \mathbb{Z}_7;$
- 19).  $\frac{a_i}{b_i} \mid \frac{-5}{337} \mid \frac{-3}{-9} \mid \frac{-1}{-11} \mid \frac{1}{-5} \mid \frac{4}{229}$   $K = \mathbb{Q};$
- 20).  $\frac{a_i}{b_i} \mid \frac{2}{7} \mid \frac{4}{3} \mid \frac{6}{7} \mid \frac{8}{1} \mid \frac{11}{16}$   $K = \mathbb{Z}_{17};$
- 21).  $\frac{a_i}{b_i} \mid \frac{1}{8} \mid \frac{3}{10} \mid \frac{5}{9} \mid \frac{9}{9} \mid \frac{11}{7}$   $K = \mathbb{Z}_{13};$
- 22).  $\frac{a_i}{b_i} \mid \frac{1}{11} \mid \frac{4}{16} \mid \frac{6}{17} \mid \frac{9}{9} \mid \frac{12}{16}$   $K = \mathbb{Z}_{19};$
- 23).  $\frac{a_i}{b_i} \mid \frac{0}{4} \mid \frac{2}{4} \mid \frac{4}{0} \mid \frac{5}{1} \mid \frac{6}{3}$   $K = \mathbb{Z}_7;$
- 24).  $\frac{a_i}{b_i} \mid \frac{0}{2} \mid \frac{1}{4} \mid \frac{2}{4} \mid \frac{3}{0} \mid \frac{4}{3}$   $K = \mathbb{Z}_5;$
- 25).  $\frac{a_i}{b_i} \mid \frac{-2}{19} \mid \frac{-1}{6} \mid \frac{0}{3} \mid \frac{2}{51} \mid \frac{3}{234}$   $K = \mathbb{Q};$
- 26).  $\frac{a_i}{b_i} \mid \frac{2}{0} \mid \frac{3}{12} \mid \frac{8}{7} \mid \frac{10}{11} \mid \frac{13}{7}$   $K = \mathbb{Z}_{19};$
- 27).  $\frac{a_i}{b_i} \mid \frac{1}{0} \mid \frac{3}{15} \mid \frac{6}{10} \mid \frac{9}{2} \mid \frac{12}{11}$   $K = \mathbb{Z}_{17};$
- 28).  $\frac{a_i}{b_i} \mid \frac{1}{4} \mid \frac{3}{6} \mid \frac{5}{6} \mid \frac{9}{0} \mid \frac{10}{7}$   $K = \mathbb{Z}_{11};$
- 29).  $\frac{a_i}{b_i} \mid \frac{-3}{227} \mid \frac{-1}{-1} \mid \frac{1}{3} \mid \frac{2}{17} \mid \frac{4}{339}$   $K = \mathbb{Q};$
- 30).  $\frac{a_i}{b_i} \mid \frac{2}{10} \mid \frac{4}{3} \mid \frac{7}{3} \mid \frac{9}{5} \mid \frac{12}{12}$   $K = \mathbb{Z}_{13}.$

## Задание № 5

Используя расширенный алгоритм Евклида, найти наибольший общий делитель многочленов  $f(x)$  и  $g(x)$  в кольце  $K[x]$  и многочлены

$u(x), v(x) \in K[x]$  такие, что  $\text{НОД}(f(x), g(x)) = f(x)u(x) + g(x)v(x)$  :

- 1).  $f(x) = x^5 + x^4 + 1, \quad g(x) = x^4 + x^2 + 1, \quad K = \mathbb{Z}_2$ ;
- 2).  $f(x) = x^5 - x^4 - 3x^2 - x - 2, \quad g(x) = x^4 + x^3 - x - 1, \quad K = \mathbb{Q}$ ;
- 3).  $f(x) = x^5 + 3x^4 + 3x^3 + 4x^2 + 2x + 2,$   
 $g(x) = x^4 + x^3 + 2x^2 + x + 1, \quad K = \mathbb{Z}_5$ ;
- 4).  $f(x) = x^6 + 2x^5 + 2x^2 + x, \quad g(x) = x^4 + x^3 + x^2 + 2, \quad K = \mathbb{Z}_3$ ;
- 5).  $f(x) = x^5 + x^3 + x + 1, \quad g(x) = x^4 + 1, \quad K = \mathbb{Z}_2$ ;
- 6).  $f(x) = x^5 - 2x^3 - 4x^2, \quad g(x) = x^4 + 2x^3 + x^2 - 2x - 2, \quad K = \mathbb{Q}$ ;
- 7).  $f(x) = x^5 + 3x^3 + 3x^2 + 2x + 3, \quad g(x) = x^4 + 2x^2 + 2x, \quad K = \mathbb{Z}_5$ ;
- 8).  $f(x) = x^5 + x^4 + 2x^2 + 2x, \quad g(x) = x^4 + 1, \quad K = \mathbb{Z}_3$ ;
- 9).  $f(x) = x^5 + x + 1, \quad g(x) = x^4 + x^3 + 1, \quad K = \mathbb{Z}_2$ ;
- 10).  $f(x) = x^5 - 3x^4 + 3x^3 - 9x^2 + 2x - 6,$   
 $g(x) = x^4 - 3x^3 - x^2 + 3x, \quad K = \mathbb{Q}$ ;
- 11).  $f(x) = x^5 + 2x^4 + x^3 + 2x^2, \quad g(x) = x^4 + x^3 + 3x^2 +$   
 $4x + 1, \quad K = \mathbb{Z}_5$ ;
- 12).  $f(x) = x^5 + 2x^4 + 2x^2 + 2x, \quad g(x) = x^4 + 2x^2 + x + 2, \quad K = \mathbb{Z}_3$ ;
- 13).  $f(x) = x^5 + x^3 + x, \quad g(x) = x^4 + x + 1, \quad K = \mathbb{Z}_2$ ;
- 14).  $f(x) = x^5 - 3x^4 + 3x^3 - 9x^2 + 2x - 6,$   
 $g(x) = x^4 + x^2 - 2, \quad K = \mathbb{Q}$ ;
- 15).  $f(x) = x^5 + 8x^3 + x^3 + 6x^2 + x, \quad g(x) = x^4 + x^3 + x^2 +$   
 $3x + 2, \quad K = \mathbb{Z}_{11}$ ;
- 16).  $f(x) = x^5 + x^4 + x^2 + 2x, \quad g(x) = x^4 + x^3 + x^2 + 2x + 1,$   
 $K = \mathbb{Z}_3$ ;
- 17).  $f(x) = x^5 + x^4 + 1, \quad g(x) = x^5 + x^2 + x + 1, \quad K = \mathbb{Z}_2$ ;
- 18).  $f(x) = x^5 - x^4 - 3x^3 + 3x^2 - 4x + 4, \quad g(x) = x^4 + x^3 -$   
 $3x^2 - 4x - 4, \quad K = \mathbb{Q}$ ;
- 19).  $f(x) = x^5 + 2x^4 + x^2 + 2x, \quad g(x) = x^4 + x^3 - x^2 - 2x - 2,$   
 $K = \mathbb{Z}_7$ ;
- 20).  $f(x) = x^5 + x^4 + 2x + 2, \quad g(x) = x^4 + 2x^3 + 2x, \quad K = \mathbb{Z}_3$ ;
- 21).  $f(x) = x^6 + x^5 + x^4 + x, \quad g(x) = x^5 + x + 1, \quad K = \mathbb{Z}_2$ ;
- 22).  $f(x) = x^5 + x^3 - x^2 - 1, \quad g(x) = x^4 + 2x^3 + 2x^2 + x, \quad K = \mathbb{Q}$ ;
- 23).  $f(x) = x^5 + 2x^4 + 4x^2 + 6, \quad g(x) = x^4 + x^3 + 3x^2 + 5x,$   
 $K = \mathbb{Z}_{11}$ ;
- 24).  $f(x) = x^5 + 2x^3 + 2x^2 + x + 2, \quad g(x) = x^4 + x^3 + 2x^2 +$   
 $x + 1, \quad K = \mathbb{Z}_3$ ;

- 25).  $f(x) = x^5 + 2x^4 + 3x^3 + 2x^2 + 5x + 5$ ,  $g(x) = x^4 + 3x^3 + x^2 + 6x$ ,  $K = \mathbb{Z}_7$ ;  
 26).  $f(x) = x^5 - 2x^4 - x^3 - 5x^2 - 2x - 3$ ,  $g(x) = x^4 - 6x^2 - 8x - 3$ ,  $K = \mathbb{Q}$ ;  
 27).  $f(x) = x^5 + x^4 + 5x^3 + 2x^2 - x + 2$ ,  $g(x) = x^4 + 6x^3 + 6x^2 + 4x + 6$ ,  $K = \mathbb{Z}_{11}$ ;  
 28).  $f(x) = 2x^5 + 2x^2$ ,  $g(x) = x^4 + x^2 + x$ ,  $K = \mathbb{Z}_3$ ;  
 29).  $f(x) = x^5 + 4x^3 + 3x^2 + 4x + 1$ ,  $g(x) = x^4 + x^3 + 4x + 4$ ,  $K = \mathbb{Z}_5$ ;  
 30).  $f(x) = x^5 + x^4 + x^3 + x^2 - 2x - 2$ ,  $g(x) = x^4 + 3x^3 - x - 3$ ,  $K = \mathbb{Z}_7$ .

### Задание № 6

В  $\mathbb{Z}_p[x]/(m(x))$  найти обратный к многочлену  $f(x)$  :

- 1).  $p = 2$ ,  $m(x) = x^4 + x + 1$ ,  $f(x) = x^3 + x^2 + x + 1$ ;
- 2).  $p = 3$ ,  $m(x) = x^4 + 2x^3 + x + 1$ ,  $f(x) = 2x^3 + x^2 + 2x + 1$ ;
- 3).  $p = 5$ ,  $m(x) = x^3 + x^2 + 1$ ,  $f(x) = x^2 + 4x + 3$ ;
- 4).  $p = 2$ ,  $m(x) = x^4 + x^3 + 1$ ,  $f(x) = x^3 + x + 1$ ;
- 5).  $p = 3$ ,  $m(x) = x^4 + x^3 + x^2 + x + 1$ ,  $f(x) = x^3 + 2x + 2$ ;
- 6).  $p = 5$ ,  $m(x) = x^3 + x^2 + 2$ ,  $f(x) = x^2 + 3x + 2$ ;
- 7).  $p = 2$ ,  $m(x) = x^4 + x^3 + x^2 + x + 1$ ,  $f(x) = x^3 + x^2 + 1$ ;
- 8).  $p = 3$ ,  $m(x) = x^4 + 2x^3 + x^2 + 2x + 1$ ,  $f(x) = x^3 + 2x^2 + 1$ ;
- 9).  $p = 5$ ,  $m(x) = x^3 + x^2 + 3x + 1$ ,  $f(x) = x^2 + 4x + 3$ ;
- 10).  $p = 2$ ,  $m(x) = x^5 + x^3 + 1$ ,  $f(x) = x^4 + x^2 + x + 1$ ;
- 11).  $p = 3$ ,  $m(x) = x^5 + 2x^3 + x^2 + x + 2$ ,  $f(x) = x^4 + 2x^2 + x + 2$ ;
- 12).  $p = 5$ ,  $m(x) = x^3 + x^2 + 3x + 4$ ,  $f(x) = x^2 + 3x + 2$ ;
- 13).  $p = 2$ ,  $m(x) = x^5 + x^2 + 1$ ,  $f(x) = x^4 + x^3 + x + 1$ ;
- 14).  $p = 3$ ,  $m(x) = x^4 + 2x^3 + x^2 + x + 2$ ,  $f(x) = x^3 + 2x + 1$ ;
- 15).  $p = 5$ ,  $m(x) = x^3 + x^2 + 4x + 1$ ,  $f(x) = x^2 + 3x + 4$ ;
- 16).  $p = 2$ ,  $m(x) = x^5 + x^4 + x^3 + x^2 + 1$ ,  $f(x) = x^4 + x^3 + x^2 + 1$ ;
- 17).  $p = 3$ ,  $m(x) = x^4 + x^2 + x + 1$ ,  $f(x) = x^3 + x^2 + 2x + 2$ ;
- 18).  $p = 5$ ,  $m(x) = x^3 + x^2 + 4x + 3$ ,  $f(x) = x^2 + 3x + 4$ ;
- 19).  $p = 2$ ,  $m(x) = x^5 + x^4 + x^3 + x + 1$ ,  $f(x) = x^3 + x^2 + x + 1$ ;
- 20).  $p = 3$ ,  $m(x) = x^4 + x^2 + 2x + 1$ ,  $f(x) = x^3 + 2x^2 + 2x + 1$ ;
- 21).  $p = 5$ ,  $m(x) = x^3 + 4x^2 + 3x + 1$ ,  $f(x) = 2x^2 + x + 2$ ;
- 22).  $p = 2$ ,  $m(x) = x^5 + x^4 + x^2 + x + 1$ ,  $f(x) = x^3 + x^2 + x + 1$ ;
- 23).  $p = 3$ ,  $m(x) = x^4 + x^3 + x^2 + 2x + 2$ ,  $f(x) = x^3 + 2x^2 + 2x + 1$ ;

- 24).  $p = 5$ ,  $m(x) = x^3 + 4x^2 + 3x + 4$ ,  $f(x) = x^2 + 4x + 4$ ;  
 25).  $p = 2$ ,  $m(x) = x^5 + x^3 + x^2 + x + 1$ ,  $f(x) = x^3 + x + 1$ ;  
 26).  $p = 3$ ,  $m(x) = x^4 + x^3 + x^2 + x + 1$ ,  $f(x) = x^3 + 2x^2 + x + 1$ ;  
 27).  $p = 5$ ,  $m(x) = x^3 + 4x^2 + 4x + 2$ ,  $f(x) = x^2 + 3x + 3$ ;  
 28).  $p = 2$ ,  $m(x) = x^6 + x^5 + 1$ ,  $f(x) = x^5 + x^4 + x^2 + x + 1$ ;  
 29).  $p = 3$ ,  $m(x) = x^5 + 2x^4 + 2x^2 + 2x + 1$ ,  
 $f(x) = x^4 + 2x^3 + 2x^2 + 2$ ;  
 30).  $p = 5$ ,  $m(x) = x^3 + 3x^2 + 2x + 2$ ,  $f(x) = x^2 + 4x + 3$ .

### Задание № 7

Вычислить выражение  $f(x) = F(g_1(x), g_2(x), \dots, g_n(x))$  над  $K[x]$ , работая над полями  $K[x]/(m_s(x))$  для различных  $s$ , где  $m_s(x) = x - a_s$ ,  $a_s \in K$ , и пользуясь алгоритмом интерполяции, основанным на китайской теореме об остатках :

- 1).  $f_1(f_2(x))$ ,  $f_1(x) = x^2 + 3x + 2$ ,  $f_2(x) = x^2 + 5x + 1$ ,  
 $K = \mathbb{Z}_5$ ;
- 2).  $(f_2 - f_1)(f_3(x))$ ,  $f_1(x) = x^3 + 3x + 2$ ,  
 $f_2(x) = x^3 + 2x^2 + x + 5$ ,  $f_3(x) = x^2 + 4x + 6$ ,  $K = \mathbb{Z}_5$ ;
- 3).  $(f_1 + 2f_2)(x) \cdot f_3(x)$ ,  $f_1(x) = x^3 - 2x^2 + 1$ ,  
 $f_2(x) = x^2 + 3x + 3$ ,  $f_3(x) = 2x^2 + 5x - 4$ ,  $K = \mathbb{Z}_7$ ;
- 4).  $(f_3 - f_1)(f_2(x))$ ,  $f_1(x) = x^2 + 3x + 2$ ,  
 $f_2(x) = x^3 + x + 3$ ,  $f_3(x) = x^2 + 5x + 1$ ,  $K = \mathbb{Z}_5$ ;
- 5).  $f_1(f_2(x))$ ,  $f_1(x) = x^2 + 4x + 6$ ,  $f_2(x) = x^3 + 2x^2 + x + 5$ ,  
 $K = \mathbb{Z}_7$ ;
- 6).  $f_1((f_3 - 2f_2)(x))$ ,  $f_1(x) = x^3 - 2x^2 + 1$ ,  
 $f_2(x) = x^2 + 3x + 3$ ,  $f_3(x) = 2x^2 + 5x - 4$ ,  $K = \mathbb{Z}_5$ ;
- 7).  $(f_3 - f_1)(x) \cdot f_2(x)$ ,  $f_1(x) = x^2 + 3x + 2$ ,  
 $f_2(x) = x^3 + x + 3$ ,  $f_3(x) = x^2 + 5x + 1$ ,  $K = \mathbb{Z}_5$ ;
- 8).  $(f_2 + f_1)(x) \cdot f_3(x)$ ,  $f_1(x) = x^3 + 3x + 2$ ,  
 $f_2(x) = x^3 + 2x^2 + x + 5$ ,  $f_3(x) = x^2 + 4x + 6$ ,  $K = \mathbb{Z}_7$ ;
- 9).  $f_1(f_2(x))$ ,  $f_1(x) = x^3 - 2x^2 + 1$ ,  $f_2(x) = x^2 + 3x + 3$ ,  
 $K = \mathbb{Z}_7$ ;
- 10).  $f_3(x) \cdot (f_1 + f_2)(x)$ ,  $f_1(x) = x^2 + 3x + 2$ ,  
 $f_2(x) = x^3 + x + 3$ ,  $f_3(x) = x^2 + 5x + 1$ ,  $K = \mathbb{Z}_7$ ;
- 11).  $(f_2 + f_1)(f_3(x))$ ,  $f_1(x) = x^3 + 3x + 2$ ,  
 $f_2(x) = x^3 + 2x^2 + x + 5$ ,  $f_3(x) = x^2 + 4x + 6$ ,  $K = \mathbb{Z}_7$ ;
- 12).  $f_1(f_2(x))$ ,  $f_1(x) = x^2 + 3x + 3$ ,  $f_2(x) = 2x^2 + 5x - 4$ ,  
 $K = \mathbb{Z}_5$ ;

- 13).  $f_1(x) \cdot (f_2 + f_3)(x)$ ,  $f_1(x) = x^2 + 3x + 2$ ,  
 $f_2(x) = x^3 + x + 3$ ,  $f_3(x) = x^2 + 5x + 1$ ,  $K = \mathbb{Z}_7$ ;
- 14).  $f_1(f_2(x))$ ,  $f_1(x) = x^3 + 2x^2 + x + 5$ ,  
 $f_2(x) = x^2 + 4x + 6$ ,  $K = \mathbb{Z}_7$ ;
- 15).  $(f_1 + f_2)(x) \cdot f_1(x)$ ,  $f_1(x) = x^3 - 2x^2 + 1$ ,  
 $f_2(x) = 2x^2 + 5x - 4$ ,  $K = \mathbb{Z}_7$ ;
- 16).  $f_1(f_2(x))$ ,  $f_1(x) = x^2 + 3x + 2$ ,  $f_2(x) = x^3 + x + 3$ ,  
 $K = \mathbb{Z}_7$ ;
- 17).  $f_1(x) \cdot f_2(x)$ ,  $f_1(x) = x^3 + 3x + 2$ ,  
 $f_2(x) = x^3 + 2x^2 + x + 5$ ,  $K = \mathbb{Z}_7$ ;
- 18).  $f_1(f_2(x))$ ,  $f_1(x) = 2x^2 + 5x - 4$ ,  $f_2(x) = x^2 + 3x + 3$ ,  
 $K = \mathbb{Z}_5$ ;
- 19).  $f_1(f_2(x))$ ,  $f_1(x) = x^3 + x + 3$ ,  $f_2(x) = x^2 + 5x + 1$ ,  
 $K = \mathbb{Z}_7$ ;
- 20).  $f_1(x) \cdot (f_2 - 2f_3)(x)$ ,  $f_1(x) = x^3 + 3x + 2$ ,  
 $f_2(x) = x^3 + 2x^2 + x + 5$ ,  $f_3(x) = x^2 + 4x + 6$ ,  $K = \mathbb{Z}_7$ ;
- 21).  $f_1(f_2(x))$ ,  $f_1(x) = x^3 - 2x^2 + 1$ ,  $f_2(x) = 2x^2 + 5x - 4$ ,  
 $K = \mathbb{Z}_7$ ;
- 22).  $(f_1 + f_3)(f_2(x))$ ,  $f_1(x) = x^2 + 3x + 2$ ,  
 $f_2(x) = x^3 + x + 3$ ,  $f_3(x) = x^2 + 5x + 1$ ,  $K = \mathbb{Z}_7$ ;
- 23).  $f_1(f_2(x))$ ,  $f_1(x) = x^3 + 3x + 2$ ,  $f_2(x) = x^2 + 4x + 6$ ,  
 $K = \mathbb{Z}_7$ ;
- 24).  $f_1(f_2(x))$ ,  $f_1(x) = x^2 + 3x + 3$ ,  $f_2(x) = x^3 - 2x^2 + 1$ ,  
 $K = \mathbb{Z}_7$ ;
- 25).  $f_1(f_2(x))$ ,  $f_1(x) = x^2 + 5x + 1$ ,  $f_2(x) = x^2 + 3x + 2$ ,  
 $K = \mathbb{Z}_5$ ;
- 26).  $(f_1 + f_2)(x) \cdot f_2(x)$ ,  $f_1(x) = x^3 + 3x + 2$ ,  
 $f_2(x) = x^3 + 2x^2 + x + 5$ ,  $K = \mathbb{Z}_7$ ;
- 27).  $(f_1 - f_2)(x) \cdot f_2(x)$ ,  $f_1(x) = x^3 - 2x^2 + 1$ ,  
 $f_2(x) = x^2 + 3x + 3$ ,  $K = \mathbb{Z}_7$ ;
- 28).  $f_2^2((f_1 - f_3)(x))$ ,  $f_1(x) = x^2 + 3x + 2$ ,  
 $f_2(x) = x^3 + x + 3$ ,  $f_3(x) = x^2 + 5x + 1$ ,  $K = \mathbb{Z}_7$ ;
- 29).  $f_3((f_2 - f_1)(x))$ ,  $f_1(x) = x^3 + 3x + 2$ ,  
 $f_2(x) = x^3 + 2x^2 + x + 5$ ,  $f_3(x) = x^2 + 4x + 6$ ,  $K = \mathbb{Z}_5$ ;
- 30).  $f_1(f_2(x))$ ,  $f_1(x) = 2x^2 + 5x - 4$ ,  $f_2(x) = x^3 - 2x^2 + 1$ ,  
 $K = \mathbb{Z}_7$ .

## Задание № 8

Вычислить выражение  $f(x) = F(g_1(x), g_2(x), \dots, g_n(x))$  над  $\mathbb{Z}[x]$ , работая над полями  $\mathbb{Z}_{m_s}$  для различных взаимно простых модулей  $m_s$  и пользуясь китайской теоремой об остатках:

- 1).  $(f_1(x) + f_2(x)) \cdot (f_2(x) + f_3(x))$ ,  $f_1(x) = x^2 + 5x + 2$ ,  
 $f_2(x) = x^3 - x^2 + 1$ ,  $f_3(x) = 3x^2 + 2x + 3$ ;
- 2).  $(f_1(x) + f_3(x)) \cdot f_2(x)$ ,  $f_1(x) = x^2 + 5x + 3$ ,  
 $f_2(x) = x^3 - x^2 + 1$ ,  $f_3(x) = 3x^2 + 2x + 3$ ;
- 3).  $(f_3(x) - f_1(x)) \cdot f_2(x)$ ,  $f_1(x) = x^2 + x + 2$ ,  
 $f_2(x) = x^3 + x^2 + 5$ ,  $f_3(x) = 3x^2 + 2x + 3$ ;
- 4).  $(f_1(x) + f_2(x)) \cdot (f_3(x) - 2f_2(x))$ ,  $f_1(x) = x^2 + 2x + 3$ ,  
 $f_2(x) = x^2 + x + 1$ ,  $f_3(x) = 3x^2 + 4x + 5$ ;
- 5).  $(f_1(x) + f_2(x)) \cdot f_3(x)$ ,  $f_1(x) = x^2 + 5x + 2$ ,  
 $f_2(x) = x^3 - x^2 + 1$ ,  $f_3(x) = 3x^2 + 2x + 3$ ;
- 6).  $f_1(x) \cdot f_2(x)$ ,  $f_1(x) = x^3 - x^2 + 1$ ,  $f_2(x) = 3x^2 + 2x + 3$ ;
- 7).  $f_1(x) \cdot f_2(x)$ ,  $f_1(x) = x^2 + 5x + 2$ ,  $f_2(x) = 3x^3 + 2x^2 + 3$ ;
- 8).  $(f_2(x) - f_1(x)) \cdot (f_3(x) + f_1(x))$ ,  $f_1(x) = x^2 + 2x + 4$ ,  
 $f_2(x) = x^3 + x^2 + 3x + 4$ ,  $f_3(x) = x^3 + x^2 + 2x$ ;
- 9).  $f_2(f_1(x))$ ,  $f_1(x) = x^2 + 5x + 2$ ,  $f_2(x) = 3x^2 + 2x + 3$ ;
- 10).  $(f_1(f_2(x)))$ ,  $f_1(x) = x^2 + 5x + 2$ ,  $f_2(x) = 3x^2 + 2x + 3$ ;
- 11).  $(f_1(x) - 2f_2(x)) \cdot (f_1(x) + f_3(x))$ ,  $f_1(x) = x^3 + 2x^2 + x + 3$ ,  
 $f_2(x) = x^2 - x + 1$ ,  $f_3(x) = x^3 - 2x^2 + 3x + 1$ ;
- 12).  $(f_1(f_2(x)))$ ,  $f_1(x) = x^2 + 12x + 36$ ,  $f_2(x) = x^2 + 3x + 4$ ;
- 13).  $f_2(f_1^2(x))$ ,  $f_1(x) = x + 2$ ,  $f_2(x) = 3x^2 + 2x - 1$ ;
- 14).  $f_1(x) \cdot f_2(x) \cdot f_3(x)$ ,  $f_1(x) = 3x^2 + 2x + 1$ ,  
 $f_2(x) = x^2 + 3x + 4$ ,  $f_3(x) = x + 5$ ;
- 15).  $(f_1 + f_2)(f_3^2(x))$ ,  $f_1(x) = 3x^2 + 2x - 1$ ,  
 $f_2(x) = x^2 + 3x + 4$ ,  $f_3(x) = x + 2$ ;
- 16).  $(f_3(x) - 2f_2(x)) \cdot f_1^3(x)$ ,  $f_1(x) = x + 2$ ,  
 $f_2(x) = x^2 - x - 2$ ,  $f_3(x) = 3x^2 + 2x - 1$ ;
- 17).  $f_1^2(x) \cdot f_2(x)$ ,  $f_1(x) = 3x^2 + 2x + 1$ ,  $f_2(x) = x^2 + x + 1$ ;
- 18).  $f_1^2(x) \cdot f_2(x)$ ,  $f_1(x) = x^2 + 3x + 5$ ,  $f_2(x) = 2x^2 + x + 2$ ;
- 19).  $f_1(f_2(x))$ ,  $f_1(x) = x^3 + 2x + 1$ ,  $f_2(x) = x^2 + x + 3$ ;
- 20).  $f_2(f_1(x))$ ,  $f_1(x) = x^3 + 3x^2 + 2$ ,  $f_2(x) = x^2 + 7x + 4$ ;
- 21).  $f_1((f_2 + f_3)(x))$ ,  $f_1(x) = 2x^2 + 3$ ,  $f_2(x) = x^2 + 2$ ,  $f_3(x) = 3x + 3$ ;
- 22).  $(f_1(x) \cdot f_2)(f_3(x))$ ,  $f_1(x) = 3x + 10$ ,  $f_2(x) = x - 4$ ,  
 $f_3(x) = x^2 + 3x + 5$ ;
- 23).  $f_1^3(x) \cdot f_2(x)$ ,  $f_1(x) = 2x + 3$ ,  $f_2(x) = x^2 + 3x + 5$ ;



- 24).  $f_1^2(x) \cdot (f_2^2(x))$ ,  $f_1(x) = x + 7$ ,  $f_2(x) = x^2 + x + 2$ ;  
 25).  $f_1(f_2(x))$ ,  $f_1(x) = x^3 + 2x - 1$ ,  $f_2(x) = x^2 + 4x + 2$ ;  
 26).  $f_2(f_1(x))$ ,  $f_1(x) = x^3 + 2x - 1$ ,  $f_2(x) = x^2 + 4x + 2$ ;  
 27).  $f_1(f_2^2(x))$ ,  $f_1(x) = x^2 + 2$ ,  $f_2(x) = 2x + 3$ ;  
 28).  $f_1^2(x) \cdot f_2(x)$ ,  $f_1(x) = 3x + 4$ ,  $f_2(x) = x^2 + 3x + 5$ ;  
 29).  $f_2^2(x) \cdot f_1(x)$ ,  $f_1(x) = 3x + 4$ ,  $f_2(x) = x^2 + 3x + 5$ ;  
 30).  $f_1(x) \cdot f_2(f_3^2(x))$ ,  $f_1(x) = x^2 + 2x + 3$ ,  $f_2(x) = x^2 + 3x + 7$ ,  
 $f_3(x) = x + 1$ .

### Задание № 9

Решить систему сравнений в кольце  $K[x]$  :

- 1). 
$$\begin{cases} f(x) \equiv 8 \pmod{x-1} \\ f(x) \equiv 0 \pmod{x+1} \\ f(x) \equiv -2x \pmod{x^2+1} \\ f(x) \equiv 1 \pmod{x} \end{cases} \quad K = \mathbb{Q};$$
- 2). 
$$\begin{cases} f(x) \equiv 4 \pmod{x-1} \\ f(x) \equiv 1 \pmod{x+1} \\ f(x) \equiv 4x+3 \pmod{x^2+x+3} \end{cases} \quad K = \mathbb{Z}_7;$$
- 3). 
$$\begin{cases} f(x) \equiv x \pmod{x^2+3x+3} \\ f(x) \equiv 2 \pmod{x-1} \\ f(x) \equiv 2 \pmod{x+1} \\ f(x) \equiv 0 \pmod{x-2} \end{cases} \quad K = \mathbb{Z}_5;$$
- 4). 
$$\begin{cases} f(x) \equiv 3x+9 \pmod{x^2+x+1} \\ f(x) \equiv 6 \pmod{x-5} \\ f(x) \equiv 6 \pmod{x-4} \end{cases} \quad K = \mathbb{Z}_{11};$$
- 5). 
$$\begin{cases} f(x) \equiv 9 \pmod{x+1} \\ f(x) \equiv 24 \pmod{x-2} \\ f(x) \equiv 2 \pmod{x} \\ f(x) \equiv 29 \pmod{x+3} \end{cases} \quad K = \mathbb{Q};$$
- 6). 
$$\begin{cases} f(x) \equiv 5x+8 \pmod{x^2+x+3} \\ f(x) \equiv -1 \pmod{x-3} \\ f(x) \equiv 0 \pmod{x-7} \\ f(x) \equiv 9 \pmod{x+1} \end{cases} \quad K = \mathbb{Z}_{13};$$

$$\begin{aligned}
7). \quad & \begin{cases} f(x) \equiv 2 \pmod{x-1} \\ f(x) \equiv 2 \pmod{x-2} \\ f(x) \equiv 4 \pmod{x-3} \\ f(x) \equiv 3 \pmod{x+2} \end{cases} \quad K = \mathbb{Z}_7; \\
8). \quad & \begin{cases} f(x) \equiv -x \pmod{x^2+x+1} \\ f(x) \equiv 0 \pmod{x-1} \\ f(x) \equiv 3 \pmod{x-2} \end{cases} \quad K = \mathbb{Z}_5; \\
9). \quad & \begin{cases} f(x) \equiv -7x+5 \pmod{x^2+x+1} \\ f(x) \equiv 19 \pmod{x-2} \\ f(x) \equiv 19 \pmod{x+3} \end{cases} \quad K = \mathbb{Q}; \\
10). \quad & \begin{cases} f(x) \equiv 9x+8 \pmod{x^2+x+6} \\ f(x) \equiv 6 \pmod{x-1} \\ f(x) \equiv 4 \pmod{x-4} \\ f(x) \equiv 6 \pmod{x-6} \end{cases} \quad K = \mathbb{Z}_{11}; \\
11). \quad & \begin{cases} f(x) \equiv 3x-5 \pmod{x^2+1} \\ f(x) \equiv 7 \pmod{x-2} \\ f(x) \equiv 1 \pmod{x-7} \end{cases} \quad K = \mathbb{Z}_{13}; \\
12). \quad & \begin{cases} f(x) \equiv -1 \pmod{x^2+x+4} \\ f(x) \equiv 3 \pmod{x} \\ f(x) \equiv 2 \pmod{x-1} \\ f(x) \equiv 3 \pmod{x-3} \end{cases} \quad K = \mathbb{Z}_7; \\
13). \quad & \begin{cases} f(x) \equiv -3x-12 \pmod{x^2+2x+2} \\ f(x) \equiv -2 \pmod{x+1} \\ f(x) \equiv 22 \pmod{x-2} \\ f(x) \equiv 18 \pmod{x+2} \end{cases} \quad K = \mathbb{Q}; \\
14). \quad & \begin{cases} f(x) \equiv x+3 \pmod{x^2+x+2} \\ f(x) \equiv 4 \pmod{x-2} \\ f(x) \equiv 1 \pmod{x-4} \end{cases} \quad K = \mathbb{Z}_5; \\
15). \quad & \begin{cases} f(x) \equiv 2x+2 \pmod{x^2+x+2} \\ f(x) \equiv 2x \pmod{x^2+2x+2} \\ f(x) \equiv 0 \pmod{x-1} \end{cases} \quad K = \mathbb{Z}_3;
\end{aligned}$$

$$\begin{aligned}
16). \quad & \begin{cases} f(x) \equiv 2x + 9 \pmod{x^2 + x + 8} \\ f(x) \equiv 3 \pmod{x - 1} \\ f(x) \equiv 0 \pmod{x + 1} \\ f(x) \equiv 7 \pmod{x - 3} \end{cases} & K = \mathbb{Z}_{11}; \\
17). \quad & \begin{cases} f(x) \equiv 3x + 4 \pmod{x^2 + 3x + 3} \\ f(x) \equiv -9 \pmod{x + 2} \\ f(x) \equiv -4 \pmod{x + 1} \end{cases} & K = \mathbb{Q}; \\
18). \quad & \begin{cases} f(x) \equiv 2x + 1 \pmod{x^2 + x + 2} \\ f(x) \equiv 10 \pmod{x - 6} \\ f(x) \equiv -1 \pmod{x - 4} \end{cases} & K = \mathbb{Z}_{13}; \\
19). \quad & \begin{cases} f(x) \equiv 4 \pmod{x^2 + 1} \\ f(x) \equiv 2 \pmod{x - 4} \\ f(x) \equiv 2 \pmod{x + 1} \end{cases} & K = \mathbb{Z}_7; \\
20). \quad & \begin{cases} f(x) \equiv 3x + 2 \pmod{x^2 + 2x + 3} \\ f(x) \equiv 4 \pmod{x - 1} \\ f(x) \equiv 1 \pmod{x + 1} \end{cases} & K = \mathbb{Z}_5; \\
21). \quad & \begin{cases} f(x) \equiv -x + 6 \pmod{x^2 + 1} \\ f(x) \equiv 5x - 4 \pmod{x^2 - 1} \\ f(x) \equiv 9 \pmod{x - 2} \end{cases}, & K = \mathbb{Q}; \\
22). \quad & \begin{cases} f(x) \equiv 6 \pmod{x^2 + 2x + 2} \\ f(x) \equiv 7 \pmod{x - 5} \\ f(x) \equiv 1 \pmod{x - 3} \end{cases} & K = \mathbb{Z}_{11}; \\
23). \quad & \begin{cases} f(x) \equiv -2x + 1 \pmod{x^2 + x + 5} \\ f(x) \equiv 8 \pmod{x - 1} \\ f(x) \equiv 6 \pmod{x + 2} \\ f(x) \equiv 4 \pmod{x - 5} \end{cases} & K = \mathbb{Z}_{13}; \\
24). \quad & \begin{cases} f(x) \equiv -x - 2 \pmod{x^2 + 2x + 2} \\ f(x) \equiv 1 \pmod{x - 2} \\ f(x) \equiv 5 \pmod{x - 3} \\ f(x) \equiv 2 \pmod{x - 5} \end{cases} & K = \mathbb{Z}_7;
\end{aligned}$$

$$\begin{aligned}
25). \quad & \begin{cases} f(x) \equiv 2 \pmod{x-2} \\ f(x) \equiv 14 \pmod{x+1} \\ f(x) \equiv 14 \pmod{x-3} \\ f(x) \equiv 2 \pmod{x-1} \end{cases} \quad K = \mathbb{Q}; \\
26). \quad & \begin{cases} f(x) \equiv -x+3 \pmod{x^2+2x+4} \\ f(x) \equiv 1 \pmod{x-3} \\ f(x) \equiv 2 \pmod{x-2} \end{cases} \quad K = \mathbb{Z}_5; \\
27). \quad & \begin{cases} f(x) \equiv x \pmod{x^2+x+4} \\ f(x) \equiv 8 \pmod{x-2} \\ f(x) \equiv -1 \pmod{x-3} \end{cases} \quad K = \mathbb{Z}_{11}; \\
28). \quad & \begin{cases} f(x) \equiv 5x+5 \pmod{x^2+x+4} \\ f(x) \equiv 1 \pmod{x-5} \\ f(x) \equiv 4 \pmod{x+4} \end{cases} \quad K = \mathbb{Z}_{13}; \\
29). \quad & \begin{cases} f(x) \equiv 0 \pmod{x-1} \\ f(x) \equiv -2 \pmod{x} \\ f(x) \equiv -18 \pmod{x+1} \\ f(x) \equiv 18 \pmod{x-2} \end{cases} \quad K = \mathbb{Q}; \\
30). \quad & \begin{cases} f(x) \equiv x+2 \pmod{x^2+x+2} \\ f(x) \equiv 1 \pmod{x} \\ f(x) \equiv 2 \pmod{x-1} \end{cases} \quad K = \mathbb{Z}_3.
\end{aligned}$$

### Задание № 10

Найти наибольший общий делитель двух многочленов в кольце  $\mathbb{Z}[x]$ , используя псевдоделение:

- 1).  $f_1(x) = 2x^5 + 6x^4 + 14x^3 + 16x^2 + 14x + 4$ ,  
 $f_2(x) = 6x^4 + 16x^3 + 18x^2 + 16x - 8$ ;
- 2).  $f_1(x) = 3x^5 + 9x^4 + 12x^3 + 27x^2 + 12x + 18$ ,  
 $f_2(x) = 12x^4 + 6x^3 + 42x^2 + 12x + 36$ ;
- 3).  $f_1(x) = 6x^5 + 12x^4 + 10x^3 + 20x^2 + 4x + 8$ ,  
 $f_2(x) = 6x^4 + 18x^3 + 6x^2 - 18x - 12$ ;
- 4).  $f_1(x) = 3x^5 + 9x^4 + 6x^3 + 3x^2 + 18x + 15$ ,  
 $f_2(x) = 6x^4 + 18x^3 + 12x^2 + 18x + 18$ ;
- 5).  $f_1(x) = 5x^5 + 10x^4 + 25x^3 + 45x^2 + 20x + 35$ ,  
 $f_2(x) = 10x^4 + 15x^3 + 40x^2 + 15x + 30$ ;

- 6).  $f_1(x) = 4x^5 + 16x^4 + 12x^3 - 4x^2 - 16x - 12$ ,  
 $f_2(x) = 8x^4 + 8x^3 - 40x^2 + 8x - 48$ ;
- 7).  $f_1(x) = 2x^5 + 4x^4 + 8x^3 + 18x^2 + 16x + 12$ ,  
 $f_2(x) = 12x^5 + 18x^4 + 12x^3 + 12x^2 + 6x + 12$ ;
- 8).  $f_1(x) = 3x^5 + 3x^4 - 12x^3 - 12x^2 + 24x - 48$ ,  
 $f_2(x) = 6x^4 - 6x^2 + 6x - 84$ ;
- 9).  $f_1(x) = 10x^5 + 40x^4 - 20x^3 - 50x^2 + 50x - 30$ ,  
 $f_2(x) = 15x^4 + 25x^3 - 45x^2 + 15x - 10$ ;
- 10).  $f_1(x) = 8x^5 + 28x^4 + 12x^3 - 4x^2 + 24x + 20$ ,  
 $f_2(x) = 12x^4 + 20x^3 - 8x^2 - 4x + 12$ ;
- 11).  $f_1(x) = 4x^5 - 8x^4 - 12x^3 + 24x^2 - 16x + 32$ ,  
 $f_2(x) = 6x^4 + 6x^3 - 42x^2 - 6x + 36$ ;
- 12).  $f_1(x) = 3x^5 + 9x^4 + 6x^3 + 27x^2 + 45x + 54$ ,  
 $f_2(x) = 6x^4 + 48x^3 + 102x^2 + 54x + 54$ ;
- 13).  $f_1(x) = 15x^5 - 45x^4 + 10x^3 - 5x^2 - 80x + 15$ ,  
 $f_2(x) = 10x^4 - 30x^3 + 30x^2 - 70x - 60$ ;
- 14).  $f_1(x) = 2x^5 + 14x^4 + 24x^3 + 6x^2 + 20x - 16$ ,  
 $f_2(x) = 4x^4 + 24x^3 + 32x^2 + 2x + 8$ ;
- 15).  $f_1(x) = 6x^5 + 12x^4 - 18x^3 - 36x^2 + 12x + 24$ ,  
 $f_2(x) = 15x^4 + 75x^3 + 105x^2 + 75x + 90$ ;
- 16).  $f_1(x) = 4x^5 + 16x^4 - 4x^3 - 64x^2 - 48x$ ,  
 $f_2(x) = 6x^5 - 138x^3 - 108x^2 + 240x$ ;
- 17).  $f_1(x) = 6x^5 + 15x^4 + 15x^3 + 15x^2 + 9x$ ,  
 $f_2(x) = 18x^5 + 45x^4 + 27x^3 + 36x^2 - 18x - 108$ ;
- 18).  $f_1(x) = 5x^5 + 10x^4 - 15x^3 - 30x^2 + 10x + 20$ ,  
 $f_2(x) = 15x^5 - 30x^4 - 15x^3 + 30x^2 - 30x + 60$ ;
- 19).  $f_1(x) = 12x^5 + 8x^4 + 60x^3 + 40x^2 + 48x + 32$ ,  
 $f_2(x) = 6x^4 + 28x^3 + 40x^2 + 34x + 12$ ;
- 20).  $f_1(x) = 6x^5 - 3x^4 + 6x^3 - 3x^2 - 12x + 6$ ,  
 $f_2(x) = 12x^4 - 30x^3 + 24x^2 - 30x + 12$ ;
- 21).  $f_1(x) = 6x^5 - 14x^4 + 10x^3 - 14x^2 + 4x$ ,  
 $f_2(x) = 24x^4 + 40x^3 - 40x^2 - 40x + 16$ ;
- 22).  $f_1(x) = 15x^5 + 25x^4 - 5x^3 - 25x^2 - 10x$ ,  
 $f_2(x) = 30x^4 - 40x^3 - 10x^2 - 40x - 40$ ;
- 23).  $f_1(x) = 12x^5 + 6x^4 - 60x^3 - 30x^2 + 48x + 24$ ,  
 $f_2(x) = 24x^4 + 84x^3 + 60x^2 + 84x + 36$ ;

- 24).  $f_1(x) = 18x^5 + 30x^4 - 90x^3 - 150x^2 + 72x + 120$ ,  
 $f_2(x) = 36x^4 - 48x^3 - 144x^2 - 48x - 180$ ;
- 25).  $f_1(x) = 27x^5 + 36x^4 + 9x^3 - 27x^2 - 36x - 9$ ,  
 $f_2(x) = 18x^4 + 42x^3 + 30x^2 + 42x + 12$ ;
- 26).  $f_1(x) = 36x^5 + 9x^4 + 144x^3 + 36x^2 + 108x + 27$ ,  
 $f_2(x) = 48x^5 + 12x^4 + 48x^3 + 12x^2 - 96x - 24$ ;
- 27).  $f_1(x) = 8x^5 - 10x^4 - 52x^3 + 18x^2 + 36x$ ,  
 $f_2(x) = 16x^4 + 44x^3 - 56x^2 - 156x - 72$ ;
- 28).  $f_1(x) = 6x^5 + 2x^4 + 8x^3 - 2x^2 + 2x - 4$ ,  
 $f_2(x) = 12x^5 - 20x^4 + 44x^3 - 48x^2 + 40x - 16$ ;
- 29).  $f_1(x) = 10x^5 - 50x^4 + 50x^3 - 250x^2 + 40x - 200$ ,  
 $f_2(x) = 4x^4 - 4x^3 - 64x^2 - 68x - 60$ ;
- 30).  $f_1(x) = 45x^5 + 18x^4 + 225x^3 + 90x^2 + 270x + 108$ ,  
 $f_2(x) = 15x^4 + 6x^3 + 45x^2 + 33x + 6$ .

### Задание № 11

Разложить многочлен на неприводимые множители над полем  $K$  :

- 1).  $x^4 + 6x^3 + 5x^2 + 6x + 4$ ,  $K = \mathbb{Z}_7$ ;
- 2).  $x^4 + 9$ ,  $K = \mathbb{C}$ ;
- 3).  $x^4 + 3x^3 + 2x^2 + 2x + 1$ ,  $K = \mathbb{Z}_5$ ;
- 4).  $x^4 + 5x^3 + 4x^2 + 3x + 4$ ,  $K = \mathbb{Z}_7$ ;
- 5).  $x^4 + 2x^3 + 6x^2 + 6x + 1$ ,  $K = \mathbb{Z}_{11}$ ;
- 6).  $x^4 + 16$ ,  $K = \mathbb{R}$ ;
- 7).  $x^4 + 3x^3 + 3x^2 + 5x + 3$ ,  $K = \mathbb{Z}_7$ ;
- 8).  $x^5 + x + 1$ ,  $K = \mathbb{Z}_2$ ;
- 9).  $x^4 + 2x^3 + 4x^2 + 2x + 3$ ,  $K = \mathbb{Q}$ ;
- 10).  $x^4 + 5x^2 + 2$ ,  $K = \mathbb{Z}_7$ ;
- 11).  $x^4 + 3x^3 + 10x^2 + x + 2$ ,  $K = \mathbb{Z}_{11}$ ;
- 12).  $x^6 + 64$ ,  $K = \mathbb{C}$ ;
- 13).  $x^4 + 3x^3 + 2x^2 + x + 4$ ,  $K = \mathbb{Z}_5$ ;
- 14).  $x^4 + 4x^3 + x^2 + 6x + 4$ ,  $K = \mathbb{Z}_7$ ;
- 15).  $x^6 + 8$ ,  $K = \mathbb{R}$ ;
- 16).  $x^4 + 2x^3 + 4x^2 + 10x + 6$ ,  $K = \mathbb{Z}_{11}$ ;
- 17).  $x^4 + 2x^3 + 2x + 2$ ,  $K = \mathbb{Z}_3$ ;
- 18).  $x^4 + 5x^3 + 2x^2 + 2x + 1$ ,  $K = \mathbb{Z}_7$ ;
- 19).  $x^4 + x^3 - 2x^2 - 6x - 4$ ,  $K = \mathbb{Q}$ ;
- 20).  $x^4 + 3x^3 + 6x^2 + 5x + 6$ ,  $K = \mathbb{Z}_{11}$ ;

- 21).  $x^4 + x^2 + 2x + 6, \quad K = \mathbb{Z}_7;$
- 22).  $x^6 + 2x^5 + 6x^4 + 8x^3 + 10x^2 + 6x + 3, \quad K = \mathbb{C};$
- 23).  $x^4 + 3x^3 + 3x + 2, \quad K = \mathbb{Z}_5;$
- 24).  $x^4 + 3x^3 + 9x^2 + 8x + 6, \quad K = \mathbb{Z}_{11};$
- 25).  $x^4 + 6x^3 + 2x^2 + x + 1, \quad K = \mathbb{Z}_7;$
- 26).  $x^4 + 2x^3 + 4x^2 + 4x + 4, \quad K = \mathbb{R};$
- 27).  $x^5 + x^4 + 1, \quad K = \mathbb{Z}_2;$
- 28).  $x^5 + x^4 + x + 1, \quad K = \mathbb{Z}_3;$
- 29).  $x^4 + 4x^3 + 2x + 5, \quad K = \mathbb{Z}_7;$
- 30).  $x^4 + 4x^3 + 2x^2 + 2x + 10, \quad K = \mathbb{Z}_{11}.$

## Задание № 12

Является ли многочлен  $f(x)$  приводимым в кольце  $\mathbb{Z}_p[x]$ ? Ответ обосновать :

- 1).  $f(x) = x^4 + x^3 + x^2 + x + 1, \quad p = 3;$
- 2).  $f(x) = x^5 + x^2 + 1, \quad p = 2;$
- 3).  $f(x) = x^4 + 2x^3 + 2x + 1, \quad p = 3;$
- 4).  $f(x) = x^5 + x^4 + 1, \quad p = 2;$
- 5).  $f(x) = x^4 + 2x^3 + x^2 + 2x + 1, \quad p = 3;$
- 6).  $f(x) = x^5 + x^3 + x^2 + x + 1, \quad p = 2;$
- 7).  $f(x) = x^4 + 2x^2 + x + 2, \quad p = 3;$
- 8).  $f(x) = x^5 + x^4 + x^2 + 1, \quad p = 2;$
- 9).  $f(x) = x^4 + 2x^3 + x^2 + x + 2, \quad p = 3;$
- 10).  $f(x) = x^5 + x^4 + x^3 + x + 1, \quad p = 2;$
- 11).  $f(x) = x^4 + 2x + 2, \quad p = 3;$
- 12).  $f(x) = x^5 + x + 1, \quad p = 2;$
- 13).  $f(x) = x^4 + x^2 + 2x + 2, \quad p = 3;$
- 14).  $f(x) = x^5 + x^3 + 1, \quad p = 2;$
- 15).  $f(x) = x^4 + x^2 + x + 1, \quad p = 3;$
- 16).  $f(x) = x^5 + x^2 + x + 1, \quad p = 2;$
- 17).  $f(x) = x^4 + x^3 + x^2 + x + 1, \quad p = 3;$
- 18).  $f(x) = x^5 + x^4 + x^2 + x + 1, \quad p = 2;$
- 19).  $f(x) = x^4 + x^2 + 2x + 1, \quad p = 3;$
- 20).  $f(x) = x^5 + x^4 + x^3 + x^2 + 1, \quad p = 2;$
- 21).  $f(x) = x^4 + x^3 + 2x + 1, \quad p = 3;$
- 22).  $f(x) = x^6 + x^3 + 1, \quad p = 2;$
- 23).  $f(x) = x^4 + x^3 + x^2 + 2x + 2, \quad p = 3;$
- 24).  $f(x) = x^6 + x^5 + 1, \quad p = 2;$

- 25).  $f(x) = x^3 + x^2 + x + 2, \quad p = 3;$   
 26).  $f(x) = x^6 + x + 1, \quad p = 2;$   
 27).  $f(x) = x^4 + 2x^2 + 2x + 1, \quad p = 3;$   
 28).  $f(x) = x^6 + x^4 + x^2 + x + 1, \quad p = 2;$   
 29).  $f(x) = x^4 + 2x^3 + x + 2, \quad p = 3;$   
 30).  $f(x) = x^6 + x^2 + 1, \quad p = 2.$

### Задание № 13

Является ли многочлен приводимым в кольце  $A[x]$ ?

- 1).  $x^4 + 2x^3 - 5x^2 + 3x - 1, \quad A = \mathbb{Z};$
- 2).  $x^4 + 7x^3 + 14x^2 + 28x + 53, \quad A = \mathbb{Q};$
- 3).  $x^4 + 6x^3 - 9x^2 + 3x + 12, \quad A = \mathbb{Z};$
- 4).  $x^5 + 3x^3 - 2x - 52, \quad A = \mathbb{Q};$
- 5).  $x^3 + 5x^2 - 4x + 1, \quad A = \mathbb{Z};$
- 6).  $4x^4 - 25x^3 + 5x^2 + 15, \quad A = \mathbb{Q};$
- 7).  $x^6 - 2x^3 + 1, \quad A = \mathbb{Z};$
- 8).  $x^5 + 15x^4 - 6x^3 + 27x^2 + 12, \quad A = \mathbb{Q};$
- 9).  $x^4 - 3x^3 + 2x^2 + x - 1, \quad A = \mathbb{Z};$
- 10).  $x^3 + 4x^2 - 3x + 7, \quad A = \mathbb{Q};$
- 11).  $x^5 + 3x^4 - 6x^3 + 27x^2 - 12, \quad A = \mathbb{Z};$
- 12).  $x^4 + x^3 - x^2 - 7x - 6, \quad A = \mathbb{Q};$
- 13).  $x^3 + 7x^2 - 8x + 2, \quad A = \mathbb{Z};$
- 14).  $x^3 + 5x - 3, \quad A = \mathbb{Q};$
- 15).  $x^4 + 2x^3 - 7x^2 + 5x - 1, \quad A = \mathbb{Z};$
- 16).  $x^4 + 4x^3 - 16x^2 + 8x - 2, \quad A = \mathbb{Q};$
- 17).  $x^3 - 5x^2 + 10x + 15, \quad A = \mathbb{Z};$
- 18).  $x^4 - 5x^3 + 6x^2 + 3x - 1, \quad A = \mathbb{Q};$
- 19).  $x^4 + 2x^3 - 17x^2 + 9x - 9, \quad A = \mathbb{Z};$
- 20).  $x^3 + 8x^2 + 6x + 10, \quad A = \mathbb{Q};$
- 21).  $x^4 + 6x^3 + 9x^2 - 2x - 6, \quad A = \mathbb{Z};$
- 22).  $x^3 + 10x^2 - 11x + 3, \quad A = \mathbb{Q};$
- 23).  $2x^4 + 5x^3 - 15x^2 + 25x - 10, \quad A = \mathbb{Z};$
- 24).  $x^4 + 3x^3 + 3x^2 - 12x + 5, \quad A = \mathbb{Q};$
- 25).  $x^4 + 5x^3 - 3x^2 + 11x - 7, \quad A = \mathbb{Z};$
- 26).  $x^4 + 3x^3 - 9x^2 + 12x + 21, \quad A = \mathbb{Q};$
- 27).  $x^3 + 11x^2 - 13x + 1, \quad A = \mathbb{Z};$
- 28).  $x^3 + 7x^2 + 6x + 3, \quad A = \mathbb{Q};$
- 29).  $x^4 - 7x^3 + 21x^2 - 35x + 56, \quad A = \mathbb{Z};$
- 30).  $x^4 + 3x^3 - 13x^2 + 8x - 4, \quad A = \mathbb{Q}.$



### Задание № 14

Найти число неприводимых многочленов степени  $n$  над полем  $\mathbb{Z}_p$  :

- |                        |                        |
|------------------------|------------------------|
| 1). $n = 11, p = 2$ ;  | 16). $n = 8, p = 2$ ;  |
| 2). $n = 9, p = 3$ ;   | 17). $n = 4, p = 3$ ;  |
| 3). $n = 8, p = 7$ ;   | 18). $n = 5, p = 5$ ;  |
| 4). $n = 7, p = 11$ ;  | 19). $n = 5, p = 7$ ;  |
| 5). $n = 12, p = 2$ ;  | 20). $n = 4, p = 11$ ; |
| 6). $n = 10, p = 3$ ;  | 21). $n = 9, p = 2$ ;  |
| 7). $n = 9, p = 7$ ;   | 22). $n = 5, p = 3$ ;  |
| 8). $n = 13, p = 2$ ;  | 23). $n = 6, p = 5$ ;  |
| 9). $n = 8, p = 3$ ;   | 24). $n = 3, p = 7$ ;  |
| 10). $n = 7, p = 7$ ;  | 25). $n = 5, p = 11$ ; |
| 11). $n = 3, p = 11$ ; | 26). $n = 7, p = 2$ ;  |
| 12). $n = 10, p = 2$ ; | 27). $n = 7, p = 3$ ;  |
| 13). $n = 6, p = 3$ ;  | 28). $n = 7, p = 5$ ;  |
| 14). $n = 4, p = 5$ ;  | 29). $n = 6, p = 7$ ;  |
| 15). $n = 4, p = 7$ ;  | 30). $n = 6, p = 11$ . |

### Задание № 15

В  $\mathbb{Z}_p[x]/(m(x))$  найти обратный к многочлену  $f(x)$  :

- 1).  $p = 5, m(x) = x^4 + x^3 + x^2 + 1, f(x) = x^3 + 2x^2 + 2x + 2$ ;
- 2).  $p = 3, m(x) = x^4 + 2x^3 + x^2 + 1, f(x) = x^3 + x^2 + 2x + 1$ ;
- 3).  $p = 2, m(x) = x^5 + x^3 + 1, f(x) = x^4 + x^3 + x + 1$ ;
- 4).  $p = 5, m(x) = x^4 + 2x^3 + 2x^2 + 1, f(x) = x^3 + 3x^2 + 2x + 1$ ;
- 5).  $p = 3, m(x) = x^4 + 2x^3 + x + 1, f(x) = x^3 + 2x^2 + 2$ ;
- 6).  $p = 2, m(x) = x^6 + x^4 + x^2 + x + 1, f(x) = x^4 + x^3 + x + 1$ ;
- 7).  $p = 5, m(x) = x^4 + 2x^3 + x^2 + 2, f(x) = x^3 + 3x + 2$ ;
- 8).  $p = 3, m(x) = x^4 + x^3 + 2x + 1, f(x) = x^3 + 2x + 1$ ;
- 9).  $p = 2, m(x) = x^5 + x^2 + 1, f(x) = x^3 + x^2 + 1$ ;
- 10).  $p = 5, m(x) = x^4 + x^3 + 2x^2 + 2, f(x) = x^3 + 4x^2 + 1$ ;
- 11).  $p = 3, m(x) = x^4 + x + 2, f(x) = 2x^3 + x^2 + 2$ ;
- 12).  $p = 2, m(x) = x^5 + x^4 + x^3 + x^2 + 1, f(x) = x^4 + x^2 + x + 1$ ;
- 13).  $p = 5, m(x) = x^4 + 2x^3 + x^2 + 3, f(x) = 2x^3 + 3x^2 + x + 1$ ;
- 14).  $p = 3, m(x) = x^4 + x^2 + 2x + 1, f(x) = x^3 + x^2 + 2x + 2$ ;

- 15).  $p = 2, \quad m(x) = x^5 + x^3 + x^2 + x + 1, \quad f(x) = x^3 + x^2 + x + 1;$
- 16).  $p = 5, \quad m(x) = x^4 + 2x^3 + 2x + 1, \quad f(x) = 2x^3 + x^2 + x + 4;$
- 17).  $p = 3, \quad m(x) = x^4 + x^3 + 2, \quad f(x) = x^3 + x^2 + 2x + 1;$
- 18).  $p = 5, \quad m(x) = x^4 + 2x^3 + 2x + 2, \quad f(x) = 3x^3 + x^2 + 4;$
- 19).  $p = 3, \quad m(x) = x^4 + 2x^3 + x^2 + 1, \quad f(x) = 2x^3 + x + 1;$
- 20).  $p = 2, \quad m(x) = x^6 + x^5 + x^3 + x^2 + 1, \quad f(x) = x^3 + x^2 + 1;$
- 21).  $p = 5, \quad m(x) = x^4 + x^3 + x + 3, \quad f(x) = x^3 + 4x + 2;$
- 22).  $p = 3, \quad m(x) = x^4 + 2x^3 + x^2 + 1, \quad f(x) = 2x^3 + x + 1;$
- 23).  $p = 2, \quad m(x) = x^5 + x^4 + x^3 + x + 1, \quad f(x) = x^4 + x + 1;$
- 24).  $p = 5, \quad m(x) = x^4 + 2x^3 + x + 3, \quad f(x) = x^3 + 3x^2 + x + 4;$
- 25).  $p = 3, \quad m(x) = x^4 + x^2 + x + 1, \quad f(x) = x^3 + 2x^2 + 2x + 1;$
- 26).  $p = 5, \quad m(x) = x^4 + x^3 + 2x + 3, \quad f(x) = 4x^3 + 3x^2 + 2;$
- 27).  $p = 3, \quad m(x) = x^4 + x^2 + x + 2, \quad f(x) = x^3 + 2x^2 + 1;$
- 28).  $p = 2, \quad m(x) = x^5 + x^4 + x^2 + x + 1, \quad f(x) = x^4 + x^3 + 1;$
- 29).  $p = 5, \quad m(x) = x^4 + x^3 + 2x + 4, \quad f(x) = x^3 + x^2 + x + 1;$
- 30).  $p = 3, \quad m(x) = x^4 + x + 2, \quad f(x) = 2x^3 + x^2 + 1.$

### Задание № 16

Найти все унитарные неприводимые многочлены из кольца  $\mathbb{Z}_p[x]$  вида:

- 1).  $x^2 + ax + b, \quad p = 13, \quad a = 4, 5;$
- 2).  $x^3 + ax^2 + b, \quad p = 13, \quad a = 10, 11;$
- 3).  $x^3 + ax^2 + b, \quad p = 11, \quad a = 1, 2;$
- 4).  $x^2 + ax + b, \quad p = 13, \quad a = 0, 1;$
- 5).  $x^3 + ax^2 + b, \quad p = 13, \quad a = 8, 9;$
- 6).  $x^3 + ax + b, \quad p = 11, \quad a = 1, 2;$
- 7).  $x^2 + ax + b, \quad p = 13, \quad a = 2, 3;$
- 8).  $x^3 + ax^2 + b, \quad p = 13, \quad a = 0, 1;$
- 9).  $x^3 + ax^2 + b, \quad p = 11, \quad a = 3, 4;$
- 10).  $x^3 + ax + b, \quad p = 13, a = 3, 4, 5;$
- 11).  $x^3 + ax^2 + b, \quad p = 13, \quad a = 2, 3;$
- 12).  $x^2 + ax + b, \quad p = 7, \quad a = 0, 1, 2, 3;$
- 13).  $x^3 + ax^2 + b, \quad p = 11, \quad a = 7, 8;$
- 14).  $x^2 + ax + b, \quad p = 13, \quad a = 8, 9;$
- 15).  $x^3 + ax + b, \quad p = 13, a = 0, 1, 2;$
- 16).  $x^3 + ax^2 + b, \quad p = 11, \quad a = 5, 6;$
- 17).  $x^3 + ax^2 + b, \quad p = 13, \quad a = 4, 5;$
- 18).  $x^2 + ax + b, \quad p = 13, \quad a = 6, 7;$
- 19).  $x^3 + ax + b, \quad p = 11, \quad a = 9, 10;$

- 20).  $x^2 + ax + b$ ,  $p = 13$ ,  $a = 12$ ;
- 21).  $x^3 + ax^2 + b$ ,  $p = 13$ ,  $a = 12$ ;
- 22).  $x^2 + ax + b$ ,  $p = 7$ ,  $a = 4, 5, 6$ ;
- 23).  $x^3 + ax^2 + b$ ,  $p = 11$ ,  $a = 9, 10$ ;
- 24).  $x^2 + ax + b$ ,  $p = 13$ ,  $a = 10, 11$ ;
- 25).  $x^3 + ax + b$ ,  $p = 13$ ,  $a = 9, 10, 11$ ;
- 26).  $x^3 + ax + b$ ,  $p = 11$ ,  $a = 3, 4$ ;
- 27).  $x^3 + ax^2 + b$ ,  $p = 13$ ,  $a = 6, 7$ ;
- 28).  $x^3 + ax + b$ ,  $p = 13$ ,  $a = 6, 7, 8$ ;
- 29).  $x^3 + ax + b$ ,  $p = 11$ ,  $a = 7, 8$ ;
- 30).  $x^3 + ax + b$ ,  $p = 11$ ,  $a = 5, 6$ .

### Задание № 17

Построить фактор-кольцо  $\mathbb{Z}_p[x]/(m(x))$ . Является ли это кольцо полем?

- |   |  |
|---|--|
| 1). $\mathbb{Z}_3[x]/(x^3 + 2x^2 + 1)$ ;          | 16). $\mathbb{Z}_2[x]/(x^5 + x^4 + x^3 + x + 1)$ ;   |
| 2). $\mathbb{Z}_5[x]/(x^2 + x + 2)$ ;             | 17). $\mathbb{Z}_7[x]/(x^2 + 3x + 5)$ ;              |
| 3). $\mathbb{Z}_2[x]/(x^5 + x^2 + 1)$ ;           | 18). $\mathbb{Z}_2[x]/(x^4 + x^3 + 1)$ ;             |
| 4). $\mathbb{Z}_7[x]/(x^2 + 6x + 3)$ ;            | 19). $\mathbb{Z}_2[x]/(x^5 + x^4 + x^3 + x^2 + 1)$ ; |
| 5). $\mathbb{Z}_5[x]/(x^2 + 2x + 3)$ ;            | 20). $\mathbb{Z}_2[x]/(x^6 + x^5 + x^3 + x^2 + 1)$ ; |
| 6). $\mathbb{Z}_2[x]/(x^6 + x + 1)$ ;             | 21). $\mathbb{Z}_2[x]/(x^5 + x^3 + 1)$ ;             |
| 7). $\mathbb{Z}_2[x]/(x^5 + x^3 + x^2 + x + 1)$ ; | 22). $\mathbb{Z}_7[x]/(x^2 + 4x + 5)$ ;              |
| 8). $\mathbb{Z}_7[x]/(x^2 + x + 3)$ ;             | 23). $\mathbb{Z}_2[x]/(x^5 + x^4 + x^2 + x + 1)$ ;   |
| 9). $\mathbb{Z}_2[x]/(x^3 + x + 1)$ ;             | 24). $\mathbb{Z}_3[x]/(x^3 - 2x^2 - x - 2)$ ;        |
| 10). $\mathbb{Z}_3[x]/(x^2 + x + 2)$ ;            | 25). $\mathbb{Z}_3[x]/(x^3 + 2x^2 + x + 1)$ ;        |
| 11). $\mathbb{Z}_5[x]/(x^2 + 4x + 2)$ ;           | 26). $\mathbb{Z}_5[x]/(x^2 + 3x + 3)$ ;              |
| 12). $\mathbb{Z}_2[x]/(x^6 + x^5 + 1)$ ;          | 27). $\mathbb{Z}_7[x]/(x^2 + 5x + 3)$ ;              |
| 13). $\mathbb{Z}_3[x]/(x^2 + 2x + 2)$ ;           | 28). $\mathbb{Z}_2[x]/(x^6 + x^5 + x^2 + x + 1)$ ;   |
| 14). $\mathbb{Z}_7[x]/(x^2 + 2x + 5)$ ;           | 29). $\mathbb{Z}_3[x]/(x^3 - x^2 - 2)$ ;             |
| 15). $\mathbb{Z}_2[x]/(x^3 + x^2 + 1)$ ;          | 30). $\mathbb{Z}_3[x]/(x^3 - x + 1)$ .               |

## Задание № 18

Разложить на свободные от квадратов множители в кольце  $\mathbb{Q}[x]$  :

- 1).  $x^9 - x^8 - 2x^5 + 2x^4 + x - 1$ ;
- 2).  $x^7 - 2x^5 - x^4 + x^3 + 2x^2 - 1$ ;
- 3).  $x^8 + 4x^7 + 7x^6 + 6x^5 - 6x^3 - 7x^2 - 4x - 1$ ;
- 4).  $x^8 - x^6 - 2x^5 + 2x^3 + x^2 - 1$ ;
- 5).  $x^7 - 2x^5 + x^4 + x^3 - 2x^2 + 1$ ;
- 6).  $x^8 - x^6 + 2x^5 - 2x^3 + x^2 - 1$ ;
- 7).  $x^9 + 2x^8 + 2x^7 + 3x^6 + 4x^5 + 4x^4 + 3x^3 + 2x^2 + 2x + 1$ ;
- 8).  $x^9 - 4x^8 + 8x^7 - 11x^6 + 12x^5 - 12x^4 + 11x^3 - 8x^2 + 4x - 1$ ;
- 9).  $x^9 + 4x^8 + 8x^7 + 11x^6 + 12x^5 + 12x^4 + 11x^3 + 8x^2 + 4x + 1$ ;
- 10).  $x^9 - 2x^8 + 2x^7 - 3x^6 + 4x^5 - 4x^4 + 3x^3 - 2x^2 + 2x - 1$ ;
- 11).  $x^7 + 2x^6 - 3x^4 - 3x^3 + 2x + 1$ ;
- 12).  $x^5 + 3x^4 + x^3 - x^2 - 4$ ;
- 13).  $x^8 + 2x^6 - 2x^2 - 1$ ;
- 14).  $x^8 + 2x^7 + 2x^6 + 2x^5 - 2x^3 - 2x^2 - 2x - 1$ ;
- 15).  $x^5 - x^3 - x^2 + 1$ ;
- 16).  $x^6 - 3x^5 + 6x^3 - 3x^2 - 3x + 2$ ;
- 17).  $x^6 + 3x^5 - 6x^3 - 3x^2 + 3x + 2$ ;
- 18).  $x^7 - 3x^6 + 2x^5 - 2x^4 + x^3 + 5x^2 + 4$ ;
- 19).  $x^7 + 3x^6 + 2x^5 + 2x^4 + x^3 - 5x^2 - 4$ ;
- 20).  $x^{10} + x^8 - 2x^6 - 2x^4 + x^2 + 1$ ;
- 21).  $x^8 - 2x^7 + 2x^5 - 2x^4 + 2x^3 - 2x + 1$ ;
- 22).  $x^8 + 2x^7 - 2x^5 - 2x^4 - 2x^3 + 2x + 1$ ;
- 23).  $x^8 - x^7 - 2x^6 + x^5 + 2x^4 + x^3 - 2x^2 - x + 1$ ;
- 24).  $x^8 - 3x^7 + 2x^6 + 3x^5 - 6x^4 + 3x^3 + 2x^2 - 3x + 1$ ;
- 25).  $x^8 + 3x^7 + 2x^6 - 3x^5 - 6x^4 - 3x^3 + 2x^2 + 3x + 1$ ;
- 26).  $x^8 + x^7 - 2x^6 - x^5 + 2x^4 - x^3 - 2x^2 + x + 1$ ;
- 27).  $x^9 + x^8 - 2x^5 - 2x^4 + x + 1$ ;
- 28).  $x^7 - 2x^6 + 3x^4 - 3x^3 + 2x - 1$ ;
- 29).  $x^6 + 2x^5 + 2x^4 - 2x^2 - 2x - 1$ ;
- 30).  $x^6 - 2x^5 + 2x^4 - 2x^2 + 2x - 1$ .

### Задание № 19

В поле Галуа  $GF(q)$  найти примитивный элемент :

- |                 |                  |                  |
|-----------------|------------------|------------------|
| 1). $q = 43$ ;  | 11). $q = 181$ ; | 21). $q = 89$ ;  |
| 2). $q = 109$ ; | 12). $q = 131$ ; | 22). $q = 73$ ;  |
| 3). $q = 197$ ; | 13). $q = 61$ ;  | 23). $q = 163$ ; |
| 4). $q = 47$ ;  | 14). $q = 179$ ; | 24). $q = 137$ ; |
| 5). $q = 113$ ; | 15). $q = 103$ ; | 25). $q = 79$ ;  |
| 6). $q = 193$ ; | 16). $q = 67$ ;  | 26). $q = 157$ ; |
| 7). $q = 53$ ;  | 17). $q = 173$ ; | 27). $q = 107$ ; |
| 8). $q = 127$ ; | 18). $q = 101$ ; | 28). $q = 97$ ;  |
| 9). $q = 191$ ; | 19). $q = 71$ ;  | 29). $q = 193$ ; |
| 10). $q = 59$ ; | 20). $q = 167$ ; | 30). $q = 151$ . |

### Задание № 20

Найти минимальный многочлен элемента  $\beta$  в  $\mathbb{Z}_p[x]$ , если  $\alpha$  – корень неприводимого многочлена  $m(x)$  из кольца  $\mathbb{Z}_p[x]$  :

- 1).  $\beta = \alpha + 1$ ,  $m(x) = x^4 + x^3 + x^2 + x + 1$ ,  $p = 2$ ;
- 2).  $\beta = \alpha + 2$ ,  $m(x) = x^3 + 2x^2 + 1$ ,  $p = 3$ ;
- 3).  $\beta = \alpha + 3$ ,  $m(x) = x^3 + x^2 + 1$ ,  $p = 5$ ;
- 4).  $\beta = 5\alpha + 1$ ,  $m(x) = x^3 + x^2 + 1$ ,  $p = 7$ ;
- 5).  $\beta = \alpha + 1$ ,  $m(x) = x^4 + x + 1$ ,  $p = 2$ ;
- 6).  $\beta = 2\alpha + 2$ ,  $m(x) = x^3 + 2x + 2$ ,  $p = 3$ ;
- 7).  $\beta = 2\alpha + 4$ ,  $m(x) = x^3 + x + 1$ ,  $p = 5$ ;
- 8).  $\beta = 3\alpha + 4$ ,  $m(x) = x^3 + x^2 + x + 2$ ,  $p = 7$ ;
- 9).  $\beta = \alpha + 1$ ,  $m(x) = x^5 + x^3 + 1$ ,  $p = 2$ ;
- 10).  $\beta = 2\alpha + 1$ ,  $m(x) = x^3 + 2x^2 + x + 1$ ,  $p = 3$ ;
- 11).  $\beta = 3\alpha + 1$ ,  $m(x) = x^3 + 2x^2 + 1$ ,  $p = 5$ ;
- 12).  $\beta = 2\alpha + 3$ ,  $m(x) = x^3 + 2x^2 + x + 4$ ,  $p = 7$ ;
- 13).  $\beta = \alpha + 1$ ,  $m(x) = x^5 + x^2 + 1$ ,  $p = 2$ ;
- 14).  $\beta = \alpha + 1$ ,  $m(x) = x^3 + x^2 + 2x + 1$ ,  $p = 3$ ;
- 15).  $\beta = 4\alpha + 3$ ,  $m(x) = x^3 + 2x + 1$ ,  $p = 5$ ;
- 16).  $\beta = 2\alpha + 5$ ,  $m(x) = x^3 + x + 1$ ,  $p = 7$ ;
- 17).  $\beta = \alpha + 1$ ,  $m(x) = x^5 + x^4 + x^3 + x^2 + 1$ ,  $p = 2$ ;
- 18).  $\beta = 2\alpha + 1$ ,  $m(x) = x^3 + x^2 + x + 2$ ,  $p = 3$ ;
- 19).  $\beta = 2\alpha + 3$ ,  $m(x) = x^3 + x^2 + 2$ ,  $p = 5$ ;

- 20).  $\beta = 4\alpha + 3, \quad m(x) = x^3 + x^2 + 3, \quad p = 7;$
- 21).  $\beta = \alpha + 1 \quad m(x) = x^5 + x^4 + x^3 + x + 1, \quad p = 2;$
- 22).  $\beta = \alpha + 2, \quad m(x) = x^3 + x^2 + 2 \quad p = 3;$
- 23).  $\beta = 4\alpha + 1, \quad m(x) = x^3 + x + 4, \quad p = 5;$
- 24).  $\beta = 2\alpha + 5, \quad m(x) = x^3 + x^2 + x + 5, \quad p = 7;$
- 25).  $\beta = \alpha + 1, \quad m(x) = x^5 + x^4 + x^2 + x + 1, \quad p = 2;$
- 26).  $\beta = 2\alpha + 2, \quad m(x) = x^3 + 2x + 1, \quad p = 3;$
- 27).  $\beta = 3\alpha + 2, \quad m(x) = x^3 + 3x^2 + 4x + 1, \quad p = 5;$
- 28).  $\beta = 6\alpha + 3, \quad m(x) = x^3 + 2x^2 + x + 6, \quad p = 7;$
- 29).  $\beta = \alpha + 1, \quad m(x) = x^5 + x^3 + x^2 + x + 1, \quad p = 2;$
- 30).  $\beta = 2\alpha + 1, \quad m(x) = x^3 + 2x^2 + 2x + 2, \quad p = 3.$

### Задание № 21

Разложить в кольце  $\mathbb{Z}_p[x]$  многочлен на неприводимые множители :

- 1).  $x^{2^4} - x, \quad p = 2, \quad GF(2^4) \equiv \mathbb{Z}_2[x]/(x^4 + x^3 + 1);$
- 2).  $x^{3^3} - x, \quad p = 3, \quad GF(3^3) \equiv \mathbb{Z}_3[x]/(x^3 + 2x^2 + 1);$
- 3).  $x^{2^5} - x, \quad p = 2, \quad GF(2^5) \equiv \mathbb{Z}_2[x]/(x^5 + x^3 + 1);$
- 4).  $x^{2^6} - x, \quad p = 2, \quad GF(2^6) \equiv \mathbb{Z}_2[x]/(x^6 + x^5 + 1);$
- 5).  $x^{5^2} - x, \quad p = 5, \quad GF(5^2) \equiv \mathbb{Z}_5[x]/(x^2 + x + 2);$
- 6).  $x^{3^4} - x, \quad p = 3, \quad GF(3^4) \equiv \mathbb{Z}_3[x]/(x^4 + x + 2);$
- 7).  $x^{7^2} - x, \quad p = 7, \quad GF(7^2) \equiv \mathbb{Z}_7[x]/(x^2 + 5x + 3);$
- 8).  $x^{2^7} - x, \quad p = 2, \quad GF(2^7) \equiv \mathbb{Z}_2[x]/(x^7 + x + 1);$
- 9).  $x^{5^3} - x, \quad p = 5, \quad GF(5^3) \equiv \mathbb{Z}_5[x]/(x^3 + x^2 + 2);$
- 10).  $x^{11^2} - x, \quad p = 11, \quad GF(11^2) \equiv \mathbb{Z}_{11}[x]/(x^2 - 2x - 5).$

## Список литературы

1. Яблокова, С. И. Основы алгебраической алгоритмики. Ч. 1 / С. И. Яблокова. — Ярославль : ЯрГУ, 2008.
2. Яблокова, С. И. Основы алгебраической алгоритмики. Ч. 2 / С. И. Яблокова. — Ярославль : ЯрГУ, 2009.
3. Ноден, П. Алгебраическая алгоритмика / П. Ноден, К. Китте — М. : Мир, 1999.
4. Акритас, А. Основы компьютерной алгебры с приложениями / А. Акритас. — М. : Мир, 1994.

Учебное издание

Яблокова Светлана Ивановна

# Задачи по алгебраической алгоритмике

*Часть 2*

*Практикум*

Редактор, корректор Л. Н. Селиванова  
Верстка С. И. Яблокова

Подписано в печать 20.04.18. Формат 60×84 1/8  
Усл.- печ. л. 6,5. Уч.- изд. л. 2,0.  
Тираж 3 экз. Заказ

Оригинал-макет подготовлен  
в редакционно-издательском отделе ЯрГУ.

Ярославский государственный университет  
им. П.Г. Демидова  
150003, Ярославль, ул. Советская, 14.