Г. Б. Поднебесова

# КОМПЬЮТЕРНАЯ АЛГЕБРА

Челябинск
2023

УДК 681.14:512(021)
ББК 32.973:21.14я73
П 44

**Поднебесова, Г.Б. Компьютерная алгебра:** учебно-практическое пособие / Г.Б. Поднебесова. – Челябинск: Изд-во ЗАО «Библиотека А. Миллера». 2023. – 82 с.

ISBN 978-5-93162-447-1

Учебное пособие содержит материал для изучения курса «Компьютерная алгебра». Пособие предназначено для организации аудиторной и самостоятельной работы студентов, обучающихся по направлению 09.03.02 «Информационные системы и технологии».

Учебное пособие адресовано преподавателям и учителям, которым интересна данная предметная область.

Рецензенты:
С.А. Загребина, д-р физ.-мат. наук, профессор ЮУрГУ
А.Л. Королев, канд. техн. наук, доцент ЮУрГГПУ

ISBN 978-5-93162-447-1

## Содержание

## Введение

Компьютерная алгебра являются одной из областей математики и информатики, особенно активно развивающейся в последние годы. Усилия специалистов в этой области направлены как на разработку новых алгоритмов, так и на создание систем компьютерной математики, которые все чаще используются и в научных исследованиях, и в практических приложениях.

Дисциплина «Компьютерная алгебра» относится к модулю части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины/модули» основной профессиональной образовательной программы по направлению подготовки 09.03.02 «Информационные системы и технологии» (уровень образования бакалавриат).

Курс «Компьютерная алгебра» ставит целью познакомить студентов с характеристикой основных понятий компьютерной математики: число, числовые системы, числовые поля, полиномы и др.

Для характеристики ключевых понятий в курс включены аналитические подходы к определению понятий целого числа, наибольшего общего делителя, обратного элемента и др.

В качестве ключевого понятия компьютерной математики взято понятие алгоритма символьных преобразований. Особенностью данного пособия является описание и примеры использования модулярных методов при работе с длинными целыми числами и полиномами.

Для организации изучения данного курса предполагается проведение лекционных и практических занятий.

На лекционных занятиях рекомендуется рассмотрение теоретических вопросов компьютерной математики, их взаимосвязей и основных характеристик.

Основной целью практических занятий является знакомство студентов с основными алгоритмами, используемыми в системах компьютерной математики.

Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы представлены в таблице 1.

Таблица 1 – Планируемые результаты обучения

| № п/п | Код и наименование компетенции по ФГОС |
|---|---|
| **Код и наименование индикатора достижения компетенции** | |
| 1 | ПК-1 готовность применять знания теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов |
| | ПК-1.1 Знать основные принципы теоретической информатики, фундаментальной и прикладной математики в сфере анализа и синтеза информационных систем и процессов |
| | ПК-1.2 Уметь применять знания теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов |
| | ПК-1.3 Иметь навыки владения основными принципами теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов |

| № п/п | Код и наименование индикатора достижения компетенции | Образовательные результаты по дисциплине |
|---|---|---|
| 1 | ПК-1.1 Знать основные принципы теоретической информатики, фундаментальной и прикладной математики в сфере анализа и синтеза информационных систем и процессов | З.1 характеристику числовых систем;<br>З.2 определение основных понятий абстрактной и компьютерной алгебры;<br>З.3 способы кодирования информации;<br>З.4 алгоритмы компьютерной алгебры для анализа и синтеза информационных систем и процессов. |
| 2 | ПК-1.2 Уметь применять знания теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов | У.1 выполнять операции на множестве целых и комплексных чисел при разработке информационных систем;<br>У.2 применять алгоритмы компьютерной алгебры для анализа и синтеза информационных систем и процессов. |
| 3 | ПК-1.3 Иметь навыки владения основными принципами теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов | В.1 методами описания алгоритмов компьютерной алгебры для анализа и синтеза информационных систем и процессов;<br>В.2 основными алгоритмами компьютерной алгебры для программирования вычислительного блока систем. |

## Содержание разделов дисциплины

1. Представление данных в компьютере.

Арифметические вычисления и операции. Представление целых чисел в компьютере. Умножение длинных чисел. Представление и работа с другими математическими объектами. Представление полиномов. Представление рациональных, алгебраических и трансцендентных функций.

2. Алгоритмы компьютерной математики.

Отношение делимости, его простейшие свойства. Классы вычетов. Наибольший общий делитель (НОД), наименьшее общее кратное (НОК). Алгоритм Евклида и теорема Ламе. Расширенный алгоритм Евклида. Алгоритм Евклида. Простые числа. Разложение целых чисел на множители; разложение больших целых чисел на множители. Точные вычисления, использующие модулярную арифметику. Представление больших целых чисел в памяти компьютера.

3. Полиномы от одной и нескольких переменных.

Отношение делимости полиномов. Теорема о делении с остатком. Схема Горнера. Корни полинома, теорема Безу. НОД и НОК полиномов. Алгоритм Евклида для полиномов от одной переменной. Взаимно простые полиномы. Приводимые и неприводимые полиномы. Разложение на неприводимые множители, единственность разложения. Лексикографический порядок следования членов. Понятие о стандартном базисе. Алгоритм Бухбергера.

4. Компьютерная система Wolfram Alpha. Применение алгоритмов компьютерной математики.

Полиномы от одной и нескольких переменных в Wolfram Alpha. Дифференцирование в системах компьютерной математики. Задача интегрирования. Интегрирование рациональных функций. Интегрирование более сложных функций. Криптосистема RSA.

## Темы и планы практических занятий

**Модуль 1. Представление данных в компьютере.**

1. Разработка кейса по СКМ (2 часа):

– работа в Publisher;

– изучение шаблона кейс.pub;

– разработка кейса.

**Модуль 2. Алгоритмы компьютерной математики.**

1. Вычисление наибольшего общего делителя (НОД). Расширенный алгоритм Евклида (2 часа).

– вычисления НОД методом разложения на множители;

– вычисления НОД методом с помощью алгоритма Евклида;

– расширенный алгоритм Евклида.

2. Модулярная арифметика (2 часа):

– восстановление произведения двух чисел по их модулярным компонентам.

3. Разложение на множители (2 часа)

– разложение на множители методом деления;

– разложение на множители методом Ферма.

**Модуль 3. Полиномы от одной и нескольких переменных.**

1. Вычисление полиномов (2 часа):

– бинарный метод и метод множителей;

– схема Горнера, обобщенная схема Горнера.

2. Нахождение НОД полиномов (2 часа):

– применение неравенства Ландау-Миньотта;

– вычисление модулярного НОД.

**Модуль 4. Компьютерная система WolframAlpha. Применение алгоритмов компьютерной математики.**

1. Полиномы от одной и нескольких переменных в WolframAlpha (2 часа):

– основные функции для работы с полиномами от одной переменной;

– вычисление НОД полиномов от одной переменной в WolframAlpha.

– основные функции для работы с полиномами от нескольких переменных;

– вычисление НОД полиномов от нескольких переменных в WolframAlpha.

2. Криптосистема RSA (2 часа).

- вычисление n и $\varphi(n)$;
- подписывание сообщения;
- проверка подписи.

## Модуль 1. Представление данных в компьютере

Практическое занятие№1

### Разработка кейса по СКА

В кейсе должно быть представлено:

1. Функциональное назначение;
2. Тип архитектуры;
3. Средства реализации;
4. Области применения;
5. Примеры (принтскрины);
6. Интегральные оценки качества.

**Пример**:

Аналитик-С – среда аналитических вычислений.

Официальный сайт проекта: http://www.sgau.ru/analitik_c/

**Основные характеристики**:

Язык реализации – PHP.

Платформа реализации – сервер Apache.

Открытый исходный код.

Синтаксис и функциональность языка Аналитик:

– поддержка символов латиницы, кириллицы и греческих;

– двуязычность ключевых слов: пусть(let), вычислить(calculate) и др.

Базовые функции – комбинаторика, полиномы, матрицы, дифференциалы, интегралы, тригонометрия, графика) + специальные расширения (управление в технических системах.

Коллектив разработчиков: аспиранты и студенты СГТУ и СГАУ.

1. Для разработки кейса использовать шаблон кейс.pub (рис. 1) (доступен по ссылке СКА).

2. Темы для разработки кейса находятся в файле СКА_задание.docx.

3. Пример кейса в Publisher представлен на рисунке 2.

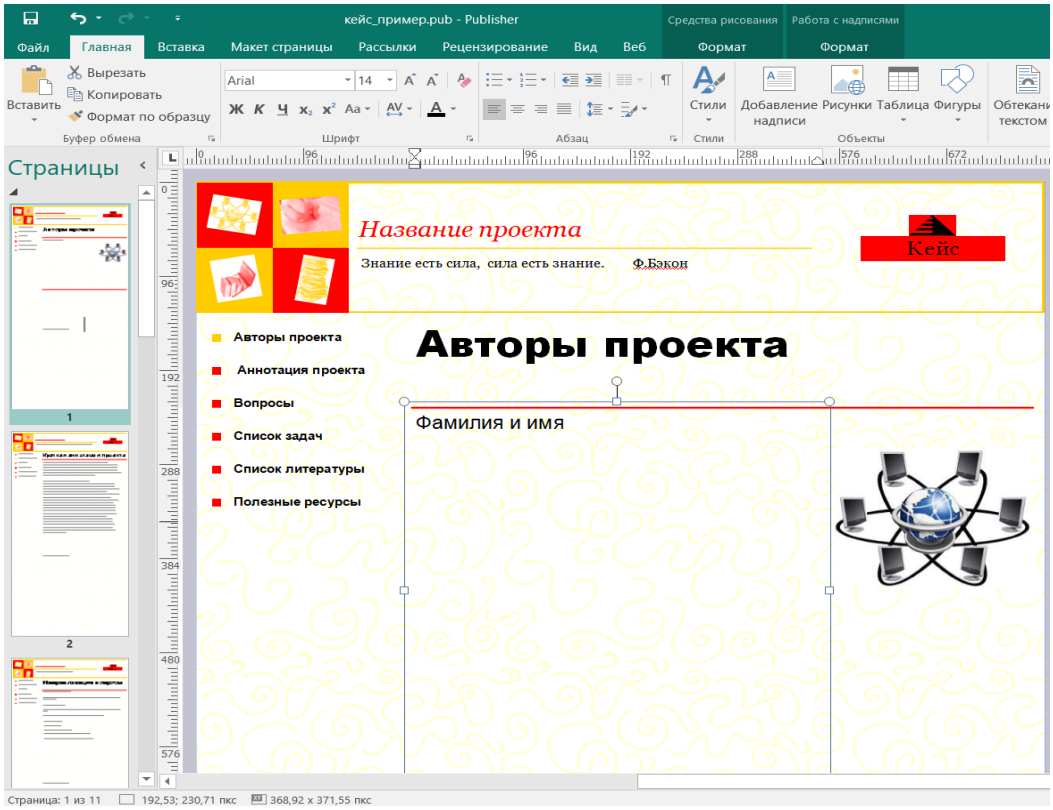



Рис. 1 – Главное окно

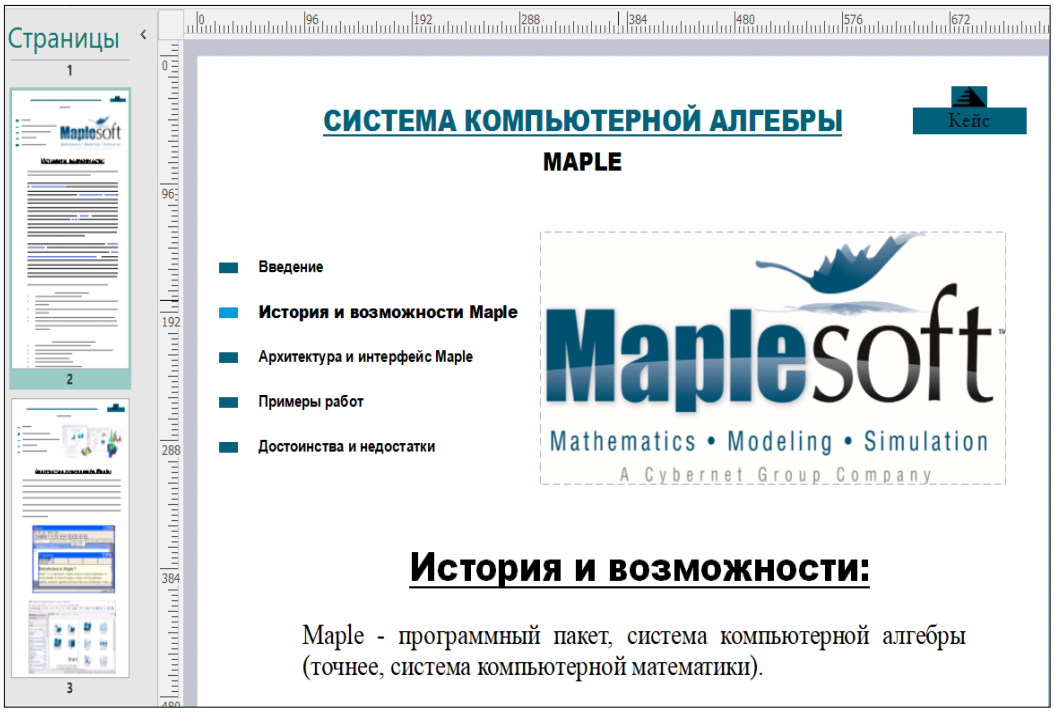



Рис. 2 – Пример кейса в Publisher

4. Готовый кейс сохранить в формате web-страницы. В строке выбора *Тип файла* при сохранении выбрать *Веб-страница в одном файле* (рис.3).

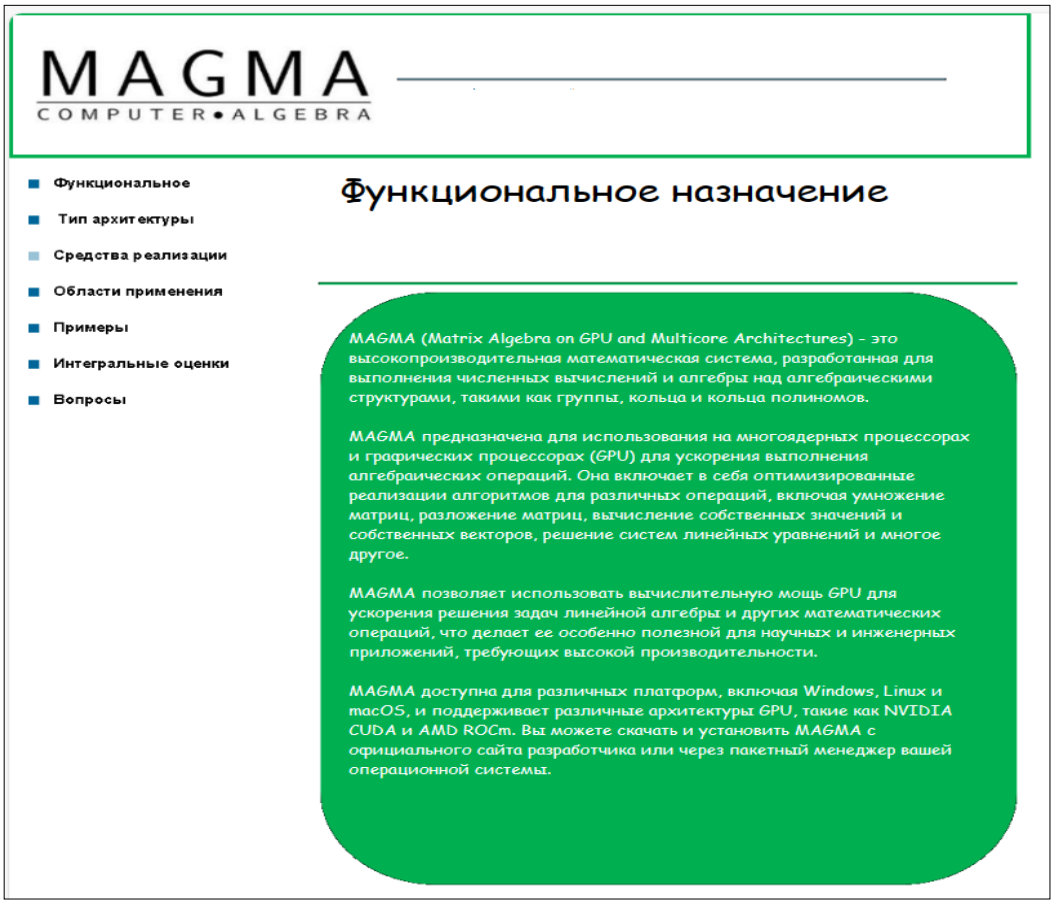


Рис. 3 – Внешний вид кейса в виде сайта

## *Вопросы к модулю 1*

1. Чем отличаются численные методы от аналитических вычислений?
2. Выделить особенности аналитических вычислений на компьютерах?
3. Что является предметом изучения компьютерной алгебры?
4. Какая основная задача компьютерной алгебры?
5. Перечислить интегрированные системы компьютерной алгебры?
6. Как оценивается качество (эффективность) алгоритма?

7. Какие уровни сложности алгоритмов компьютерной алгебры выделяют?

8. Что понимают под временной сложностью алгоритмов?

9. На чем основывается эффективность алгоритма?

10. Как представляются в компьютере целые числа?

11. Какое время счета требуется для выполнения сложения и вычитания?

12. В чем суть метода умножения А.А. Карацубы?

13. Какое представление полиномов называется нормальным, каноническим, разрешенным, полным?

14. Как представляются в компьютере рациональные, алгебраические и трансцендентные функции?

15. Какие классы трансцендентных функций встречаются в системах компьютерной алгебры?

16. Сформулировать теорему Риша.

17. Как представляются матрицы в компьютере?

18. Выделить особенности представления плотных матриц, разреженных матриц.

19. В чем суть метода Барейса?

20. Как представляются ряды в системах компьютерной алгебры?

## Модуль 2. Алгоритмы компьютерной математики

Практическое занятие№2

### Вычисление наибольшего общего делителя (НОД). Расширенный алгоритм Евклида.

**1. Вычисление НОД.**

$a = \prod_{p|a} p^{\alpha_p}$ , $b = \prod_{p|b} p^{\beta_p}$ – каноническое разложения целых положительных чисел $a$ и $b$. $d$ = НОД($a$, $b$), где $d = \prod_{\substack{p|a \\ p|b}} p^{\min(\alpha_p,\ \beta_p)}$ .

**Пример 1.** Найти наибольший общий делитель чисел a = 24 и b = 18.

Раскладываем числа a и b на простые множители. $24 = 2^3 \cdot 3$, $18 = 2 \cdot 3^2$. Берем множители, входящие в оба разложения в минимальной степени. Получаем $d = 2 \cdot 3 = 6$. Следовательно, НОД(24, 18) = 6.

**Задание 1**. Найти НОД чисел 24 и 35, 26 и 39, 35 и 72.

2. **Вычисление НОД с помощью алгоритма Евклида**.

$$
\begin{aligned}
a &= bq_0 + r_1, && 0 \le r_1 < |b|, \\
b &= r_1 q_1 + r_2, && 0 \le r_2 < r_1, \\
&\ldots && \ldots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, && 0 \le r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n + r_{n+1}.
\end{aligned}
\qquad (15)
$$

**Пример 2.** Найти наибольший общий делитель чисел a = 24 и b = 18 с помощью алгоритма Евклида.

Делим целое число a = 24 на b = 18, получаем неполное частное q = 1 и остаток r = 6. Продолжаем деление, пока $r_{i+1}$ не будет равно нулю.

$24 = 18 \cdot 1 + 6$

Далее, делим b = 18 на остаток r = 6, получаем неполное частное $q_1 = 3$ и остаток $r_1 = 0$.

$18 = 6 \cdot 3 + 0$

Последний ненулевой остаток есть НОД. Следовательно, НОД(24, 18) = 6.

**Задание 2**. Найти НОД чисел 37 и 26, 64 и 23, 54 и 18.

3. **Алгоритмы вычислений с дробями**.

a) Требуется вычислить произведение

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{p}{q}.$$

Очевидный способ: вычислить p = a · c, q = d · b и затем сократить на НОД этих чисел. Однако, используя равенство НОД(p, q) = НОД(a, d) · НОД(b, c), можно более эффективно вычислить два НОД в правой части равенства, чем вычислять один НОД в левой части, так как аргументы у них меньше.

Получим следующую последовательность действий для вычисления произведения:

НОД(a, d); НОД(b, c); a' = a/ НОД(a, d); b' = b / НОД(b, c);

c' = c / НОД(b, c); d' = d / НОД(a, d); p = a' · c', q = d' · b'.

**Задание 3**.

1) $\frac{25}{28} \cdot \frac{12}{45}$, вычислять НОД 1 способом;

2) $\frac{12}{25} \cdot \frac{15}{32}$, вычислять НОД, используя простой алгоритм;

b) Требуется найти сумму

$$\frac{a}{b} + \frac{c}{d} = \frac{p}{q}.$$

Вместо формул p = a · d + b · c, q = b · d с последующим вычислением НОД(p, q) и сокращением на него чисел p и q более эффективна следующая последовательность вычислений:

НОД(b, d); q' = b · d / НОД(b, d); b' = b / НОД(b, d); d' = d / НОД(b, d);

p' = a · d'+b' · c; НОД(p', q'); p = p' / НОД(p', q'); q = q' / НОД(p', q').

Для большей наглядности лучше всего взять дроби со знаменателями, имеющими НОД, отличный от 1. Для вычисления НОД можно воспользоваться любым способом.

**Задание 4**.

1) $\frac{15}{32}+\frac{18}{40}$, проверить прямым способом;

**Самостоятельно:**

Таблица 2 – Задания на умножение и сложение дробей

| | | | |
|---|---|---|---|
| 1. | $\frac{48}{69}\cdot\frac{26}{144}, \frac{36}{45}+\frac{15}{84}$ | 7. | $\frac{18}{39}\cdot\frac{26}{66}, \frac{46}{55}+\frac{16}{88}$ |
| 2. | $\frac{36}{45}\cdot\frac{25}{48}, \frac{13}{36}+\frac{16}{48}$ | 8. | $\frac{33}{40}\cdot\frac{25}{48}, \frac{13}{35}+\frac{16}{45}$ |
| 3. | $\frac{36}{44}\cdot\frac{26}{48}, \frac{34}{102}+\frac{28}{72}$ | 9. | $\frac{66}{104}\cdot\frac{20}{39}, \frac{34}{92}+\frac{28}{42}$ |
| 4. | $\frac{21}{36}\cdot\frac{36}{42}, \frac{12}{54}+\frac{24}{32}$ | 10. | $\frac{22}{38}\cdot\frac{54}{44}, \frac{41}{64}+\frac{26}{48}$ |
| 5. | $\frac{35}{104}\cdot\frac{26}{48}, \frac{25}{56}+\frac{48}{75}$ | 11. | $\frac{34}{92}\cdot\frac{23}{51}, \frac{25}{45}+\frac{29}{65}$ |
| 6. | $\frac{35}{96}\cdot\frac{26}{48}, \frac{24}{55}+\frac{58}{75}$ | 12. | $\frac{55}{105}\cdot\frac{34}{70}, \frac{19}{48}+\frac{38}{72}$ |

## 4. Расширенный алгоритм Евклида.

Расширенный алгоритм Евклида базируется на следующем рекуррентном соотношении:

$$\begin{cases} u_0 = 1, \quad v_0 = 0, \quad r_0 = a, \\ u_1 = 0, \quad v_1 = 1, \quad r_1 = b, \\ u_{i+1} = u_{i-1} - q_i u_i, \quad v_{i+1} = v_{i-1} - q_i v_i, \quad r_{i+1} = r_{i-1} - q_i r_i, \end{cases}$$

из которого следует классический результат $r_n = НОД(a, b) = u_n \cdot a + v_n \cdot b$.

**Пример**.

Пусть a=318, b=264. Используя расширенный алгоритм Евклида, найдем наибольший общий делитель чисел a и b, и коэффициенты Безу.

**Решение.** Заполним таблицу 2.

| | | |
|---|---|---|
| $u_0=1$ | $v_0=0$ | $r_0=318$ |
| $u_1=0$ | $v_1=1$ | $r_1=264$ |
| $u_2= u_0 - q_1 u_1$ | $u_3= u_1 - q_2 u_2$ | $u_4= u_2 - q_3 u_3$ |
| $v_2 =v_0 - q_1 v_1$ | $v_3 =v_1 - q_2 v_2$ | $v_4 =v_2 - q_3 v_3$ |
| $r_2 =r_0 - q_1 r_0$ | $r_3 =r_1 - q_2 r_2$ | $r_4 =r_2 - q_3 r_3$ |
| $u_2= 1-1\cdot 0=1$ | $u_3= 0-4\cdot 1= -4$ | $u_4= 1-1\cdot (-4)=5$ |
| $v_2 =0-1\cdot 1= -1$ | $v_3 =1-4\cdot (-1)=5$ | $v_4=-1-1\cdot 5= -6$ |

$r_2 = 318 - 1 \cdot 264 = -54$ $r_3 = 264 - 4 \cdot 54 = 48$ $r_4 = 54 - 1 \cdot 48 = 6$

$u = 5$ ,$v = -6$ НОД(a, b) = 6

Таблица 3 – Пример вычисления НОД

| i | $q_i$ | $u_i$ | $v_i$ | $r_i$ | $u_{i+1}$ | $v_{i+1}$ | $r_{i+1}$ |
|---|---|---|---|---|---|---|---|
| 0 | | 1 | 0 | 318 | 0 | 1 | 264 |
| 1 | 1 | 0 | 1 | 264 | 1 | -1 | 54 |
| 2 | 4 | 1 | -1 | 54 | -4 | 5 | 48 |
| 3 | 1 | -4 | 5 | 48 | 5 | -6 | 6 |
| 4 | 8 | 5 | -6 | 6 | | | 0 |

**Задание 5.** Найти наибольший общий делитель и коэффициенты Безу следующих чисел: 42 и 13 (найти обратный элемент).

**Самостоятельно:**

Найти наибольший общий делитель и коэффициенты Безу (см. таб. 4).

Таблица 4 – Задание для самостоятельного выполнения

| | | | |
|---|---|---|---|
| 1. | 506 и 34 | 7. | 691 и 28 |
| 2. | 610 и 56 | 8. | 309 и 45 |
| 3. | 571 и 78 | 9. | 336 и 77 |
| 4. | 902 и 35 | 10. | 550 и 91 |
| 5. | 305 и 65 | 11. | 303 и 82 |
| 6. | 357 и 68 | 12. | 521 и 73 |

Индивидуальное задание № 1

**Вычисление НОД целых чисел**

1. Найти наибольший общий делитель (см. Пример 1).

Таблица 5 – Задание для вычисления НОД

| | | | |
|---|---|---|---|
| 1. | 48 и 54 | 7. | 32 и 48 |
| 2. | 52 и 64 | 8. | 36 и 42 |
| 3. | 56 и 32 | 9. | 60 и 72 |
| 4. | 24 и 68 | 10. | 84 и 36 |
| 5. | 42 и 84 | 11. | 90 и 64 |
| 6. | 72 и 48 | 12. | 68 и 24 |

2. Найти наибольший общий делитель, используя алгоритм Евклида (табл. 6).

3. Реализовать алгоритм вычисления НОД на языке программирования (+ 0,2 балла).

Таблица 6 – Задание для вычисления НОД с помощью алгоритм Евклида

| | | | |
|---|---|---|---|
| 1. | 342 и 94 | 7. | 422 и 184 |
| 2. | 524 и 82 | 8. | 386 и 87 |
| 3. | 462 и 241 | 9. | 452 и 185 |
| 4. | 386 и 96 | 10. | 368 и 108 |
| 5. | 582 и 166 | 11. | 264 и 122 |
| 6. | 423 и 205 | 12. | 308 и 158 |

4. Вычисления с дробями.

Таблица 7 – Задания на умножение и сложение дробей

| | | | |
|---|---|---|---|
| 1. | $\frac{106}{24}+\frac{18}{140}, \frac{102}{224}\cdot\frac{216}{80}$ | 7. | $\frac{102}{224}+\frac{216}{80}, \frac{106}{24}\cdot\frac{18}{140}$ |
| 2. | $\frac{24}{128}+\frac{116}{32}, \frac{72}{224}\cdot\frac{52}{134}$ | 8. | $\frac{210}{76}+\frac{36}{312}, \frac{54}{84}\cdot\frac{64}{156}$ |
| 3. | $\frac{28}{124}+\frac{132}{40}, \frac{42}{88}\cdot\frac{128}{242}$ | 9. | $\frac{54}{84}+\frac{64}{156}, \frac{418}{52}\cdot\frac{32}{304}$ |
| 4. | $\frac{418}{52}+\frac{32}{304}, \frac{28}{214}\cdot\frac{160}{30}$ | 10. | $\frac{72}{224}+\frac{52}{134}, \frac{48}{168}\cdot\frac{96}{64}$ |
| 5. | $\frac{312}{48}+\frac{36}{156}, \frac{210}{76}\cdot\frac{36}{312}$ | 11. | $\frac{42}{88}+\frac{128}{242}, \frac{28}{124}\cdot\frac{132}{40}$ |
| 6. | $\frac{28}{214}+\frac{160}{30}, \frac{24}{128}\cdot\frac{116}{32}$ | 12. | $\frac{48}{168}+\frac{96}{64}, \frac{102}{224}\cdot\frac{216}{80}$ |

Индивидуальное задание № 2

**Расширенный алгоритм Евклида**

1. Найти наибольший общий делитель и коэффициенты Безу следующих чисел:

Таблица 8 – Задание для вычисления НОД и коэффициентов Безу

| | | | |
|---|---|---|---|
| 1. | 3249; 99 | 7. | 3388; 97 |
| 2. | 2304; 81 | 8. | 2023; 98 |
| 3. | 1445; 280 | 9. | 1350; 72 |
| 4. | 1156; 224 | 10. | 1176; 66 |
| 5. | 1620; 55 | 11. | 1114; 54 |
| 6. | 2645; 68 | 12. | 1944; 66 |

2. Реализовать расширенный алгоритм Евклида в Excel (+ 0,2 балла).

3. Найти обратный элемент, если он существует.

Таблица 9 – Задание для вычисления обратного элемента

| | | | |
|---|---|---|---|
| 1. | к 528 по mod 247 | 7. | к 539по mod 171 |
| 2. | к 749 по mod 316 | 8. | к 528 по mod 247 |
| 3. | к 692 по mod 293 | 9. | к 943 по mod 277 |
| 4. | к 724 по mod 381 | 10. | к 539по mod 171 |
| 5. | к 815 по mod 223 | 11. | к 926 по mod 357 |
| 6. | к 833 по mod 213 | 12. | к 573 по mod 169 |

Практическое занятие №3

## Модулярная арифметика

Хотим перемножить два больших числа a и b. Для этого:

1. Находим последовательность наименьших простых чисел, произведение которых больше произведения этих двух. Обозначим их $n_1$, $n_2$, $n_3$, …, $n_r$.

2. Представим модулярное разложение выбранных чисел a и b по модулям $n_1$, $n_2$, $n_3$, …, $n_r$: $a_1, a_2, …, a_{r;}$ $b_1, b_2, …, b_r$.

3. Восстановим число x. Для этого вычислим $z_1$, $z_2$, …, $z_r$.

4. Определим последнюю цифру числа, используя формулу $x^{(j)}=\Sigma z_i \cdot N_i$.

5. Найдем модулярное представление числа $x' = (x – x_0) /10$: $x' = ((x_1 – x_0) \cdot y_1 \bmod n_1, (x_2 – x_0) \cdot y_2 \bmod n_2, …, (x_r – x_0) \cdot y_r \bmod n_r)$. Если все модулярные компоненты равны нулю, то вычисление закончено. Иначе переходим к пункту 4.

**Пример.**

1. Для чисел 56 и 35 возьмем из таблицы наименьшие простые числа $3 \cdot 17 > 35$, $11 \cdot 7 > 56$, произведение которых больше предполагаемого. Получили $n_1 = 3$, $n_2 = 7$, $n_3 = 11$, $n_4 = 17$.

2. Раскладываем каждое из чисел 56 и 35 по модулю этих четырех простых чисел:

| | 56 | 35 | x |
|---|---|---|---|
| 3 | 2 | 2 | 1 |
| 7 | 0 | 0 | 0 |
| 11 | 1 | 2 | 2 |
| 17 | 5 | 1 | 5 |

Столбец «x» получен следующим образом: $x_1= (2 \cdot 2) \bmod 3=1$, $x_2=(0 \cdot 0) \bmod 7=0$, $x_3=(1 \cdot 2) \bmod 11=2$, $x_4=(5 \cdot 1) \bmod 17=5$

Получили: $x_1=1$, $x_2=0$, $x_3=2$, $x_4=5$.

3. Восстановим число x.

4. Вычислим $z_1$, $z_2$, $z_3$, $z_4$.

$z_1=x_1 \bmod n_1=1 \bmod 3=1$

$z_2=c_2(x_2-z_1) \bmod n_2= c_2 \cdot (0-1) \bmod 7= c_2 \cdot (-1) \bmod 7$ $N_2= n_1$

$c_2N_2 \equiv 1(\bmod n_2) \Rightarrow c_2 \cdot n_1 \equiv 1(\bmod n_2)=3 \cdot c_2 \equiv 1(\bmod 7)$,т.е. $c_2$ - обратное к 3 по mod 7 (см. Таблицу 10)

Таблица 10 – Вычисление обратного числа к 3

| i | $q_i$ | $u_i$ | $v_i$ | $r_i$ | $u_{i+1}$ | $v_{i+1}$ | $r_{i+1}$ |
|---|---|---|---|---|---|---|---|
| 0 | | 1 | 0 | 7 | 0 | 1 | 3 |
| 1 | 2 | 0 | 1 | 3 | 1 | -2 | 1 |
| 2 | 3 | **1** | **-2** | 1 | | | 0 |

$u=1$ $v=-2$ $1=7 \cdot 1 + 3 \cdot (-2)$

$c_2=-2$ ( $-2 \bmod 7 = 5$) $\Rightarrow c_2=5$

$z_2=5 \cdot (-1) \bmod 7=-5 \bmod 7=2$

$z_3=c_3 \cdot (x_3-N_2z_2-z_1) \bmod n_3$

$z_3=c_3(2-3 \cdot z_2-1) \bmod 11= c_3 \cdot (2-3 \cdot 2-1) \bmod 11=c_3 \cdot (-5) \bmod 11$;

$N_3=n_1 \cdot n_2 \Rightarrow N_3=3 \cdot 7=21$

$c_3 N_3 =1( \bmod n_3 ) = c_3 \cdot n_1 \cdot n_2= 1 ( \bmod n_3 ) \Rightarrow c_3 \cdot 21 \equiv 1 ( \bmod 11)$

$c_3$ –обратное к 21 по модулю 11 (см. Таблицу 11)

Таблица 11 – Вычисление обратного числа к 21

| i | $q_i$ | $u_i$ | $v_i$ | $r_i$ | $u_{i+1}$ | $v_{i+1}$ | $r_{i+1}$ |
|---|---|---|---|---|---|---|---|
| 0 | | 1 | 0 | 21 | 0 | 1 | 11 |
| 1 | 1 | 0 | 1 | 11 | 1 | -1 | 10 |
| 2 | 1 | 1 | -2 | 10 | -1 | 3 | 1 |
| 3 | | **-1** | **3** | 1 | | | 0 |

$u=-1$ $v=3$ $1=21 \cdot (-1) + 11 \cdot 2$

$c_3 = -1$ ($-1 \bmod 11 = 10$) $\Rightarrow c_3 =10$

$z_3 = c_3 \cdot (-5) \bmod 11 = 10 \cdot (-5) \bmod 11 = -50 \bmod 11 = 5$

$z_4 = c_4 (x_4 - (N_3 z_3 + N_2 z_2 + z_1)) \bmod n_4$

$z_4 = c_4 (5 - (21 \cdot 5 + 3 \cdot 2 + 1)) \bmod 17 = c_4 (-107) \bmod 17 = (-1287) \bmod 17 = 8$

$N_4 = n_1 \cdot n_2 \cdot n_3 = 3 \cdot 7 \cdot 11 = 231$

$c_4 N_4 \equiv 1 (\bmod n_4) = c_4 (n_1 \cdot n_2 \cdot n_3) \equiv 1 (\bmod n_4) \Rightarrow c_4 \cdot 231 \equiv 1 (\bmod 17)$

$c_4$ – обратное к 231 по модулю 17 (см. Таблицу 12)

$u = -5$ $v = 68$ $1 = 231 \cdot (-5) + 17 \cdot 68$

$c_4 = -5$ ($-5 \bmod 17 = 12$) $\Rightarrow c_4 = 12$

Таблица 12 – Вычисление обратного числа к 231

| i | $q_i$ | $u_i$ | $v_i$ | $r_i$ | $u_{i+1}$ | $v_{i+1}$ | $r_{i+1}$ |
|---|---|---|---|---|---|---|---|
| 0 | | 1 | 0 | 231 | 0 | 1 | 17 |
| 1 | 13 | 0 | 1 | 17 | 1 | -13 | 10 |
| 2 | 1 | 1 | -13 | 10 | -1 | 14 | 7 |
| 3 | 1 | -1 | 14 | 7 | 2 | -27 | 3 |
| 4 | 2 | 2 | -27 | 3 | -5 | 68 | 1 |
| 5 | 3 | **-5** | **68** | 1 | | | 0 |

5. Определим последнюю цифру числа.

$x^{(1)} = (z_1 \cdot N_1 + z_2 \cdot N_2 + z_3 \cdot N_3 + z_4 \cdot N4) \bmod 10 = (z_1 + z_2 \cdot n_1 + z_3 \cdot n_1 \cdot n_2 + z_4 \cdot n_1 \cdot n_2 \cdot n_3) \bmod 10$

$x^{(1)} = (1 + 2 \cdot 3 + 5 \cdot 21 + 8 \cdot 231) \bmod 10 = (1 + 6 + 105 + 8 \cdot 231) \bmod 10 = 20 \bmod 10 = 0$

$x_0 = 0$

6. Перейдем к определению следующей цифры.

Обратное к 10 по модулю $n_1$ равно1 ($10 \cdot y_1 \equiv 1 (\bmod 3)$, обратное к 10 по модулю $n_2$ равно 5 ($10 \cdot y_2 \equiv 1 (\bmod 7)$, обратное к 10 по модулю $n_3$ равно 10 ($10 \cdot y_3 \equiv 1 (\bmod 11)$, обратное к 10 по модулю 17 равно 12 ($10 \cdot y_4 \equiv 1 (\bmod 17)$. Таким образом, $y_1 = 1$, $y_2 = 5$, $y_3 = 10$, $y_4 = 12$.

Определяем модулярные компоненты числа.

$x' = ((x_1 - x_0) \cdot y_1 \bmod n_1, (x_2 - x_0) \cdot y_2 \bmod n_2, (x_3 - x_0) \cdot y_3 \bmod n_3, (x_4 - x_0) \cdot y_4 \bmod n_4)$. Т.к. $x_1=1$, $x_2=0$, $x_3=2$, $x_4=5$, $x_0=0$

$x' = ((1-0) \cdot 1 \bmod 3, (0-0) \cdot 5 \bmod 7, (2-0) \cdot 10 \bmod 11, (5-0) \cdot 12 \bmod 17 =$

$= (1 \bmod 3, 0 \bmod 7, 20 \bmod 11, 60 \bmod 17) = (1, 0, 9, 9)$.

7. Определим предпоследнюю цифру числа.

$x_1'=1, x_2'=0, x_3'=9, x_4'=9$

$n_1=3, n_2=7, n_3=11, n_4=17$

$z_1=x_1' \bmod n_1=1 \bmod 3=1$

$z_2=c_2(x_2'-z_1) \bmod n_2=c_2\cdot(0-1) \bmod n_2=c_2\cdot(-1) \bmod 7$

$c_2\cdot N_2=1 (\text{mod } n_2)\Rightarrow c_2\cdot n_1\equiv 1 \bmod 7=c_2\cdot 3\equiv 1 \bmod 7$

См. таблицу 10.

$c_2=5$

$z_2=-5 \bmod 7=2$

$z_3=c_3(x_3'-(N_2\cdot z_2+z_1)) \bmod n_3$

$z_3=c_3\cdot(9-3\cdot 2-1) \bmod 11=c_3\cdot 2 \bmod 11=20 \bmod 11=9$

$c_3 N_3\equiv 1(\text{mod } n_3)\Rightarrow c_3\cdot n_1\cdot n_2\equiv 1 (\text{mod } n_3)\Rightarrow c_3\cdot 21\equiv 1 \bmod 11$

См. таблицу 11.

$c_3=-1\Rightarrow c_3=10$

$z_4=c_4(x_4'-(N_3\cdot z_3+N_2\cdot z_2+z_1)) \bmod 17$

$z_4=c_4(9-(21\cdot 9+3\cdot 2+1)) \bmod 17=c_4(9-196) \bmod 17=12(-187) \bmod 17=0$

$c_4 N_4\equiv 1(\text{mod } n_4)\Rightarrow c_4(n_1\cdot n_2\cdot n_3)\equiv 1(\text{mod } n_4)$

$c_4\cdot(231)\equiv 1(\text{mod } 17)$. См. таблицу 12.

$c_4=12$

$x^{(2)}=(z_1\cdot N_1+z_2\cdot N_2+z_3\cdot N_3+z_4\cdot N_4) \bmod 10=(z1+z_2\cdot n_1+z_3\cdot n_1\cdot n_2+z_4\cdot n_1\cdot n_2\cdot n_3) \bmod 10$

$x^{(2)}=(1\cdot 1+2\cdot 3+9\cdot 21+0\cdot 17) \bmod 10=(1+6+9) \bmod 10=16 \bmod 10=6$

Найдем модулярное представление числа по формуле

$x''=((x_1'-x_0)\cdot y_1 \bmod n_1, (x_2'-x_0)\cdot y_2 \bmod n_2, (x_3'-x_0)\cdot y_3 \bmod n_3, (x_4'-x_0)\cdot y_4 \bmod n_4)$.

$x_0=6$

$x_1'=1, x_2'=0, x_3'=9, x_4'=9$

$y_1=1, y_2=5, y_3=10, y_4=12$

$x''=(1-6)\cdot 1 \bmod 3, (0-6)\cdot 5 \bmod 7, (9-6)\cdot 10 \bmod 11, (9-6)\cdot 12 \bmod 17=$

= (-5 mod 3, -30 mod 7, 30 mod 11, 36 mod 17) = (1, 5, 5, 2)

8. Вычислим $z_1$, $z_2$, $z_3$, $z_4$ и определим следующую цифру числа.

$x_1''=1$, $x_2''=5$, $x_3''=8$, $x_4''=2$

$n_1=3$, $n_2=7$, $n_3=11$, $n_4=17$

$z_1 = x_1''$ mod $n_1$ =1 mod 3 = 1

$z_2 = c_2 ( x_2'' - z_1 )$ mod $n_2 = c_2 ( 5 – 1 )$ mod 7 = 20 mod 7 = 6

$c_2 \cdot N_2 = 1$ (mod $n_2$ )$\Rightarrow c_2 \cdot n_1 \equiv 1$ mod 7= $c_2 \cdot 3 \equiv 1$ mod 7

См. таблицу 10.

$c_2=5$

$z_3=c_3(x_3''-N_2 \cdot z_2-z_1)$ mod $n_3$

$z_3=c_3(8-3\cdot6-1)$ mod 11= $c_3\cdot(-11)$ mod 11= -110 mod 11=0

$c_3 \; N_3 \equiv 1$(mod $n_3$ )$\Rightarrow c_3 \cdot n_1 \cdot n_2 \equiv 1$ (mod $n_3$ )$\Rightarrow c_3 \cdot 21 \equiv 1$ mod 11

См. таблицу 11.

$c_3$= -1$\Rightarrow c_3$ =10

$z_4=c_4(x_4''-N_3\cdot z_3-N_2\cdot z_2-z_1)$ mod $n_4$

$c_4 \cdot (231) \equiv 1$(mod 17). См. таблицу 12.

$c_4$ =12

$z_4=c_4(2-21\cdot0-3\cdot6-1)$ mod 17=$c_4$(-17) mod 17=0

$x^{(3)}$= ($z_1 \cdot N_1 + z_2 \cdot N_2 + z_3 \cdot N_3 + z_4 \cdot N4$) mod 10=($z1 + z_2 \cdot n_1 + z_3 \cdot n_1 \cdot n_2 + z_4 \cdot n_1 \cdot n_2 \cdot n_3$) mod 10

$x^{(3)}$=(1+6·3+0+0) mod 10=(1+18) mod 10=19 mod 10=9

Найдем модулярное представление числа по формуле

$x''' = ((x_1'' – x_0) \cdot y_1$ mod $n_1$, $(x_2'' – x_0) \cdot y_2$ mod $n_2$, $(x_3'' – x_0) \cdot y_3$ mod $n_3$, $(x_4'' – x_0) \cdot y_4$ mod $n_4$).

$y_1 = 1$, $y_2 = 5$, $y_3 = 10$, $y_4 = 12$

$x_0 = 9$

$x_1'' = 1$, $x_2'' = 5$, $x_3'' = 8$, $x_4'' = 2$

$x''' = ((1 - 9) \cdot$ mod 3, $(5 - 9) \cdot 5$ mod 7, $(8 - 9) \cdot 10$ mod 11, $(2 - 9) \cdot 12$ mod 17) =

= (-8 mod 3, -20 mod 7, -10 mod 11, -84 mod 17) = ( 1, 1, 1, 1)

9. Вычислим $z_1$, $z_2$, $z_3$, $z_4$ и определим следующую цифру числа.

$x_1''' = 1$, $x_2''' = 1$, $x_3''' = 1$, $x_4''' = 1$

$n_1 = 3$, $n_2 = 7$, $n_3=11$, $n_4 = 17$

$z_1 = x_1'' \bmod n_1 = 1 \bmod 3 = 1$

$z_2 = c_2( x_2''' - z_1 ) \bmod n_2 = c_2(1-1) \bmod 7 = 0$

$z_3 = c_3( x_3''' – N_2 \cdot z_2 – z_1 ) \bmod n_3 = c_3(1-3 \cdot 0-1) \bmod 11= 0$

$z_4 = c_4( x_4''' – N_3 \cdot z_3 – N_2 \cdot z_2 – z_1 ) \bmod n_4 = c_4 (1 - 21 \cdot 0 - 3 \cdot 0 - 1) \bmod 17 = 0$

$x^{(4)} = (z_1 + z_2 \cdot n_1 + z_3 \cdot n_1 \cdot n_2 + Z_4 \cdot n_1 \cdot n_2 \cdot n_3) \bmod 10$

$x^{(4)} = (1+0 \cdot 3+0 \cdot 3 \cdot 7+0 \cdot 3 \cdot 7 \cdot 11) \bmod 10=1$

Найдем модулярное представление числа.

$x'''' = ((x_1''' – x_0) \cdot y_1 \bmod n_1, (x_2''' – x_0) \cdot y_2 \bmod n_2, (x_3''' – x_0) \cdot y_3 \bmod n_3, (x_4''' – x_0) \cdot y_4 \bmod n_4)$.

$y_1=1$, $y_2=5$, $y_3=10$, $y_4=12$

$x_0=1$

$x_1'''=1$, $x_2'''=1$, $x_3'''=1$, $x_4'''=1$

$x'''' = ((1 - 1) \cdot 1 \bmod 3, (1 - 1) \cdot 5 \bmod 7, (1 - 1) \cdot 10 \bmod 11, (1 - 1) \cdot 12 \bmod 17) =$

$= (0 \bmod 3, 0 \bmod 7, 0 \bmod 11, 0 \bmod 17) = (0, 0, 0, 0)$

Модулярное представление равно нулю, следовательно, вычисление закончено.

Получили число 1960.

Таблица 13 – Задание по вариантам

| | | | |
|---|---|---|---|
| 1. | 46 и 78 | 13. | 61 и 58 |
| 2. | 34 и 89 | 14. | 45 и 69 |
| 3. | 65 и 38 | 15. | 53 и 55 |
| 4. | 79 и 27 | 16. | 73 и 51 |
| 5. | 66 и 45 | 17. | 85 и 39 |
| 6. | 88 и 43 | 18. | 58 и 76 |
| 7. | 91 и 52 | 19. | 71 и 54 |
| 8. | 27 и 84 | 20. | 59 и 62 |
| 9. | 56 и 64 | 21. | 61 и 83 |
| 10. | 37 и 92 | 22. | 75 и 41 |
| 11. | 33 и 67 | 23. | 43 и 95 |
| 12. | 48 и 77 | 24. | 84 и 25 |

**Задание.** Найти произведение двух целых чисел (по вариантам). Взаимно-простые числа n1, n2, n3, n4 выбрать самостоятельно (табл. 13).

Индивидуальное задание № 3

**Модулярная арифметика**

1. Восстановить произведение двух целых чисел по их модулярным компонентам.

Таблица 14 – Задание на восстановление произведения двух целых чисел по их модулярным компонентам.

| | | | |
|---|---|---|---|
| 1. | $n_1=3\ n_2=7\ n_3=13\ n_4=17$<br>$x_1=1\ x_2=1\ x_3=12\ x_4=13$<br>$x_1=2\ x_2=2\ x_3=5\ x_4=10$ | 7. | $n_1=3\ n_2=7\ n_3=13\ n_4=17$<br>$x_1=2\ x_2=2\ x_3=0\ x_4=14$<br>$x_1=0\ x_2=1\ x_3=10\ x_4=2$ |
| 2. | $n_1=3\ n_2=11\ n_3=13\ n_4=17$<br>$x_1=1\ x_2=4\ x_3=11\ x_4=3$<br>$x_1=0\ x_2=1\ x_3=0\ x_4=10$ | 8. | $n_1=3\ n_2=7\ n_3=11\ n_4=13$<br>$x_1=0\ x_2=2\ x_3=6\ x_4=7$<br>$x_1=2\ x_2=0\ x_3=2\ x_4=9$ |
| 3. | $n_1=3\ n_2=7\ n_3=13\ n_4=17$<br>$x_1=2\ x_2=6\ x_3=10\ x_4=11$<br>$x_1=0\ x_2=3\ x_3=6\ x_4=11$ | 9. | $n_1=3\ n_2=7\ n_3=13\ n_4=17$<br>$x_1=0\ x_2=0\ x_3=11\ x_4=12$<br>$x_1=0\ x_2=0\ x_3=3\ x_4=8$ |
| 4. | $n_1=3\ n_2=7\ n_3=13\ n_4=17$<br>$x_1=0\ x_2=0\ x_3=6\ x_4=16$<br>$x_1=0\ x_2=0\ x_3=6\ x_4=11$ | 10. | $n_1=3\ n_2=7\ n_3=13\ n_4=17$<br>$x_1=2\ x_2=6\ x_3=5\ x_4=15$<br>$x_1=1\ x_2=3\ x_3=0\ x_4=1$ |
| 5. | $n_1=7\ n_2=11\ n_3=13\ n_4=17$<br>$x_1=2\ x_2=6\ x_3=7\ x_4=4$<br>$x_1=5\ x_2=3\ x_3=8\ x_4=13$ | 11. | $n_1=3\ n_2=7\ n_3=11\ n_4=13$<br>$x_1=0\ x_2=5\ x_3=9\ x_4=10$<br>$x_1=0\ x_2=1\ x_3=3\ x_4=10$ |
| 6. | $n_1=3\ n_2=7\ n_3=13\ n_4=17$<br>$x_1=2\ x_2=0\ x_3=12\ x_4=9$<br>$x_1=0\ x_2=4\ x_3=0\ x_4=5$ | 12. | $n_1=3\ n_2=7\ n_3=13\ n_4=17$<br>$x_1=1\ x_2=1\ x_3=12\ x_4=13$<br>$x_1=2\ x_2=0\ x_3=9\ x_4=1$ |

2. Сравнить два числа по их модулярным компонентам (дополнительное задание на 0.2 балла).

Таблица 15 – Задание на сравнение двух целых чисел по их модулярным компонентам

| | | | |
|---|---|---|---|
| 1. | $n_1=3\ n_2=13\ n_3=17$<br>$x_1=0\ x_2=0\ x_3=10$<br>$x_1=1\ x_2=11\ x_3=3$ | 7. | $n_1=3\ n_2=13\ n_3=17$<br>$x_1=2\ x_2=0\ x_3=14$<br>$x_1=0\ x_2=5\ x_3=6$ |
| 2. | $n_1=3\ n_2=7\ n_3=17$<br>$x_1=2\ x_2=0\ x_3=9$<br>$x_1=0\ x_2=4\ x_3=5$ | 8. | $n_1=7\ n_2=11\ n_3=13$<br>$x_1=6\ x_2=7\ x_3=10$<br>$x_1=3\ x_2=1\ x_3=6$ |
| 3. | $n_1=3\ n_2=7\ n_3=17$<br>$x_1=1\ x_2=5\ x_3=10$<br>$x_1=2\ x_2=2\ x_3=10$ | 9. | $n_1=7\ n_2=11\ n_3=19$<br>$x_1=5\ x_2=6\ x_3=4$<br>$x_1=5\ x_2=10\ x_3=16$ |
| 4. | $n_1=7\ n_2=13\ n_2=17$<br>$x_1=1\ x_2=12\ x_4=13$<br>$x_1=6\ x_2=9\ x_3=14$ | 10. | $n_1=3\ n_2=7\ n_3=23$<br>$x_1=1\ x_2=5\ x_3=15$<br>$x_1=0\ x_2=2\ x_3=3$ |
| 5. | $n_1=3\ n_2=11\ n_3=13$<br>$x_1=0\ x_2=9\ x_3=10$<br>$x_1=1\ x_2=4\ x_3=11$ | 11. | $n_1=7\ n_2=11\ n_3=13$<br>$x_1=1\ x_2=0\ x_3=8$<br>$x_1=3\ x_2=2\ x_3=10$ |
| 6. | $n_1=7\ n_2=11\ n_3=13$<br>$x_1=5\ x_2=3\ x_3=7$<br>$x_1=0\ x_2=1\ x_3=4$ | 12. | $n_1=3\ n_2=7\ n_3=11$<br>$x_1=0\ x_2=5\ x_3=9$<br>$x_1=1\ x_2=5\ x_3=6$ |

Практическое занятие №4

## Разложение на множители

1. Деление и разложение на множители.

Если число n>1, то его можно делить на последовательные простые числа p = 2, 3, 5, …, до тех пор, пока не будет найдено наименьшее p для которого n mod p = 0. Тогда p будет наименьшим простым множителем числа n. Ту же процедуру можно применить к n/p, взяв его за новое значение n, пробовать разделить это новое значение числа n на p и его большие простые числа. Из теоремы 10 следует, что это действие необходимо выполнять пока $p \le \sqrt{n}$. Отметим, что мы должны обладать вспомогательной

последовательностью пробных делителей 2 = d0 < d1 < d2 < d3 < …, которая включает в себя все простые числа $\le \sqrt{n}$. Ниже приведена процедура, реализующая данный метод.

**Задание 1**. Выполнить по вариантам разложение на множители.

Таблица 16 – Задание для разложения на множители

| | | | |
|---|---|---|---|
| 1. | n=98; n=52; n=124 | 7. | n=58; n=92; n=104 |
| 2. | n=48; n=56; n=178 | 8. | n=88; n=58; n=128 |
| 3. | n=86; n=64; n=165 | 9. | n=68; n=77; n=112 |
| 4. | n=66; n=85; n=192 | 10. | n=94; n=70; n=182 |
| 5. | n=178; n=76; n=108 | 11. | n=96; n=75; n=184 |
| 6. | n=84; n=44; n=102 | 12. | n=69; n=125; n=228 |

2**.** Метод Ферма.

Допустим, что n = u · v, где u ≤ v. Для практических целей можно допустить, что n нечетно; это означает, что u и v тоже нечетны. Поэтому можно положить:

$$x = (u + v) / 2, \qquad y = (v - u) / 2;$$

$$n = x^2 - y^2, \qquad 0 \le y < x \le n.$$

Метод Ферма заключается в том, что ищутся такие значения x и y, которые удовлетворяют этому соотношению. Следующий алгоритм показывает, как, не выполняя операции деления, можно разложить число на множители.

По данному нечетному числу n алгоритм определяет наибольший множитель числа n, не превосходящий $\sqrt{n}$:

1. $x' := 2\lfloor\sqrt{n}\rfloor + 1;\quad y' := 1;\quad r := \lfloor\sqrt{n}\rfloor^2 - n.$
2. Если r ≤ 0, то перейти на шаг 4.
3. $r := r - y',\ y' := y' + 2$ и на шаг 2.
4. Если r = 0, то все.
5. $r := r + x',\ x' := x' + 2$ и на шаг 3.

Имеем $n = ((x' - y')/2)((x' + y' - 2)/2)$,

$(x' + y' - 2)/2$ – наибольший множитель числа n, не превосходящий $\sqrt{n}$.

**Пример.**

n=300, $\sqrt{300}$ = 17, $17^2$ = 289. Вычисляем r, x', y'.

r = 289 - 300 = -11, x' = 2 · 17 + 1= 35, y' = 1.

Получили x' = 41, y' = 21.

Подставляем, (41 – 21) / 2 = 10, (41 + 21 - 2) / 2 = 30. 10 · 30 = 300.

**Задание 2**. Разложить число на два множителя методом Ферма.

Таблица 17 – Задание для разложения на множители методом Ферма

| | | | |
|---|---|---|---|
| 1. | 612; 867; 1581 | 7. | 629; 204; 3744 |
| 2. | 384; 615; 1749 | 8. | 684; 380; 2204 |
| 3. | 429; 779; 1664 | 9. | 741; 333; 2301 |
| 4. | 476; 697; 1925 | 10. | 861; 533; 2109 |
| 5. | 525; 245; 1836 | 11. | 429; 608; 4389 |
| 6. | 312; 891; 2173 | 12. | 475; 943; 1953 |

3. Вероятностный метод.

а) Для вычисления $a^d \bmod m$ рассмотрим следующий алгоритм.

Предполагается, что натуральные числа a и d не превосходят по величине m.

1. Представим d в двоичной системе счисления

$$d \equiv d_0 2^r + \ldots + d_{r-1} \cdot 2 + d_r, \text{ где } d_i \text{ равны } 0 \text{ или } 1, \quad d_0 = 1.$$

2. Положим $a_0 = a$ и затем для $i = 1, \cdots, r$ вычислим

$$a_i \equiv a_{i-1}^2 \cdot a^{d_i} \pmod{m}.$$

3. $a_r$ есть искомый вычет $a^d \bmod m$.

Справедливость этого алгоритма вытекает из сравнения

$$a_i \equiv a^{d_0 2^i + \ldots + d_i} \pmod{m},$$

легко доказываемого индукцией по i.

**Пример.**

a = 3, d = 4, m = 6.

$d = (100)_2$, $d_0=1$, $d_1=0$, $d_2=0$, $a_0=3$.

$a_i \equiv a_{i-1}^2 \cdot a^{d_i} \pmod{m}$.

$a_1 = a_0^2 \cdot a^{d1} \pmod{m} = 3^2 \cdot 3^0 \pmod{6} = 9 \bmod 6 = 3$

$a_2 = a_1^2 \cdot a^{d2} \pmod{m} = 3^2 \cdot 3^0 \pmod{6} = 9 \bmod 6 = 3$

Проверяем, $3^4 \bmod 6 = 729 \bmod 6 = 3$.

**Задание 3**. Вычислить $a^d \bmod m$ вероятностным методом.

Таблица 18 – Задание для вычисления $a^d \bmod m$ вероятностным методом

| | | | |
|---|---|---|---|
| 1. | 1) a= 3; d=5; m=7;<br>2) a= 4; d=6; m=12;<br>3) a= 7; d=3; m=11 | 7. | 1) a= 3; d=7; m=14;<br>2) a= 2; d=8; m=19;<br>3) a= 7; d=3; m=9 |
| 2. | 1) a= 2; d=7; m=8;<br>2) a= 5; d=3; m=13;<br>3) a= 4; d=4; m=7 | 8. | 1) a= 3; d=7; m=10;<br>2) a= 4; d=6; m=10;<br>3) a= 7; d=3; m=14 |
| 3. | 1) a= 3; d=5; m=12;<br>2) a= 7; d=3; m=11;<br>3) a= 5; d=4; m=15 | 9. | 1) a= 3; d=3; m=11;<br>2) a= 4; d=6; m=13;<br>3) a= 7; d=4; m=11 |
| 4. | 1) a= 3; d=7; m=8;<br>2) a= 4; d=6; m=14;<br>3) a= 7; d=3; m=18 | 10. | 1) a= 4; d=5; m=7;<br>2) a= 4; d=6; m=23;<br>3) a= 7; d=3; m=10 |
| 5. | 1) a= 4; d=5; m=9;<br>2) a= 2; d=6; m=18;<br>3) a= 7; d=3; m=16 | 11. | 1) a= 5; d=4; m=7;<br>2) a= 3; d=5; m=13;<br>3) a= 2; d=7; m=7 |
| 6. | 1) a= 4; d=4; m=6;<br>2) a= 4; d=6; m=21;<br>3) a= 7; d=3; m=8 | 12. | 1) a= 6; d=5; m=7;<br>2) a= 3; d=6; m=15;<br>3) a= 4; d=7; m=17 |

b) Рассмотрим метод, основанный на замене проверки $a^{n-1} \equiv 1 (\text{mod } n)$ проверкой несколько иного условия. Если n - простое число, $n-1=2^s \cdot t$, где t – нечетно, то согласно теореме Ферма для каждого a с условием НОД(a,n)=1 хотя бы одна из скобок в произведении

$$\left(a^t-1\right)\cdot\left(a^t+1\right)\cdot\left(a^{2t}+1\right)\cdot\ldots\cdot\left(a^{2^{s-1}\cdot t}+1\right)=a^{n-1}-1$$

делится на n. Обращение этого свойства можно использовать, чтобы отличать составные числа от простых.

Пусть n – нечетное составное число, $n-1=2^s t$, где t – нечетно. Назовем целое число a, 1<a<n, «хорошим» для n, если нарушается одно из двух условий:

1) n делится на a;

2) $a^t \equiv 1 (\text{mod } n)$ или существует целое k, $0 \le k < s$, такое, что $a^{2^k \cdot t} \equiv -1 (\text{mod } n)$.

Из сказанного ранее следует, что для простого числа n не существует «хороших» чисел a. Если же n составное число, то, как доказал Рабин, их существует не менее $\frac{3}{4}(n-1)$.

c) Теперь рассмотрим вероятностный алгоритм, отличающий составные числа от простых чисел.

1. Выберем случайным образом число a, 1<a<n, и проверим для этого числа указанные выше свойства 1) и 2).
2. Если хотя бы одно из них нарушается, то число n составное.
3. Если выполнены оба условия 1) и 2), возвращаемся к шагу 1.

Из изложенного следует, что составное число не будет определено как составное после однократного выполнения шагов 1-3 с вероятностью не большей $4^{-1}$. А вероятность не определить его после k повторений не превосходит $4^{-k}$, то есть убывает очень быстро.

**Задание 4**. Используя вероятностный алгоритм, проверить являются ли простыми следующие числа:

1) 68;

2) 1125;

3) 197;

3) 83.

Индивидуальное задание № 4

**Разложение на множители**

1. Разложить на множители числа, используя два метода (метод Ферма и метод деления и разложения на множители).

Таблица 19 – Задание для вычисления

| | | | |
|---|---|---|---|
| 1. | 395; 1057 | 7. | 655; 1043 |
| 2. | 1921; 129 | 8. | 2771; 453 |
| 3. | 202; 3611 | 9. | 2123; 187 |
| 4. | 341; 5667 | 10. | 1903; 905 |
| 5. | 393; 1067 | 11. | 381; 3749 |
| 6. | 515; 1651 | 12. | 1639; 2021 |

2. Вычислить $a^d \bmod m$, используя вероятностный метод.

Таблица 20 – Задание для вычисления $a^d \bmod m$ вероятностным методом

| | | | |
|---|---|---|---|
| 1. | a= 3; d=9; m=12 | 7. | a= 11; d=4; m=14 |
| 2. | a= 6; d=6; m=18 | 8. | a= 8; d=6; m=12 |
| 3. | a= 8; d=5; m=21 | 9. | a= 9; d=8; m=19 |
| 4. | a= 9; d=6; m=23 | 10. | a= 4; d=11; m=22 |
| 5. | a= 11; d=5; m=18 | 11. | a= 7; d=7; m=23 |
| 6. | a= 12; d=4; m=15 | 12. | a= 5; d=11; m=24 |

3. Реализовать алгоритм разложения на множители на языке программирования (+ 0,3 балла).

### *Вопросы к модулю 2*

1. Какие числа называются сравнимыми по модулю m?
2. Что является классами вычетов по модулю m
3. Перечислить свойства классов вычетов по модулю m?
4. Что является полной системой вычетов по модулю m?
5. Какие числа называются взаимно-обратными?
6. Сформулировать китайскую теорему об остатках.
7. В чем состоит принцип модулярного исчисления?
8. Какое число называется простым?
9. Какие числа называются взаимно-простыми?
10. Записать соотношение Безу.
11. Сформулировать основную теорему арифметики?
12. Какое представление целого числа называется его каноническим разложением?
13. В чем состоит метод составления таблицы простых чисел, известный под названием «Решето Эратосфена»?
14. Какой делитель двух чисел a и в называется наибольшим общим делителем?
15. В чем суть алгоритма Евклида?
16. Чему равно число итераций, необходимых для вычисления НОД?
17. Как записывается число в позиционной системе счисления?

18. Как осуществляются переводы из одной позиционной системы счисления в другую?

19. Какой элемент является единицей коммутативного кольца?

20. Что является мультипликативной группой?

21. Какой элемент называется неприводимым?

22. Привести методы разложения на множители.

23. Как сравнить два числа, зная только их модулярные компоненты?

## Модуль 3. Полиномы от одной и нескольких переменных

Практическое занятие №5

### Вычисление полиномов

1. Бинарный метод.

Запишем n в двоичной системе счисления и заменим в этой записи каждую цифру «1» парой букв SX, а каждую цифру «0» – буквой S, после чего вычеркнем крайнюю левую пару букв SX. Результат, читаемый слева на право, превращается в правило вычисления $x^n$, если букву S интерпретировать как операцию возведения в квадрат (S – square – квадрат), а букву «x» – как операцию умножения на x.

**Пример**. Пусть $n = (23)_{10} = (10111)_2$. Тогда строим последовательность SX S SX SX SX, удаляем из нее начальную пару SX и в итоге получаем следующее правило вычисления: S SX SX SX. Согласно этому правилу, мы должны возвести x в квадрат, снова возвести в квадрат, умножить на x, возвести в квадрат, умножить на x, возвести в квадрат, умножить на x и т.д.; при этом мы последовательно вычисляем: $x^2$, $x^4$, $x^5$, $x^{10}$, $x^{11}$, $x^{22}$, $x^{23}$.

**Задание 1**. Подсчитать количество умножений для вычисления $x^n$, используя бинарный метод.

1) n = 78;

2) n = 56;

3) n = 92.

2. Метод множителей.

Рассмотрим метод множителей**,** когда значение n известно заранее. Если $n = p \cdot q$, где p - наименьший простой множитель числа n и q ›1, то для вычисления $x^n$ мы можем сначала вычислить $x^p$, а затем возвести это число в степень q. В случае, когда n простое, мы можем вычислить сначала число $x^{n-1}$, а затем умножить его на x. Многократное применение этих правил дает нам процедуру вычисления $x^n$ для любого данного n.

**Пример.** Пусть мы хотим вычислить $x^{55}$. Вычисляем сначала $y = x^5 = x^4x = (x^2)^2x$, а затем находим $y^{11} = y^{10}y = (y^5)^2y = (y^4y)^2y = ((y^2)^2y)^2y$. Весь

процесс вычисления использует восемь умножений, в то время как бинарный метод потребовал бы девяти. В среднем метод множителей лучше бинарного, но встречаются случаи (начиная с n = 33), когда более экономным оказывается бинарный метод.

**Задание 2**. Подсчитать количество умножений для вычисления $x^n$.

1) n = 78;

2) n = 145;

3) n = 236.

3. Схема Горнера.

Начинаем с $a_n$, умножаем на x, прибавляем $a_{n-1}$, умножаем на x и т.д. Этот способ вычисления обычно называют «схемой Горнера».

$$f(x) = (\ldots(a_n x+a_{n-1})x+\ldots)x+a_0$$

**Пример**. Вычислить полином $f(x)=x^5 - 2x^4 + 3x^2 - x + 1$ при x = 2 указанным способом.

$$f(x) = ((((x - 2)x + 0)x+3)x - 1)x + 1$$

$$f(2) = ((((2 - 2)2 + 0)2+3)2 - 1)2 + 11= 11$$

**Задание 3**. Вычислить полиномы, используя схему Горнера. Подсчитать количество умножений и сложений для вычисления f(x).

1) $f(x) = x^3 - 5x^2 + 6x - 1$, при x = 5;

2) $f(x) = 3x^6 - 5x^5 - 7x^4 + 2x^3 - 8$, при x = 2;

3) $f(x) = x^5 + 2x^3 - 5x^2 + 2x - 1$

4. Обобщение схемы Горнера.

Позволяет вычислить сразу как полином, так и его производную

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1.$$

Это удобно сделать, положив

$c_0=a_n$, $b_0=0$

$c_j=c_{j-1}x+a_{n-j}$, $b_j=b_{j-1}x+c_{j-1}$, $1\le j\le n$.

Здесь $c_n=f(x)$ и $b_n=f'(x)$.

**Пример:** Вычислить полином и его производную:
$f(x) = 2x^5-x^4+2x^3- x^2+1$ при x=1.

Вычисляем полином, то есть находим его значение при x=1.
$c_0 = 2$, $c_j=c_{j-1}x+a_{n-j}$, n=5, $a_5=2$, $a_4=-1$, $a_3=2$, $a_2=-1$, $a_1=0$, $a_0=1$.
$c_1 = c_0x+a_4 = 2\cdot1+(-1) = 1$
$c_2 = c_1x+a_3 = 1\cdot1+2 = 3$
$c_3 = c_2x+a_2 = 3\cdot1+(-1) = 2$
$c_4 = c_3x+a_1 = 2\cdot1+0 = 2$
$c_5 = c_4x+a_0 = 2\cdot1+1 = 3$
То есть, f(1) = 3.
Вычислим производную:
$b_0 = 0$, $b_j = b_{j-1}x + c_{j-1}$, $c_0 = 2$, $c_1 = 1$, $c_2 = 3$, $c_3 = 2$, $c_4 = 2$, $c_5 = 3$.
$b_1=b_0x+c_0=0 \cdot 1+2=2$
$b_2=b_1x+c_1=2 \cdot 1+1=3$
$b_3=b_2x+c_2=3 \cdot 1+3=6$
$b_4=b_3x+c_3=6 \cdot 1+2=8$
$b_5=b_4x+c_4=8 \cdot 1+2=10$
$f'(x)= 10x^4-4x^3+6x^2-2x$
$f'(1)=10$.

**Задание 4**. Вычислить полиномы и их производную.

1) $f(x)=x^4-2x^3+2x^2+5$, при x=3.
2) $f(x)=3x^6-5x^4 - x^3+2x^2-2x+8$, при x=2.
3) $f(x)=2x^5-x^4+2x^3 - x^2+1$, при x=1.

Индивидуальное задание №5

**Вычисление полиномов**

1. Бинарный метод и метод множителей. Подсчитать количество умножений для вычисления $x^n$.

Таблица 21 – Задание для вычисления степени

| | | | |
|---|---|---|---|
| 1. | n=65, n=87 | 7. | n=81, n=75 |
| 2. | n=98, n=118 | 8. | n=90, n=67 |
| 3. | n=76, n=89 | 9. | n=103, n=71 |
| 4. | n=77, n=123 | 10. | n=85, n=94 |
| 5. | n=69, n=93 | 11. | n=79, n=101 |
| 6. | n=82, n=104 | 12. | n=97, n=62 |

2. Схема Горнера.

Вычислить полиномы, используя схему Горнера. Подсчитать количество умножений и сложений для вычисления f(x) при x=2.

Таблица 22 – Задание для вычисления полинома

| | | | |
|---|---|---|---|
| 1. | $f(x)=5x^6-5x^5-7x^4+2x^3-8$ | 7. | f(x)=5x6-2x5-3x4+2x3+2 |
| 2. | $f(x)=2x^6+4x^5-9x^4+2x^2-2$ | 8. | f(x)=7x6+9x5+6x4+2x3+9 |
| 3. | $f(x)=4x^6-5x^5-2x^4+2x^3-1$ | 9. | f(x)=x6-4x5-7x4+2x3 |
| 4. | $f(x)=-2x^6-3x^5+5x^4+2x^3$ | 10. | f(x)=5x5-x4+2x3+3x2 -3 |
| 5. | $f(x)=7x^6+8x^5+x^4+2x^3-5$ | 11. | f(x)=4x5-8x4+2x3-6x2+1 |
| 6. | $f(x)=3x^6+x^5+2x^4+7$ | 12. | f(x)=x6+x5+5x4+2x3+6 |

3. Обобщение схемы Горнера. Вычислить полиномы и их производную при x = 3.

Таблица 23 – Задание для вычисления полинома и производной

| | | | |
|---|---|---|---|
| 1. | $f(x)=2x^6+4x^5-9x^4-x^2-2$ | 7. | $f(x)=3x^6-2x^5-3x^4-x^3-$ |
| 2. | $f(x)=3x^6+x^5-x^4+4x$ | 8. | $f(x)= -x^6+x^5+3x^4-x^3+6$ |
| 3. | $f(x)=2x^6-3x^5-4x^4-x^3-8$ | 9. | $f(x)= 2x^7 +x^6-4x^5-4x^4-x^3$ |
| 4. | $f(x)=4x^6+9x^5+6x^4-x^3+9$ | 10. | $f(x)=3x^5-x^4-x^3+3x^2 -3$ |
| 5. | $f(x)= -4x^6+8x^5+x^4-x^3-3$ | 11. | $f(x)=4x^5-8x^4-x^3-6x^2+1$ |
| 6. | $f(x)=x^7-4x^6-3x^5-2x^4-x^3-1$ | 12. | $f(x)=x^6+8x^5+4x^4-x^3-2$ |

4. Реализовать алгоритм вычисления полинома на языке программирования (+ 0,3 балла).

## Практическое занятие №6

## **Нахождение НОД полиномов**

Для вычисления НОД полиномов воспользуемся алгоритмом:

*M*:=*граница_Ландау_Миньотта (A, B)*

цикл до бесконечности

*p*:=*найти_большое_простое (2M);*

если *степень_остатка (p, A)* или *степень_остатка (p, B)*

то C:=*модулярный НОД (A, B, p);*

если *делит (C, A)* и *делит (C, B)*

то выход *C*;

где – алгоритм *граница_Ландау_Миньотта* применяет следствие 1 к неравенству Ландау-Миньотта;

алгоритм *найти_большое_простое* возвращает простое число, большее, чем его аргумент (каждый раз новое число);

алгоритм *степень_остатка* проверяет, что редукция по модулю $p$ не меняет степень, то есть $p$ не делит старший коэффициент;

алгоритм *модулярный_НОД* применяет алгоритм Евклида по модулю $p$;

алгоритм *делит* проверяет, что полиномы делятся над кольцом целых чисел.

**Пример.** Имеем два полинома $A(x) = x^8+2x^6-x^5+4x^3-6x^2$ и $B(x) = x^6+2x^4+4x-4$. Используя следствие 1 к неравенству Ландау-Миньотта определим верхнюю границу:

$$2^{\min(\alpha,\beta)}\, НОД(a_\alpha, b_\beta)\min\left[\frac{1}{|a_\alpha|}\sqrt{\sum_{i=0}^{\alpha} a_i^2}, \frac{1}{|b_\beta|}\sqrt{\sum_{i=0}^{\beta} b_i^2}\right]$$

Для наших полиномов:

$$M = 2^6 \cdot НОД(1,1)\cdot \min\left[\frac{1}{|1|}\cdot\sqrt{1^2+2^2+(-1)^2+4^2+(-6)^2}, \frac{1}{|1|}\cdot\sqrt{1^2+2^2+4^2+(-4)^2}\right] =$$

$$= 64\cdot 1\cdot \min\left[\sqrt{58}, \sqrt{37}\right] = 64\cdot\sqrt{37} \approx 384$$

p=2·M=767. Это очень большое число, возьмем в качестве p число 7. p не делит старший коэффициент полиномов.

Выполним деление полиномов по модулю 7.

$$\begin{array}{l} \_x^8+2x^6-x^5+4x^3-6x^2 \;\;|\; x^6+2x^4+4x-4 \\ \underline{-6x^8-12x^6-24x^3+24x^2} \quad -6x^2 \\ 7x^8+14x^6-x^5+28x^3-30x^2 \end{array}$$

$(7x^8+14x^6-x^5+28x^3-30x^2) \bmod 7 \equiv 6x^5+5x^2$

$$\begin{array}{l} \_x^6+2x^4+4x-4 \;\;|\; 6x^5+5x^2 \\ \underline{36x^6+30x^3} \qquad 6x \\ -35x^6+2x^4-30x^3+4x-4 \end{array}$$

$(-35x^6+2x^4-30x^3+4x-4) \bmod 7 \equiv 2x^4+5x^3+4-4$

$$\begin{array}{l} \_6x^5+5x^2 \;\;|\; 2x^4+5x^3+4-4 \\ \underline{-8x^5-20x^4-16x^2+16x} \quad -4x \\ 14x^5+20x^4+21x^2-16x \end{array}$$

$(14x^5+20x^4+21x^2-16x) \bmod 7 \equiv 6x^4+5x$. Продолжим деление:

$$\begin{array}{l} \_6x^4+5x \;\;|\; 2x^4+5x^3+4-4 \\ \underline{-8x^4-20x^3-16x+16} \quad -4 \\ 14x^4+20x^3+21x-16 \end{array}$$

$(14x^4+20x^3+21x-16) \bmod 7 \equiv 6x^3+5$

$$\begin{array}{l} \_2x^4+5x^3+4x-4 \;\;|\; 6x^3+5 \\ -12x^4 - 10x \qquad\qquad -2x \\ 14x^4+5x^3+14x-4 \end{array}$$

$(14x^4+5x^3+14x-4) \bmod 7 \equiv 5x^3-4$. Продолжим деление:

$$\begin{array}{l} \_5x^3 - 4 \;\;|\; 6x^3+5 \\ -30x^3-25 \quad -2x-5 \\ 35x^3+21 \end{array}$$

$(35x^3+21) \bmod 7 \equiv 0$

Следовательно, НОД полиномов равен $6x^3+5$. НОД должен быть нормированным, то есть его старший коэффициент должен быть равен 1. Надо найти число a, обратное к 6 по модулю 7, такое, что $6 \cdot a \equiv 1 (\mathrm{mod}\ 7)$. Это число 6. Умножим коэффициенты полученного НОД на 6 и возьмем их по модулю 7: $(36x^3+30) \bmod 7 = x^3+2$. Таким образом,

**НОД(A(x), B(x)) = $x^3+2$**

Проверим, делятся ли полиномы на $x^3 + 2$ (не модулярно):

$$\begin{array}{l} \_x^8+2x^6-x^5+4x^3-6x^2 \;\;|\; x^3+2 \quad . \\ x^8+2x^5 \qquad\qquad x^5+2x^3-3x^2 \\ \_2x^6 \qquad -3x^5+4x^3 \\ 2x^6 \qquad + 4x^3 \\ \_-3x^5 - 6x^2 \\ -3x^5 - 6x^2 \\ 0 \end{array}$$

$$\begin{array}{l} \_x^6+2x^4+4x-4 \;\;|\; x^3+2 \quad . \\ x^6+2x^3 \qquad x^3+2x-2 \\ \_2x^4-2x^3+4x \\ 2x^4 + 4x \\ \_-2x^3-4 \\ -2x^3-4 \\ 0 \end{array}$$

**Задание 1.** Найти НОД(F(x), T(x)), если
$F(x) := x^7 - 3x^6 + 2x^5 - 2x^3 + 2x^2$
$T(x) := 2x^6 - 2x^5 - x^4 + x^3 + 2x - 2$

**Задание 2.** Найти НОД(K(x), L(x)), если
$K(x) := x^8 - 2x^7 + 2x^6 - 6x^5 - 3x^4 - 2x^2 - 6$
$L(x) := 2x^6 + x^5 + 6x^4 + 2x^3 - 3x$

Индивидуальное задание №6

## Нахождение НОД полиномов

**1. Найти наибольший общий делитель полиномов.**

Вычислить верхнюю границу данных полиномов, используя неравенство Ландау-Миньотта. Выполнить деление по модулю 5.

Таблица 24 – Задание для вычисления НОД полиномов

| | |
|---|---|
| 1. | $A(x) := 3x^8 + 2x^7 + 2x^6 + 6x^5 - x^4 + 4x^3$,<br>$B(x) := 2x^6 - x^5 + 5x^4 - x^3 + x^2 - 2$ |
| 2. | $A(x) := x^8 - x^7 - 3x^6 - x^5$,<br>$B(x) := 2x^7+2x^6+2x^4+2x^3 - x - 1$ |
| 3. | $A(x) := x^8 - 2x^7 - 6x^5 + 3x^6 - x^2 - 3$,<br>$B(x) := 2x^6 + 3x^4 + x^3 - 10x^2 + 3x - 3$ |
| 4. | $B(x) := 3x^8 - 6x^7 + 2x^6 - 4x^5 - 4x^4 + 8x^3$,<br>$A(x) := 2x^6 - 2x^5 - 6x^4 + 4x^3 - x + 2$ |
| 5. | $B(x) := 2x^8 + 6x^7 + x^6 + x^5 - 6x^4 - 2x - 6$,<br>$A(x) := x^7 + x^6 - 6x^5 + 3x^4 + 9x^3$ |
| 6. | $T(x) := x^8 - 2x^7 - 2x^6 + 4x^5 + 2x^4 - 4x^3 - x - 2$,<br>$F(x) := 2x^5 - 5x^4 + 2x^3 - 2x^2 - 4x$ |
| 7. | $K(x) := 2x^8 - x^7 + 6x^6 - x^2 + 3x$,<br>$L(x) := x^6 - x^5 - 7x^4 + 3x^3 + x - 3$ |
| 8. | $L(x) := 2x^8 - 5x^7 + x^6 + 2x^5 - x^2 + x$,<br>$K(x) := x^7 - 3x^6 + 2x^5 - x^3 + x^2 - 2x + 2$ |
| 9. | $A(x) := x^7 + x^6 - 6x^5 + 3x^3 + 9x^2 - 2x - 6$,<br>$F(x) := 2x^5 + 5x^4 + 9x^2 - 2x - 6$ |
| 10. | $K(x) := x^8 - x^4 - x^3 - x^2$,<br>$A(x) := 2x^7 - 2x^6 - 2x^5 + 2x^4 - 3x^2 + 3$ |
| 11. | $T(x) := x^8 - 2x^7 + 3x^6 - 6x^5 + 3x^4 - 2x^3 + 9x^2 - 6x$,<br>$A(x) := 2x^6 - x^5 + 9x^4 - 3x^3 + 8x^2 - 3$ |
| 12. | $B(x) := x^7 - 4x^5 + 3x^3 + 6x^2 - 2x - 4$,<br>$A(x) := 2x^5 + 3x^4 + x^3 + 6x^2 - 2x - 4$ |

**2. Найти наибольший общий делитель полиномов. Выполнить деление по модулю 7.**

Таблица 25 – Задание для вычисления НОД полиномов

| | |
|---|---|
| 1. | $T(x) := x^7 + x^6 - 6x^5 + 3x^3 + 9x^2 - 2x - 6$,<br>$F(x) := 2x^5 + 5x^4 + 9x^2 - 2x - 6$ |
| 2. | $B(x) := 2x^8 - 5x^7 + x^6 + 2x^5 - x^2 + x$,<br>$K(x) := x^7 - 3x^6 + 2x^5 - x^3 + x^2 - 2x + 2$ |
| 3. | $A(x) := 2x^8 - x^7 + 6x^6 - x^2 + 3x$,<br>$B(x) := x^6 - x^5 - 7x^4 + 3x^3 + x - 3$ |
| 4. | $L(x) := x^8 - 2x^7 + 3x^6 - 6x^5 + 3x^4 - 2x^3 + 9x^2 - 6x$,<br>$A(x) := 2x^6 - x^5 + 9x^4 - 3x^3 + 8x^2 - 3$ |

| | |
|---|---|
| 5. | $A(x) := x^8 - 2x^7 - 6x^5 + 3x^6 - x^2 - 3$,<br>$B(x) := 2x^6 + 3x^4 + x^3 - 10x^2 + 3x - 3$ |
| 6. | $K(x) := x^8 - x^7 - 3x^6 - x^5$,<br>$B(x) := 2x^7 + 2x^6 + 2x^4 + 2x^3 - x - 1$ |
| 7. | $L(x) := 3x^8 + 2x^7 + 2x^6 + 6x^5 - x^4 + 4x^3$,<br>$B(x) := 2x^6 - x^5 + 5x^4 - x^3 + x^2 - 2$ |
| 8. | $K(x) := x^8 - x^4 - x^3 - x^2$,<br>$A(x) := 2x^7 - 2x^6 - 2x^5 + 2x^4 - 3x^2 + 3$ |
| 9. | $B(x) := x^7 - 3x^6 + 2x^5 + 3x^3 - 6x^2 - x + 2$,<br>$T(x) := 2x^6 - 4x^5 + x^4 + x^3 - 9x^2 + 6x$ |
| 10. | $K(x) := x^7 - 4x^5 + 3x^3 + 6x^2 - 2x - 4$,<br>$A(x) := 2x^5 + 3x^4 + x^3 + 6x^2 - 2x - 4$ |
| 11. | $K(x) := 2x^7 - 7x^6 + 3x^5 + 3x^3 - 9x^2$,<br>$L(x) := x^6 - 3x^5 + x^4 - 9x^2 - 3x + 9$ |
| 12. | $F(x) := x^8 - 2x^7 + 2x^6 - 4x^5 + 3x^4 + 4x^2 - 4$,<br>$T(x) := 2x^6 - x^5 + 7x^4 - 3x^3 + 6x^2 - 2x$ |

### *Вопросы к модулю 3*

1. Что является степенью полинома, старшим коэффициентом полинома?

2. Какой полином называется нормированным? приводимым? неприводимым?

3. Сформулировать китайскую теорему об остатках для 2-х полиномов, для r полиномов?

4. Что такое результант полиномов?

5. Какие существуют методы вычисления $x^n$?

6. Что понимают под аддитивной сложностью числа n?

7. Какой способ вычисления полиномов называется «схемой Горнера»?

8. Как выполняется евклидово деление в поле?

9. Для чего используется неравенство Ландау-Миньотта?

10. Записать алгоритм вычисления НОД двух полиномов по модулю простого числа p.

11. Что такое «моном»?

12. Какая система записи полиномов называется «лексикографической»? «общей степени»?

13. Чем отличается рекурсивная форма записи полиномов от распределенной?

14. Какой полином считается редуцированным относительно G (G – конечное множество полиномов)?

15. Какая система образующих называется стандартным базисом?

16. Как вычислить базис Гребнера?

17. Дать определение содержания (cont(p)) полинома p.

18. Какой полином называется примитивным?

19. Сформулировать лемму Гаусса.

20. Как вычислить НОД двух полиномов от нескольких переменных?

## Модуль 4. Компьютерная система Wolfram Alpha. Применение алгоритмов компьютерной математики

Практическое занятие №7.1

### Работа с полиномами от одной переменной в Wolfram Alpha

1. Основные операции над полиномами.

Над полиномами можно выполнять обычные операции сложения, вычитания, умножения и деления. Для получения результата умножения используется функция Expand. Обратную операцию можно выполнить с помощью функции Simplify.

**Пример.**

(x^3+2 x^2+3 x+4) - (x^2-1)

Result

$$x^3 + x^2 + 3x + 5$$

Simplify (x^5+2 x^4+2 x^3+2 x^2-3 x-4)

Results

$$(x-1)(x+1)\left(x^3 + 2x^2 + 3x + 4\right)$$

$$(x-1)(x+1)(x(x(x+2)+3)+4)$$

$$x(x(x(x(x+2)+2)+2)-3)-4$$

Expand (-1 + x) (1 + x) (4 + x (3 + x (2 + x)))

Result

$$x^5 + 2x^4 + 2x^3 + 2x^2 - 3x - 4$$

(6 terms)

**Задание 1.**

1) выполнить операции сложения и вычитания для полиномов: x^3+2 x^2+3 x+4 и x^2-1;

2) привести пример использования функции Expand и Simplify.

2. Разложение полиномов.

Factor poly – выполняет разложение полинома над целыми числами.

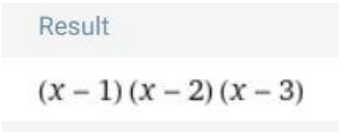
Factor poly, Modulus->p – выполняет разложение по модулю простого числа p.

Factor n – возвращает список простых множителей числа n.

Factor poly – возвращает список множителей полинома с их показателями степени.

**Пример.**

Factor x^3-6 x^2+11 x-6




Factor x^3-6 x^2+11 x-6, Modulus->3


Factor 1234554367


**Задание 2.**

Даны два полинома:

F[x]:=x^6-4 x^5+5 x^4-2 x^3

T[x]:=x^4-4 x^3+5 x^2-3 x+2

1) Разложить полиномы, в том числе и по модулю простого числа:

Factor F[x]

Factor T[x], Modulus->5 и др.

2) Получить список простых множителей числа 45541124367.

3. Функции для работы с полиномами.

Polynomial Remainder p, q, x – возвращает остаток от деления p на q как полиномов от x

Polynomial GCD poly1, poly2, … – возвращает наибольший общий делитель ряда полиномов poly1, poly2, …. С опцией Modulus->p функция возвращает наибольший общий делитель по модулю простого числа p.

**Пример.**

Decompose[x^4 + x^2 + 1, x]

Result

$(x^2 + x + 1) \circ x^2$

T[x]:=2 x^3-6 x^2+4 x-6

K[x]:=x^2+3 x+2

Polynomial Remainder (2 x^3-6 x^2+4 x-6, x^2+3 x+2, x)

18 □ 36 x

K[x]:=x^2+3 x+2

L[x]:=36 x+18

Polynomial Remainder (x^2+3 x+2, 36 x+18, x)

$\frac{3}{4}$

Polynomial GCD (2 x^3-6 x^2+4 x-6, x^2+3 x+2)

1

Polynomial GCD (x^2+3 x+2, x+1)

x + 1

Polynomial GCD (x^2-2 x+1, x-1)

x + 6

**Задание 3.**

Даны два полинома:

F[x]:=x^6-4 x^5+5 x^4-2 x^3

T[x]:=x^4-4 x^3+5 x^2-3 x+2

1) Найти НОД этих полиномов;
2) Найти НОД этих полиномов по модулю 5;
3) Найти остатки от деления F[x] и T[x] на x-2.

**Задание 4.**

Найти НОД и остатки от деления этих полиномов на их НОД, если:

1) F[x] = x^7-3 x^6+2 x^5-2 x^3+2 x^2

   T[x] = 2 x^6-2 x^5-x^4+x^3+2 x-2

2) K[x] = x^8-2 x^7+2 x^6-6 x^5-3 x^4-2 x^2-6

L[x] = 2 x^6+x^5=6 x^4+2 x^3-3 x

Индивидуальное задание №7.1

**Работа с полиномами от одной переменной в Wolfram Alpha**

1. Привести примеры на использование функций Expand и Simplify (по два примера).

2. Найти НОД двух полиномов с помощью функции PolynomialRemainder.

Найти частное от деления двух полиномов с помощью функции PolynomialQuotient (на каждой итерации).

3. Найти также НОД этих полиномов по модулю p и q (p, q – простые).

Таблица 26 – Задание для вычисления НОД полиномов

| | |
|---|---|
| 1. | $A(x) := 2x^8 - x^7 + 6x^6 - x^2 + 3x$,<br>$B(x) := x^6 - x^5 - 7x^4 + 3x^3 + x - 3$ |
| 2. | $B(x) := 2x^8 - 5x^7 + x^6 + 2x^5 - x^2 + x$,<br>$K(x) := x^7 - 3x^6 + 2x^5 - x^3 + x^2 - 2x + 2$ |
| 3. | $T(x) := x^7 + x^6 - 6x^5 + 3x^3 + 9x^2 - 2x - 6$,<br>$F(x) := 2x^5 + 5x^4 + 9x^2 - 2x - 6$ |
| 4. | $L(x) := x^8 - 2x^7 + 3x^6 - 6x^5 + 3x^4 - 2x^3 + 9x^2 - 6x$,<br>$A(x) := 2x^6 - x^5 + 9x^4 - 3x^3 + 8x^2 - 3$ |
| 5. | $F(x) := x^8 - 2x^7 + 2x^6 - 4x^5 + 3x^4 + 4x^2 - 4$,<br>$T(x) := 2x^6 - x^5 + 7x^4 - 3x^3 + 6x^2 - 2x$ |
| 6. | $B(x) := x^7 - 3x^6 + 2x^5 + 3x^3 - 6x^2 - x + 2$,<br>$T(x) := 2x^6 - 4x^5 + x^4 + x^3 - 9x^2 + 6x$ |
| 7. | $K(x) := x^8 - x^7 - 3x^6 - x^5$,<br>$B(x) := 2x^7 + 2x^6 + 2x^4 + 2x^3 - x - 1$ |
| 8. | $L(x) := 3x^8 + 2x^7 + 2x^6 + 6x^5 - x^4 + 4x^3$,<br>$B(x) := 2x^6 - x^5 + 5x^4 - x^3 + x^2 - 2$ |
| 9. | $K(x) := 2x^7 - 7x^6 + 3x^5 + 3x^3 - 9x^2$,<br>$L(x) := x^6 - 3x^5 + x^4 - 9x^2 - 3x + 9$ |
| 10. | $K(x) := x^7 - 4x^5 + 3x^3 + 6x^2 - 2x - 4$,<br>$A(x) := 2x^5 + 3x^4 + x^3 + 6x^2 - 2x - 4$ |
| 11. | $A(x) := x^8 - 2x^7 - 6x^5 + 3x^6 - x^2 - 3$,<br>$B(x) := 2x^6 + 3x^4 + x^3 - 10x^2 + 3x - 3$ |
| 12. | $K(x) := x^8 - x^4 - x^3 - x^2$,<br>$A(x) := 2x^7 - 2x^6 - 2x^5 + 2x^4 - 3x^2 + 3$ |

Практическое занятие №7.2

## Работа с полиномами от нескольких переменных в Wolfram Alpha

1. Примеры использования функций Expand и Simplify.

Expand[(x-y)^3]

$x^3 - 3\,x^2\,y + 3\,x\,y^2 - y^3$

Expand[(x^1000+1) (x^1000-1)]

$x^{2000} - 1$

Simplify[x^2-2 x y+y^2]

$(x - y)^2$

Simplify[(x^4+3 x^3-2 x^2-6 x)/(x^2+3 x)]

$x^2 - 2$

Самостоятельно: привести по два примере на использование функций Expand и Simplify (для полиномов от нескольких переменных).

2. Функции для работы с полиномами от нескольких переменных:

PolynomialMod[poly,m] – возвращает полином poly, приведенный по модулю m;

PolynomialQuotient[p, q, x] – возвращает частное от деления p и q как полиномов от x, игнорируя какой – либо остаток;

PolynomialRemainder[p, q, x] – возвращает остаток от деления p на q как полиномов от x;

PolynomialQ[expr,var] – проверяет, является ли expr полиномом от var;

GroebnerBasis[{poly1,poly2,…},{x1,x2,…}] – возвращает список полиномов, которые образуют базис Грёбнера для идеала, порожденного полиномами polyi;

PolynomialGCD[poly1,poly2,…] – возвращает НОД ряда полиномов;

PolynomialLCM[poly1,poly2,…] – возвращает НОК ряда полиномов;

**Примеры:**

PolynomialMod[x^2-2 x y-y^2,5]

$x^2 \square 3\,x\,y \square 4\,y^2$

PolynomialQuotient [x^2-2 x y+y^2,x-y,y]

x □ y

PolynomialQuotient[2 x^2-4 x^2 y+y^2,x^2-y,y]

3 $x^2$ □ y

PolynomialQuotient[2 x^2-4 x^2 y+y^2,x^2-y,x]

2 □ 4 y

PolynomialRemainder[2 x^2-4 x^2 y+y^2,x^2-y,x]

2 y □ 3 $y^2$

PolynomialRemainder[2 x^2-4 x^2 y+y^2,x^2-y,y]

2 $x^2$ □ 3 $x^4$

PolynomialRemainder[x^2-2 x y+y^2,x-y,x]

0

PolynomialRemainder[x^2-2 x y+y^2,x-y,y]

0

PolynomialQ[y^2-x y^3+y^3,x]

True

GroebnerBasis[{x^3 y z-x z^2,x y^2 z-x y z,x^2 y^2-z},{x,y,z}]

Result

$\{y z^2 - z^2, x y^2 z - x y z, x^2 z^2 - z^3, x^2 y z - z^2, x^2 y^2 - z\}$

PolynomialGCD[x^2-2 x y+y^2,x-y]

x □ y

PolynomialLCM[x^2-2 x y+y^2,x-y]

$(x - y)^2$

**Задание.**

1) проверить все примеры;

2) привести по 2 примера на каждую из перечисленных выше функций.

3. Нахождение наибольшего общего делителя с помощью функции PolynomialRemainder.

**Пример.**

Expand(2x - y ) (x-1))

Result

$$2x^2 - xy - 2x + y$$

Expand[(x^2 - y) (x-1)]

PolynomialGCD(x^3 - x^2 + y - x y,2 x^2 - x y - 2 x + y)

Result

$$x - 1$$

Input

$$\text{PolynomialRemainder}\left[-x^2 + x^3 + y - xy, 2x^2 - xy - 2x + y, x\right]$$

Result Enlarge

$$x\left(\frac{y^2}{4} - y\right) - \frac{y^2}{4} + y$$

Input

$$\text{PolynomialRemainder}\left[2x^2 - xy - 2x + y, y - \frac{y^2}{4} + x\left(-y + \frac{y^2}{4}\right), x\right]$$

Result

0

Проверка:

Input

$$\text{PolynomialRemainder}\left[y - \frac{y^2}{4} + x\left(-y + \frac{y^2}{4}\right), x - 1, x\right]$$

Result

0

То есть НОД полиномов x^3 - x^2 - x y + y и 2 x^2 - x y - 2 x + y по x равен x -1.

**Задание.**

Для полиномов от двух переменных найти НОД с помощью функции PolynomialRemainder. Проверить с помощью функции PolynomialGCD.

Индивидуальное задание №7.2

**Работа с полиномами от нескольких переменных в Wolfram Alpha**

1. С помощью функции Expand подобрать два полинома и найти их НОД с помощью функции PolynomialRemainder (для полиномов от двух переменных).

2. Привести пример на использование каждой из функций: PolynomialLCM, PolynomialQ, PolynomialQuotient, PolynomialMod.

Практическое занятие №8

**Криптосистема RSA**

Криптосистема RSA (авторы Р. Ривест, А. Шамир, Л. Адлеман) разработана в 1978 году. Эту криптосистему можно использовать для шифрования сообщений и для получения цифровой подписи. Рассмотрим алгоритм цифровой подписи.

1. Выбираем два больших, не равных между собой простых числа p и q, находим $n = p \cdot q$, вычисляем $= (p - 1) \cdot (q - 1)$. (Рекомендуется, чтобы длина n составляла 1024 бита).

2. Выбираем целое число e, чтобы $e < \varphi(n)$, НОД$(e, \varphi(n)) = 1$ и вычисляется d, удовлетворяющее условию $e \cdot d \equiv 1 (\mathrm{mod}\ \varphi(n))$.

3. Секретный ключ: p, q, d (на самом деле, только d, т.к. p и q после получения n и d могут быть уничтожены).

4. Пара чисел n, e – открытый ключ – предоставляется всем абонентам криптосистемы RSA.

5. Процедура подписывания сообщения M – это возведение числа M в степень d по модулю n: $S = M^d \pmod n$. Число S есть цифровая подпись, которую может выработать только владелец секретного ключа.

6. Процедура проверки подписи S, соответствующей сообщению M, – это возведение числа S в целую степень e по модулю n: $M' = S^e \pmod n$.

Если $M' = M$, то сообщение M признается подписанным пользователем, который составил ранее открытый ключ e. То есть составить криптограмму, соответствующую данному открытому ключу и данному сообщению можно только по известному секретному ключу d.

Таким образом, секретный ключ служит для подписывания сообщений, открытый – для проверки подписи.

Легко построить и систему шифрованной переписки в RSA.

**Пример**. Зашифруем аббревиатуру RSA, используя p = 17, q = 31. ([Алферов, 2001]). Для этого вычислим $n = p \cdot q = 527$ и $\varphi(n) = (p - 1) \cdot (q - 1) = 480$. Выберем в качестве e число, взаимно простое с $\varphi(n)$ , например, e = 7. С помощью расширенного алгоритма Евклида найдем целые числа u и v. Получаем: u = 2, v = -137. Так как $-137 \equiv 343 \pmod{480}$, то d = 343.

Теперь представим данное сообщение в виде последовательности чисел из [0, 526]. Для этого буквы R, S, A закодируем пятимерными двоичными векторами, воспользовавшись двоичной записью их порядковых номеров в английском алфавите: R соответствует $18 = (10010)_2$, S – $19 = (10011)_2$, A –$1 = (00001)_2$. Тогда RSA в двоичном представлении RSA – 100101001100001. Укладываясь в заданный отрезок [0, 526], получим два двоичных числа: (100101001), (100001). То есть, $M_1 = 297$, $M_2 = 33$.

Далее последовательно шифруем $M_1$ и $M_2$:

$C_1 = M_1^e \pmod{n} = 297^7 \pmod{527} = 474$;

$C_2 = M_2^e \pmod{n} = 33^7 \pmod{527} = 407$.

В итоге получаем шифротекст: $C_1 = 474$, $C_2 = 407$.

Произведем расшифрование. Для этого вычислим $D_1$ и $D_2$.

$D_1 = C_1^d \pmod{n} = 474^{343} \pmod{527} = 297$;

$D_1 = C_2^d \pmod{n} = 407^{343} \pmod{527} = 33$.

Возвращаясь к буквенной записи, получаем после расшифрования аббревиатуру RSA.

**Задание**. Зашифровать аббревиатуру TCN, используя p=17, q=29 (e=11).

**Самостоятельно**: Зашифровать свои инициалы (p, q взять отличные от 17 и 29).

Индивидуальное задание №8

**Криптография. Система RSA**

1. Зашифровать следующие аббревиатуры, используя систему RSA:

Таблица 27 – Задание для шифрования подписи

| | | | |
|---|---|---|---|
| 1. | GYD (p=7, q=47) | 7. | POK (p=19, q=53) |
| 2. | LET (p=17, q=59) | 8. | RES (p=21, q=41) |
| 3. | PTE (p=19, q=47) | 9. | SPO (p=11, q=71) |
| 4. | QIL (p=19, q=61) | 10. | SFI (p=23, q=89) |
| 5. | TAR (p=23, q=67) | 11. | FOP (p=17, q=61) |
| 6. | ASD (p=13, q=73) | 12. | DGA (p=13, q=71) |

2. Расшифровать сообщение.

Таблица 28 – Задание для расшифровывания подписи

| | | | |
|---|---|---|---|
| 1. | $C_1 = 194$ n=1147<br>$C_2 = 659$ e=7 | 7. | $C_1 = 119$ n=527<br>$C_2 = 360$ e=7 |
| 2. | $C_1 = 459$ n=703<br>$C_2 = 37$ e=5 | 8. | $C_1 = 17$ n=527<br>$C_2 = 17$ e=7 |
| 3. | $C_1 = 77$ n=221<br>$C_2 = 118$ e=7 | 9. | $C_1 = 44$ n=527<br>$C_2 = 37$ e=7 |
| 4. | $C_1 = 86$ n=377<br>$C_2 = 64$ e=11 | 10. | $C_1 = 179$ n=253<br>$C_2 = 80$ e=7 |
| 5. | $C_1 = 261$ n=713<br>$C_2 = 23$ e=7 | 11. | $C_1 = 153$ n=209<br>$C_2 = 43$ e=13 |
| 6. | $C_1 = 261$ n=713<br>$C_2 = 23$ e=7 | 12. | $C_1 = 153$ n=209<br>$C_2 = 43$ e=13 |

3. Реализовать алгоритм шифрования RSA на языке программирования (+0,5 балла).

### *Вопросы к модулю 4*

1. Является ли дифференцирование алгоритмической процедурой?

2. В чем заключается алгоритмическая трудность вычисления неопределенных интегралов?

3. Сформулировать задачу интегрирования.

4. В каких классах не разрешима проблема интегрирования?

5. В чем состоит задача интегрирования рациональных функций?

6. Какие недостатки имеет прямой метод интегрирования рациональных функций?

7. Разбивается ли при помощи анализа Фурье пространственная или временная функция на синусоидальные составляющие?

8. Как называется переход от набора значений к коэффициентам?

9. Какую сложность имеет быстрый алгоритм интерполяции?

10. Какое комплексное число w называется комплексным корнем степени n из единицы?

11. По какой теореме преобразование Фурье превращает сложную операцию свёртки в простое умножение?

12. Что собой представляет быстрое преобразование Фурье?

13. Чем занимается наука криптография?

14. Что понимают под шифрованием?

15. Что такое надежность шифра?

16. Как называется не санкционированное действие при расшифровке сообщения?

17. Что собой представляют системы криптографии с закрытым ключом?

18. Что собой представляют системы криптографии с открытым ключом?

## Тестовые задания

1. При проведении вычислений компьютер использует определенные способы вычислений, которые называются:

1) численные методы;

2) прямой перебор;

3) аналитические вычисления.

2. Сущность аналитических вычислений заключается:

1) в том, чтобы результатом была какая-то общая формула, не требующая вычислений с округлениями;

2) в вычислении искомого значения путем проведения набора вспомогательных вычислений;

3) в том, что результатом является большое количество арифметических действий.

3. В чем состоит особенность систем компьютерной алгебры?

1) обычно эти вычисления проводятся в системе с плавающей запятой пользователь передоверяет компьютеру много таких функций, которые раньше он выполнял самостоятельно;

2) нет верного ответа.

4. Изучение компьютерной алгебры сводится к пониманию того, как осуществляются вычисления компьютером.

1) да;

2) нет.

5. Какая основная задача компьютерной алгебры?

1) изучение алгебры с помощью компьютера;

2) изучение алгоритмов аналитических преобразований с точки зрения их эффективной реализации на компьютере;

3) получение результата с использованием аппарата алгебры.

6. Какая из систем относится к системам компьютерной алгебры?

1) Statistica;

2) MathCAD;

3) Macromedia.

7. Чему равны p и q в выражении $\frac{a}{b}+\frac{c}{d}=\frac{p}{q}$?

1) p=a·c, q=d·b;

2) p=a+c, q=b+d;

3) p=ad+bc, q=bd.

8. Поставить в соответствие алгоритмам порядок их сложности:

1) базовые алгоритмические операции;

2) скалярные алгоритмы?

a) $O(n^3)$;

b) $O(n^2)$;

c) $O(1)$;

d) $O(n)$.

9. При выполнении сложения длинных чисел, как получаем переносимый разряд? Например, для 7+8.

1) в следующий разряд переносим 15 mod 10=5;

2) 7 mod 10=7, в следующий разряд переносим 8 mod 10=0;

3) в следующий разряд переносим 15 div 10=1.

10. Если в представлении полинома явно представлены все члены, то оно называется

1) каноническим;

2) разреженным;

3) плотным;

4) нормальным.

11. Если две различные записи соответствуют всегда двум различным объектам, то такое представление полиномов называют:

1) каноническим;

2) разреженным;

3) плотным;

4) нормальным.

12. Какой из классов функций не относится к трансцендентным?

1) тригонометрических;

2) рациональных;

3) экспоненциальных.

13. Решения полиномиальных уравнений, чаще всего радикалы (то есть числа, содержащие в своей записи корни) называются:

1) трансцендентной функцией;

2) рациональной функцией;

3) алгебраической функцией.

14. Алгебраическое выражение типа $\sqrt[3]{x^2-1}$ относятся к классу:

1) простых радикалов;

2) вложенных радикалов;

3) общих алгебраических выражений.

15. Какой из классов функций относится к трансцендентным?

1) алгебраических;

2) рациональных;

3) экспоненциальных.

16. Проблема однозначности представления возникает при работе:

1) с рациональными функциями;

2) с трансцендентными функциями;

3) с алгебраическими объектами.

17. Теорема Риша применима только к функциям?

1) да;

2) нет.

18. Как оценивается качество любого алгоритма?

1) по длине кода;

2) по количеству подпрограмм;

3) по изменению функции, которая характеризует рост времени.

19. Барейс предложил семейство методов исключения для матриц:

1) с использованием рядов;

2) без использования дробей;

3) на основе канонического разложения.

20. Матричное произведение, обращение матриц, метод наименьших квадратов относятся к алгоритмам сложности?

1) O(n);

2) $O(n^2)$;

3) $O(n^3)$.

21. Пусть a и b – целые числа. Говорят, что b делит a, если

1) $a=bq+r$, $0 \le r < b$;

2) $a=br+q$, $0 \le r < b$;

3) $a=bq$.

22. Если целое число p отлично от 0 и ±1, и имеет делителями ±1, ±p, то оно

1) простое;

2) составное;

3) ассоциированное;

4) взаимно простое.

23. Целые числа a и b называются взаимно простыми, если

1) a|b, b|a;

2) их наибольший общий делитель равен 1;

3) они имеют положительный простой делитель, не превосходящий корня из a.

24. a=36, b=48. Чему равно d=НОД(a,b)?

1) $2\ 3^2$;

2) $2^4\ 3$;

3) $2^2\ 3^3$;

4) $2^2\ 3$.

25. Дан алгоритм Евклида.

**begin**

**repeat**

r:=a **mod** b; a:=b; b:=r

**until** b=0;

qcd:=a

**end;** Сколько операций сравнения будет выполнено в этом алгоритме, если a=500, b=13?

1) 1;

2) 2;

3) 3;

4) 4.

26. Вероятность того, что два натуральных числа, выбранные случайно окажутся взаимно простыми

1) <30%;

2) >60%;

3) <60%.

27. Если m делит b-a, то числа a и b называют:

1) сравнимыми по модулю m;

2) взаимно обратными по модулю m;

3) ассоциированными.

28. Объединение всех классов вычетов по модулю m

1) называется системой наименьших вычетов по модулю m;

2) называется полной системой вычетов по модулю m;

3) совпадает с множеством целых чисел.

29. Любые два класса вычетов по модулю m пересекаются?

1) да;

2) нет.

30. Какой остаток получится для суммы сравнений $6 \equiv 12 \pmod 3$ и $5 \equiv 8 \pmod 3$?

1) 0;

2) 1;

3) 2.

31. Поставить в соответствие:

1) полной системой вычетов по модулю m называют;

2) системой наименьших неотрицательных вычетов по модулю m называют;

3) классами вычетов по модулю m называют.

a) совокупность чисел 0, 1, 2, …, m - 1;

b) некоторые классы эквивалентности на множестве целых чисел;

c) совокупность m целых чисел, содержащую точно по одному представителю из каждого класса вычетов по модулю m.

32. Если $ab=1(\mathrm{mod}\ m)$, то числа a и b называются

1) простыми;

2) взаимно-простыми;

3) обратными;

4) ассоциированными.

33. Данный метод заключается в осуществлении нескольких малых вычислений по модулям взаимно-простых чисел и получении необходимого результата при помощи теоремы об остатках. Это –

1) алгоритм Евклида;

2) решето Эратосфена;

3) модулярное исчисление.

34. Из предложенных теорем выбрать теорему Евклида:

1) множество положительных простых чисел бесконечно;

2) всякое целое положительное число представимо в виде произведения положительных простых чисел;

3) положительное составное число a имеет по крайней мере один положительный делитель;

35. Если общий делитель двух целых чисел равен ±1, такие числа называют:

1) простыми;

2) взаимно-простыми;

3) составными;

4) взаимно-обратными.

36. Для соотношения 180 4+(-77) 7=1 найти обратный элемент к 7 по модулю 180?

1) 4;

2) 7;

3) 103;

4) 180.

37. Число итераций, необходимое для вычисления НОД (а, в) равно:

1) $n \le \frac{6}{\pi^2}$

2) $n \le 2^q \left|\frac{a_p}{b_q}\right| \sqrt{\sum_{i=0}^{p} a_i^2}$

3) нет верного ответа.

38. Представление числа в виде $a=\varepsilon p_1^{l1} p_2^{l2} \ldots . p_s^{ls,}$, $\varepsilon=\pm 1$ называется

1) записью в позиционной системе счисления;

2) каноническим разложением на простые множители4

3) нет верного ответа.

39. Выбрать правильную запись числа $(635)_8$ в двоичной системе счисления:

1) $(110011101)_2$;

2) $(11000110101)_2$;

3) $(011000110101)_2$.

40. Выбрать правильную запись числа $(10001110011)_2$ в шестнадцатеричной системе счисления:

1) $(2163)_{16}$;

2) $(4346)_{16}$;

3) $(473)_{16}$;

4) $(573)_{16}$.

41. Поставить в соответствие:

1) $n_1, n_2,\ldots, n_r$;

2) $z_1, z_2,\ldots, z_r$;

3) $y_1, y_2,\ldots, y_r$.

a) цифры числа x;

b) обратные к 10 по модулям $n_1, n_2,\ldots, n_r$ соответственно;

c) модулярные компоненты числа x;

d) попарно взаимно-простые числа.

42. Системой наименьших неотрицательных вычетов по модулю 6 является:

1) {0,1,2,3,4,5};

2) {0,1,2,3,4,5,6};

3) {0,1,2,3,4,5,6,7}.

43. Поставить в соответствие.

1) M={0,1,…,Q-1};

2) $A=(a_s, a_{s-1},\ldots, a_1)_Q$.

a) основание системы счисления;

b) смешанная система счисления;

c) цифры Q-ичной позиционной системы счисления;

d) запись числа в Q-ичной позиционной системы счисления.

44. В какой системе счисления число 21 запишется как 30?

1) 5;

2) 6;

3) 7;

4) 8.

45. Чему равна функция Эйлера φ(n), если n=10?

1) 4;

2) 6;

3) 8.

46. Найти обратное к 5 по модулю 6.

1) 3;

2) 4;

3) 5;

4) 6.

47. Кольцо **K[x]** называется кольцом полиномов от x над **K**, если **K[x]** -

1) простым расширением кольца **K** с помощью x;

2) простое трансцендентным расширением кольца **K** с помощью x;

3) нет верного ответа.

48. Если **K**[x]-простое трансцендентное расширение кольца **K** с помощью x, то кольцо **K[x]** называется:

1) полиномом над полем **K;**

2) нормированным полиномом;

3) кольцом полиномов от x над **K.**

49. Пусть a - полином из **K[x]**, $a=a_nx^n + \ldots+a_2x^2 + a_1x+ a_0$, $a_n \neq 0$. Поставить в соответствие:

1) n;

2) $a_0, a_1\ldots,a_n$;

3) $a_n$.

a) степень полинома;

b) коэффициенты полинома

c) старший коэффициент полинома

50. Если полином можно представить в виде произведения двух полиномов положительной степени, то полином a называют:

1) простым;

2) приводимым;

3) неприводимым.

51. Если полином можно представить в виде произведения двух полиномов, то такой полином называют:

1) неприводимым;

2) нормированным;

3) нет верного ответа.

52. Данное число x возвести в степень n ($n=(10101_2)$), используя бинарный метод. Выбрать правильную последовательность вычисления x

1) $x^2x^4x^5x^{10}\ x^{20}\ x^{21}$;

2) $x^2x^4x^8x^9\ x^{18}\ x^{19}$;

3) $x^2x^3x^6x^{12}\ x^{24}\ x^{25}$.

53. Используя бинарный метод записать правило вычисления $x^n$, $n=(25)_{10}$

1) SSXSSX;

2) SSSXSXX;

3) SXSSSX.

54. Данное число x возвести в степень n ($n=(10011_2)$), используя бинарный метод. Выбрать правильную последовательность вычисления x

1) $x^2x^4x^5x^{10}\ x^{11}\ x^{22}$;

2) $x^2x^3x^6x^7\ x^{14}\ x^{15}$;

3) $x^2x^4x^8x^9\ x^{18}\ x^{19}$.

55. Используя бинарный метод записать правило вычисления $x^n$, $n=(28)_{10}$

1) SXSXSX;

2) SXSXSS;

3) SSSXSX.

56. Сколько умножений потребуется для вычисления $x^{13}$, используя метод множителей?

1) 5;

2) 6;

3) 8.

57. Для вычисления полинома степени n $a=a_nx^n+a_{n-1}x^{n-1}+a_1x+a_0$, $a_n\neq0$ есть метод, позволяющий реорганизовать эти вычисления. Это

1) схема Горнера;

2) бинарный метод;

3) метод множителей.

58. Алгоритмом Евклида используется для:

1) вычисления полинома;

2) разложения на множители;

3) нахождения НОД двух полиномов.

59. Наибольший общий делитель коэффициентов $a_0$, $a_1$…, $a_n$ в кольце **K** называется:

1) содержанием полинома;

2) примитивной частью полинома;

3) нет верного ответа.

60. Неравенство Ландау-Миньотта позволяет:

1) оценить старшие коэффициенты полиномов;

2) найти границу для коэффициентов НОД двух полиномов;

3) определить количество итераций для вычисления НОД.

61. Восстановить правильную последовательность в алгоритме вычисления НОД двух полиномов:

1) то c:=модулярный_НОД(a,b,p);

2) p:=найти_большое_простое (2 m);

3) m:=граница_Ландау_Миньотта (a,b);

4) то выход c;

5) цикл до бесконечности;

6) если степень_остатка(p,a) или степень_остатка(p,b);

7) если делит (c,a) и делит (c,b);

62. Если полином имеет положительную степень и обладает только тривиальными делителями, то он называется:

1) простым;

2) составным;

3) приводимым.

63. Получить n, используя правило вычисления $x^n$ – SXSXSSSX (первая единица не вычеркнута)?

1) 24;

2) 25;

3) 32.

64. Полином f, содержание которого есть 1 в **K**, называется:

1) приведенным;

2) примитивным;

3) нормированным.

65. Если $a=b_1 \cdot q_1+b_2$; $\deg(b_1)>\deg(b_2)$, $b_1=b_2 \cdot q_2+b_3$; $\deg(b_2)>\deg(b_3)$. Чему равно $b_2$?

1) $b_2=b_3 \cdot q_3+b_4$;

2) $b_2=b_3 \cdot q_2+b_4$;

3) $b_2=b_1 \cdot q_3+b_3$.

66. Результант полиномов равен нулю. Это означает, что:

1) коэффициенты полинома равны нулю;

2) полиномы имеют общий делитель положительной степени;

3) нет верного ответа.

67. При помощи анализа Фурье пространственная или временная функция разбивается на синусоидальные составляющие?

1) да;

2) нет.

68. Переход от набора значений к его коэффициентам называется:

1) сверткой;

2) интерполяцией;

3) преобразованием Фурье.

69. Быстрый алгоритм интерполяции имеет сложность:

1) $O(n)$;

2) $O(n^2)$;

3) $O(n^3)$.

70. Поставить в соответствие шагам алгоритма их назначение:

1) вычисление значений;

2) интерполяция.

a) дополнить коэффициенты полиномов a и b нулевыми коэффициентами старших степеней так, чтобы коэффициентов стало по 2n;

b) при помощи FFT, вычислить значения полиномов a и b в точках, являющихся корнями степени 2n из единицы;

c) получить коэффициенты полинома c при помощи обратного FFT, применяемого к значениям полинома c в корнях степени 2n из единицы.

71. Комплексным корнем степени n из единицы называют такое комплексное число w, что

1) $w^n=1$;

2) $w^n=-1$;

3) w=1.

72. Преобразование Фурье превращает сложную операцию свёртки в простое умножение:

1) по теореме Парсеваля;

2) по теореме Планшереля;

3) по теореме о свёртке.

73. Аббревиатура FFT – это:

1) дискретное преобразование Фурье;

2) быстрое преобразование Фурье;

3) нет верного ответа.

74. Минимальное расширение кольца **K**, являющееся подкольцом кольца **L**, и содержащее элементы $x_1,\dots,x_m$ из **L** называется:

1) m – кратным расширением кольца **K**;

2) m – кратным трансцендентным расширением кольца **K**;

3) подкольцом кольца **L**.

75. Если для любых элементов $a_{(i)}$ кольца **K** из равенства

$\sum_{(i)\in M} a_{(i)}x_1^{i_1}\dots x_m^{i_m}=0,\ M\in N^m,$ следует равенство нулю всех коэффициентов $a_{(i)}$, то элементы $x_1,\dots,x_m$ кольца **L** называются:

1) алгебраически зависимыми над кольцом **К**;

2) алгебраически независимыми над кольцом **К**;

3) нет верного ответа.

76. Произведение степеней переменных это:

1) моном;

2) полином;

3) S-полином.

77. Если кольцо $\mathbf{K}[x_1][x_2]\ldots[x_m]$ определяется формулами $\mathbf{K}[x_1][x_2]=(\mathbf{K}[x_1])[x_2]$, $\mathbf{K}[x_1][x_2]\ldots[x_m]=(\mathbf{K}[x_1][x_2]..[x_{m-1}])[x_m]$, то оно является

1) кольцом полиномов над **K** от $x_1,...,x_m$;

2) m – кратным расширением кольца **К**;

3) m – кратным трансцендентным расширением кольца **К**.

78. Поставить в соответствие. Кольцо $\mathbf{K}[x_1,\ldots,x_m]$ называется:

1) кольцом полиномов над **K** от $x_1,...,x_m$;

2) m – кратным расширением кольца **K**;

3) m – кратным трансцендентным расширением кольца **K**.

a) если кольцо $\mathbf{K}[x_1][x_2]\ldots[x_m]$ определяется формулами $\mathbf{K}[x_1][x_2]=(\mathbf{K}[x_1])[x_2]$, $\mathbf{K}[x_1][x_2]\ldots[x_m]=(\mathbf{K}[x_1][x_2]..[x_{m-1}])[x_m]$;

b) если для любого $s \in \{1,\ldots,m\}$ кольцо $\mathbf{K}[x_1,\ldots,x_s]$ является простым трансцендентным расширением кольца $\mathbf{K}[x_1,\ldots,x_{s-1}]$ при помощи $x_s$;

c) если кольцо $\mathbf{K}[x_1,\ldots,x_m]$ является m – кратным расширением ненулевого коммутативного кольца **K**;

d) если элементы $x_1,...,x_m$ кольца **L** называются алгебраически независимыми над кольцом **К**.

79. В определении порядка (<) на мономах одно из условий лишнее.

1) для любых мономов a и b, если b не равно 1, то a<ab;

2) для любых мономов a и b, если a равно 1, то ab=ba=1;

3) если a<b, то для любого монома c имеем ac<bc.

80. Полином f редуцирован относительно G, если:

1) ни один старший моном элемента множества G не делит старшего монома полинома;

2) из него можно вычесть кратное некоторого элемента множества G, чтобы исключить его старший моном;

3) все ответы верные.

81. Полином f редуцирован относительно G, если:

1) из него можно вычесть кратное некоторого элемента множества G, чтобы исключить его старший моном;

2) из него можно вычесть кратное каждого элемента множества G, чтобы исключить его старший моном;

3) нет верного ответа.

82. Пусть $G=\{g_1=x-1;\ g_2=2y-1\}$ и $f=2xy$. Выбрать две возможные редукции полинома f с помощью $g_1$ и с помощью $g_2$

1) $f-2yg_1=2y$ , $f-xg_2=x$;

2) $f-2yg_1=y$ , $f-xg_2=2x$;

3) $f-2yg_1=2x$ , $f-xg_2=y$.

83. Пусть $G=\{g_1=2x-1;\ g_2=y-2\}$ и $f=2xy$. Выбрать две возможные редукции полинома f с помощью $g_1$ и с помощью $g_2$

1) $f-2yg_1= y$ , $f-xg_2= 4x$;

2) $f-yg_1= y$ , $f-2xg_2= 4x$;

3) $f-yg_1= 4x$ , $f-2xg_2= y$.

84. НОД всех коэффициентов полинома $p=\sum_{i=0}^{n} a_i x_i$ обозначается:

1) pp(p);

2) p/cont(p);

3) cont(p).

85. По формуле pp(p)=p/cont(p) определяется

1) содержание полинома p;

2) примитивная часть полинома p;

3) НОД всех коэффициентов полинома p.

86. Произведение всех переменных двух полиномов p и q, каждая в степени, равная максимуму ее степеней в этих членах и коэффициентов этих членов – это:

1) редуцированный полином;

2) S-полином полиномов p и q;

3) наименьшее общее кратное двух полиномов.

87. Алгоритм вычисления НОД двух полиномов от нескольких переменных опирается на:

1) лемму Гаусса;

2) теорему Дирихле;

3) теорему Ламе.

88. Для записи полиномов используются различные системы. Дан полином $(x+y)^2+x+y+1$. Поставить в соответствие.

1) лексикографическая;

2) общей степени, затем лексикографическая;

3) общей степени, затем обратная лексикографическая.

a) $y^2+2xy+x^2+y+x+1$;

b) $x^2+ y^2+2xy +x+y+1$;

c) $x^2+2xy+x+y^2+y+1$;

d) $x^2+2xy+y^2+x+y+1$.

89. Дан полином $(x+y)^2+x+y+1$. Его можно переписать в виде $x^2+2xy+x+y^2+y+1$. Эта форма записи называется:

1) рекурсивной;

2) распределенной;

3) нет верного ответа.

90. Для полинома $x^2+2xy+y^2+x+y+1$ выбрать рекурсивную форму записи:

1) $(x+y)^2+(x+y)+1$;

2) $(x^2+2xy+y^2)+x+y+1$;

3) $x^2+x(2y+1)+(y^2+y+1)$.

91. Поставить в соответствие.

1) прямой метод;

2) метод Эрмита.

a) представляет остающийся после вычисления интеграл в виде суммы логарифмов;

b) использует разложение дроби q/r на простейшие дроби;

c) позволяет определить рациональную часть интеграла рациональной функции без использования дополнительных величин.

92. Найти алгоритм, который для любого элемента $a \in A$ либо выдает такой элемент $b \in B$, что $a = b'$, либо доказывает, что в B не существует такого элемента b, что $a = b'$ - это задача:

a) интегрирования;

b) дифференцирования;

c) нет верного ответа.

93. Если каждый элемент множества A принадлежит множеству B, то множество A называется:

1) объектом множества B;

2) равным множеству B;

3) подмножеством множества B.

94. Символ $\subset$ называется знаком

1) принадлежности;

2) следствия;

3) включения;

4) тождественности.

95. Над множеством вводятся операции, с помощью которых можно получить из любых двух множеств новые множества.

Поставить в соответствие:

1) $\{x \mid x \in A \ \& \ x \in B\}$;

2) $\{x \mid x \in A \ \& \ x \notin B\}$.

a) дополнение;

b) объединение;

c) пересечение;

d) разность.

96. Какая операция соответствует в записи $A\ B=\{x \mid x\in A \vee x\in B\}$?

1) / (разность);

2) \ (дополнение);

3) $\cap$ (пересечение);

4) $\cup$ (объединение).

97. Множество A содержится в универсальном множестве U, т.е. $\forall$ A, $A\subset U$. Множество $A^{|}$ является дополнением множества A. Чему равно пересечение множеств A и $A^{|}$ ($A\cap A^{|}$)?

1) U;

2) A;

3) Ø.

98. Множество A содержится в универсальном множестве U, т.е. $\forall$ A, $A\subset U$. Чему равно объединение множеств A и U ($A\cup U$).

1) U;

2) A;

3) Ø.

99. Если $\forall x, y, z,\ (xRy \,\&\, yRz)\rightarrow xRz$, то бинарное отношение R на множестве A называется:

1) симметричным;

2) рефлексивным;

3) транзитивным;

4) антисимметричным.

100. Бинарное отношение R на множестве A называется отношением эквивалентности на A, если оно:

1) антирефлексивно, симметрично и транзитивно на A;

2) рефлексивно, симметрично и транзитивно на A;

3) рефлексивно, антисимметрично и транзитивно на A.

101. Отображение $A \times A$ в A называется:

1) бинарной операцией;

2) прямым произведением;

3) нет верного ответа.

102. Если $\forall b,c \in A\ (a * b = a * c) \to b = c$, то относительно операции * элемент $a \in A$ называется:

1) нейтральным;

2) симметричным;

3) регулярным.

103. Какая из бинарных операций не ассоциативна и не коммутативна:

1) сложение;

2) вычитание;

3) умножение;

4) пересечение;

5) объединение.

104. Верно ли следующее утверждение? Множество всех нечетных чисел замкнуто относительно сложения, но не замкнуто относительно умножения.

1) да;

2) нет.

105. Какое из множеств замкнуто относительно сложения и умножения?

1) четных чисел;

2) нечетных чисел;

3) нет верного ответа.

106. Какой тип имеет алгебра целых чисел $\langle Z,+,\cdot \rangle$?

1) (2,1);

2) (2,0);

3) (2,2).

107. Упорядоченная тройка $\mathbf{A} = \langle A, V, V_0 \rangle$, где А - непустое множество, V - множество операций на А, $V_0$- множество отношений на А называется:

1) полем;

2) кольцом;

3) алгебраической системой;

4) нет верного ответа.

108. Если главные операции удовлетворяют условиям (аксиомам):

a. бинарная операция $*$ ассоциативна, т.е. $\forall a,b,c \in P \;\; a*(b*c)=(a*b)*c$;

b. в P имеется нейтральный элемент относительно $*$, т.е. $\exists e \in P \;\; \forall a \in P \;\; a*e=e*a=a$;

c. $\forall a \in P \;\; a*a'=a'*a=e$, то алгебра $\mathbf{P}=\langle P,*,' \rangle$ типа (2,1) называется:

1) полем;

2) группой;

3) кольцом;

4) нет верного ответа.

109. Поставить в соответствие. Кольцо называется:

1) коммутативным;

2) нулевым;

3) областью целостности.

a) если $|\mathbf{K}| = \{0_K\}$;

b) если $a \cdot b = b \cdot a, \;\; \forall a,b \in K$;

c) если $a \neq 0, b \neq 0$ и $ab=0$ или $ba=0$;

d) если оно коммутативно, $0_K \neq 1_K$ и $\forall a,b \in K(a \cdot b = 0 \rightarrow a=0 \vee b=0)$.

110. Коммутативное кольцо, в котором нуль отличен от единицы, и всякий ненулевой элемент является обратимым элементом кольца, называется:

1) нулевым кольцом;

2) полем;

3) мультипликативным моноидом;

4) нет верного ответа.

111. Уравнение bx=a имеет единственное решение $ab^{-1}$, если a и b – это элементы:

1) поля;

2) кольца;

3) группы.

112. Поставить в соответствие. Умножение натуральных чисел:

1) ассоциативно;

2) коммутативно;

3) дистрибутивно.

a) $\forall\, a, b, c \in N \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

b) $\forall\, a, b \in N \quad a \cdot b = b \cdot a$;

c) $\forall\, a, b, c \in N \quad (a + b) \cdot c = a \cdot c + b \cdot c \,\&\, c \cdot (a + b) = c \cdot a + c \cdot b$.

## Заключение

В настоящее время уделяется большое внимание вопросам фундаментализации обучения информатике. В учебных планах вузов предусмотрено изучение теоретической информатики, как по направлениям подготовки бакалавров, так и по направлениям подготовки магистров.

Компьютерная алгебра, сообщая результат в виде аналитического выражения, позволяет увидеть «изнутри» процессы, которые описаны математическими моделями. Изучение компьютерной алгебры сводится к пониманию того, как осуществляются вычисления компьютером.

Для организации самостоятельной работы студентов в пособии представлены индивидуальные задания и вопросы к тестам.

При изучении дисциплины «Компьютерная алгебра» может быть использована модульно-рейтинговая система контроля знаний студентов. В приложении приведен пример рейтинга по дисциплине.

## Список использованной литературы


1. Аладьев В.З. Системы компьютерной алгебры Maple: искусство программирования / В. З. Аладьев. – М. : Лаб. Базовых Знаний, 2006. – 792 с.
2. Ахо, А. Построение и анализ вычислительных алгоритмов /А. Ахо, Дж. Хопкрофт, Дж. Ульман. – М. : Мир, 1979. – 536 с.
3. Бабаш А.В. Криптография / А. В. Бабаш, Г. П. Шанкин; ред. В. П. Шерстюк, Э. А. Применко. – М. : СОЛОН-ПРЕСС, 2007. – 512 с.
4. Бухбергер Б. Компьютерная алгебра: символьные и алгебраические вычисления. – М. : Мир, 1986. – 392 с.
5. Дьяконов В.П. Mathematica 5/6/7. Полное руководство. – М.: ДМК Пресс, 2010. – 624 с.
6. Дэвенпорт Д. Компьютерная алгебра: Системы и алгоритмы алгебраических вычислений /Дж. Дэвенпорт, И. Сирэ, Э. Турнье; Пер. с фр. Е. В. Панкратьева и др. – М. : Мир, 1991. – 352 с.
7. Кокс Д. Идеалы, многообразия и алгоритмы / Д. Кокс, Дж. Литтл, Д. О'Ши. – М. : Мир, 2000. – 688 с.
8. Кормен Т. Алгоритмы: построение и анализ, 2-е издание. : Пер. с англ. / Т. Кормен, Ч. Лейзерсон, Р. Ривест. – М.: МЦИМО, 2011. – 1296 с.
9. Матрос Д.Ш. Элементы абстрактной и компьютерной алгебры: учеб. пособие для вузов /Д. Ш. Матрос, Г. Б. Поднебесова. – М.: Академия, 2004. – 240 с.
10. Поднебесова Г.Б. Абстрактная и компьютерная алгебра. Практикум / Г. Б. Поднебесова. – Челябинск : Изд-во Южно-Ур. гос. гуманитар.-пед. ун-та, 2016. – 125 с.
11. Поднебесова Г.Б. Основы компьютерной алгебры. Элективный курс: учебное пособие / Г. Б. Поднебесова. – М. : БИНОМ. Лаборатория знаний, 2008. – 112 с.

# Приложение

## Приложение 1. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

**Лекции**

| *Наименование раздела дисциплины (модуля)/ Тема и содержание* | *Трудоемкость (кол-во часов)* |
|---|---|
| ***1. Представление данных в компьютере*** | ***2*** |
| ***Формируемые компетенции, образовательные результаты:*** ПК-1: З.2 (ПК.1.1 ) | |
| 1.1. Аналитические вычисления на компьютере. Абстрактная алгебра<br>1. Арифметические вычисления и операции. Представление целых чисел в компьютере. Умножение длинных чисел.<br>2. Представление и работа с другими математическими объектами.<br>3. Представление полиномов.<br>4. Представление рациональных, алгебраических и трансцендентных функций.<br>Учебно-методическая литература: 2, 4, 5, 6, 9 | 2 |
| ***2. Алгоритмы компьютерной математики*** | ***6*** |
| ***Формируемые компетенции, образовательные результаты:*** ПК-1: З.1 (ПК.1.1 ), У.1 (ПК.1.2), В.1 (ПК.1.3), З.3 (ПК.1.1 ) | |
| 2.1. Элементы теории делимости в кольце целых чисел<br>1. Основная теорема арифметики.<br>2. Теорема Евклида.<br>3. Алгоритм Евклида. Расширенный алгоритм Евклида.<br>4. Теорема Ламе.<br>Учебно-методическая литература: 2, 4, 9 | 2 |
| 2.2. Позиционные системы счисления<br>1. Основные определения.<br>2. Смешанная система счисления.<br>3. Перевод чисел из одной системы счисления в другую.<br>Учебно-методическая литература: 2, 4, 9 | 2 |
| 2.3. Элементы теории сравнений в кольце целых чисел<br>1. Сравнимость по модулю.<br>2. Вычеты.<br>3. Классы вычетов.<br>4. Теоремы Эйлера и Ферма.<br>5. Китайская теорема об остатках.<br>6. Модулярная арифметика.<br>Учебно-методическая литература: 2, 4, 9 | 2 |
| ***3. Полиномы от одной и нескольких переменных*** | ***4*** |
| ***Формируемые компетенции, образовательные результаты:*** ПК-1: У.2 (ПК.1.2), В.2 (ПК.1.3) | |
| 3.1. Полиномы от одной переменной. Нахождение НОД<br>1. Основные определения.<br>2. Полиномы над полем.<br>3. Простое трансцендентное расширение кольца.<br>4. Вычисления полиномов. Бинарный метод и метод множителей.<br>5. Неравенство Ландау- Миньотта.<br>6. Вычисление НОД.<br>Учебно-методическая литература: 2, 3, 5, 9 | 2 |

| | |
|---|---|
| 3.2. Нахождение НОД полиномов от нескольких переменных<br>1. Кольцо полиномов от нескольких переменных.<br>2. Содержание полинома.<br>3. Примитивная часть полинома.<br>4. Лемма Гаусса.<br>4. Алгоритм вычисления НОД.<br>Учебно-методическая литература: 2, 5, 6, 9 | 2 |
| ***4. Компьютерная система Wolfram Alpha. Применение алгоритмов компьютерной математики*** | ***4*** |
| ***Формируемые компетенции, образовательные результаты:***<br>ПК-1: З.4 (ПК.1.1 ), У.2 (ПК.1.2), В.2 (ПК.1.3) | |
| 4.1. Кодирование. Криптография<br>1. Кодирование информации.<br>2. Блочное и алфавитное кодирование.<br>3. Классификация шифров.<br>4. Системы с открытым ключом.<br>5. Системы с закрытым ключом.<br>6. Криптосистема RSA.<br>Учебно-методическая литература: 2, 6, 9 | 2 |
| 4.2. Интегрирование и дифференцирование. Преобразование Фурье<br>1. Задача интегрирования.<br>2. Интегрирование рациональных функций.<br>3. Интегрирование более сложных функций.<br>4. Анализ Фурье. Методы анализа Фурье.<br>5. Применение преобразования Фурье.<br>Учебно-методическая литература: 2, 3, 9<br>Профессиональные базы данных и информационные справочные системы: 1 | 2 |

## Практические работы

| *Наименование раздела дисциплины (модуля)/ Тема и содержание* | *Трудоемкость (кол-во часов)* |
|---|---|
| ***1. Представление данных в компьютере*** | ***2*** |
| ***Формируемые компетенции, образовательные результаты:*** ПК-1: З.1 (ПК.1.1 ), У.1 (ПК.1.2), В.1 (ПК.1.3), З.3 (ПК.1.1 ) | |
| 1.1. Разработка кейса по СКМ<br>- работа в Publisher;<br>- изучение шаблона кейс.pub;<br>- разработка кейса.<br>Учебно-методическая литература: 3, 9, 10, 11 | 2 |
| ***2. Алгоритмы компьютерной математики*** | ***6*** |
| ***Формируемые компетенции, образовательные результаты:*** ПК-1: У.2 (ПК.1.2), В.2 (ПК.1.3) | |
| 2.1. Расширенный алгоритм Евклида. Вычисление НОД<br>- соотношение Безу;<br>- нахождение обратного числа по модулю простого числа;<br>- прямой метод;<br>- алгоритм Евклида;<br>- вычисление НОД разложением на множители.<br>Учебно-методическая литература: 3, 4, 9, 10, 11 | 2 |
| 2.2. Модулярная арифметика<br>- восстановление произведения по модулярным компонентам двух чисел.<br>Учебно-методическая литература: 2, 4 | 2 |
| 2.2. Разложение на множители<br>- деление и разложение на множители;<br>- метод Ферма;<br>- вероятностный метод.<br>Учебно-методическая литература: 3, 9, 10, 11 | 2 |
| ***3. Полиномы от одной и нескольких переменных*** | ***4*** |
| ***Формируемые компетенции, образовательные результаты:*** ПК-1: З.4 (ПК.1.1 ), У.2 (ПК.1.2), В.2 (ПК.1.3) | |
| 3.1. Вычисление полиномов<br>- бинарный метод и метод множителей;<br>- схема Горнера, обобщенная схема Горнера.<br>Учебно-методическая литература: 3, 5, 6, 9, 10, 11 | 2 |
| 3.2. Нахождение НОД полиномов<br>- применение неравенства Ландау-Миньотта;<br>вычисление модулярного НОД.<br>Учебно-методическая литература: 4, 5, 6, 9, 10, 11 | 2 |
| ***3. Компьютерная система Wolfram Alpha. Применение алгоритмов компьютерной математики*** | ***4*** |
| ***Формируемые компетенции, образовательные результаты:*** ПК-1: З.4 (ПК.1.1 ), У.2 (ПК.1.2), В.2 (ПК.1.3) | |
| 3.1. Полиномы от одной и нескольких переменных в Wolfram Alpha:<br>- основные функции для работы с полиномами от одной и нескольких переменных.<br>Учебно-методическая литература: 1, 3, 9, 10, 11 | 2 |
| 3.1. Криптосистема RSA<br>- вычисление открытого ключа;<br>- вычисление закрытого ключа;<br>- шифрование подписи.<br>Учебно-методическая литература: 2, 3, 9, 10, 11 | 2 |

# Приложение 2. Содержание самостоятельной работы

## Самостоятельная работа студентов

| *Наименование раздела дисциплины (модуля)/ Тема для самостоятельного изучения* | *Трудоемкость (кол-во часов)* |
|---|---|
| ***1. Представление данных в компьютере*** | ***10*** |
| ***Формируемые компетенции, образовательные результаты:*** ПК-1: З.2 (ПК.1.1 ) | |
| 1.1. Аналитические вычисления на компьютере. Абстрактная алгебра<br>***Задание для самостоятельного выполнения студентом:***<br>Разработать кейс по одной из тем:<br>Maxima, Axiom, Maple, Matab, MathCAD, TRIP, Reduce, Derive, Cadabra, Singular, Magma, MuPAD, GAP, GINV, Jasymca<br>Учебно-методическая литература: 1, 2, 5, 6, 9, 10, 11 | 10 |
| ***2. Алгоритмы компьютерной математики*** | ***10*** |
| ***Формируемые компетенции, образовательные результаты:*** ПК-1: З.1 (ПК.1.1 ), У.1 (ПК.1.2), В.1 (ПК.1.3), З.3 (ПК.1.1 ) | |
| 2.1. Модулярная арифметика<br>***Задание для самостоятельного выполнения студентом:***<br>Восстановить произведение двух целых больших чисел по их модулярным компонентам (по списку):<br>Пример:<br>$n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$<br>$x_1=0$ $x_2=0$ $x_3=11$ $x_4=12$<br>$x_1=0$ $x_2=0$ $x_3=3$ $x_4=8$<br>Учебно-методическая литература: 2, 3, 5, 9, 10, 11 | 10 |
| ***3. Полиномы от одной и нескольких переменных*** | ***10*** |
| ***Формируемые компетенции, образовательные результаты:*** ПК-1: У.2 (ПК.1.2), В.2 (ПК.1.3) | |
| 3.1. Полиномы от одной и нескольких переменных в Wolfram Alpha<br>***Задание для самостоятельного выполнения студентом:***<br>Вопросы для теста:<br>1. Какое кольцо называется простым расширением кольца, простым трансцендентным расширением кольца?<br>2. Что является степенью полинома, старшим коэффициентом полинома?<br>3. Какой полином называется нормированным? приводимым? неприводимым?<br>4. Сформулировать китайскую теорему об остатках для 2-х полиномов, для r – полиномов?<br>5. Что такое результант полиномов?<br>6. Какие существуют методы вычисления x в степени n?<br>7. Что такое аддитивная сложность числа n?<br>8. Какой способ вычисления полиномов называется “Схемой Горнера»”?<br>9. Для чего используется неравенство Ландау-Миньотта?<br>10. Записать алгоритм вычисления НОД двух полиномов по модулю простого числа p.<br>Учебно-методическая литература: 3, 9, 10, 11 | 10 |
| ***4. Компьютерная система Wolfram Alpha. Применение алгоритмов компьютерной математики*** | ***10*** |
| ***Формируемые компетенции, образовательные результаты:*** ПК-1: З.4 (ПК.1.1 ), У.2 (ПК.1.2), В.2 (ПК.1.3) | |
| 4.1. Кодирование. Криптография<br>***Задание для самостоятельного выполнения студентом:***<br>Зашифровать аббревиатуру (из списка), используя криптосистему RSA.<br>Учебно-методическая литература: 2, 3, 5, 9, 10, 11 | 10 |

**Приложение 3. Рейтинг**

| № | Фамилия, Имя | СКА | Доп. балл | Тест1 | Модуль1 | Алгоритм Евклида | Вычис-ление НОД | Модулярная арифметика | Разложение на множители | Доп. балл | Тест2 | Модуль2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

| № | Фамилия, Имя | Вычис-ление полино-мов | НОД полино-мов | Доп. балл | Тест3 | Модуль3 | Wolfram Alpha Практ. | Wolfram Alpha | RSA | Доп. балл | Тест4 | Модуль4 | Итог | **Оценка** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

## Приложение 4. Работа в Wolfram Alpha

Доступ по ссылке: https://www.wolframalpha.com/

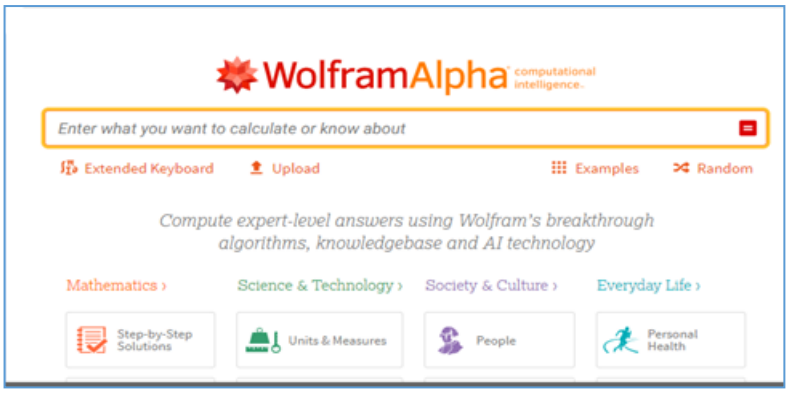



Рис. 1 – Главное окно

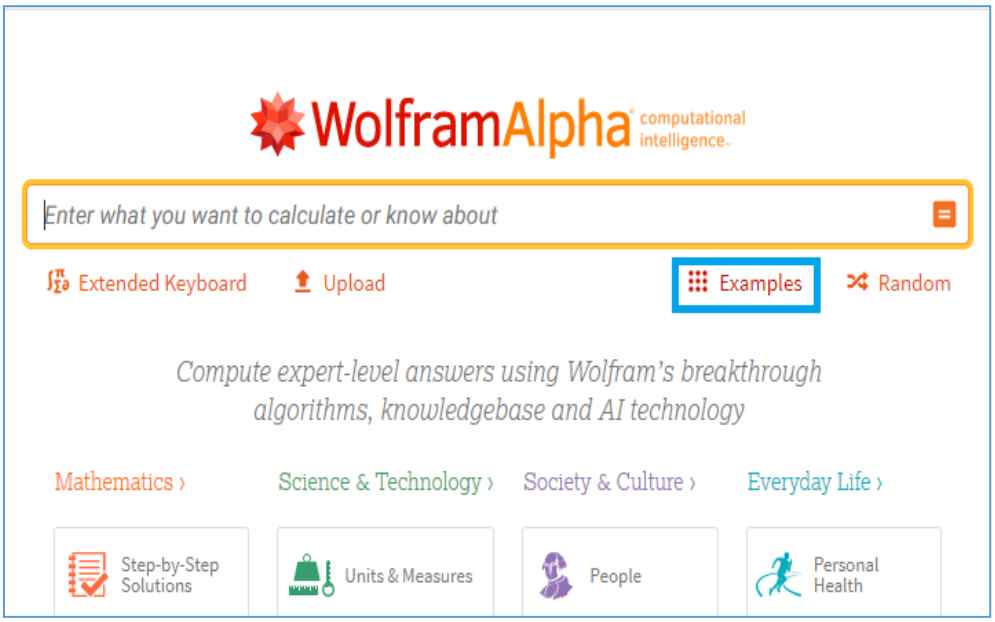



Рис. 2 – Помощь – Examples (->Algebra)

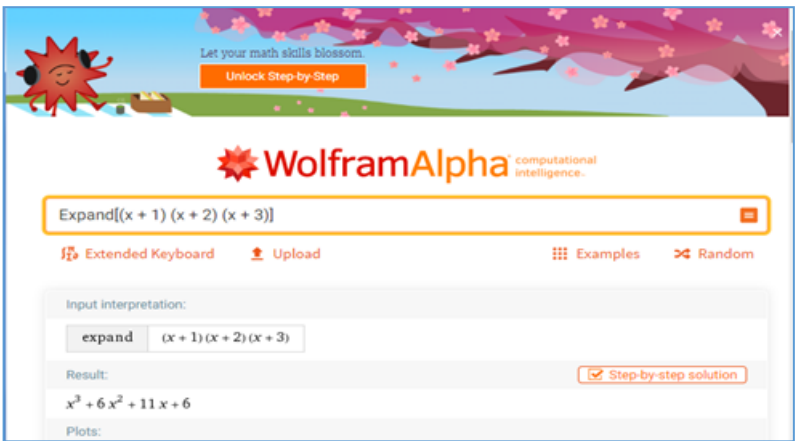



Рис. 3 – Функция Expand (раскрывает скобки)

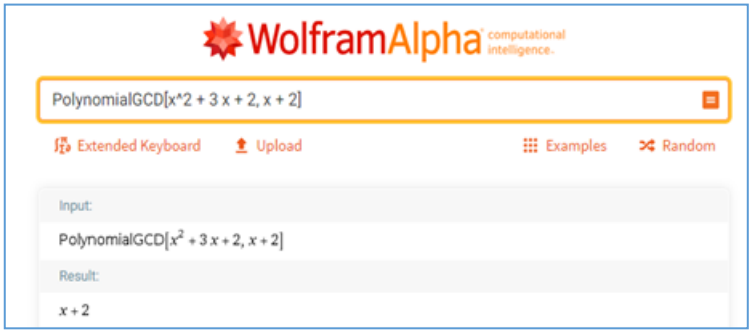



Рис. 4 – Функция Symplify (обратная Expand)


Рис. 5 – Вычисление НОД полиномов


Рис. 6 – Вычисление остатка от деления полиномов

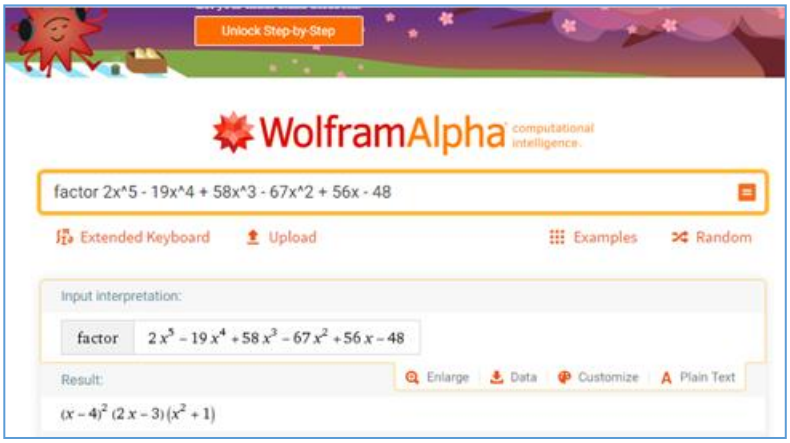



Рис. 7 – Разложение полиномов

*Учебное издание*

Поднебесова Галина Борисовна

# Компьютерная алгебра

**Учебно-практическое пособие**

ISBN 978-5-93162-447-1

Издательство ЗАО «Библиотека Миллера»

454091, г. Челябинск, ул. Свободы, 159

Подписано в печать 20.12.2023.
Объем 4,83 усл. печ..л.
Формат 60×84/16
Бумага типографская
Тираж 100 экз.
Заказ № 447.

Отпечатано в типографии Южно-Уральского государственного
гуманитарно-педагогического университета
454080, г. Челябинск, пр. Ленина, 69