

Г. Б. Поднебесова

**ТЕОРЕТИЧЕСКИЕ ОСНОВЫ
ИНФОРМАТИКИ**

Часть 1

Челябинск
2024

УДК 001.8(021)

ББК 73я73

П 44

Поднебесова Г.Б. Теоретические основы информатики. В 2-х частях.
Часть 1: учебно-практическое пособие / Г.Б. Поднебесова. – Челябинск: Изд-во ЗАО «Библиотека А. Миллера». 2024. – 100 с.

ISBN 978-5-93162-895-0 (общий)

ISBN 978-5-93162-896-7 (часть 1)

Учебное пособие содержит материал для изучения курса «Теоретические основы информатики». Пособие предназначено для организации аудиторной и самостоятельной работы студентов, обучающихся по направлению 04.03.05 «Педагогическое образование» с двумя профилями подготовки «Информатика. Иностранный язык» и «Математика. Информатика».

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

Рецензенты:

С.А. Загребина, д-р физ.-мат. наук, профессор ЮУрГУ

А.А. Рузаков, канд. пед. наук, доцент ЮУрГГПУ

ISBN 978-5-93162-895-0 (общий)

ISBN 978-5-93162-896-7 (часть 1)

© Г.Б. Поднебесова, 2024

Содержание

Введение	4
Содержание разделов дисциплины.....	6
Модуль 1. Представление данных в компьютере.....	9
Модуль 2. Алгоритмы компьютерной математики	19
Модуль 3. Полиномы от одной и нескольких переменных.....	46
Модуль 4. Система компьютерной математики Wolfram Alpha.	
Применение алгоритмов компьютерной математики.....	55
Заключение	87
Список использованной литературы	88
Приложение	89
Приложение 1. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	89
Приложение 2. Содержание самостоятельной работы.....	94
Приложение 3. Рейтинг	96
Приложение 4. Работа в Wolfram Alpha.....	97

Введение

Курс Теоретические основы информатики вводит студентов в современные проблемы теоретической информатики. Основной акцент в курсе делается на методологические аспекты и математический аппарат информатики, составляющие ядро широкого спектра информационных технологий. 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.

Курс «Теоретические основы информатики» состоит из двух частей и изучается в двух семестрах. В первой части курса студенты знакомятся с базовыми алгоритмами, такими как вычисление наибольшего общего делителя, нахождение обратного к числу, разложение целого числа на простые множители и др., и примерами применения этих алгоритмов в более сложных вычислениях.

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 данной части курса предполагается проведение лекционных и практических занятий.

В качестве формы контроля усвоения материала используется рейтинговая система оценки учебных достижений студентов.

Изучение данной дисциплины предусмотрено в обязательной части Блока 1 «Дисциплины/модули» основной профессиональной образовательной программы ФГОС ВО. 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 способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач
	ПК.1.1 знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета)
	ПК.1.2 умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО

№ п/п	Код и наименование индикатора достижения компетенции	Образовательные результаты по дисциплине
1	ПК.1.1 знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета)	<p>3.1 иметь представление об общих проблемах и задачах теоретической информатики;</p> <p>У.1 применять алгоритмы для кодирования информации;</p> <p>В.1 методами кодирования информации;</p> <p>3.2 определение основных понятий абстрактной и компьютерной алгебры;</p> <p>У.2 применять алгоритмы компьютерной алгебры для вычислений;</p> <p>В.2 основными алгоритмами компьютерной алгебры для программирования вычислительного блока систем</p>
2	ПК.1.2 умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО	<p>3.3 теоретическую информатику, фундаментальную и прикладную математику для обеспечения качества учебно-воспитательного процесса;</p> <p>У.3 структурировать информацию для формирования необходимых образовательных результатов;</p> <p>В.3 методами анализа для отбора содержания преподаваемых дисциплин;</p> <p>3.4 характеристику числовых систем;</p> <p>У.4 выполнять операции на множестве целых чисел;</p> <p>В.4 методами описания алгоритмов компьютерной математики</p>

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. Система компьютерной математики 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. Аналитические вычисления в WolframAlpha. Работа с простыми числами в WolframAlpha (2 часа):

- выполнение арифметических операций;
- вычисление суммы и произведения;
- основные функции для работы с простыми числами;
- разложение чисел на простые множители;
- вычисление следующего и предыдущего простого числа.

2. Разработка кейса по теме Системы компьютерной математики (2 часа):

Разработать кейс по одной из систем компьютерной математики. В кейсе должно быть описано: функциональное назначение системы; тип архитектуры; средства реализации; области применения; примеры (принтскрины); интегральные оценки качества.

Модуль 2. Алгоритмы компьютерной математики

1. Системы счисления (2 часа):

- вычисления в различных системах счисления;
- переводы целых чисел;
- переводы дробных чисел;
- переводы произвольных чисел.

2. Расширенный алгоритм Евклида (2 часа).

- соотношение Безу;
- нахождение обратного числа по модулю простого числа.

3. Вычисление наибольшего общего делителя (НОД) (2 часа).

- прямой метод, алгоритм Евклида;
- вычисление НОД разложением на множители.

4. Модулярная арифметика (4 часа):

– восстановление произведения двух чисел по их модулярным компонентам.

5. Разложение на множители (2 часа)

- деление и разложение на множители;
- метод Ферма;
- вероятностный метод.

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. Система компьютерной математики WolframAlpha.

Применение алгоритмов компьютерной математики

1. Полиномы от одной переменной в WolframAlpha (2 часа):

- основные функции для работы с полиномами от одной переменной;
- вычисление НОД;
- вычисление частного и остатка от деления полиномов.

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

- основные функции для работы с полиномами от нескольких переменных;

- вычисление НОД и НОК полиномов.

3. Интегрирование и дифференцирование в WolframAlpha (2 часа):

- основные функции для вычисления интегралов;
- функции для вычисления производных.

4. Шифрование методом RSA (2 часа).

- вычисление открытого и закрытого ключа;
 - шифрование подписи.

Модуль 1. Представление данных в компьютере

Практическое занятие №1

Аналитические вычисления в Wolfram Alpha

1. Организация вычислений.

1) $56 \cdot 34 / 8$

238

2) $(53 + 34^2 + 25^3) / (3 \cdot 53 - 4 \cdot 25)$

16834

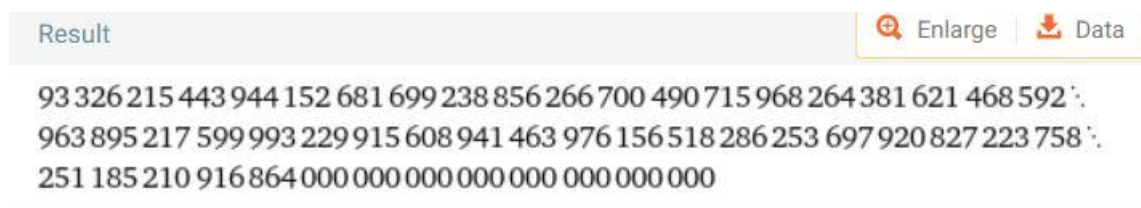
59

2. Целочисленные вычисления.

3) **Factorial[7]**

5040

4) **100!**



Result Enlarge Data

93 326 215 443 944 152 681 699 238 856 266 700 490 715 968 264 381 621 468 592
963 895 217 599 993 229 915 608 941 463 976 156 518 286 253 697 920 827 223 758
251 185 210 916 864 000 000 000 000 000 000 000 000 000 000

Для представления выражения в виде вещественного числа используется функция **N** (записывается в виде **N[expr]**, где **expr** – выражение).

5) **N[100!]**

9.33262×10^{157}

Арифметика произвольной точности – **N[expr, число цифр результата]**.

6) **N[Pi,18]**

3.14159265358979324

3. Матрицы.

Matrix(m) – представление в матричном виде;

Det(m) – вычисление определителя матрицы **m**;

Transpose(m) – транспонирование матрицы.

Можно использовать панель **MathInput**.

Matrix((1,2,3),(3,3,3),(5,7,9))

Input

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \\ 5 & 7 & 9 \end{pmatrix}$$

Det((1,0,0),(0,1,0),(0,0,1))

1

Transpose((1,2,3),(3,3,3),(5,7,9))

Result

$$\begin{pmatrix} 1 & 3 & 5 \\ 2 & 3 & 7 \\ 3 & 3 & 9 \end{pmatrix}$$

Задание 1:

Ввести элементы матрицы 3x3, вычислить определитель, транспонировать матрицу. Ввести две матрицы 2x2, найти произведение матриц.

4. Вычисление сумм и произведений.

$$\sum_{i=1}^{10} \sum_{j=2}^5 i \cdot j$$

770

$$\prod_{i=1}^5 (x+i)^2$$

$$(1+x)^2 (2+x)^2 (3+x)^2 (4+x)^2 (5+x)^2$$

Sum[i^2,{i,1,10}]

385

Product[k^2,{k,1,5}]

14400

$$\sum_{i=1}^{100} i$$

5050

Задание 2:

Sum[x^i y^j,{i,1,4},{j,1,i}]

Sum[1/(n*n),{n,1,10}]

Sum[(x^n)/n!,{n,1,10}]

Product[i,{i,1,10}]

4. Поиск корней уравнений.

Roots[x^2+2*x+15==0,x]

Самостоятельно:

Roots[x^2+2*x-15==0,x]

Задание 3:

Привести 2-3 примера вычисления корней уравнения.

5. Функции времени и даты.

AbsoluteTime – возвращает полное количество лет, прошедших с 1 января 1900 годы;

Now – возвращает текущую дату;

TimeUsed – возвращает полное количество секунд процессорного времени, используемое в текущем сеансе Mathematica.

Проверить самостоятельно.

Работа с простыми числами в WolframAlpfa

Next Prime [n] – дает наименьшее простое число, превосходящее n;

Next Prime [n, -1] – дает наибольшее простое число, меньшее n;

Random Prime n – возвращает n случайных простых чисел.

Примеры:

Next Prime [34, -1]

31

Next Prime [34]

37

Random Prime 10

```
Result
{347, 733, 733, 421, 727, 107, 631, 71, 41, 607}
(prime numbers chosen at random from the range 2 to 1000)
```

Задание 4:

- 1) Получить простые числа, близкие к 65, 346, 1235.
- 2) Получить 5 случайных простых чисел.

Prime Factor r – дает список простых множителей r (factor –множитель);

Smallest Prime Factor [r] – дает наименьший простой множитель числа n;

Prime PowerQ n – определяет, является ли n степенью рационального простого числа;

Примеры:

PrimeFactor 45

```
Result
32 × 5 (3 prime factors, 2 distinct)
```

Smallest Prime Factor 95

5

Prime Factor 78/42

```
Result
2 × 3 × 13
-----
2 × 3 × 7
```

Prime PowerQ 17

True

Prime PowerQ 45

False

Задание 5:

- 1) Проверить примеры для чисел 85, 564.
- 2) Привести по два примера на каждую функцию.

Chinese Remainder [list1, list2] – дает наименьшее неотрицательное целое r, такое, что Mod[r, list2]==list1;

`Mod [n, list]` – вычисляет остаток от деления n на каждое число из списка `list`.

Примеры:

Chinese Remainder `[{0, 1, 2}, {4, 9, 121}]`

244

Mod `[244, {4, 9, 121}]`

`{0,1,2}`

Задание б:

1) Проверить примеры для списков: `{2,4,9}` и `{5,16,41}`.

2) Подобрать с помощью функции `Mod` два набора списков для вычислений по китайской теореме.

`Provable PrimeQ n` (`PrimeQ n`) – выдает `true`, если число n простое и `false`, если n составное;

`PrimeQ Certificate n` – выдает свидетельство того, что n является простым или составным;

The certificate of primality used in this package for large n is based on the theory of elliptic curves. The basic idea was discovered by S. Goldwasser and J. Kilian.

Примеры:

PrimeQ 127

```
Result
127 is a prime number
```

Provable PrimeQ 128

```
Result
128 is not a prime number
Prime factorization
27 (7 prime factors, 1 distinct)
```

PrimeQ Certificate 1023

Result

1023 is not a prime number

Prime factorization

$3 \times 11 \times 31$ (3 distinct prime factors)

Задание 7:

- 1) Проверить примеры для чисел 913, 1093.
- 2) Привести пример на каждую функцию.

Практическое занятие №2

Разработка кейса по теме Системы компьютерной математики

1. На основе изученного теоретического материала подготовить кейс на тему **Система компьютерной алгебры Maple**.
2. Открыть шаблон кейса **кейс.pub** (рис.1).

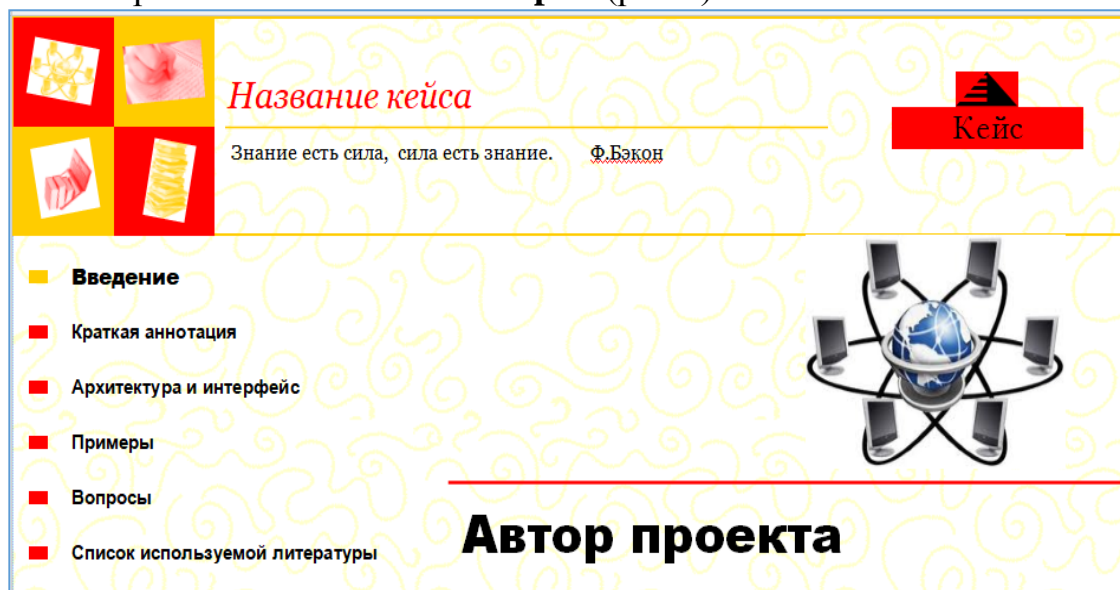


Рис. 1 – Главное окно

3. Найти информацию, соответствующую теме кейса, заполнить раздел Краткая аннотация (рис. 2):
 - история создания системы;
 - возможности.
4. Сформулировать вопросы для осуждения данной темы (рис. 3).

Ответы на вопросы должны содержаться в краткой аннотации проекта.

5. Раздел Примеры (рис. 4) должен содержать примеры, соответствующие теме кейса. Поместить принтскрины вычислений в системе (не менее двух). Пример будет доступен по нажатию на рисунок слева от формулировки.

6. Заполнить Список используемой литературы (по требованиям ГОСТ).

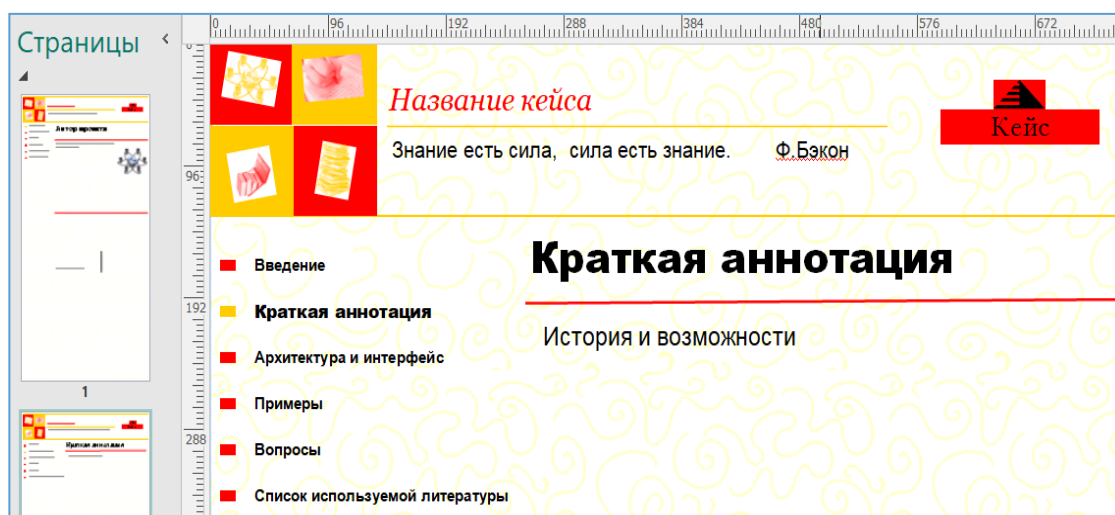


Рис.2 – Краткая аннотация проекта

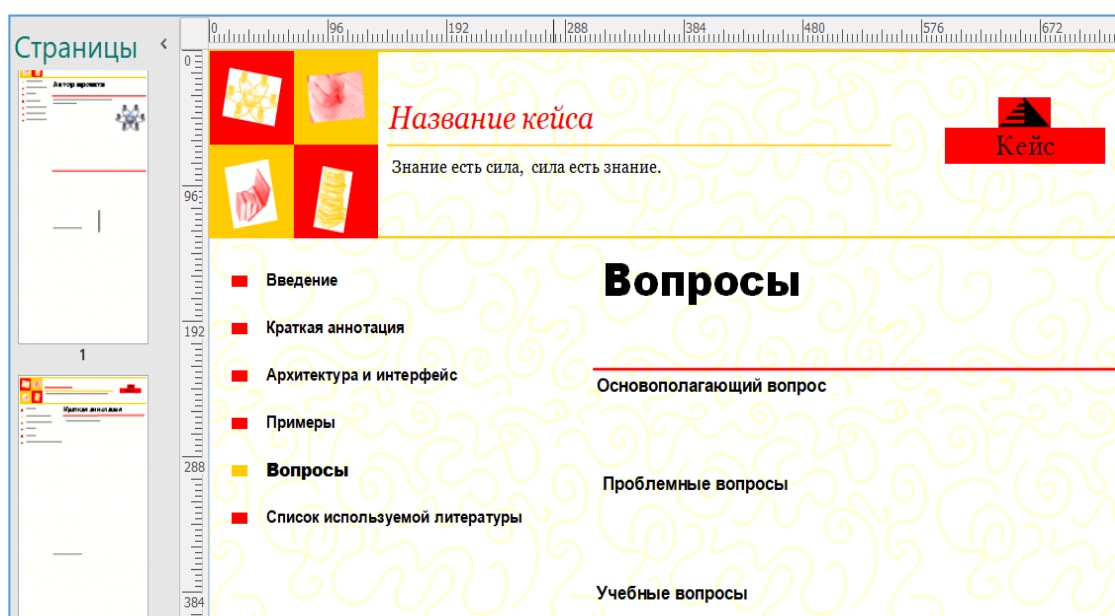


Рис. 3 – Вопросы для проверки

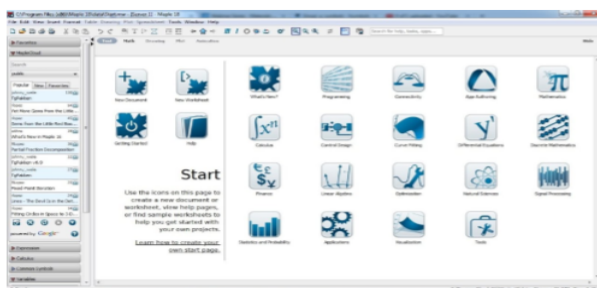
7. Готовый кейс сохранить. Выбрать тип файла – Веб-страница в одном файле.

СИСТЕМА КОМПЬЮТЕРНОЙ АЛГЕБРЫ

Кейс

MAPLE

- Введение
- Краткая аннотация
- Архитектура и интерфейс
- Примеры
- Вопросы
- Список используемой литературы



Примеры:

Графическое изображение функции двух переменных

График

$$z^2 + y^2$$

с

z

и

y

в диапазоне от -1 до 1:

```
plot3d (x ^ 2 + y ^ 2, x = -1..1, y = -1..1);
```

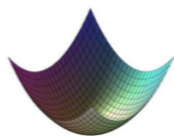


График функции одной переменной

График

$$x \sin(x)$$

с

x

в диапазоне от -10 до 10:

```
plot (x * sin (x), x = -10..10);
```

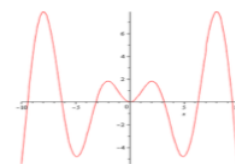


Рис. 4 – Примеры вычислений в системе Maple

Самостоятельно:

Разработать кейс по предложенной теме.

Задание для кейса:

1. Система компьютерной алгебры Maple.
2. Пакет прикладных программ MatLab.
3. PTC MathCAD.
4. Свободная система компьютерной алгебры Maxima.
5. Reduce – бесплатная система компьютерной алгебры общего назначения, имеющая расширенные возможности для применения в физике.
6. Derive – система компьютерной алгебры.
7. CAS Cadabra (тензорная алгебра).
8. Singular (полиномиальные вычисления).
9. Magma – система компьютерной математики.
10. MuPAD (программный пакет компьютерной алгебры).
11. CAS GAP (алгебра групп).
12. GINV (Grobner INVolutive).

13. Mathematica – система компьютерной алгебры.
14. Jasymsca Java Symbolic Calculator.
15. TRIP – система компьютерной алгебры, посвященная небесной механике.
16. Axiom (свободная система компьютерной алгебры общего назначения).
17. KANT / KASH (алгебра и теория чисел).
18. Macaulay2 – специализированная система для исследований в области алгебраической геометрии и коммутативной алгебры.
19. CAS Sage – система компьютерной алгебры.
20. CAS Fermat (полиномы, матрицы).



Рис. 5 – Пример кейса

1. Защита кейса.

Подготовить разработанный кейс к защите.

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 №3

Системы счисления

Пусть Q – натуральное число больше 1 и $M = \{0, 1, \dots, Q-1\}$. Говорят, что натуральное число a записано в позиционной системе с основанием Q , если

$$a = a_s Q^s + a_{s-1} Q^{s-1} + \dots + a_1 Q + a_0 \quad (1),$$

где s – целое неотрицательное, $a_0, \dots, a_s \in M$ и $a_s \neq 0$.

Если каждое число множества $M = \{0, 1, \dots, Q-1\}$ обозначено специальным символом, то эти символы называются цифрами Q -ичной позиционной системы.

Представление (1) записывается тогда в сокращенном виде

$$a = (a_s, a_{s-1} \dots a_1)_Q$$

и называется записью в Q -ичной позиционной системе.

Запись $a = (2315)_{10}$ означает, что $a = 2 \cdot 10^3 + 3 \cdot 10^2 + 1 \cdot 10^1 + 5$, запись $b = (101001)_2$, означает, что $b = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1$.

Например, основание десятичной системы счисления – десять (цифры 0, 1, 2, 3, 4, 5, 6, 7, 8, 9), шестеричной – 6 (цифры 0, 1, 2, 3, 4, 5), двоичной – два (цифры 0, 1), шестнадцатеричной – 16 (цифры 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 и буквы А, В, С, D, E, F).

Следующие примеры иллюстрируют операции сложения в шестнадцатеричной, двоичной системах счисления и вычитание в пятеричной:

$$\begin{array}{r} (4253)_6 \\ + (2542)_6 \\ \hline (11235)_6 \end{array} \quad \begin{array}{r} (10011)_2 \\ + (11001)_2 \\ \hline (101100)_2 \end{array} \quad \begin{array}{r} (42044)_5 \\ - (23141)_5 \\ \hline (13403)_5 \end{array}$$

Операция умножения целых многозначных чисел в двоичной системе счисления производится по тем же правилам, что и в десятичной системе («столбиком»). При ее выполнении удобно пользоваться таблицами умножения. Ниже приведена таблица умножения в пятеричной системе.

Таблица 2 – Умножение в пятеричной системе счисления

x	1	2	3	4
1	1	2	3	4
2	2	4	11	13
3	3	11	14	22
4	4	13	22	31

Пример, иллюстрирующий операцию умножения («столбиком») в пятеричной системе:

$$\begin{array}{r}
 132 \\
 \underline{24} \\
 1133 \\
 \underline{314} \cdot \\
 4323
 \end{array}$$

Таблица 3 – Задание 1

1	3501 + 4335 10304 – 432 43 × 13 1232 : 13	7	3401 + 3035 2114 – 1332 42 × 14 542 : 13	4	1351 + 5340 10304 – 5312 43 × 14 414 : 12
2	5201 + 3305 2214 – 542 32 × 15 432 : 13	8	2054 + 3531 3104 – 1412 43 × 15 2032 : 123	5	3251 + 1523 11304 – 532 34 × 15 501 : 15
3	2121 + 3025 51221 – 5043 43 × 13 521 : 14	9	4321 + 3435 2304 – 1414 31 × 14 2521 : 113	6	2345 + 5432 2104 – 305 32 × 13 444 : 14
10	2305 + 2431 4304 – 3032 35 × 14 2032 : 113	11	5301 + 2035 3304 – 1304 40 × 15 4232 : 32	12	4401 + 2235 4304 – 2422 35 × 15 2541 : 104

Задание 1. Составить таблицы сложения и умножения в шестеричной системе счисления. Выполнить указанные действия.

П.1. **Перевод Q→P.** Задача перевода произвольного числа x в Q-ичной системе.

Пример.

$$x = (371)_8 = (3 \cdot 8^2 + 7 \cdot 8 + 1)_{10} = (3 \cdot 64 + 7 \cdot 8 + 1)_{10} = (249)_{10}$$

$$x = (AF,4)_{16} = (10 \cdot 16 + 15 + 4 \cdot 16^{-1})_{10} = (160 + 15 + 0,25)_{10} = (175,25)_{10}$$

Задание 2.

- 1) Перевести числа из восьмеричной системы счисления в десятичную;
- 2) Перевести числа из шестнадцатеричной системы счисления в десятичную;
- 3) Перевести числа из двоичной системы счисления в десятичную.

Таблица 4 – Задание 2

1	$(126,34)_8$	$(3B4,15)_{16}$	$(1010,011)_2$	7	$(605,55)_8$	$(E09,93)_{16}$	$(10,0011)_2$
2	$(772,04)_8$	$(1A4,49)_{16}$	$(100,0101)_2$	8	$(518,34)_8$	$(3B4,15)_{16}$	$(10100,11)_2$
3	$(203,14)_8$	$(AC9,12)_{16}$	$(10001,01)_2$	9	$(712,6)_8$	$(5D9,12)_{16}$	$(110,00011)_2$
4	$(22,36)_8$	$(A49,62)_{16}$	$(10,01011)_2$	10	$(327,34)_8$	$(F34,54)_{16}$	$(1110,101)_2$
5	$(53,33)_8$	$(1D9,62)_{16}$	$(100,0011)_2$	11	$(605,14)_8$	$(E09,93)_{16}$	$(10,0011)_2$
6	$(667,34)_8$	$(F34,54)_{16}$	$(1000,0101)_2$	12	$(11,263)_8$	$(A21,65)_{16}$	$(10,0001)_2$

П.2. Перевод $P \rightarrow Q$. Поскольку для перевода любого числа достаточно уметь переводить отдельно его целую и дробную части, то можно рассмотреть оба эти случая отдельно:

1⁰. Перевод целых чисел.

Пример. $N = (47)_{10}$. Перевести это число в двоичную систему с использованием десятичной арифметики.

Применяя теорему 3 при $Q = 2$ получим:

$$\begin{array}{r}
 \underline{47} \mid \underline{2} \\
 \underline{46} \quad \underline{23} \mid \underline{2} \\
 1 \quad \underline{22} \quad \underline{11} \mid \underline{2} \\
 \quad 1 \quad \underline{10} \quad \underline{5} \mid \underline{2} \\
 \quad \quad 1 \quad \underline{4} \quad \underline{2} \mid \underline{2} \\
 \quad \quad \quad 1 \quad \underline{2} \quad \underline{1} \mid \underline{2} \\
 \quad \quad \quad \quad 0 \quad \underline{0} \quad 0 \\
 \quad \quad \quad \quad \quad 1
 \end{array}$$

Поскольку числа «ноль» и «единица» в обеих системах счисления обозначаются одинаковыми цифрами 0 и 1, то в процессе деления сразу получены двоичные изображения цифр:

$$N = (101111)_2.$$

Пример. $N = (3060)_{10}$. Перевести это число в шестнадцатеричную систему счисления с использованием десятичной арифметики.

$$\begin{array}{r} \underline{3060} \quad \underline{|16} \\ \underline{16} \quad \underline{191} \quad \underline{|16} \\ \underline{146} \quad \underline{16} \quad \underline{11} \quad \underline{|16} \\ \underline{144} \quad \underline{31} \quad \underline{0} \quad 0 \\ \underline{20} \quad \underline{16} \quad 11 \\ \underline{16} \quad 15 \\ 4 \end{array}$$

Таким образом, $q_0 = (4)_{10}$, $q_1 = (15)_{10}$, $q_2 = (11)_{10}$. Для окончательной записи числа N в шестнадцатеричной системе нужно каждый из коэффициентов записать одной шестнадцатеричной цифрой:

$$N = (BF4)_{16}.$$

Задание 3.

- 1) Перевести числа из десятичной системы счисления в восьмеричную;
- 2) Перевести числа из десятичной системы счисления в двоичную;
- 3) Перевести числа из десятичной системы счисления в шестнадцатеричную.

Таблица 5 – Задание 3

1	34; 5067	7	28; 6912
2	56; 6107	8	45; 3091
3	78; 5718	9	77; 3368
4	35; 9024	10	91; 5503
5	65; 3056	11	82; 3039
6	68; 3579	12	73; 5213

2⁰. Перевод дробных чисел.

Пример. $x = (0.2)_{10}$. Перевести это число в двоичную систему счисления с использованием средств двоичной арифметики (вертикальной чертой отделим получающиеся целые части произведений, которые и дают искомые коэффициенты разложения):

$$\begin{array}{r}
 0.2 \\
 \underline{\quad 2} \\
 0 \mid 4 \\
 \underline{\quad 2} \\
 0 \mid 8 \\
 \underline{\quad 2} \\
 1 \mid 6 \\
 \underline{\quad 2} \\
 1 \mid 2
 \end{array}$$

С точки зрения точности изображения числа на этом данный процесс можно прекратить. Однако, если считать число 0.2 точным и продолжить этот процесс перевода, то легко заметить, что мы будем дальше получать периодически повторяющиеся результаты, поэтому $x = (0.0011\ 0011 \dots)$.

Задание 4.

- 1) Перевести числа из десятичной системы счисления в восьмеричную;
- 2) Перевести числа из десятичной системы счисления в двоичную;
- 3) Перевести числа из десятичной системы счисления в шестнадцатеричную.

Таблица 6 – Задание 4

1	555.067	7	269.122
2	621.071	8	309.17
3	571.812	9	33.685
4	920.204	10	55.034
5	310.56	11	370.039
6	325.79	12	502.133

3⁰. Перевод произвольных чисел.

Для достижения единообразия действий и устранения деления как более сложной операции по сравнению с умножением целесообразно перевод произвольных чисел сводить к случаю перевода правильных дробей, что может быть достигнуто следующим образом.

Пусть $x > 1$ – произвольное число, заданное своим изображением в системе счисления с основанием P . Для перевода числа x в Q -ичную систему предварительно подберем число $M = Q^K$ (K -целое) так, чтобы число $\bar{x} = \frac{x}{M}$ удовлетворяло условию $\bar{x} < 1$. Полученную правильную дробь можно перевести в Q -ичную систему с использованием только операций умножения. Для получения Q -ичного изображения исходного числа x достаточно число \bar{x} умножить на $M = Q^K$, что равносильно перенесению занятой в Q -ичном изображении числа \bar{x} на K разрядов вправо.

Перевести число $x = (367)_{10}$ в двоичную систему счисления. Непосредственный перевод в двоичную систему потребовал бы 8 операций деления. Вместо этого можно предварительно перевести число x , например, в восьмеричную систему счисления: $x = (557)_8$. При этом будет выполнено только две операции деления. Для получения изображения числа x достаточно каждую полученную восьмеричную цифру записать ее двоичным изображением: $x = (101\ 101\ 111)_2$.

Пример. Представим число $(74.81)_{10}$ в шестнадцатеричной системе приведенным выше способом. Возьмем $M = 16^2 = 256$. Разделим 74.81 на 256 , получим дробное число $0.29222\dots$. Переведем число в шестнадцатеричную систему. Умножаем дробную часть на 16 . Берем в ответ только целые части выполненного умножения.

$$\begin{array}{r}
 0.292 \\
 \underline{\quad 16} \\
 4.672 \\
 \underline{\quad 16}
 \end{array}$$

10.752

16

12.032

.....

Получили число $0.4(10)(12) = 0.4AC$. Умножим на $M = 16^2$, т.е. перенесем запятую на два знака вправо. Получили $N = (4A.C)_{16}$.

Проверим делением.

74|16 0.81

64|4 16

10 12.96

.....

Получили число $4(10).(12)$. Такое же получилось и первым способом. $N=(4A.C)_{16}$.

Задание 5.

1) Перевести числа из десятичной системы счисления в восьмеричную, преобразовав их предварительно в дробь (см. таб. 7):

Таблица 7 – Задание 5 1)

1	555.067	7	269.122
2	621.071	8	309.17
3	571.812	9	33.685
4	920.204	10	55.034
5	310.56	11	370.039
6	325.79	12	502.133

2) Перевести числа из десятичной системы в восьмеричную и в двоичную, выполнить указанные действия, перевести результат из двоичной системы в восьмеричную и в десятичную, сравнить результат (см. таб. 8).

Таблица 8 – Задание 5 2)

1	869 – 122	7	555 – 267
2	909 – 107	8	621 – 371
3	433 – 285	9	571 – 312
4	755 – 154	10	920 – 204
5	470 – 139	11	810 – 156
6	502 – 133	12	725 – 279

Для самостоятельного решения:

1. Записать год своего рождения в восьмеричной системе счисления.
2. Записать почтовый индекс в двоичной системе счисления (предварительно перевести в восьмеричную систему счисления).

Индивидуальное задание №1

Системы счисления

1. Выполните следующие действия в пятеричной системе счисления:

- | | |
|---|---|
| 1. а) $203.01 + 3341.42$;
б) $2340 - 1211$;
в) $413.31 \cdot 23.14$;
г) $421 / 23$ | 7. а) $223.42 + 3140.01$;
б) $4314 - 3234$;
в) $120.33 \cdot 14.23$;
г) $320 / 44$ |
| 2. а) $4213 + 33213$;
б) $223.21 - 241.211$;
в) $233.21 \cdot 112.2$;
г) $220 / 1$ | 8. а) $3123.21 + 343.4$;
б) $2233 - 2134$;
в) $302.34 \cdot 14.22$;
г) $243 / 14$ |
| 3. а) $1123 + 1021$;
б) $2123.42 - 1402.11$;
в) $210.23 \cdot 22.13$;
г) $442 / 12$; | 9. а) $22413 + 230$;
б) $423.41 - 404.31$;
в) $141.23 \cdot 10.23$;
г) $423 / 34$ |
| 4. а) $110.32 + 243.02$;
б) $1332 - 1034$;
в) $331.4 \cdot 102.12$;
г) $202 / 14$ | 10. а) $21234 + 2441$;
б) $2231.2 - 423.42$;
в) $224.31 \cdot 44.12$;
г) $131 / 14$ |
| 5. а) $2044 + 20312$;
б) $1231.2 - 123.14$;
в) $123.12 \cdot 22.11$;
г) $343 / 24$ | 11. а) $23410 + 1424$;
б) $234.21 - 124.34$;
в) $341.12 \cdot 42.13$;
г) $231 / 12$ |
| 6. а) $2031.2 + 1424.42$;
б) $1412 - 1323$;
в) $203.41 \cdot 21.42$;
г) $341 / 22$ | 12. а) $233.41 + 2012.33$;
б) $4123 - 2441$;
в) $221.21 \cdot 32.14$;
г) $231 / 41$ |

2. Перевести заданные числа из десятичной системы счисления в восьмеричную и шестнадцатеричную системы счисления (первое число – в восьмеричную, второе – в шестнадцатеричную), затем полученные числа перевести в двоичную систему счисления, сложить и выполнить перевод

результата сначала в восьмеричную систему счисления, а затем в десятичную систему счисления.

Таблица 9 – Задание на перевод чисел

1.	45.78 и 72.59	7.	37.67 и 56.65
2.	28.65 и 42.92	8.	12.47 и 60.76
3.	44.18 и 84.23	9.	57.68 и 17.96
4.	32.92 и 90.27	10.	39.85 и 87.52
5.	76.39 и 47.28	11.	98.03 и 52.85
6.	38.29 и 58.52	12.	23.06 и 81.76

Указание: при переводе из десятичной системы счисления в восьмеричную и шестнадцатеричную числа предварительно преобразуйте в дробь (способ перевода нормализованных чисел).

3. **Подсчитать средний возраст членов своей семьи.** Возраст каждого перевести из десятичной системы в восьмеричную, из восьмеричной в двоичную, сложить, разделить на общее количество членов семьи (в двоичной системе счисления), перевести в восьмеричную систему, затем в десятичную и сравнить результат.

Практическое занятие №4

Расширенный алгоритм Евклида

Расширенный алгоритм Евклида базируется на следующем рекуррентном соотношении:

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

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

Таблица 10 – Вычисление НОД(318, 264)

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

Решение. Заполнить таблицу 10, используя формулы, приведенные выше.

$$\begin{array}{lll}
 u_2 = u_0 - q_1 u_1 & u_3 = u_1 - q_2 u_2 & u_4 = u_2 - q_3 u_3 \\
 v_2 = v_0 - q_1 v_1 & v_3 = v_1 - q_2 v_2 & v_4 = v_2 - q_3 v_3 \\
 r_2 = r_0 - q_1 r_0 & r_3 = r_1 - q_2 r_2 & r_4 = r_2 - q_3 r_3 \\
 u_2 = 1 - 1 \cdot 0 = 1 & u_3 = 0 - 4 \cdot 1 = -4 & u_4 = 1 - 1 \cdot (-4) = 5 \\
 v_2 = 0 - 1 \cdot 1 = -1 & v_3 = 1 - 4 \cdot (-1) = 5 & v_4 = -1 - 1 \cdot 5 = -6 \\
 r_2 = 318 - 1 \cdot 264 = -54 & r_3 = 264 - 4 \cdot 54 = 48 & r_4 = 54 - 1 \cdot 48 = 6
 \end{array}$$

Задание. Найти наибольший общий делитель и коэффициенты Безу следующих чисел: 142 и 103. Найти обратный элемент, если он существует.

Самостоятельно:

Найти наибольший общий делитель и коэффициенты Безу (см. таб. 11).

Таблица 11 – 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

Практическое занятие №5

Вычисление наибольшего общего делителя (НОД)

1. Вычислить НОД.

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

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

2. Вычисление НОД с помощью алгоритма Евклида.

$$\begin{array}{ll}
 a = bq_0 + r_1, & 0 \leq r_1 < |b|, \\
 b = r_1q_1 + r_2, & 0 \leq r_2 < r_1,
 \end{array} \tag{15}$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1},$$

$$r_{n-1} = r_n q_n + r_{n+1}.$$

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, $\text{НОД}(24, 18) = 6$.

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

3. Алгоритмы вычислений с дробями.

а) Требуется вычислить произведение

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

Очевидный способ: вычислить $p = a \cdot c$, $q = d \cdot b$ и затем сократить на НОД этих чисел. Однако, используя равенство $\text{НОД}(p, q) = \text{НОД}(a, d) \cdot \text{НОД}(b, c)$, 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:

$$\begin{aligned} &\text{НОД}(a, d); \text{НОД}(b, c); a' = a / \text{НОД}(a, d); b' = b / \text{НОД}(b, c); \\ &c' = c / \text{НОД}(b, c); d' = d / \text{НОД}(a, d); p = a' \cdot c', q = d' \cdot b'. \end{aligned}$$

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;

б) Требуется найти сумму

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

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

$$\text{НОД}(b, d); q' = b \cdot d / \text{НОД}(b, d); b' = b / \text{НОД}(b, d); d' = d / \text{НОД}(b, d);$$

$$p' = a \cdot d' + b' \cdot c; \text{НОД}(p', q'); p = p' / \text{НОД}(p', q'); q = q' / \text{НОД}(p', q').$$

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:

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. $\frac{55}{105} \cdot \frac{34}{70}, \frac{19}{48} + \frac{38}{72}$

Индивидуальное задание № 2

Расширенный алгоритм Евклида

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

Таблица 12 – Задание для вычисления НОД

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. Найти обратный элемент, если он существует.

Таблица 13 – Задание для вычисления обратного элемента

1.	к 528 по mod 247	7.	к 539 по 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 539 по 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

Индивидуальное задание № 3

Вычисление НОД целых чисел

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

Таблица 14 – Задание для вычисления НОД разложением на множители

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 (см.

Пример 2).

Таблица 15 – Задание для вычисления НОД с помощью алгоритма 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

3. Вычисления с дробями.

- | | | | |
|----|---|-----|---|
| 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. | $\frac{48}{168} + \frac{96}{64}, \frac{102}{224} \cdot \frac{216}{80}$ |

Практическое занятие №6-7

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 $n_1, n_2, n_3, \dots, n_r$.

2. Представим модулярное разложение выбранных чисел a и b по модулям $n_1, n_2, n_3, \dots, n_r$: $a_1, a_2, \dots, a_r; b_1, b_2, \dots, b_r$.

3. Восстановим число x . Для этого вычислим z_1, z_2, \dots, z_r .

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

5. Найдем модулярное представление числа $x' = (x - x_0) / 10$: $x' = ((x_1 - x_0) \cdot y_1 \bmod n_1, (x_2 - x_0) \cdot y_2 \bmod n_2, \dots, (x_r - x_0) \cdot y_r \bmod n_r)$. 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 .

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

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

$c_2 N_2 \equiv 1 \pmod{n_2} \Rightarrow c_2 \cdot n_1 \equiv 1 \pmod{n_2} = 3 \cdot c_2 \equiv 1 \pmod{7}$, т.е. c_2 - обратное к 3 по mod 7 (см. Таблицу 16)

Таблица 16 – 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

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

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

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

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

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

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

$$c_3 N_3 \equiv 1 \pmod{n_3} = c_3 \cdot n_1 \cdot n_2 \equiv 1 \pmod{n_3} \Rightarrow c_3 \cdot 21 \equiv 1 \pmod{11}$$

c_3 – обратное к 21 по модулю 11 (см. Таблицу 17)

Таблица 17 – 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

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

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

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

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

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

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

Таблица 18 – 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

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

c_4 – обратное к 231 по модулю 17 (см. Таблицу 18)

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

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

5. Определим последнюю цифру числа.

$$x^{(1)} = (z_1 \cdot N_1 + z_2 \cdot N_2 + z_3 \cdot N_3 + z_4 \cdot N_4) \bmod 10 = (z_1 + z_2 \cdot n_1 + z_3 \cdot n_1 \cdot n_2 + z_4 \cdot n_1 \cdot n_2 \cdot n_3) \bmod 10$$

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

$$x_0 = 0$$

6. Перейдем к определению следующей цифры.

Обратное к 10 по модулю n_1 равно 1 ($10 \cdot y_1 \equiv 1 \pmod{3}$), обратное к 10 по модулю n_2 равно 5 ($10 \cdot y_2 \equiv 1 \pmod{7}$), обратное к 10 по модулю n_3 равно 10

$(10 \cdot y_3 \equiv 1 \pmod{11})$, обратное к 10 по модулю 17 равно 12 ($10 \cdot y_4 \equiv 1 \pmod{17}$). Т.е. $y_1=1, y_2=5, y_3=10, y_4=12$.

Определяем модулярные компоненты числа.

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

$x' = ((1-0) \cdot 1 \pmod{3}, (0-0) \cdot 5 \pmod{7}, (2-0) \cdot 10 \pmod{11}, (5-0) \cdot 12 \pmod{17}) = (1 \pmod{3}, 0 \pmod{7}, 20 \pmod{11}, 60 \pmod{17}) = (1, 0, 9, 9)$.

7. Определим предпоследнюю цифру числа.

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

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

$z_1 = x_1' \pmod{n_1} = 1 \pmod{3} = 1$

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

$c_2 \cdot N_2 \equiv 1 \pmod{n_2} \Rightarrow c_2 \cdot n_1 \equiv 1 \pmod{7} = c_2 \cdot 3 \equiv 1 \pmod{7}$

См. таблицу 1.

$c_2=5$

$z_2 = -5 \pmod{7} = 2$

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

$z_3 = c_3 \cdot (9 - 3 \cdot 2 - 1) \pmod{11} = c_3 \cdot 2 \pmod{11} = 20 \pmod{11} = 9$

$c_3 N_3 \equiv 1 \pmod{n_3} \Rightarrow c_3 \cdot n_1 \cdot n_2 \equiv 1 \pmod{n_3} \Rightarrow c_3 \cdot 21 \equiv 1 \pmod{11}$

См. таблицу 2.

$c_3 = -1 \Rightarrow c_3 = 10$

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

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

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

$c_4 \cdot (231) \equiv 1 \pmod{17}$

См. таблицу 3.

$c_4 = 12$

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

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

Найдем модулярное представление числа по формуле

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

$$x_0 = 6$$

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

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

$$x'' = (1 - 6) \cdot 1 \bmod 3, (0 - 6) \cdot 5 \bmod 7, (9 - 6) \cdot 10 \bmod 11, (9 - 6) \cdot 12 \bmod 17 = \\ = (-5 \bmod 3, -30 \bmod 7, 30 \bmod 11, 36 \bmod 17) = (1, 5, 5, 2)$$

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

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

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

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

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

$$c_2 \cdot N_2 \equiv 1 \pmod{n_2} \Rightarrow c_2 \cdot n_1 \equiv 1 \pmod{7} = c_2 \cdot 3 \equiv 1 \pmod{7}$$

См. таблицу 1.

$$c_2 = 5$$

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

$$z_3 = c_3 (8 - 3 \cdot 6 - 1) \bmod 11 = c_3 \cdot (-11) \bmod 11 = -110 \bmod 11 = 0$$

$$c_3 \cdot N_3 \equiv 1 \pmod{n_3} \Rightarrow c_3 \cdot n_1 \cdot n_2 \equiv 1 \pmod{n_3} \Rightarrow c_3 \cdot 21 \equiv 1 \pmod{11}$$

См. таблицу 2.

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

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

$$z_4 = c_4 (2 - 21 \cdot 0 - 3 \cdot 6 - 1) \bmod 17 = c_4 (-17) \bmod 17 = 0$$

$$x^{(3)} = (z_1 \cdot N_1 + z_2 \cdot N_2 + z_3 \cdot N_3 + z_4 \cdot N_4) \bmod 10 = (z_1 + z_2 \cdot n_1 + z_3 \cdot n_1 \cdot n_2 + z_4 \cdot n_1 \cdot n_2 \cdot n_3) \bmod 10$$

$$x^{(3)} = (1 + 6 \cdot 3 + 0 + 0) \bmod 10 = (1 + 18) \bmod 10 = 19 \bmod 10 = 9$$

Найдем модулярное представление числа по формуле

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

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

$$x_0 = 9$$

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

$$x'' = ((1 - 9) \cdot \bmod 3, (5 - 9) \cdot 5 \bmod 7, (8 - 9) \cdot 10 \bmod 11, (2 - 9) \cdot 12 \bmod 17) = (-8 \bmod 3, -20 \bmod 7, -10 \bmod 11, -84 \bmod 17) = (1, 1, 1, 1)$$

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.

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

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

$$x_0 = 1$$

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

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

Таблица 19 – Задание для самостоятельной работы

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

Модулярное представление равно нулю, следовательно, вычисление закончено.

Получили число 1960.

Задание. Найти произведение двух целых чисел (см. таблицу 19).
Взаимно-простые числа n_1, n_2, n_3, n_4 выбрать самостоятельно.

Индивидуальное задание № 4

Модулярная арифметика

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

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

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

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

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

Практическое занятие №8

Разложение на множители

1. Деление и разложение на множители.

Если число $n > 1$, то его можно делить на последовательные простые числа $p = 2, 3, 5, \dots$, до тех пор, пока не будет найдено наименьшее p для которого $n \bmod p = 0$. Тогда p будет наименьшим простым множителем числа n . Ту же процедуру можно применить к n/p , взяв его за новое значение n , попробовать разделить это новое значение числа n на p и его большие простые числа. Из теоремы 10 следует, что это действие необходимо выполнять пока $p \leq \sqrt{n}$. Отметим, что мы должны обладать вспомогательной последовательностью пробных делителей $2 = d_0 < d_1 < d_2 < d_3 < \dots$, которая включает в себя все простые числа $\leq \sqrt{n}$. Ниже приведена процедура, реализующая данный метод.

Задание 1. Выполнить по вариантам.

Таблица 20 – Задание для самостоятельной работы

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 $n = u \cdot v$, где $u \leq v$. Для практических целей можно допустить, что n нечетно; это означает, что u и v тоже нечетны. Поэтому можно положить:

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

$$n = x^2 - y^2, \quad 0 \leq y < x \leq n.$$

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. $x' := 2\lceil\sqrt{n}\rceil + 1$; $y' := 1$; $r := \lceil\sqrt{n}\rceil^2 - n$.
2. Если $r \leq 0$, 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.

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

Задание 2. Разложить числа методом Ферма.

Таблица 21 – Задание для самостоятельной работы

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.		12.	

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

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

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

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

легко доказываемого индукцией по i .

Пример.

Вычислить $a^d \bmod m$, для $a = 3$, $d = 4$, $m = 6$.

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

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

$$a_1 = a_0^2 \cdot a^{d_1} \pmod{m} = 3^2 \cdot 3^0 \pmod{6} = 9 \pmod{6} = 3$$

$$a_2 = a_1^2 \cdot a^{d_2} \pmod{m} = 3^2 \cdot 3^0 \pmod{6} = 9 \pmod{6} = 3$$

Проверим, $3^4 \pmod{6} = 3$.

Задание 3. Вычислить $a^d \pmod{m}$.

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

b) Рассмотрим метод, основанный на замене проверки $a^{n-1} \equiv 1 \pmod{n}$ 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 $\text{НОД}(a, n) = 1$ хотя бы одна из скобок в произведении

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

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

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 $\frac{3}{4}(n-1)$.

с) 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;

4) 83.

Индивидуальное задание № 5

Разложение на множители

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

Таблица 22 – Задание для разложения чисел

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

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

Таблица 23 – Задание для вычисления $a^d \bmod m$

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.	$a=5; d=11; m=24$

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 b 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 №9

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 $y = x^5 = x^4 x = (x^2)^2 x$, а затем находим $y^{11} = y^{10} y = (y^5)^2 y = (y^4 y)^2 y = ((y^2)^2 y)^2 y$. 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».

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

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

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

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

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

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

Это удобно сделать, положив

$$\begin{aligned} c_0 &= a_n, & b_0 &= 0 \\ c_j &= c_{j-1}x + a_{n-j}, & b_j &= b_{j-1}x + c_{j-1}, & 1 \leq j \leq n. \end{aligned}$$

Здесь $c_n = f(x)$ и $b_n = f'(x)$.

Пример: Вычислить полином и его производную:

$$f(x) = 2x^5 - x^4 + 2x^3 - x^2 + 1 \text{ при } x = 1.$$

Вычисляем полином, то есть находим его значение при $x = 1$.

$$c_0 = 2, c_j = c_{j-1}x + a_{n-j}, n = 5, a_5 = 2, a_4 = -1, a_3 = 2, a_2 = -1, a_1 = 0, a_0 = 1.$$

$$c_1 = c_0x + a_4 = 2 \cdot 1 + (-1) = 1$$

$$c_2 = c_1x + a_3 = 1 \cdot 1 + 2 = 3$$

$$c_3 = c_2x + a_2 = 3 \cdot 1 + (-1) = 2$$

$$c_4 = c_3x + a_1 = 2 \cdot 1 + 0 = 2$$

$$c_5 = c_4x + a_0 = 2 \cdot 1 + 1 = 3$$

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 №6

Вычисление полиномов

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

Таблица 24 – Задание для вычисления бинарным методом и методом множителей

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 25 – Задание для вычисления с помощью схемы Горнера

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

3. Обобщение схемы Горнера.

Вычислить полиномы и их производную при $x=3$.

Таблица 26 – Задание для вычисления с помощью обобщенной схемы Горнера

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

Практическое занятие №10

Нахождение НОД полиномов

Для вычисления НОД полиномов воспользуемся алгоритмом:

$M :=$ граница Ландау Миньотта (A, B)

цикл до бесконечности

$r :=$ найти большое простое ($2M$);

если степень остатка (r, A) или степень остатка (r, B)

то $C :=$ модулярный НОД (A, B, r);

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:

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

Для наших полиномов:

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

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

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

Выполним деление полиномов по модулю 7.

$$\begin{array}{r} \underline{x^8 + 2x^6 - x^5 + 4x^3 - 6x^2} \quad | \underline{x^6 + 2x^4 + 4x - 4} \\ -6x^8 - 12x^6 - 24x^3 + 24x^2 \quad -6x^2 \\ \hline 7x^8 + 14x^6 - x^5 + 28x^3 - 30x^2 \\ (7x^8 + 14x^6 - x^5 + 28x^3 - 30x^2) \bmod 7 \equiv 6x^5 + 5x^2 \end{array}$$

$$\begin{array}{r} \underline{x^6 + 2x^4 + 4x - 4} \quad | \underline{6x^5 + 5x^2} \\ \underline{36x^6 + 30x^3} \quad 6x \\ -35x^6 + 2x^4 - 30x^3 + 4x - 4 \\ \hline (-35x^6 + 2x^4 - 30x^3 + 4x - 4) \bmod 7 \equiv 2x^4 + 5x^3 + 4 - 4 \end{array}$$

$$\begin{array}{r} \underline{6x^5 + 5x^2} \quad | \underline{2x^4 + 5x^3 + 4 - 4} \\ \underline{-8x^5 - 20x^4 - 16x^2 + 16x} \quad -4x \\ \hline 14x^5 + 20x^4 + 21x^2 - 16x \\ (14x^5 + 20x^4 + 21x^2 - 16x) \bmod 7 \equiv 6x^4 + 5x. \text{ Продолжим деление:} \end{array}$$

$$\begin{array}{r} \underline{6x^4 + 5x} \quad | \underline{2x^4 + 5x^3 + 4 - 4} \\ \underline{-8x^4 - 20x^3 - 16x + 16} \quad -4 \\ \hline 14x^4 + 20x^3 + 21x - 16 \\ (14x^4 + 20x^3 + 21x - 16) \bmod 7 \equiv 6x^3 + 5 \end{array}$$

$$\begin{array}{r} \underline{2x^4+5x^3+4x-4} \quad | \quad \underline{6x^3+5} \\ -12x^4 \quad -10x \qquad \qquad \qquad -2x \\ \hline 14x^4+5x^3+14x-4 \end{array}$$

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

$$\begin{array}{r} \underline{5x^3-4} \quad | \quad \underline{6x^3+5} \\ -30x^3-25 \qquad \qquad \qquad -2x-5 \\ \hline 35x^3+21 \end{array}$$

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

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 $6 \cdot a \equiv 1 \pmod{7}$. 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,

$$\text{НОД}(A(x), B(x)) = x^3+2$$

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

$$\begin{array}{r} \underline{x^8+2x^6-x^5+4x^3-6x^2} \quad | \quad \underline{x^3+2} \\ x^8+2x^5 \qquad \qquad \qquad x^5+2x^3-3x^2 \\ \hline -2x^6 \quad -3x^5+4x^3 \\ \underline{2x^6 \qquad \qquad +4x^3} \\ -3x^5 \quad -6x^2 \\ \underline{-3x^5 \quad -6x^2} \\ 0 \end{array}$$

$$\begin{array}{r} \underline{x^6+2x^4+4x-4} \quad | \quad \underline{x^3+2} \\ x^6+2x^3 \qquad \qquad \qquad x^3+2x-2 \\ \hline -2x^4-2x^3+4x \\ \underline{2x^4 \quad +4x} \\ -2x^3-4 \\ \underline{-2x^3-4} \\ 0 \end{array}$$

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 №7

Нахождение НОД полиномов

Найти наибольший общий делитель полиномов.

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

- $A(x) := 3x^8 + 2x^7 + 2x^6 + 6x^5 - x^4 + 4x^3,$
 $B(x) := 2x^6 - x^5 + 5x^4 - x^3 + x^2 - 2$
- $A(x) := x^8 - x^7 - 3x^6 - x^5,$
 $B(x) := 2x^7 + 2x^6 + 2x^4 + 2x^3 - x - 1$
- $A(x) := x^8 - 2x^7 - 6x^5 + 3x^6 - x^2 - 3,$
 $B(x) := 2x^6 + 3x^4 + x^3 - 10x^2 + 3x - 3$
- $B(x) := 3x^8 - 6x^7 + 2x^6 - 4x^5 - 4x^4 + 8x^3,$
 $A(x) := 2x^6 - 2x^5 - 6x^4 + 4x^3 - x + 2$
- $B(x) := 2x^8 + 6x^7 + x^6 + x^5 - 6x^4 - 2x - 6,$
 $A(x) := x^7 + x^6 - 6x^5 + 3x^4 + 9x^3$
- $T(x) := x^8 - 2x^7 - 2x^6 + 4x^5 + 2x^4 - 4x^3 - x - 2,$
 $F(x) := 2x^5 - 5x^4 + 2x^3 - 2x^2 - 4x$
- $K(x) := 2x^8 - x^7 + 6x^6 - x^2 + 3x,$
 $L(x) := x^6 - x^5 - 7x^4 + 3x^3 + x - 3$
- $L(x) := 2x^8 - 5x^7 + x^6 + 2x^5 - x^2 + x,$
 $K(x) := x^7 - 3x^6 + 2x^5 - x^3 + x^2 - 2x + 2$
- $A(x) := x^7 + x^6 - 6x^5 + 3x^3 + 9x^2 - 2x - 6,$
 $F(x) := 2x^5 + 5x^4 + 9x^2 - 2x - 6$
- $K(x) := x^8 - x^4 - x^3 - x^2,$
 $A(x) := 2x^7 - 2x^6 - 2x^5 + 2x^4 - 3x^2 + 3$
- $T(x) := x^8 - 2x^7 + 3x^6 - 6x^5 + 3x^4 - 2x^3 + 9x^2 - 6x,$
 $A(x) := 2x^6 - x^5 + 9x^4 - 3x^3 + 8x^2 - 3$
- $B(x) := x^7 - 4x^5 + 3x^3 + 6x^2 - 2x - 4,$
 $A(x) := 2x^5 + 3x^4 + x^3 + 6x^2 - 2x - 4$

2. Выполнить деление по модулю 7.

- $T(x) := x^7 + x^6 - 6x^5 + 3x^3 + 9x^2 - 2x - 6,$
 $F(x) := 2x^5 + 5x^4 + 9x^2 - 2x - 6$
- $B(x) := 2x^8 - 5x^7 + x^6 + 2x^5 - x^2 + x,$
 $K(x) := x^7 - 3x^6 + 2x^5 - x^3 + x^2 - 2x + 2$
- $A(x) := 2x^8 - x^7 + 6x^6 - x^2 + 3x,$
 $B(x) := x^6 - x^5 - 7x^4 + 3x^3 + x - 3$
- $L(x) := x^8 - 2x^7 + 3x^6 - 6x^5 + 3x^4 - 2x^3 + 9x^2 - 6x,$
 $A(x) := 2x^6 - x^5 + 9x^4 - 3x^3 + 8x^2 - 3$
- $A(x) := x^8 - 2x^7 - 6x^5 + 3x^6 - x^2 - 3,$
 $B(x) := 2x^6 + 3x^4 + x^3 - 10x^2 + 3x - 3$
- $K(x) := x^8 - x^7 - 3x^6 - x^5,$
 $B(x) := 2x^7 + 2x^6 + 2x^4 + 2x^3 - x - 1$
- $L(x) := 3x^8 + 2x^7 + 2x^6 + 6x^5 - x^4 + 4x^3,$
 $B(x) := 2x^6 - x^5 + 5x^4 - x^3 + x^2 - 2$

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

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 результат 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 ($\text{cont}(p)$) полинома p .
18. Какой полином называется примитивным?
19. Сформулировать лемму Гаусса.
20. Как вычислить НОД двух полиномов от нескольких переменных?

Модуль 4. Система компьютерной математики Wolfram Alpha.

Применение алгоритмов компьютерной математики

Практическое занятие №11

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.

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

Result

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

$$\text{Simplify } (x^5+2x^4+2x^3+2x^2-3x-4)$$

Results

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

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

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

$$\text{Expand } (-1+x)(1+x)(4+x(3+x(2+x)))$$

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

Result

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

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

Result

$x(x + 1)(x + 2) \pmod{3}$

Factor 1234554367

Result

$83 \times 601 \times 24749$ (3 distinct prime factors)

Задание 2.

Даны два полинома:

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

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

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

Factor F[x]

Factor T[x], Modulus->5

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

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

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

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

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

1

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

$$L[x] = 36x + 18$$

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

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

1

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

$$x + 1$$

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

$$x + 6$$

Задание 3.

Даны два полинома:

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

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

- 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:

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

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

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

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

Индивидуальное задание №8.1

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).

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

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 примера 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]

$$x^2 \pmod{3x}$$

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

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

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

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

2

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

2 >

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

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

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

GroebnerBasis[[$x^3yz-xz^2, xy^2z-xyz, x^2y^2-z$], { x, y, z }]

Result

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

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

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

$(x-y)^2$

Задание.

- 1) проверить 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($x^3 - x^2 + y - xy$, $2x^2 - xy - 2x + y$)

Result

$$x - 1$$

Input

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

Result

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

 Enlarge

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 $x^3 - x^2 - xy + y$ и $2x^2 - xy - 2x + y$ по x равен $x - 1$.

Задание.

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

Индивидуальное задание №8.2

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 №13

Дифференцирование и интегрирование в WolframAlpha

1. Вычисление производных

$D[f, x]$ – возвращает частную производную функции f по переменной x . Возможно вычисление частных производных n -го порядка по x , смешанных и обобщенных производных.

$Derivative[n1, n2, \dots][f]$ – основная (общая) форма представления функции, полученной в результате $n1$ -кратного дифференцирования функции f по первому аргументу, $n2$ -кратного дифференцирования функции f по второму аргументу и т.д.

$$D[a \text{ Cos}[x], x]$$

$$-a \text{ Sin}[x]$$

$$D[b x^3 + b x, x]$$

$$b + 3 b x^2$$

$$D[\text{Log}[x] x^2, x]$$

$$x + 2 x \text{ Log}[x]$$

$$D[x^{2/b}, x]$$

$$\frac{3x^2}{b}$$

Derivative[2] [x y]

(x y)"

Самостоятельно. Вычислить производную функций по вариантам.

Использовать функции Sin[x], Log[x], Log[2, x].

Таблица 27 – Задание для вычисления производной

1.	$y=2^x$	$y=\frac{\sqrt{x}}{2}$	$y=e^{\sqrt{3+x}}$	$5\sqrt{x} * e^{-x}$	Вычислите $f'(3\pi/4)$, если $f(x)=5\sin(x)+3x^2-(9\pi/4)x-1$
2.	$f(x)=\text{ctg}(x)$	$y=\sqrt{2x}$	$y=(3-7x)^9$	$y=2\sqrt{x+\cos(x)}/5$	Вычислите $f'(3\pi/4)$, если $f(x)=\sin(x)+x^2-(7\pi/4)x+1$
3.	$f(x)=\log(3x)$	$y=x+\frac{1}{x}$	$\ln(\sin(x))$,	$\frac{\sqrt{3x}}{3^x+1}$	Вычислите $f'(\pi/3)$, если $f(x)=-3\sin(x)-7x^2+14\pi/(3x+8)$
4.	$f(x)=\ln(x)$	$y=-\sqrt{3x}$	$\sin(\ln(x))$	$\frac{2^x - \log_2(x)}{\ln(2) * x}$	Вычислите $f'(\pi/4)$, если $f(x)=-2\sin(x)-5x^2+11\pi/(2x-7)$
5.	$f(x)=\sqrt{x}$	$y=\frac{x+3}{x}$	$0.51+\sin(x)$	$\frac{1-\sin(2x)}{\sin(x)-\cos(x)}$	Вычислите $f'(\pi/3)$, если $f(x)=\sin(2x)+3x^2-(5\pi/4)x-2$
6.	$y=3x^2$	$y=2-\frac{x}{2}-x^2$	$\sqrt[3]{\sin(x)}$	$\frac{5^{2x}}{\sin(3x)+7}$	Вычислите $f'(3\pi/4)$, если $f(x)=3\cos(5x)+4x^3-(3\pi/4)x+1$
7.	$f(x)=\cos(x)$	$y=4-x^2$	$\sqrt[3]{\log_2(x)}$	$y=(\text{tg}(x)-2)/5x$	Вычислите $f'(3\pi/4)$, если $f(x)=8\sqrt{x+7\sin(x)}-3x^7+8$
8.	$y=4x^4$	$y=x^5+2x^3-\frac{1}{2x}$	$y=\frac{1}{\sqrt{x+\frac{1}{x}}}$	$f(x)=3x^7-\frac{5}{x^2}$	Вычислите $f'(\pi/4)$, если $f(x)=8\sqrt{x+7\sin(x)}-3x^7$
9.	$y=e^x$	$y=2x^2-3x+5$	$y=\sqrt[3]{2x^2-1}$	$(3-5x+x^2)/100$	Вычислите $f'(\pi/4)$, если $f(x)=8\sqrt{x+7\sin(x)}-3x^7$
10.	$y=\text{tg}(x)$	$y=x^4-x^2$	$3x^{11}\sqrt{x}$	$\frac{x^2}{x^2+1}$	Вычислите $f'(\pi/4)$, если $f(x)=(\text{ctg}(x)+2)/3x+x^2$
11.	$y=\sin(x)$	$y=\sqrt{x}-\frac{1}{\sqrt{x}}$	$y=(\sqrt{x}+1)^{1/2}$	$y=\sqrt{x^2+1}$	Вычислите $f'(\pi/4)$, если $f(x)=(\text{tg}(x)+2)/2x+x^5-5$
12.	$y=x^3$	$y=\sqrt[3]{\sqrt{x}}$	$y=\sqrt{1+\sqrt{x}}$	$y=(x+1)^2-2^x$	Вычислите $f'(\pi/4)$, если $f(x)=(\sin(x)+4)/3x-3x^7+2$

2. Интегрирование.

Вычисление неопределенных интегралов в символьном виде:

`Integrate [f, x]` – возвращает неопределенный интеграл (первообразную) подынтегральной функции f по переменной x . Можно использовать знак интеграла.

Integrate [a x^b, x]

$$\frac{a x^{1+b}}{1+b}$$

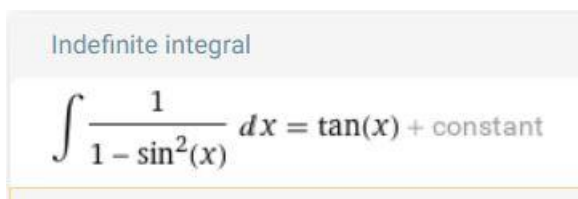
$$\int a x^b dx$$

$$\frac{a x^{1+b}}{1+b}$$

$$\int \sin[x] dx$$

$$- \cos[x]$$

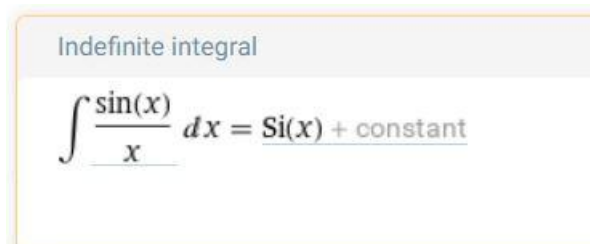
$$\int 1/(1-(\sin[x])^2) dx$$



Indefinite integral

$$\int \frac{1}{1 - \sin^2(x)} dx = \tan(x) + \text{constant}$$

$$\int \frac{\sin[x]}{x} dx$$



Indefinite integral

$$\int \frac{\sin(x)}{x} dx = \text{Si}(x) + \text{constant}$$

Самостоятельно:

1. Вычислить интегралы по вариантам. Перейти по ссылке:
https://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/7662.pdf (рис.6)

Практическое занятие №14

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 $\phi = (p - 1) \cdot (q - 1)$. (Рекомендуется, чтобы длина n составляла 1024 бита).

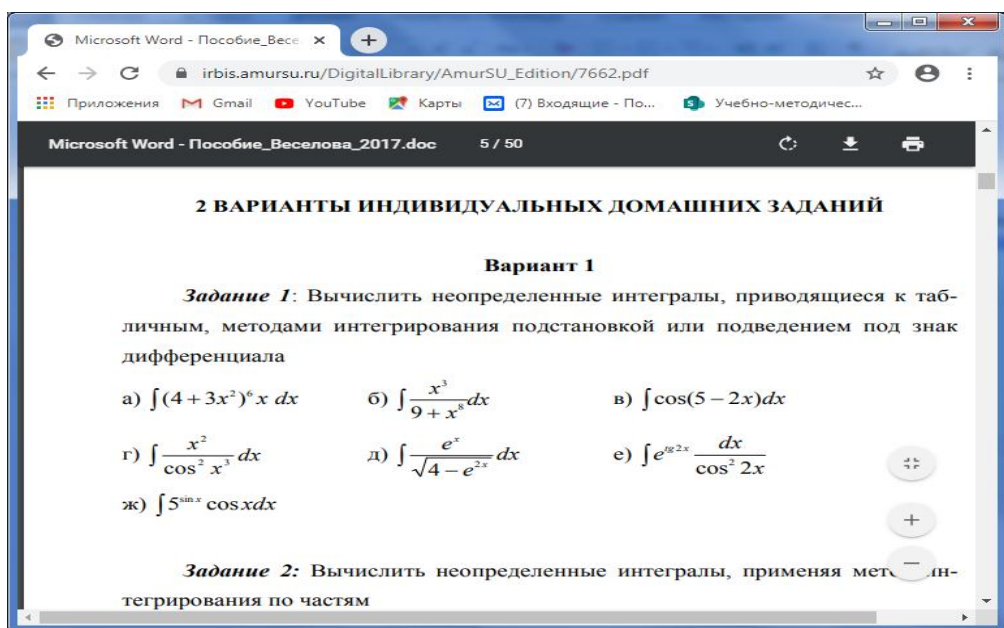


Рис. 6 – Индивидуальное задание по вариантам

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

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 $p = 17$, $q = 31$. 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 .

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

$$D_2 = C_2^d \pmod{n} = 407^{343} \pmod{527} = 33.$$

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 №9

Криптография. Система RSA

1. Зашифровать следующие аббревиатуры, используя систему RSA:

Таблица 28 – Задание для шифрования

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 29 – Задание для расшифровывания

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

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 надёжность 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) $p=a \cdot c, q=d \cdot b$;
 - 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;
 - 3) алгоритмы сложности ?
- 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 $15 \bmod 10=5$;
 - 2) $7 \bmod 10=7$, в следующий разряд переносим $8 \bmod 10=0$;
 - 3) в следующий разряд переносим $15 \operatorname{div} 10=1$.
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 $\sqrt[3]{x^2 - 1}$ относится 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) $a=bq+r, 0 \leq r < b$;
- 2) $a=br+q, 0 \leq r < b$;
- 3) $a=bq$.

22. Если целое число p отлично от 0 и ± 1 , и имеет делителями $\pm 1, \pm p$, 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 $d=\text{НОД}(a,b)$?

- 1) $2 \cdot 3^2$;
- 2) $2^4 \cdot 3$;
- 3) $2^2 \cdot 3^3$;
- 4) $2^2 \cdot 3$.

25. Дан алгоритм Евклида.

begin

repeat

$r:=a \bmod b$; $a:=b$; $b:=r$

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 $0, 1, 2, \dots, m - 1$;
 - 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 $ab \equiv 1 \pmod{m}$, 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 $180 \cdot 4 + (-77) \cdot 7 = 1$ найти обратный элемент к 7 по модулю 180?

- 1) 4;
- 2) 7;
- 3) 103;
- 4) 180.

37. Число итераций, необходимое для вычисления НОД (a, b) равно:

- 1) $n \leq \frac{6}{\pi^2}$
- 2) $n \leq 2^q \left| \frac{a_p}{b_q} \right| \sqrt{\sum_{i=0}^p a_i^2}$

3) нет верного ответа.

38. Представление числа в виде $a = \varepsilon p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}$, $\varepsilon = \pm 1$ называется

- 1) записью в позиционной системе счисления;
- 2) каноническим разложением на простые множители
- 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, \dots, n_r ;
 - 2) z_1, z_2, \dots, z_r ;
 - 3) u_1, u_2, \dots, u_r .
- a) цифры числа x ;
 - b) обратные к 10 по модулям n_1, n_2, \dots, 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) $M = \{0, 1, \dots, Q-1\}$;
 - 2) $A = (a_s, a_{s-1}, \dots, a_1)_Q$.
- 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 $\varphi(n)$, 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 $\mathbf{K}[x]$ называется кольцом полиномов от x над \mathbf{K} , если $\mathbf{K}[x]$ -

- 1) простым расширением кольца \mathbf{K} с помощью x ;
- 2) простое трансцендентным расширением кольца \mathbf{K} с помощью x ;
- 3) нет верного ответа.

48. Если $\mathbf{K}[x]$ -простое трансцендентное расширение кольца \mathbf{K} с помощью x , то кольцо $\mathbf{K}[x]$ называется:

- 1) полиномом над полем \mathbf{K} ;
- 2) нормированным полиномом;
- 3) кольцом полиномов от x над \mathbf{K} .

49. Пусть a - полином из $\mathbf{K}[x]$, $a = a_n x^n + \dots + a_2 x^2 + a_1 x + a_0$, $a_n \neq 0$.

Поставить в соответствие:

- 1) n ;
 - 2) a_0, a_1, \dots, a_n ;
 - 3) a_n .
- а) степень полинома;
- б) коэффициенты полинома
- с) 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) $x^2 x^4 x^5 x^{10} x^{20} x^{21}$;

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

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

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

1) SXXSSX;

2) SSSXSXX;

3) SXSSSX.

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

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

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

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

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 $a=a_n x^n + a_{n-1} x^{n-1} + a_1 x + a_0$, $a_n \neq 0$ 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, \dots, a_n в кольце \mathbf{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 $c := \text{модулярный_НОД}(a, b, p)$;
 - 2) $r := \text{найти_большое_простое}(2m)$;
 - 3) $m := \text{граница_Ландау_Миньотта}(a, b)$;
 - 4) то выход c ;
 - 5) цикл до бесконечности;
 - 6) если $\text{степень_остатка}(r, a)$ или $\text{степень_остатка}(r, b)$;
 - 7) если c делит (a, 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 $x^n - \text{SXSXSSSX}$ (первая единица не вычеркнута)?

- 1) 24;
 - 2) 25;
 - 3) 32.
64. Полином f , содержание которого есть 1 в \mathbf{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. Результат 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 \mathbf{K} , являющееся подкольцом кольца \mathbf{L} , и содержащее элементы x_1, \dots, x_m из \mathbf{L} называется:

- 1) m – кратным расширением кольца \mathbf{K} ;
- 2) m – кратным трансцендентным расширением кольца \mathbf{K} ;
- 3) подкольцом кольца \mathbf{L} .

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

$$\sum_{(i) \in M} a_{(i)} x_1^{i_1} \dots x_m^{i_m} = 0, \quad M \in N^m, \quad \text{следует равенство нулю всех коэффициентов } a_{(i)},$$

то элементы x_1, \dots, x_m кольца \mathbf{L} называются:

- 1) алгебраически зависимыми над кольцом \mathbf{K} ;
 - 2) алгебраически независимыми над кольцом \mathbf{K} ;
 - 3) нет верного ответа.
76. Произведение степеней переменных это:
- 1) моном;
 - 2) полином;
 - 3) S -полином.
77. Если кольцо $\mathbf{K}[x_1][x_2]\dots[x_m]$ определяется формулами $\mathbf{K}[x_1][x_2]=\mathbf{K}[x_1][x_2]$, $\mathbf{K}[x_1][x_2]\dots[x_m]=\mathbf{K}[x_1][x_2]\dots[x_{m-1}][x_m]$, то оно является
- 1) кольцом полиномов над \mathbf{K} от x_1, \dots, x_m ;
 - 2) m – кратным расширением кольца \mathbf{K} ;
 - 3) m – кратным трансцендентным расширением кольца \mathbf{K} .
78. Поставить в соответствие. Кольцо $\mathbf{K}[x_1, \dots, x_m]$ называется:
- 1) кольцом полиномов над \mathbf{K} от x_1, \dots, x_m ;
 - 2) m – кратным расширением кольца \mathbf{K} ;
 - 3) m – кратным трансцендентным расширением кольца \mathbf{K} .
- a) если кольцо $\mathbf{K}[x_1][x_2]\dots[x_m]$ определяется формулами $\mathbf{K}[x_1][x_2]=\mathbf{K}[x_1][x_2]$, $\mathbf{K}[x_1][x_2]\dots[x_m]=\mathbf{K}[x_1][x_2]\dots[x_{m-1}][x_m]$;
- b) если для любого $s \in \{1, \dots, m\}$ кольцо $\mathbf{K}[x_1, \dots, x_s]$ является простым трансцендентным расширением кольца $\mathbf{K}[x_1, \dots, x_{s-1}]$ при помощи x_s ;
- c) если кольцо $\mathbf{K}[x_1, \dots, x_m]$ является m – кратным расширением ненулевого коммутативного кольца \mathbf{K} ;
- d) если элементы x_1, \dots, x_m кольца \mathbf{L} называются алгебраически независимыми над кольцом \mathbf{K} .
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) $p/\text{cont}(p)$;

3) $\text{cont}(p)$.

85. По формуле $pp(p) = p/\text{cont}(p)$ 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.
- а) представляет остающийся после вычисления интеграл в виде суммы логарифмов;
- б) использует разложение дроби q/r на простейшие дроби;
- с) 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:

- а) интегрирования;
- б) дифференцирования;
- с) нет верного ответа.

93. Процесс декодирования при наличии ключа называется:

- а) расшифровыванием;
- д) дешифрованием;
- е) вскрытием.

94. Поставить в соответствие базовые преобразования в криптографии их характеристику.

- а) перемешивающие;
 - б) рассеивающие;
- 1) сложные локальные преобразования над отдельными частями шифруемых блоков;
- 2) простые преобразования, переставляющие между собой части шифруемых блоков;
- 3) многократное повторение операций преобразования шифруемых блоков.

95. Шеннон предложил для шифрования:

а) реализовывать сложные преобразования в виде суперпозиции нескольких простых некоммутируемых отображением;

б) использовать многократное повторение некоторого набора операций преобразования;

в) использовать очередность выборки подключений из ключа шифрования.

96. Цель процесса шифрования –

а) кодирование данных с целью защиты от несанкционированного доступа;

б) получение более компактного выходного потока данных с помощью соответствующего преобразования;

в) эффективная передача максимального количества информации в единицу времени.

97. Криптосистема RSA относится к системам:

а) с открытым ключом;

б) с закрытым ключом.

98. В системе RSA пара чисел n и e - это:

а) открытый ключ;

б) закрытый ключ.

99. Выберите основное требование к шифру.

а) наличие санкции (некоторой дополнительной информации);

б) возможность декодирования;

в) скорость расшифровки.

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.

Дисциплина «Теоретические основы информатики» относится к модулю обязательной части Блока 1 «Дисциплины/модули» основной профессиональной образовательной программы по направлению подготовки 44.03.05 «Педагогическое образование (с двумя профилями подготовки)» «Информатика. Иностранный язык» и «Математика. Информатика» (уровень образования бакалавриат).

Программа курса предусматривает аудиторные занятия (лекции и практические занятия) и самостоятельную работу студентов. В самостоятельную работу студентов входит освоение теоретического материала, выполнение индивидуальных заданий, подготовка сообщений и разработка кейса по разделам дисциплины.

В пособии имеется большое число примеров алгоритмов, используемых при разработке сложных систем.

При изучении дисциплины «Теоретические основы информатики» может быть использована модульно-рейтинговая система контроля знаний студентов. В приложении приведен пример оценки сформированности компетенций по указанным дисциплинам.

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: символные и алгебраические вычисления / Б. Бухбергер. – М. : Мир, 1986. – 392 с.
5. 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.
6. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии» [Сайт]. – URL: <https://habr.com/>
7. Кормен Т. Алгоритмы: построение и анализ, 3-е издание. : Пер. с англ. / Т. Кормен, Ч. Лейзерсон, Р. Ривест. – М.: ООО «И.Д. Вильямс», 2013. – 1328 с.
8. Матрос Д.Ш. Элементы абстрактной и компьютерной алгебры: учеб. пособие для вузов /Д. Ш. Матрос, Г.Б. Поднебесова. – М.: Академия, 2004. – 240 с.
9. Общероссийский математический портал (информационная система) [Сайт]. – URL: <http://www.mathnet.ru/>
10. Поднебесова Г. Б. Основы компьютерной алгебры: учеб. пособие / Г.Б. Поднебесова. – М. : БИНОМ. Лаборатория знаний, 2008. – 112 с.
11. Поднебесова Г. Б. Компьютерная алгебра: учебно-практическое пособие / Г.Б. Поднебесова. – Челябинск : Изд-во ЗАО «Библиотека А. Миллера», 2023. – 82 с.

Приложение

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

Лекции

<i>Наименование раздела дисциплины (модуля)/Тема и содержание</i>	<i>Трудоемкость (кол-во часов)</i>
1. Представление данных в компьютере	4
Формируемые компетенции, образовательные результаты: ПК-1: ПК.1.2	
1.1. Аналитические вычисления на компьютере 1. Особенности аналитических вычислений на компьютерах. 2. Алгебраические структуры. 3. Основные числовые системы. Учебно-методическая литература: 1, 3, 4	2
1.2. Представление данных в компьютере 1. Арифметические вычисления и операции. Представление целых чисел в компьютере. Умножение длинных чисел. 2. Представление и работа с другими математическими объектами. 3. Представление полиномов. 4. Представление рациональных, алгебраических и трансцендентных функций Учебно-методическая литература: 1, 3, 5	2
2. Алгоритмы компьютерной математики	8
Формируемые компетенции, образовательные результаты: ПК-1: ПК.1.2	
2.1. Основы теории делимости 1. Основная теорема арифметики. 2. Теорема Евклида. 3. Алгоритм Евклида. 4. Теорема Ламе. Учебно-методическая литература: 1, 3	2
2.2. Теория сравнений 1. Сравнимость по модулю. 2. Вычеты. 3. Классы вычетов. 4. Теоремы Эйлера и Ферма. Учебно-методическая литература: 1, 3	2
2.3. Модулярная арифметика 1. Китайская теорема об остатках. 2. Метод Гарнера-Кнута. 3. Сравнение двух целых чисел. 4. Определение цифр в позиционной системе счисления. 5. Восстановление произведения двух длинных целых чисел по их модулярным компонентам. Учебно-методическая литература: 1, 3, 4	2

2.4. Системы счисления 1. Основные определения. 2. Смешанная система счисления. 3. Перевод чисел из одной системы счисления в другую. Учебно-методическая литература: 1, 3, 5	2
3. Полиномы от одной и нескольких переменных	4
Формируемые компетенции, образовательные результаты: ПК-1: ПК.1.2	
3.1. Полиномы от одной переменной 1. Основные определения. 2. Вычисления полиномов. 3. Неравенство Ландау- Миньотта. 4. Соответствие модулярное-целое. 5. Вычисление НОД.	2
6. Оценка стоимости лгоритма. Учебно-методическая литература: 1, 3 Профессиональные базы данных и информационные справочные системы: 1	2
3.2. Полиномы от нескольких переменных 1. Содержание полинома. 2. Примитивная часть полинома. 3. Лемма Гаусса. 4. Алгоритм вычисления НОД. Учебно-методическая литература: 1, 3 Профессиональные базы данных и информационные справочные системы: 1	2
4. Система компьютерной математики Wolfram Alpha. Применение алгоритмов компьютерной математики	4
Формируемые компетенции, образовательные результаты: ПК-1: ПК.1.2	
4.1. Преобразование Фурье 1. Основной алгоритм. 2. Анализ Фурье. Методы анализа Фурье. 3. Применение преобразования Фурье. Учебно-методическая литература: 1, 3, 5 Профессиональные базы данных и информационные справочные системы: 1	2
4.2. Криптография 1. Кодирование информации. 2. Криптография. Основные определения. 3. Классификация шифров. 4. Системы с открытым и закрытым ключом. 5. Система шифрования RSA. Учебно-методическая литература: 1, 3, 4 Профессиональные базы данных и информационные справочные системы: 2	2

Практические занятия

<i>Наименование раздела дисциплины (модуля)/Тема и содержание</i>	<i>Трудоемкость (кол-во часов)</i>
1. Представление данных в компьютере	4
Формируемые компетенции, образовательные результаты: ПК-1: ПК.1.2	
1.1. Аналитические вычисления в WolframAlpha. Работа с простыми числами в Wolfram Alpha: - выполнение арифметических операций; - работа с действительными числами; - вычисление суммы и произведения; - основные функции для работы с простыми числами; - разложение чисел на простые множители; - вычисление следующего и предыдущего простого числа. Учебно-методическая литература: 1, 2, 5	2
1.2. Разработка кейса по теме Системы компьютерной математики Разработать кейс по одной из систем компьютерной математики. Кейс должен включать: 1. Функциональное назначение; 2. Тип архитектуры; 3. Средства реализации; 4. Области применения;	2
5. Примеры (принтскрины); 6. Интегральные оценки качества. Учебно-методическая литература: 1, 2 Профессиональные базы данных и информационные справочные системы: 2	2
2. Алгоритмы компьютерной математики	12
Формируемые компетенции, образовательные результаты: ПК-1: ПК.1.2	
2.1. Модулярная арифметика - восстановление произведения двух целых чисел по их модулярным компонентам. Учебно-методическая литература: 1, 2, 4	4
2.2. Системы счисления - вычисления в различных системах счисления; - переводы целых чисел; - переводы дробных чисел; - переводы произвольных чисел. Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1	2

2.3. Вычисление НОД - прямой метод; - алгоритм Евклида; - вычисление НОД разложением на множители. Учебно-методическая литература: 1, 2, 3, 4	2
2.4. Расширенный алгоритм Евклида - соотношение Безу; - нахождение обратного числа по модулю простого числа. Учебно-методическая литература: 1, 2, 3	2
2.5. Разложение на множители - деление и разложение на множители; - метод Ферма; - вероятностный метод. Учебно-методическая литература: 1, 2, 3	2
3. Полиномы от одной и нескольких переменных	4
Формируемые компетенции, образовательные результаты: ПК-1: ПК.1.2	
3.1. Вычисление полиномов - бинарный метод; - метод множителей; - схема Горнера; - обобщенная схема Горнера. Учебно-методическая литература: 1, 2 Профессиональные базы данных и информационные справочные системы: 1	2
3.2. Нахождение НОД полиномов - применение неравенства Ландау-Миньотта; - вычисление модулярного НОД. Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1	2
4. Система компьютерной математики Wolfram Alpha. Применение алгоритмов компьютерной математики	8
Формируемые компетенции, образовательные результаты: ПК-1: ПК.1.2	
4.1. Полиномы от одной переменной в Wolfram Alpha - основные функции для работы с полиномами от одной переменной; - вычисление НОД; - вычисление частного и остатка от деления полиномов. Учебно-методическая литература: 1, 2 Профессиональные базы данных и информационные справочные системы: 2	2
4.2. Полиномы от нескольких переменных в Wolfram Alpha - основные функции для работы с полиномами от нескольких переменных; - вычисление НОД и НОК полиномов. Учебно-методическая литература: 1, 2 Профессиональные базы данных и информационные справочные системы: 2	2

4.3. Интегрирование и дифференцирование в Wolfram Alpha - основные функции для вычисления интегралов; - функции для вычисления производных. Учебно-методическая литература: 1, 2 Профессиональные базы данных и информационные справочные системы: 2	2
4.4. Шифрование методом RSA - вычисление открытого ключа; - вычисление закрытого ключа; - шифрование подписи. Учебно-методическая литература: 1, 2 Профессиональные базы данных и информационные справочные системы: 2	2

Учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Ссылка на источник в ЭБС
<i>Основная литература</i>		
1	Матрос, Д.Ш. Элементы абстрактной и компьютерной алгебры: учеб. пособие для вузов /Д.Ш.Матрос, Г.Б. Поднебесова. – М.: Академия, 2004	
2	Поднебесова, Г.Б. Абстрактная и компьютерная алгебра: практикум / Г.Б. Поднебесова. – Челябинск: Изд-во Южно-Ур. гос. гуман.-пед. ун-та, 2017. –115 с.	http://www.iprbookshop.ru/83852.html
3	Поднебесова, Г. Б. Основы компьютерной алгебры: учебное пособие / Г.Б. Поднебесова. – М.: БИНОМ. Лаборатория знаний, 2008	
4	Бухбергер, Б. Компьютерная алгебра: символные и алгебраические вычисления. – М.: Мир, 1986.	
5	Дэвенпорт, Д. Компьютерная алгебра: Системы и алгоритмы алгебраич. вычислений / Дж. Дэвенпорт, И. Сирэ, Э. Турнье ; Пер. с фр. Е.В. Панкратьева и др. – М. : Мир, 1991	

Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

№ п/п	Наименование базы данных	Ссылка на ресурс
1	Общероссийский математический портал (информационная система)	http://www.mathnet.ru/
2	Информационная система «Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии»	https://habr.com/

Приложение 2. Содержание самостоятельной работы

<i>Наименование раздела дисциплины (модуля)/ Тема для самостоятельного изучения</i>	<i>Трудоемкость (кол-во часов)</i>
1. Представление данных в компьютере	20
Формируемые компетенции, образовательные результаты: ПК-1: ПК.1.2	
1.1. Аналитические вычисления на компьютере Задание для самостоятельного выполнения студентом: Разработать кейс по одной из тем: 1. Maxima. 2. Axiom. 3. Maple. 4. MatLab. 5. MathCAD. 6. TRIP. 7. Reduce. 8. Derive. 9. Cadabra. 10. Singular. 11. Magma. 12. MuPAD. 13. GAP. 14. GINV. 15. Jasymsa. Учебно-методическая литература: 1, 3, 5	20
2. Алгоритмы компьютерной математики	20
Формируемые компетенции, образовательные результаты: ПК-1: ПК.1.2	
2.1. Модулярная арифметика Задание для самостоятельного выполнения студентом: Восстановить произведение двух целых чисел по их модулярным компонентам: $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$; $x_1=2$ $x_2=2$ $x_3=0$ $x_4=14$; $x_1=0$ $x_2=1$ $x_3=10$ $x_4=2$. Учебно-методическая литература: 1, 2, 3, 4 Профессиональные базы данных и информационные справочные системы: 1	10
2.2. Разложение на множители Задание для самостоятельного выполнения студентом: Разложить на множители, используя метод Ферма:	10
$n=98$; $n=52$; $n=124$. Учебно-методическая литература: 1, 2 Профессиональные базы данных и информационные справочные системы: 2	10
3. Полиномы от одной и нескольких переменных	10
Формируемые компетенции, образовательные результаты: ПК-1: ПК.1.2	

<p>3.1. Полиномы от одной переменной</p> <p>Задание для самостоятельного выполнения студентом:</p> <p>1. Если полином можно представить в виде произведения двух полиномов, то такой полином называют:</p> <ol style="list-style-type: none"> 1) неприводимым; 2) нормированным; 3) нет верного ответа. <p>2. Кольцо $K[x]$ называется кольцом полиномов от x над K, если $K[x]$ -</p> <ol style="list-style-type: none"> 1) простым расширением кольца K с помощью x; 2) простое трансцендентным расширением кольца K с помощью x; 3) нет верного ответа. <p>Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1</p>	5
<p>3.2. Полиномы от нескольких переменных</p> <p>Задание для самостоятельного выполнения студентом:</p> <p>Для полиномов от двух переменных найти НОД с помощью функции PolynomialRemainder.</p> <p>Проверить с помощью функции PolynomialGCD.</p> <p>Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1</p>	5
<p>4. Система компьютерной математики Wolfram Alpha. Применение алгоритмов компьютерной математики</p>	10
<p>Формируемые компетенции, образовательные результаты: ПК-1: ПК.1.2</p>	
<p>4.1. Криптография</p> <p>Задание для самостоятельного выполнения студентом: Зашифровать следующие аббревиатуры, используя систему RSA: 1. ASD ($p=13, q=73$) 2. FOP ($p=17, q=61$) 3. GYZ ($p=7, q=47$) 4. PON ($p=19, q=53$)</p> <p>Учебно-методическая литература: 1, 3 Профессиональные базы данных и информационные справочные системы: 2</p>	10

Приложение 3. Рейтинг

№	Фамилия Имя	Аналитические вычисления лаб	СКА	Доп. балл	Тест1	Модуль1
---	-------------	------------------------------------	-----	--------------	-------	---------

Системы счисления	Алгоритм Евклида	Вычисление НОД Лаб.	Модулярная арифметика	Разложение на множители Лаб.	Доп. балл	Тест2	Модуль2
----------------------	---------------------	------------------------	--------------------------	---------------------------------------	--------------	-------	---------

Вычисление полиномов	НОД полиномов	Доп. балл	Тест3	Модуль3
-------------------------	------------------	--------------	-------	---------

WAlpha_11	WAlpha_12	Лаб№13	RSA	Доп. балл	Тест4	Модуль4	Итог	Оценка
-----------	-----------	--------	-----	--------------	-------	---------	------	--------

Приложение 4. Работа в Wolfram Alpha

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

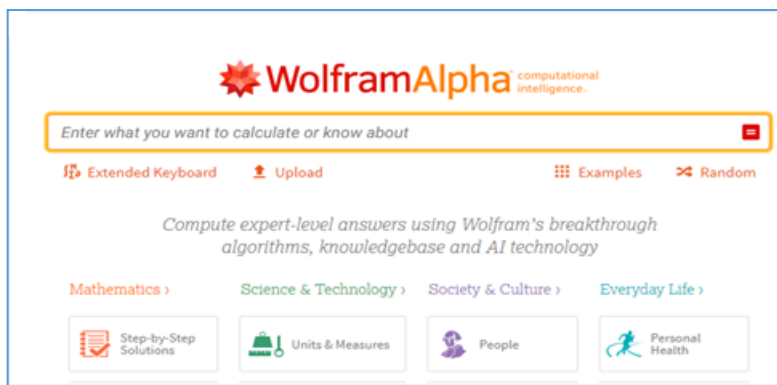


Рис. 1 – Главное окно

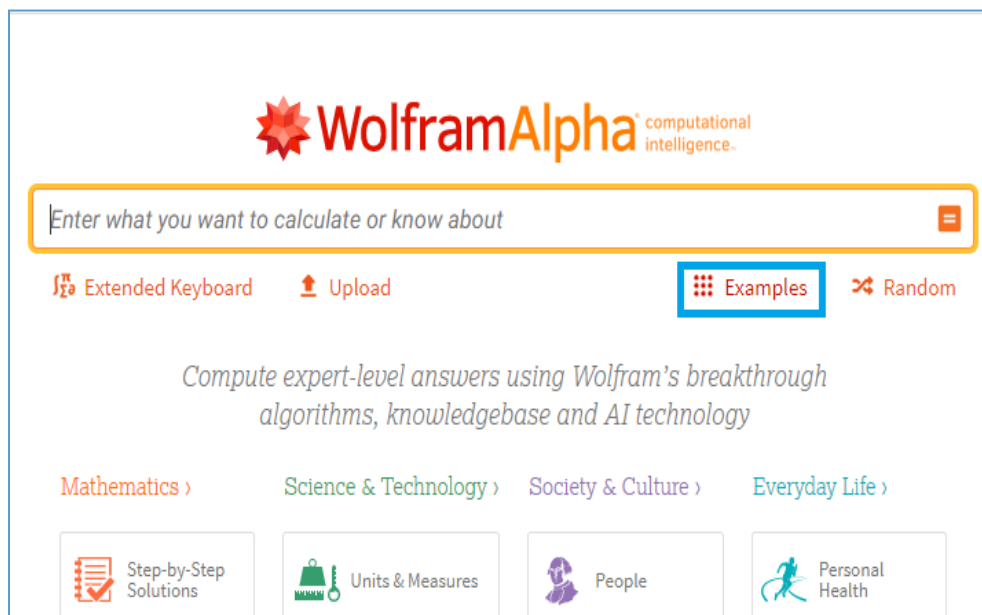


Рис. 2 – Помощь – Examples (->Algebra)

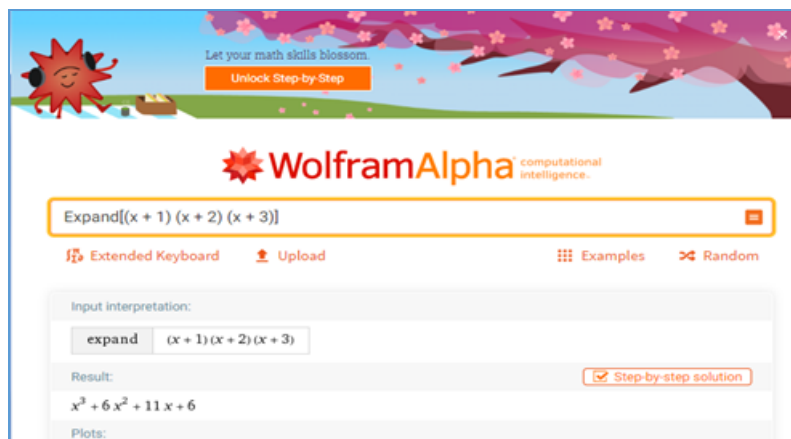


Рис. 3 – Функция Expand (раскрывает скобки)

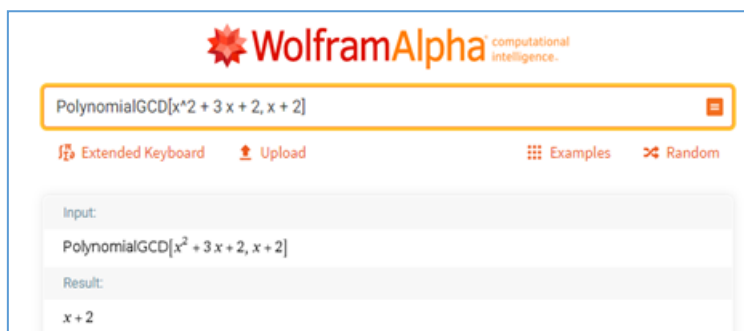


Рис. 4 – Функция Simplify (обратная Expand)



Рис. 5 – Вычисление НОД полиномов

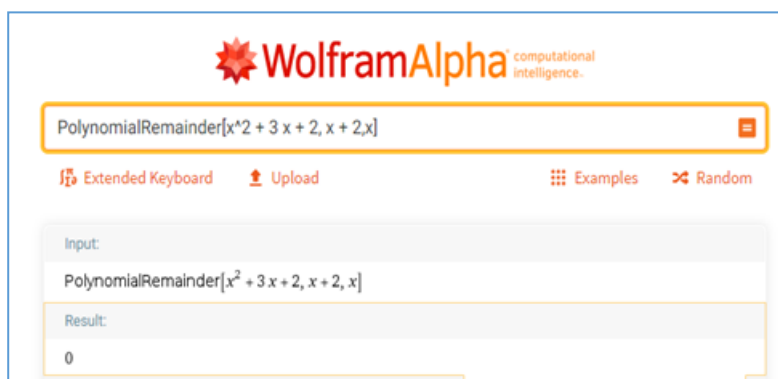


Рис. 6 – Вычисление остатка от деления полиномов



Рис. 7 – Разложение полиномов

Учебное издание

Поднебесова Галина Борисовна

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ

Часть 1

Учебно-практическое пособие

ISBN 978-5-93162-895-0 (общий)

ISBN 978-5-93162-896-7 (часть 1)

Издательство ЗАО «Библиотека А. Миллера»
454091, г. Челябинск, ул. Свободы, 159

Подписано в печать 21. 10. 2023. Формат 60x84/16 Бумага офсетная. Объем
6,00 усл. печ. л. Тираж 100 экз. Заказ № 538.

Отпечатано с готового оригинал-макета в типографии ЮУрГГПУ 454080,
Челябинск, пр. Ленина, 69