МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Г.Б. Поднебесова

АБСТРАКТНАЯ И КОМПЬЮТЕРНАЯ АЛГЕБРА

Практикум

Челябинск
2016

УДК 001.8 (076)
ББК 73я7
П 44

Поднебесова, Г.Б. Абстрактная и компьютерная алгебра [Текст]: **практикум** / Г.Б. Поднебесова. – Челябинск: Изд-во Южно-Ур. гос. гуман.-пед. ун-та, 2016. – 125 с.

ISBN 978-5-906908-47-6

В практикуме представлены материалы для изучения курсов «Абстрактная и компьютерная алгебра», «Компьютерная алгебра» и «Теоретические основы информатики и современных информационных технологий». Пособие предназначено для организации аудиторной и самостоятельной работы студентов, обучающихся по направлениям «Педагогическое образование» и «Информационные системы и технологии».

Структура пособия позволяет использовать модульно-рейтинговую систему оценивания учебных достижений студентов при изучении дисциплин «Абстрактная и компьютерная алгебра» и «Компьютерная алгебра». В работе имеется также банк тестовых заданий.

Практикум адресован преподавателям и учителям, для которых интересна данная предметная область.

Рецензенты: С.А. Загребина, д-р физ.-мат. наук, доцент
А.А. Рузаков, канд. пед. наук

ISBN 978-5-906908-47-6

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

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

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

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

В качестве ключевого понятия компьютерной алгебры взято понятие алгоритма символьных преобразований. Особенностью данного практикума является использование модулярных методов при работе с длинными целыми числами и полиномами.

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

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

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

Таблица 1

Планируемые результаты обучения

№ п/п	Компетенция (содержание и обозначение в соответствии с ФГОС ВО и ОПОП)	Конкретизированные цели освоения дисциплины		
		знать	уметь	владеть
1.	готовность применять знания теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов (СК-1)	З.1 характеристику числовых систем; З.2 определение основных понятий абстрактной и компьютерной алгебры; З.3 основные алгоритмы компьютерной алгебры	У.1 выполнять операции на множестве целых и рациональных чисел; У.2 использовать алгоритмы работы с длинными целыми числами	В.1 методами описания алгоритмов компьютерной алгебры; В.2 навыками работы в системах компьютерной алгебры

Содержание разделов дисциплины

1. Системы компьютерной алгебры.

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. Алгебры.

Определение бинарной алгебраической операции. Алгебраические структуры с одной бинарной операцией. Понятие группы. Примеры и свойства групп. Подгруппы. Алгебраические структуры с двумя бинарными алгебраическими операциями. Понятие кольца. Примеры и свойства колец. Подкольца. Поля. Основные числовые множества. Система натуральных чисел. Кольцо целых чисел. Поле рациональных чисел. Система действительных чисел. Поле комплексных чисел.

3. Кольцо целых чисел. Теория делимости в кольце целых чисел.

Кольцо целых чисел. Отношение делимости, его простейшие свойства. Кольцо классов вычетов. НОД, 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. Извлечение корней из больших целых чисел.

4. Кольцо полиномов от одной переменной. Теория делимости.

Построение кольца полиномов над полем. 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.

5. Полиномы от нескольких переменных. Лексикографический порядок следования членов. Понятие о решении систем двух алгебраических уравнений с двумя неизвестными методом последовательного исключения одного из неизвестных.

6. Быстрое преобразование Фурье.

Матрица Вандермонда. Умножение полиномов a и b степени меньше n. Комплексные корни из единицы. Основной алгоритм. Дискретное преобразование Фурье. Применение преобразования Фурье.

7. Интегрирование и дифференцирование.

Дифференцирование в системах компьютерной алгебры. Задача интегрирования. Интегрирование рациональных функций. Интегрирование более сложных функций.

Темы и планы лабораторных занятий

Модуль 1. Аналитические вычисления на компьютере. Алгебры

1. Работа с математическими объектами в системе Mathematica (2 часа).

2. Длинная арифметика (2 часа).

Модуль 2. Кольцо целых чисел

3. Системы счисления (2 часа):

– вычисления в различных системах счисления;

– переводы целых чисел;

– переводы дробных чисел;

– переводы произвольных чисел;

4. Расширенный алгоритм Евклида (2 часа).

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

6. Модулярная арифметика (2 часа):

– восстановление произведения двух чисел по их модулярным компонентам.

7. Разложение на множители (2 часа)

Модуль 3. Полиномы от одной переменной

8. Вычисление полиномов (2 часа):

– бинарный метод и метод множителей;

– схема Горнера, обобщенная схема Горнера.

9. Нахождение НОД (2 часа):

– применение неравенства Ландау-Миньотта;

– вычисление модулярного НОД.

10. Полиномы от одной переменной в пакете Mathematica (2 часа):

Модуль 4. Полиномы от нескольких переменных. Формальное интегрирование и дифференцирование

11. Полиномы от нескольких переменных в пакете Mathematica (2 часа):

– основные функции для работы с полиномами от нескольких переменных.

12. Работа с простыми числами и подпакетами расширений в системе Mathematica (2 часа).

13. Интегрирование и дифференцирование в системе Mathematica (2 часа).

14. Криптосистема RSA (2 часа).

Модуль 1. Аналитические вычисления на компьютере. Алгебры

Лабораторная работа № 1

Аналитические вычисления в пакете Mathematica

1. Организация вычислений.

1) **56*34/8** (нажать Shift+Enter)

238

2) **a:=53**

b:=34

c:=25

(a+b^2+c^3)/(3*a-4*c)

$$\frac{16834}{59}$$

Целочисленные вычисления

3) Factorial[7]

5040

4) 100!

933262154439441526816992388562667004907159682643816214685,,
929638952175999932299156089414639761565182862536979208 27,,
22375825118521091686400000000000000000000000

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

Самостоятельно:

2. Матрицы

Можно задать матрицу, используя панель BasicInput (File -> Palettes).

MatrixForm[m] – представление в матричном виде;

Det[m] – вычисление определителя матрицы m;

Transpose[m] – транспонирование матрицы.

m:={{1,2},{3,7}}

MatrixForm[m]

1 2

3 7

Det[m]

1

Transpose[m]

{{1,3},{2,7}}

Самостоятельно:

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

3. Вычисление сумм и произведений.

Можно задать матрицу, используя панель Basic-Calculation (File -> Palettes), раздел Calculus -> Common Operations для получения знаков суммы и произведения.

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

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

Самостоятельно:

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

Sum[1/(n*n),{n,1,∞}]

Sum[x^n/n!,{n,1,9,2}]

Product[i,{i,10}]

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

4. Поиск корней уравнений.

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

Самостоятельно:

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

Привести 2-3 примера вычисления корней уравнения.

5. Функции времени и даты.

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

Date[] – возвращает текущую дату;

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

Проверить самостоятельно.

Лабораторная работа № 2

Длинная арифметика

Вычисления с длинными числами осуществляются так же, как и в обычной математике, при вычислениях «в столбик». Рассмотрим операцию сложения. Даны два длинных числа, они представлены в виде массивов a и b, известны размеры i_max, j_max. Сложение осуществляется элементарно: начинаем сложение с конца (то есть с последних чисел, записанных в обоих массивах), последний элемент суммы равен сумме последних элементов массивов слагаемых, и так далее – предпоследний равен сумме предпоследних.

В результате сложении чисел может получиться число, большее 9, Переносимый разряд получаем в результате целочисленного деления суммы цифр на основание:

Пример. 9+9=18 записываем 18 mod 10=8, в следующий разряд переносим 18 div 10=1.

Замечание: размер массива суммы должен быть на 1 больше размера самого большого (по длине записи) слагаемого.

Задание 1. Написать программу вычитания длинных чисел.

```
// вычисление разности
k:=0;
for i:=n_um downto 1 do
    begin
      w[i]:=(u[i]-v[i]+k+b) mod b;
      k:=(u[i]-v[i]+k-b+1) div b;
    end;
```

где n_um – размер уменьшаемого, b – основание системы счисления, u – уменьшаемое, v – вычитаемое, k – занимаемый разряд, w – разность.

Для организации вычитания необходимо отслеживать количество занимаемых разрядов для вычитания.

Самостоятельно:

Написать программу сложения длинных чисел.

Задание 2. Написать программу умножения длинных чисел.

На каждом шаге умножения можно осуществлять сразу и сложение, то есть накопление значений в разрядах произведения (нужно следить за количеством переносимых разрядов).

Фрагмент программы, осуществляющей умножение с одновременным накоплением значений в результат:

```
// вычисление произведения
for i:=1 to n do
 w[m+i]:=0;
 j:=m;
```

```
 while j>0 do
begin
 i:=n;
 k:=0;
 while i>0 do
   begin
     t:=u[i]*v[j]+w[i+j]+k;
     w[i+j]:=t mod b;
     k:=t div b;
     i:=i-1;
   end;
   w[j]:=k;
 j:=j-1;
end;
```

Здесь u и v – массивы множителей, w – массив произведения, t – число которое получается при умножении и добавлении предыдущего значения, хранимого в соответствующем разряде произведения, k – количество переносимых разрядов, b – основание системы счисления.

Самостоятельно:

Написать программу выполнения арифметических вычислений с дробями.

Замечание: необходимо использовать вспомогательную процедуру нахождения НОД.

Вопросы к модулю 1

1. Чем отличаются численные методы от аналитических вычислений?

2. Выделить особенности аналитических вычислений на компьютере.

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 четыре уровня 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?

21. Какая пара объектов a и b называется неупорядоченной?

22. Какие отношения называются бинарными?

23. Какие бинарные отношения называются транзитивными, рефлексивными, антирефлексивными, симметричными, отношениями эквивалентности?

24. Что такое «класс эквивалентности»?

25. Какая пара называется алгеброй?

26. Какая алгебра называется моноидом?

27. Дать определение алгебраической системы.

28. Какая алгебра называется группой?

29. Какая группа называется абелевой?

30. Что такое порядок группы?

31. Дать определение подгруппы?

32. Какая алгебра называется кольцом?

33. Какая группа называется аддитивной группой кольца?

34. Дать определение подкольца.

35. Какое кольцо называется полем?

36. Что является полем рациональных чисел, полем действительных чисел?

37. Дать определение системы натуральных чисел?

38. Какими свойствами обладает система натуральных чисел?

39. Является ли система $\langle N, +, \cdot, < \rangle$ упорядоченной системой натуральных чисел?

40. Всегда ли выполнима операция вычитания в N?

41. Дать определение аддитивной группы целых чисел?

42. Какое кольцо K называется кольцом целых чисел?

Модуль 2. Кольцо целых чисел

Лабораторная работа № 3

Позиционные системы счисления

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

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

где s-целое неотрицательное, a_0, …, $a_s \in M$ и $a_s \neq 0$.

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

Представление (1) записывается тогда в сокращенном виде

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

и называется записью в Q-ичной позиционной системе.

Запись $a = (2315)_{10}$ означает, что $a = 2 \cdot 10^3 + 3 \cdot 10^2 + 1 \cdot \cdot 10^1 + 5$, 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 A,B,C, D,E,F).

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

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

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.

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

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

5 – 10
6 – 11
7 – 12
8 – 13
9 – 14
10 – 20
11 – 21

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

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

1) $(3501)_6 + (4335)_6$, $(34521)_6 - (15013)_6$;

2) $(23)_6 \cdot (15)_6$, $(432)_6 : (14)_6$.

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

Пример.

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

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

Задание 2.

1) Перевести числа из восьмеричной системы счисления в десятичную систему счисления:

$(263)_8$, $(713)_8$, $(126{,}34)_8$;

2) Перевести числа из шестнадцатеричной системы счисления в десятичную систему счисления:

$(B52)_{16}$, $(A49{,}62)_{16}$;

3) Перевести числа из двоичной системы счисления в десятичную систему счисления:

$(10011)_2$, $(1010{,}011)_2$.

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

1^0. **Перевод целых чисел**.

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

Применяя теорему 3 при Q = 2 получим:

```
_47 | 2__
 46   _23 | 2__
  1     22   _11 | 2__
          1     10   _5 | 2__
                  1    4  _2 | 2__
                         1   2  _1 | 2__
                             0   0   0
                                 1
```

Поскольку числа «нуль» 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.

```
_3060 | 16
 16     _191 | 16
_146      16    _11 | 16
 144      _31      0     0
  _20      16      11
   16      15
    4
```

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 систему счисления: $(1934)_{10}$, $(523)_{10}$;

2) Перевести числа из десятичной системы счисления в двоичную систему счисления:

$(37)_{10}$, $(156)_{10}$;

3) Перевести числа из десятичной системы счисления в шестнадцатеричную систему счисления: $(252)_{10}$, $(64932)_{10}$.

2^0. **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):

0,2
2
0 | 4
| 2
0 | 8
| 2
1 | 6
| 2
1 | 2

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…).

Задание 4.

1) Перевести числа из десятичной системы счисления в восьмеричную систему счисления: $(634,36)_{10}$, $(52,37)_{10}$;

2) Перевести числа из десятичной системы счисления в двоичную систему счисления:

$(32,6)_{10}$, $(156,5)_{10}$;

3) Перевести числа из десятичной системы счисления в шестнадцатеричную систему счисления: $(52,21)_{10}$, $(812,32)_{10}$;

3^0. **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 $\overline{\text{x}}$ 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 … . Переведем число в шестнадцатеричную систему.

Умножаем дробную часть на 16. Берем в ответ только целые части выполненного умножения.

0,292
16
4,672
16
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 шестнадцатеричную, преобразовав их предварительно в дробь:

$(452,81)_{10}$, $(4812,32)_{10}$;

2) Перевести число из десятичной системы счисления в двоичную, переведя предварительно число в восьмеричную систему:

$(61)_{10}$, $(182)_{10}$;

3) Перевести числа из десятичной системы счисления в двоичную, переведя число предварительно в шестнадцатеричную: $(527)_{10}$, $(1459)_{10}$;

4) Перевести числа из восьмеричной системы в десятичную, выполнить указанные действия и перевести в восьмеричную:

$(315)_8 + (602)_8$, $(562)_8 : (14)_8$;

5) Перевести числа из двоичной системы счисления в восьмеричную систему счисления, из восьмеричной системы счисления в десятичную систему счисления, и выполнить указанные действия:

$(10111101)_2 + (101010)_2$, $(111101{,}1)_2 \cdot (10{,}1)_2$;

6) Перевести числа из десятичной системы счисления в восьмеричную систему счисления, и в двоичную систему счисления, выполнить указанные действия, перевести результат из двоичной системы счисления в восьмеричную систему счисления и в десятичную систему счисления, сравнить результат:

$(48{,}21)_{10} + (16{,}43)_{10}$, $(172)_{10} - (85)_{10}$.

Задания для самостоятельной работы.

1. Составить таблицы сложения и умножения в семеричной системе счисления. Выполнить следующие действия:

1) $(3506)_7 + (335)_7$, $(34621)_7 - (15016)_7$;

2) $(423)_7 \cdot (16)_7$, $(1054)_7 : (24)_7$.

2. Записать год своего рождения в восьмеричной системе счисления.

3. Записать почтовый индекс в двоичной системе счисления (предварительно перевести в восьмеричную систему счисления).

4. Перевести числа из десятичной системы счисления в шестнадцатеричную систему счисления и восьмеричную систему счисления, преобразовав их предварительно в дробь: $(312,27)_{10}$, $(5025,41)_{10}$.

Индивидуальное задание № 1

Позиционные системы счисления

1. Выполните следующие действия в пятеричной системе счисления:

Вариант 1.

а) 203,01 + 3341,42; б) 2340 – 1211;

в) 413, 31 · 23,14; г) 421 / 23;

Вариант 2.

а) 4213 + 33213; б) 223,21 – 241,211;

в) 233,21 · 112,2; г) 220 / 12;

Вариант 3.

а) 110,32 + 243,02; б) 1332 – 1034;

в) 331,4 · 102,12; г) 202 / 14;

Вариант 4.

а) 1123 + 1021; б) 2123,42 – 1402,11;

в) 210,23 · 22,13; г) 442 / 12;

Вариант 5.

а) 2031,2 + 1424,42; б) 1412 – 1323;

в) 203,41 · 21,42; г) 341 / 22;

Вариант 6.

а) 2044 + 20312; б) 1231,2 – 123,14;

в) 123,12 · 22,11; г) 343 / 24;

Вариант 7.

а) 233,41 + 2012,33; б) 4123 – 2441;

в) 221,21 · 32,14; г) 231 / 41;

Вариант 8.

а) 22413 + 230; б) 423,41 – 404,31;

в) 141,23 · 10,23; г) 423 / 34;

Вариант 9.

а) 223,42 + 3140,01; б) 4314 – 3234;

в) 120,33 · 14,23; г) 320 / 44;

Вариант 10.

а) 23410 + 1424; б) 234,21 – 124,34;

в) 341,12 · 42,13; г) 231 / 12;

Вариант 11.

а) 3123,21 + 343,4; б) 2233 – 2134;

в) 302,34 · 14,22; г) 243 / 14;

Вариант 12.

а) 21234 + 2441; б) 2231,2 – 423,42;

в) 224,31 · 44,12; г) 131 / 14;

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.

Вариант 1. 45,78 и 72,59. **Вариант 7.** 37,67 и 56,65.

Вариант 2. 28,65 и 42,92. **Вариант 8.** 12,47 и 60,76.

Вариант 3. 44,18 и 84,23. **Вариант 9.** 57,68 и 17,96.

Вариант 4. 32,92 и 90,27. **Вариант 10.** 39,85 и 87,52.
Вариант 5. 76,39 и 47,28. **Вариант 11.** 98,03 и 52,85.
Вариант 6. 38,29 и 58,52. **Вариант 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.

Лабораторная работа № 4

Расширенный алгоритм Евклида. Коэффициенты Безу

Расширенный алгоритм Евклида базируется на следующем рекуррентном соотношении:

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

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

Пример.

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

Решение. Заполним таблицу 2.

Таблица 2

	q_1	u_1	v_1	r_1	u_{j+1}	v_{j+1}	r_{j+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

$u_2 = u_0 - q_1 u_1$ $u_3 = u_1 - q_2 u_2$ $u_4 = u_2 - q_3 u_3$

$v_2 = v_0 - q_1 v_1$ $v_3 = v_1 - q_2 v_2$ $v_4 = v_2 - q_3 v_3$

$r_2 = r_0 - q_1 r_0$ $r_3 = r_1 - q_2 r_2$ $r_4 = r_2 - q_3 r_3$

$u_2 = 1-1\cdot 0=1$ $u_3 = 0-4\cdot 1= -4$ $u_4 = 1-1\cdot (-4)=5$

$v_2 = 0-1\cdot 1= -1$ $v_3 = 1-4\cdot (-1)=5$ $v_4 = -1-1\cdot 5= -6$

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

$u = 5$, $v = -6$ НОД(a, b) = 6

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

1) 42 и 13 (найти обратный элемент);

2) 1824 и 852;

3) 694 и 418.

Самостоятельно:

Найти наибольший общий делитель и коэффициенты Безу следующих чисел:

1) 84 и 36; 76 и 17 (обратить класс 76 в Z/17)

2) 91 и 52; 72 и 19 (обратить класс 19 в Z/72)

Индивидуальное задание № 2

Расширенный алгоритм Евклида

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

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

2. Найти обратные элементы, если они существуют.

Вариант 1. Найти обратный элемент к 528 по mod 247.

Вариант 2. Найти обратный элемент к 749 по mod 316.

Вариант 3. Найти обратный элемент к 692 по mod 293.

Вариант 4. Найти обратный элемент к 724 по mod 381.

Вариант 5. Найти обратный элемент к 815 по mod 223.

Вариант 6. Найти обратный элемент к 833 по mod 213.

Вариант 7. Найти обратный элемент к 539по mod 171.

Вариант 8. Найти обратный элемент к 528 по mod 247.

Вариант 9. Найти обратный элемент к 943 по mod 277.

Вариант 10. Найти обратный элемент к 539по mod 171.

Вариант 11. Найти обратный элемент к 926 по mod 357.

Вариант 12. Найти обратный элемент к 573по mod 169.

Лабораторная работа №5

Вычисление НОД

1. **Вычисление НОД с использованием канонического разложения чисел на простые множители.**

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

Задание 1. Найти НОД чисел 24 и 35, 24 и 36, 35 и 72.

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

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

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

Получим следующую последовательность действий для вычисления произведения:

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

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

Задание 3.

1) $\frac{15}{28}\cdot\frac{21}{35}$, вычислять НОД 1 способом;

2) $\frac{25}{28}\cdot\frac{12}{45}$, вычислять НОД, используя алгоритм Евклида.

b) Требуется найти сумму

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

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

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

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

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

Задание 4.

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

2) $\frac{18}{24}+\frac{16}{30}$;

3) $\frac{14}{35}+\frac{20}{42}$.

Индивидуальное задание № 3

Вычисление НОД целых чисел

1. Найти наибольший общий делитель, используя теорему 11 п.3.1.

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

2. Найти наибольший общий делитель, используя алгоритм Евклида.

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

3. **Вычисления с дробями**.

Сложение	**Умножение**
Вариант 1. $\frac{106}{24}+\frac{18}{140}$	**Вариант 1**. $\frac{102}{224}\cdot\frac{216}{80}$
Вариант 2. $\frac{24}{128}+\frac{116}{32}$	**Вариант 2**. $\frac{72}{224}\cdot\frac{52}{134}$
Вариант 3. $\frac{28}{124}+\frac{132}{40}$	**Вариант 3**. $\frac{42}{88}\cdot\frac{128}{242}$

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

Лабораторная работа № 6

Модулярная арифметика

Перемножим два больших числа a и b. Для этого:

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

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

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

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

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

Пример.

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

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

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

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

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

3. Восстановим число x.

4. Вычислим z_1, z_2, z_3, z_4.

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

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

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

Таблица 3

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

u=1 v=-2 1=7·1 + 3·(-2)

c_2=-2 $\Rightarrow c_2$=5

z_2=5·(-1) mod 7=-5 mod 7=2

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

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

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

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

c_3 –обратное к 21 по модулю 11 (см. таблицу 4).

Таблица 4

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

u=-1 v=3 21 · (-1) + 11 · 2 = 1

c_3 = -1$\Rightarrow$ c_3 = 10

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

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

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

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

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

c_4 – обратное к 231 по модулю17 (см. таблицу 5).

Таблица 5

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

u = -5 v = 68 1 = 231 · (-5) + 17· 68

$c_4 = -5 \Rightarrow c_4 = 12$

5. Определим последнюю цифру числа.

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

$= (z_1 + z_2 \cdot n_1 + z_3 \cdot n_1 \cdot n_2 + z_4 \cdot n_1 \cdot n_2 \cdot n_3) \bmod 10$

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

$= 20 \bmod 10 = 0$

$x_0 = 0$

6. Перейдем к определению следующей цифры.

Обратное к 10 по модулю n_1 равно1 ($10 \cdot y_1 \equiv 1(\text{mod } 3)$, обратное к 10 по модулю n_2 равно 5 ($10 \cdot y_2 \equiv 1(\text{mod } 7)$, обратное к 10 по модулю n_3 равно 10 ($10 \cdot y_3 \equiv 1(\text{mod } 11)$, обратное к 10 по модулю 17 равно 12 ($10 \cdot y_4 \equiv 1(\text{mod } 17)$. Т.е. $y_1=1$, $y_2=5$, $y_3=10$, $y_4=12$.

Определяем модулярные компоненты числа.

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

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

7. Определим предпоследнюю цифру числа.

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

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

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

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

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

См. таблицу 1.

$c_2 = 5$

$z_2 = -5 \bmod 7 = 2$

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

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

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

См. таблицу 2.

$c_3 = -1 \Rightarrow c_3 = 10$

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

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

$= 12 \cdot (-187) \bmod 17 = 0$

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

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

См. таблицу 3.

$c_4 = 12$

$x^{(2)} = (z_1 \cdot N_1 + z_2 \cdot N_2 + z_3 \cdot N_3 + z_4 \cdot N4) \bmod 10 = (z1 + z_2 \cdot n_1 + z_3 \cdot \cdot n_1 \cdot n_2 + z_4 \cdot n_1 \cdot n_2 \cdot n_3) \bmod 10$

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

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.

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

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

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

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

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

См. таблицу 1.

$c_2 = 5$

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

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

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

См. таблицу 2.

$c_3 = -1 \Rightarrow c_3 = 10$

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

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

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

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

Найдем модулярное представление числа по формуле

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

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

$x_0=9$

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

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

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.

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

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

$x_0=1$

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

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

Модулярное представление равно нулю, следовательно, вычисление закончено.

Получили число 1960.

Задание. Найти произведение чисел 62 и 48, используя модулярную арифметику.

Индивидуальное задание № 4

Модулярная арифметика

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

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

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

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

Лабораторная работа № 7

Разложение на множители

1. Деление и разложение на множители.

Если число n>1, то его можно делить на последовательные простые числа p = 2, 3, 5, …, до тех пор, пока не будет найдено наименьшее p для которого n mod p = 0. Тогда p будет наименьшим простым множителем числа n. Ту же процедуру можно применить к n/p, взяв его за новое значение n, - пробовать разделить это новое значение числа n на p и его большие простые числа. Из теоремы 10 следует,

что это действие необходимо выполнять пока $p \le \sqrt{n}$. Отметим, что мы должны обладать вспомогательной последовательностью пробных делителей $2 = d_0 < d_1 < d_2 < d_3 <, \dots$, которая включает в себя все простые числа $\le \sqrt{n}$. Ниже приведена процедура, реализующая данный метод.

Задание 1.

1) n=78;

2) n=56;

3) n=92.

2**.** Метод Ферма.

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

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

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

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

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

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

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

Задание 2.

1) 678;

2) 1045;

3) 835.

3. Вероятностный метод.

a) 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

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

2. Положим $a_0 = a$ и затем для i = 1, …, 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

$$a_i \equiv a^{d_0 2' + \ldots + d_1} \pmod m,$$

легко доказываемого индукцией по i.

Задание 3.

1) a= 3; d=7; m=15;

2) a= 4; d=6; m=13;

3) a= 7; d=3; m=6.

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 НОД(a,n)=1 хотя бы одна из скобок в произведении

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

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, $0 \le k < s$, 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 $\frac{3}{4}(n-1)$.

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

1. Выберем случайным образом число a, $1<a<n$, и проверим для этого числа указанные выше свойства 1) и 2).

2. Если хотя бы одно из них нарушается, то число n составное.

3. Если выполнены оба условия 1) и 2), возвращаемся к шагу 1.

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

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

1) 68;

2) 1125;

3) 197;

3) 83.

Индивидуальное задание № 5

Разложение на множители

1. Разложить на множители числа, используя метод Ферма, метод деления и разложения на множители.

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

2. Разложить на множители числа, используя вероятностный метод.

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

Вопросы к модулю 2

1. Какая алгебра называется кольцом целых чисел?
2. Какие числа называются сравнимыми по модулю m?
3. Что является классами вычетов по модулю m
4. Перечислить свойства классов вычетов по модулю m?
5. Что является полной системой вычетов по модулю m?
6. Какие числа называются взаимно – обратными?
7. Сформулировать китайскую теорему об остатках.
8. В чем состоит принцип модулярного исчисления?
9. Какое число называется простым?
10. Какие числа называются взаимно-простыми?
11. Записать соотношение Безу.
12. Сформулировать основную теорему арифметики?
13. Какое представление целого числа называется его каноническим разложением?
14. В чем состоит метод составления таблицы простых чисел, известный под названием «Решето Эратосфена»?
15. Какой делитель двух чисел a и в называется наибольшим общим делителем?
16. В чем суть алгоритма Евклида?
17. Чему равно число итераций, необходимых для вычисления НОД?
18. Как записывается число в позиционной системе счисления?
19. Как осуществляются переводы из одной позиционной системы счисления в другую?
20. Какой элемент является единицей коммутативного кольца?
21. Что является мультипликативной группой?
22. Какой элемент называется неприводимым?
23. Привести методы разложения на множители.
24. Как сравнить два числа, зная только их модулярные компоненты?

Модуль 3. Полиномы от одной переменной

Лабораторная работа № 8

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 .

1) n=78;

2) n=56;

3) n=92.

2. Метод множителей.

Рассмотрим метод множителей, когда значение n известно заранее. Если n=p*q, где p – наименьший простой множитель числа n и q›1, то для вычисления x^n мы можем

сначала вычислить x^p, а затем возвести это число в степень q. В случае, когда n простое, мы можем вычислить сначала число x^{n-1}, а затем умножить его на x. Многократное применение этих правил дает нам процедуру вычисления x^n для любого данного n.

Пример. Пусть мы хотим вычислить x^{55}. Вычисляем сначала $y = x^5 = x^4x = (x^2)^2x$, а затем находим $y^{11} = y^{10}y = (y^2)^5y$. Весь процесс вычисления использует восемь умножений, в то время как бинарный метод потребовал бы девяти. В среднем метод множителей лучше бинарного, но встречаются случаи (начиная с n = 33), когда более экономным оказывается бинарный метод.

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

1) n = 78;

2) n = 145;

3) n = 236.

3. Схема Горнера.

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

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

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) $f(x) = 11x^6 - 5x^5 - 7x^4 + 2x^3 - 8$, при x = 2;

3) $f(x) = ax^4 + bx^3 + cx + d$

4. Обобщение схемы Горнера.

Позволяет вычислить сразу как полином, так и его производную

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

Это удобно сделать, положив

$c_0 = a_n$, $b_0 = 0$

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

Здесь $c_n = f(x)$ и $b_n = f'(x)$.

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.

Вариант №1 n=65, n=87	Вариант №7 n=81, n=75
Вариант №2 n=98, n=118	Вариант №8 n=90, n=67
Вариант №3 n=76, n=89	Вариант №9 n=103, n=71
Вариант №4 n=77, n=123	Вариант №10 n=85, n=94
Вариант №5 n=69, n=93	Вариант №11 n=79, n=101
Вариант №6 n=82, n=104	Вариант №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.

Вариант № 1 $f(x)=5x^6-5x^5-7x^4+2x^3-8$

Вариант № 2 $f(x)=2x^6+4x^5-9x^4+2x^2-2$
Вариант № 3 $f(x)=4x^6-5x^5-2x^4+2x^3-1$
Вариант № 4 $f(x)=-2x^6-3x^5+5x^4+2x^3$
Вариант № 5 $f(x)=7x^6+8x^5+x^4+2x^3-5$
Вариант № 6 $f(x)=3x^6+x^5+2x^4+7$
Вариант № 7 $f(x)=5x^6-2x^5-3x^4+2x^3+2$
Вариант № 8 $f(x)=7x^6+9x^5+6x^4+2x^3+9$
Вариант № 9 $f(x)=x^6-4x^5-7x^4+2x^3$
Вариант № 10 $f(x)=5x^5-x^4+2x^3+3x^2-3$
Вариант № 11 $f(x)=4x^5-8x^4+2x^3-6x^2+1$
Вариант № 12 $f(x)=x^6+x^5+5x^4+2x^3+6$

3. **Обобщение схемы Горнера**.

Вычислить полиномы и их производную при x=3.

Вариант № 1 $f(x)=2x^6+4x^5-9x^4-x^2-2$
Вариант № 2 $f(x)=3x^6+x^5-x^4+4x$
Вариант № 3 $f(x)=2x^6-3x^5-4x^4-x^3-8$
Вариант № 4 $f(x)=4x^6+9x^5+6x^4-x^3+9$
Вариант № 3 $f(x)= -4x^6+8x^5+x^4-x^3-3$
Вариант № 6 $f(x)=x^7-4x^6-3x^5-2x^4-x^3-1$
Вариант № 4 $f(x)=3x^6-2x^5-3x^4-x^3-$
Вариант № 8 $f(x)= -x^6+x^5+3x^4-x^3+6$
Вариант № 9 $f(x)= 2x^7+x^6-4x^5-4x^4-x^3$
Вариант № 10 $f(x)=3x^5-x^4-x^3+3x^2-3$
Вариант № 11 $f(x)=4x^5-8x^4-x^3-6x^2+1$
Вариант № 12 $f(x)=x^6+8x^5+4x^4-x^3-2$

Лабораторная работа № 9

Нахождение НОД полиномов

Для вычисления НОД полиномов воспользуемся алгоритмом:

M:=*граница_Ландау_Миньотта (A, B)*

цикл до бесконечности

p:=*найти_большое_простое (2M);*

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

то C:=*модулярный НОД (A, B, p);*

если *делит (C, A)* и *делит (C, B)*

то выход *C*;

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

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

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

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

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

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

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

Для наших полиномов:

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

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

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

Выполним деление полиномов по модулю 7.

$$\_x^8 + 2x^6 - x^5 + 4x^3 - 6x^2 \mid x^6 + 2x^4 + 4x - 4$$

$$-6x^8 - 12x^6 - 24x^3 + 24x^2 \quad -6x^2$$

$$7x^8 + 14x^6 - x^5 + 28x^3 - 30x^2$$

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

$$\_x^6 + 2x^4 + 4x - 4 \mid 6x^5 + 5x^2$$

$$36x^6 + 30x^3 \quad 6x$$

$$-35x^6 + 2x^4 - 30x^3 + 4x - 4$$

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

$$\_6x^5 + 5x^2 \mid 2x^4 + 5x^3 + 4 - 4$$

$$-8x^5 - 20x^4 - 16x^2 + 16x \quad -4x$$

$$14x^5 + 20x^4 + 21x^2 - 16x$$

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

$$\_6x^4 + 5x \mid 2x^4 + 5x^3 + 4 - 4$$

$$-8x^4 - 20x^3 - 16x + 16 \quad - 4$$

$$14x^4 + 20x^3 + 21x - 16$$

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

$$\_2x^4 + 5x^3 + 4x - 4 \mid 6x^3 + 5$$

$$-12x^4 - 10x \quad -2x$$

$$14x^4 + 5x^3 + 14x - 4$$

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

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

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

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

НОД(A(x), B(x)) = x^3+2

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

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

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

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 7.

1. A[x]:=3*x^8+2*x^7+2*x^6+6*x^5-x^4+4*x^3,
   B[x]:=2*x^6-x^5+5*x^4-x^3+x^2-2
2. A[x]:= x^8-x^7-3*x^6-x^5,
   B[x]:=2*x^7+2*x^6+2*x^4+2*x^3-x-1
3. A[x]:=x^8-2*x^7-6*x^5+3*x^6-x^2-3,
   B[x]:=2*x^6+3*x^4+x^3-10*x^2+3*x-3
4. B[x]:=3*x^8-6*x^7+2*x^6-4*x^5-4*x^4+8*x^3,
   A[x]:=2*x^6-2*x^5-6*x^4+4*x^3-x+2
5. B[x]:=2*x^8+6*x^7+x^6+x^5-6*x^4-2*x-6,
   A[x]:=x^7+x^6-6*x^5+3*x^4+9*x^3
6. T[x]:=x^8-2*x^7-2*x^6+4*x^5+2*x^4-4*x^3-x-2,
   F[x]:= 2*x^5-5*x^4+2*x^3-2*x^2-4*x
7. K[x]:=2*x^8-x^7+6*x^6-x^2+3*x,
   L[x]:=x^6-x^5-7*x^4+3*x^3+x-3
8. L[x]:=2*x^8-5*x^7+x^6+2*x^5-x^2+x,

K[x]:=x^7-3*x^6+2*x^5-x^3+x^2-2*x+2

9. K[x]:=x^8-x^4-x^3-x^2,
   A[x]:=2*x^7-2*x^6-2*x^5+2*x^4-3*x^2+3
10. B[x]:=x^7-4*x^5+3*x^3+6*x^2-2*x-4,
    A[x]:=2*x^5+3*x^4+x^3+6*x^2-2*x-4
11. A[x]:=x^7+x^6-6*x^5+3*x^3+9*x^2-2*x-6,
    F[x]:=2*x^5+5*x^4+9*x^2-2*x-6
12. T[x]:=x^8-2*x^7+3*x^6-6*x^5+3*x^4-2*x^3+9*x^2-6*x,
    A[x]:= 2*x^6-x^5+9*x^4-3*x^3+8*x^2-3

2. Выполнить деление по модулю 5.

1. T[x]:=x^7+x^6-6*x^5+3*x^3+9*x^2-2*x-6,
   F[x]:=2*x^5+5*x^4+9*x^2-2*x-6
2. B[x]:=2*x^8-5*x^7+x^6+2*x^5-x^2+x,
   K[x]:=x^7-3*x^6+2*x^5-x^3+x^2-2*x+2
3. A[x]:=2*x^8-x^7+6*x^6-x^2+3*x,
   B[x]:=x^6-x^5-7*x^4+3*x^3+x-3
4. L[x]:=x^8-2*x^7+3*x^6-6*x^5+3*x^4-2*x^3+9*x^2-6*x,
   A[x]:= 2*x^6-x^5+9*x^4-3*x^3+8*x^2-3
5. F[x]:=x^8-2*x^7+2*x^6-4*x^5+3*x^4+4*x^2-4,
   T[x]:=2*x^6-x^5+7*x^4-3*x^3+6*x^2-2*x
6. B[x]:=x^7-3*x^6+2*x^5+3*x^3-6*x^2-x+2,
   T[x]:=2*x^6-4*x^5+x^4+x^3-9*x^2+6*x
7. K[x]:=2*x^7-7*x^6+3*x^5+3*x^3-9*x^2,
   L[x]:=x^6-3*x^5+x^4-9*x^2-3*x+9
8. A[x]:=x^8-2*x^7-6*x^5+3*x^6-x^2-3,
   B[x]:=2*x^6+3*x^4+x^3-10*x^2+3*x-3
9. K[x]:= x^8-x^7-3*x^6-x^5,
   B[x]:=2*x^7+2*x^6+2*x^4+2*x^3-x-1
10. L[x]:=3*x^8+2*x^7+2*x^6+6*x^5-x^4+4*x^3,

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

11. K[x]:=x^8-x^4-x^3-x^2,
    A[x]:=2*x^7-2*x^6-2*x^5+2*x^4-3*x^2+3
12. K[x]:=x^7-4*x^5+3*x^3+6*x^2-2*x-4,
    A[x]:=2*x^5+3*x^4+x^3+6*x^2-2*x-4

Лабораторная работа № 10

Работа с полиномами от одной переменной в системе Matematica

1. Основные операции над полиномами.

Над полиномами можно выполнять обычные операции сложения, вычитания, умножения и деления. Для получения результата умножения используется функция Expand. Если полиномы делятся друг на друга, то применяется операция Simplify.

Пример.

```
(x^3+2*x^2+3*x+4) - (x^2-1)
Simplify[(x^5+2*x^4+2*x^3+2*x^2-3*x-4) / (x^2-1)]
```

Задание 1.

Выполнить операции сложения, вычитания, умножения и деления для полиномов:

p1:=x^3+2*x^2+3*x+4; p2:=x^2-1

2. Разложение полиномов.

Factor[poly] – выполняет разложение полинома над целыми числами;

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

FactorInteger[n] – возвращает список простых множителей числа n вместе с их показателями степени.

FactorList[poly] – возвращает список множителей полинома с их показателями степени.

Пример.

A[x]: = x ^ 3 – 6 * x ^ 2 + 11 * x - 6

Factor[A[x]]

A[x]: = x ^ 3 – 6 * x ^ 2 + 11 * x - 6

Factor[A[x],Modulus->3]

FactorInteger[1234554367]

{{83,1},{601,1},{24749,1}}

FactorList[A[x]]

Задание 2.

Даны два полинома:

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

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

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

Factor[F[x]]

Factor[T[x], Modulus->5] и др.

2) Получить список простых множителей числа 45541124367.

3) Получить список множителей полиномов T[x] и A[x] с их показателями степени.

3. Функции для работы с полиномами.

Decompose[poly, x] – выполняет разложение полинома на более простые полиномиальные множители;

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

PolynomialGCD[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]
T[x]:=2*x^3-6*x^2+4*x-6
K[x]:=x^2+3*x+2
PolynomialRemainder[T[x],K[x],x]
18+36x
K[x]:=x^2+3*x+2
L[x]:=36*x+18
PolynomialRemainder[K[x],L[x],x]
```

$\frac{3}{4}$

Задание 3.

Даны два полинома:

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

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

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

Задание 4.

Открыть справку (Help → Help Browser). Найти следующие функции:

FactorTerms, FactorTermsList, FactorSquareFree, FatorSquareFreeList; PolynomialMod, PolynomialQuotient, PolynomialLCM, Resultant.

Описать их и привести примеры. Оформить файл в Word.

Задание 5.

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

1) F(x) = x^7-3 x^6+2 x^5-2 x^3+2 x^2
   T(x) = 2 x^6-2 x^5-x^4+x^3+2 x-2
2) K(x) = x^8-2 x^7+2 x^6-6 x^5-3 x^4-2 x^2-6
   L(x) = 2 x^6+x^5=6 x^4+2 x^3-3 x

Индивидуальное задание № 8

Пакет Mathematica. Работа с полиномами от одной переменной

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). Оформить файл в MS Word.

Вариант 1. A[x]:=2*x^8-x^7+6*x^6-x^2+3*x,
B[x]:=x^6-x^5-7*x^4+3*x^3+x-3.

Вариант 2. B[x]:=2*x^8-5*x^7+x^6+2*x^5-x^2+x,
K[x]:=x^7-3*x^6+2*x^5-x^3+x^2-2*x+2.

Вариант 3. T[x]:=x^7+x^6-6*x^5+3*x^3+9*x^2-2*x-6,
F[x]:=2*x^5+5*x^4+9*x^2-2*x-6.

Вариант 4. L[x]:=x^8-2*x^7+3*x^6-6*x^5+3*x^4-2*x^^3+9*x^2-6*x,
A[x]:= 2*x^6-x^5+9*x^4-3*x^3+8*x^2-3.

Вариант 5. F[x]:=x^8-2*x^7+2*x^6-4*x^5+3*x^4+4*x^2-4,
T[x]:=2*x^6-x^5+7*x^4-3*x^3+6*x^2-2*x.

Вариант 6. B[x]:=x^7-3*x^6+2*x^5+3*x^3-6*x^2-x+2,
T[x]:=2*x^6-4*x^5+x^4+x^3-9*x^2+6*x.

Вариант 7. K[x]:=2*x^7-7*x^6+3*x^5+3*x^3-9*x^2,
L[x]:=x^6-3*x^5+x^4-9*x^2-3*x+9.

Вариант 8. L[x]:=3*x^8+2*x^7+2*x^6+6*x^5-x^4+4*x^3,
B[x]:=2*x^6-x^5+5*x^4-x^3+x^2-2.

Вариант 9. K[x]:= x^8-x^7-3*x^6-x^5,
B[x]:=2*x^7+2*x^6+2*x^4+2*x^3-x-1.

Вариант 10. A[x]:=x^8-2*x^7-6*x^5+3*x^6-x^2-3,
B[x]:=2*x^6+3*x^4+x^3-10*x^2+3*x-3.

Вариант 11. K[x]:=x^8-x^4-x^3-x^2,
A[x]:=2*x^7-2*x^6-2*x^5+2*x^4-3*x^2+3.

Вариант 12. K[x]:=x^7-4*x^5+3*x^3+6*x^2-2*x-4,
A[x]:=2*x^5+3*x^4+x^3+6*x^2-2*x-4.

Вопросы к модулю 3

1. Какое кольцо называется простым расширением кольца, простым трансцендентным расширением кольца?

2. Что является степенью полинома, старшим коэффициентом полинома?

3. Какой полином называется нормированным? приводимым? неприводимым?

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

5. Что такое результант полиномов?

6. Какие существуют методы вычисления x^n?

7. Что называется аддитивной сложностью числа n?

8. Какой способ вычисления полиномов называется «Схемой Горнера»?

9. Как выполняется евклидово деление в поле?

10. Для чего используется неравенство Ландау-Миньотта?

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

Модуль 4. Полиномы от нескольких переменных. Формальное интегрирование и дифференцирование

Лабораторная работа № 11

Работа с полиномами от нескольких переменных в системе Mathematica

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)]

$-1 + x^{2000}$

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)]

$-2 + x^2$

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

2. Функции для работы с полиномами от нескольких переменных:

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

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

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

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

GroebnerBasis[{poly1,poly2,…},{x1,x2,…}] – возвращает список полиномов, которые образуют базис Гребнера 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]

$x^2 + 3xy + 4y^2$

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

$x - y$

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

$3x^2 - y$

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

$2 - 4y$

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

$2y - 3y^2$

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

$2x^2 - 3x^4$

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

0

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

0

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

True

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

$-z^2 + yz^2, -xyz + xy^2z, x^2z^2 - z^3, x^2yz - z^2, x^2y^2 - z$

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

$x - y$

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

$(x - y)^2$

Задание.

1) Проверить все примеры;

2) Для полиномов A[x], B[x] выполнить все возможные функции:

$A[x]:= 2x^3-x^7-x^6y-xy^2-y^3+x^4y^4-x^3y^5$

$B[x]:= 3x^2y-3y^3+x^5y^3-x^4y^4+2xy^5-2y^6$

3) **Самостоятельно:** Привести по 3 примера на каждую из выше перечисленных функций.

3. Нахождение наибольшего общего делителя с помощью функции PolynomialRemainder.

Пример.

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

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

PolynomialRemainder[F[x],T[x],x]

$-2x^2 + x^3$

PolynomialRemainder[T[x], $-2x^2 + x^3$, x]

$2 - 3x + x^2$

PolynomialRemainder[$-2x^2 + x^3$, $2 - 3x + x^2$, x]

–2 + x

PolynomialRemainder[2 – 3x + x^2, –2 + x, x]

0

PolynomialRemainder[F[x], x – 2, x]

0

PolynomialRemainder[T[x], x – 2, x]

0

PolynomialGCD[F[x], T[x]]

–2 + x

Задание.

1) Найти НОД полиномов, используя функцию PolynomialRemainder.

F[x]:= $x^7+x^6-4x^3-4x^2$

T[x]:= $-3x^6+x^4+12x^2-4$

Проверить правильность вычислений с помощью функции PolynomialGCD.

2) С помощью функции Expand подобрать полиномы и найти НОД с помощью функции PolynomialRemainder (для полиномов от одной и от нескольких переменных).

Практическое занятие № 12

Работа с простыми числами в пакете Mathematica

1. Загрузить подпакет функций теории чисел <<NumberTheory`NumberTheoryFunctions`

NextPrime[*n*] – дает наименьшее простое число, превосходящее n;

PreviousPrime[n] – дает наибольшее простое число, меньшее n;

Random[Prime, {min, max}] – возвращает простое число из интервала {min, max}.

Примеры:

PreviousPrime[34]

31

NextPrime[34]

37

Random[Prime, {10, 100}]

71

Задание 1:

1) Получить простые числа, близкие к 65, 346, 1235.

2) Получить не менее 5 простых чисел из интервала {100, 200}

PrimeFactorList[r] – дает список простых множителей r (factor – множитель);

LeastPrimeFactor[n] – дает наименьший простой множитель числа n;

PrimePowerQ[n] – определяет, является ли n степенью рационального простого числа;

Примеры:

PrimeFactorList[713]

{23, 41}

LeastPrimeFactor[713]

23

PrimeFactorList[78/41]

{2,3,13,41}

PrimePowerQ[12167]

True

PrimeFactorList[12167]

{23}

PrimePowerQ[78]

False

PrimeFactorList[78]

{2,3,13}

Задание 2:

1) Проверить примеры для чисел 85, 241, 564, 1267.

2) Привести по два примера на каждую функцию.

ChineseRemainderTheorem[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:

ChineseRemainder[{0, 1, 2}, {4, 9, 121}]

244

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

{0,1,2}

Задание 3:

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.

2. Загрузить подпакет <<NumberTheory`PrimeQ`

ProvablePrimeQ[n] (PrimeQ[n]) – выдает true, если число n простое и false – если n составное;

PrimeQCertificate[n] – выдает свидетельство того, что n является простым или составным/

Сертификат определения простоты для больших n в этом подпакете основан на теории эллиптических кривых. Данная идея была предложена С. Голдвассером и Дж. Килианом.

PrimeQCertificateCheck[cert,n] – проверяет, что сертификат cert доказывает простоту или не простоту n.

Примеры:

```
PrimeQ[127]
True
ProvablePrimeQ[127]
True
PrimeQCertificate[127]
{127,3,{2,{3,2,{2}},{7,3,{2,{3,2,{2}}}}}}
PrimeQCertificate[1093 * 3511]
{2,3837522,3837523}
PrimeQCertificateCheck[%, 3837523]
True
```

Задание 4:

1) Проверить примеры для чисел 913, 1093, 12167.

2) Привести по два примера на каждую функцию.

Индивидуальное задание № 9

Пакет Mathematica. Работа с полиномами от нескольких переменных

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

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

Практическое занятие № 13

Интегрирование и дифференцирование в системе Mathematica

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,…] [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*Cos[x],x]

-a Sin[x]

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

$b + 3\,b\,x^2$

D[Log[x]*x^2,x]

x + 2 x Log[x]

D[x^2/b*x,x]

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

Derivative[2] [x*y]

(x y)''

Самостоятельно: вычислить производную функций:

1. $5\sqrt{x} * e^{x}$.
2. $e^{\sqrt{3+x}}$, ln(sin(x0)).
3. $0.5^{1+\sin(x)}$, sin(ln(x)).

4. $\sqrt[3]{\sin(x)}$, $\sqrt[3]{\log_2(x)}$.

5. $\frac{\sqrt{3x}}{3^x+1}$, $\frac{5^{2x}}{\sin(3x)+7}$.

6. $\frac{2^x-\log_2(x)}{\ln(2)*x}$.

7. $\frac{1-\sin(2x)}{\sin(x)-\cos(x)}$.

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]

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

∫a*x^b dx

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

∫Sin[x] dx

- Cos[x]

∫1/(1-(Sin[x])^2) dx

$$\frac{Cos[x]\ Sin[x]}{1-Sin[x]^2}$$

$$\int \frac{\mathbf{Sin[x]}}{\mathbf{x}}\mathbf{dx}$$

SinIntegral[x]

Самостоятельно:

1. Вычислить интегралы:

$$\int \frac{1}{z-\sqrt{3x}}dx, \quad \int \frac{1}{a^2+x^2}dx$$

$$\int \frac{1}{\sqrt{9x^2+4}}dx, \int ye^{a+y}\,dy.$$

$$\int (x^a+\frac{\sin[x]}{x}dx.$$

2. Найти интегралы от рациональных дробей:

$$\int \frac{9x^8+6x^2+5}{x^9+2x^3+5x}dx, \int \frac{5x^4+1}{(x^5+x+1)\text{^}2}dx.$$

3. Привести по два примера вычисления интегралов (алгебраических, тригонометрических функций и рациональных дробей).

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 · q, вычисляем = (p - 1) · · (q - 1). (Рекомендуется, чтобы длина n составляла 1024 бита).

2. Выбираем целое число e, чтобы e < φ(n), НОД(e, φ(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 · q = 527 и φ(n) = = (p - 1) · (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 соответствует $19 = (10011)_2$, A соответствует $1 = (00001)_2$. Тогда RSA в двоичном представлении RSA – 100101001100001. Укладываясь в заданный отрезок [0, 526], получим два двоичных числа: (100101001), (100001). То есть, $M_1 = 297$, $M_2 = 33$.

Далее последовательно шифруем M_1 и M_2:

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

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

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

Произведем расшифрование. Для этого вычислим D_1 и D_2.

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

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

Возвращаясь к буквенной записи, получаем после расшифрования аббревиатуру RSA.

Задание 1. Зашифровать инициалы PGB, используя p=13, q=29 (e=11).

Задание 2. Зашифровать свои инициалы.

Самостоятельно: зашифровать любую аббревиатуру.

Индивидуальная работа № 10

Криптография. Система RSA

1. Зашифровать следующие аббревиатуры, используя систему RSA:

Вариант 1
ASD (p=13, q=73)

Вариант 2
FOP (p=17, q=61)

Вариант 3
TIR (p=23, q=67)

Вариант 4
DGA (p=13, q=71)

Вариант 5
PTE (p=19, q=47)

Вариант 6
SPO (p=11, q=71)

Вариант 7
KOL (p=19, q=61)

Вариант 8
QFI (p=23, q=89)

Вариант 9
GYZ (p=7, q=47)

Вариант 10
PON (p=19, q=53)

Вариант 11
RET (p=17, q=59)

Вариант 12
RUS (p=21, q=41)

2. Зашифровать свои инициалы (p, q взять отличные от задания 1).

3. Расшифровать сообщение (+0.2 балла).

Вариант 1
C_1 = 77 n=221
C_2 = 118 e=7

Вариант 2
C_1 = 44 n=527
C_2 = 37 e=7

Вариант 3
C_1 = 86 n=377
C_2 = 64 e=11

Вариант 4
C_1=179 n=253
C_2 = 80 e=7

Вариант 5
C_1 = 194 n=1147
C_2 = 659 e=7

Вариант 6
C_1=119 n=527
C_2 = 360 e=7

Вариант 7
C_1 = 459 n=703
C_2 = 37 e=5

Вариант 8
C_1 = 17 n=527
C_2 = 17 e=7

Вариант 9

C_1 = 261 n=713

C_2 = 23 e=7

Вариант 10

C_1=153 n=209

C_2 = 43 e=13

Вариант 11

Вариант 12

Вопросы к модулю 4

1. Какое кольцо называется m-кратным расширением кольца **K**?

2. Какие элементы кольца называются алгебраически – независимыми?

3. Дать определение m-кратного трансцендентного расширения кольца?

4. Что собой представляем кольцо полиномов?

5. Что такое «моном»?

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

7. Чем отличается рекурсивная форма записи полиномов от распределенной?

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

9. Какая система образующих называется стандартным базисом?

10. Как вычислить базис Гребнера?

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

12. Какой полином называется примитивным?

13. Сформулировать лемму Гаусса.

14. Как вычислить НОД двух полиномов от нескольких переменных?

15. Какой элемент a поля F называется алгебраическим?

16. Какое расширение F поля P называется конечным? алгебраическим?

17. Является ли дифференцирование алгоритмической процедурой?

18. В чем заключается алгоритмическая трудность вычисления неопределенных интегралов?

19. Сформулировать задачу интегрирования.

20. В каких классах не разрешима проблема интегрирования?

21. В чем состоит задача интегрирования рациональных функций?

22. Какие недостатки имеет прямой метод интегрирования рациональных функций?

23. Как доказать, что дробь можно разложить на простейшие дроби?

24. В чем заключается метод Эрмита интегрирования рациональных функций?

25. В чем заключается метод Горвица интегрирования рациональных функций?

26. Как осуществляется обработка логарифмической части при интегрировании рациональных функций?

27. Какая функция называется элементарной над K (K – функциональное поле)?

28. Сформулировать принцип Лиувилля.

Тестовые задания

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

1) численные методы;

2) прямой перебор;

3) аналитические вычисления.

2. Сущность аналитических вычислений заключается:

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

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

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

3. В чем состоит особенность систем компьютерной алгебры?

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

2) нет верного ответа.

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

1) да;

2) нет.

5. Какая основная задача компьютерной алгебры?

1) изучение алгебры с помощью компьютера;

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

3) получение результата с использованием аппарата алгебры.

6. Какая из систем относится к системам компьютерной алгебры?

1) Statistica;
2) MathCAD;
3) Macromedia.

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

1) p=a·c, q=d·b;
2) p=a+c, q=b+d;
3) p=ad+bc, q=bd.

8. Поставить в соответствие алгоритмам порядок их сложности:

1) базовые алгоритмические операции;
2) скалярные алгоритмы;
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 mod 10=5;
2) 7 mod 10=7, в следующий разряд переносим 8 mod 10=0;
3) в следующий разряд переносим 15 div 10=1.

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

1) каноническим;
2) разреженным;

3) плотным;

4) нормальным.

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

1) каноническим;

2) разреженным;

3) плотным;

4) нормальным.

12. Какой из классов функций не относятся к трансцендентным?

1) тригонометрических;

2) рациональных;

3) экспоненциальных.

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

1) трансцендентной функцией;

2) рациональной функцией;

3) алгебраической функцией.

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

1) простых радикалов;

2) вложенных радикалов;

3) общих алгебраических выражений.

15. Классы каких функций относятся к трансцендентным?

1) алгебраических;

2) рациональных;

3) экспоненциальных.

16. Проблема однозначности представления возникает при работе:

1) с рациональными функциями;

2) с трансцендентными функциями;

3) с алгебраическими объектами.

17. Теорема Риша применима только к функциям?

1) да;

2) нет.

18. Как оценивается качество любого алгоритма?

1) по длине кода;

2) по количеству подпрограмм;

3) по изменению функции, которая характеризует рост времени.

19. Барейс предложил семейство методов исключения для матриц:

1) с использованием рядов;

2) без использования дробей;

3) на основе канонического разложения.

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

1) $O(n)$;

2) $O(n^2)$;

3) $O(n^3)$.

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

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

2) a=br+q, 0≤r<b;

3) a=bq.

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

1) простое;

2) составное;

3) ассоциированное;

4) взаимно простое.

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

1) a|b, b|a;

2) их наибольший общий делитель равен 1;

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

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

1) $2*3^2$;

2) 2^4*3;

3) 2^2*3^3;

4) 2^2*3.

25. Дан алгоритм Евклида.

```
   begin
repeat
   r:=a mod b; a:=b; b:=r
until b=0;
qcd:=a
   end;
```

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

1) 1;

2) 2;

3) 3;

4) 4.

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

1) <30%;

2) >60%;

3) <60%.

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

1) сравнимыми по модулю m;

2) взаимно обратными по модулю m;

3) ассоциированными.

28. Объединение всех классов вычетов по модулю m

1) называется системой наименьших вычетов по модулю m;

2) называется полной системой вычетов по модулю m;

3) совпадает с множеством целых чисел.

29. Любые два класса вычетов по модулю m пересекаются?

1) да;

2) нет.

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

1) 0;

2) 1;

3) 2.

31. Поставить в соответствие:

1) Полной системой вычетов по модулю m называют;

2) Системой наименьших неотрицательных вычетов по модулю m называют;

3) Классами вычетов по модулю m называют.

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

b) некоторые классы эквивалентности на множестве целых чисел;

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

32. Если ab=1(mod m), то числа a и b называются

1) простыми;

2) взаимно-простыми;

3) обратными;

4) ассоциированными.

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

1) алгоритм Евклида;

2) решето Эратосфена;

3) модулярное исчисление.

34. Из предложенных теорем выбрать теорему Евклида:

1) множество положительных простых чисел бесконечно;

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

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

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

1) простыми;

2) взаимно-простыми;

3) составными;

4) взаимно-обратными.

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

1) 4;

2) 7;

3) 103;

4) 180.

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

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

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

3) нет верного ответа.

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

1) записью в позиционной системе счисления;

2) каноническим разложением на простые 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) $n_1, n_2,\ldots, n_r$;
2) $z_1, z_2,\ldots, z_r$;
3) $y_1, y_2,\ldots, y_r$.

a) цифры числа x;

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

c) модулярные компоненты числа x;

d) попарно взаимно-простые числа.

42. Системой наименьших неотрицательных вычетов по модулю 6 является:

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

43. Поставить в соответствие.

1) $M=\{0,1,\ldots,Q-1\}$;
2) $A=(a_s, a_{s-1},\ldots, a_1)_Q$.

a) основание системы счисления;

b) смешанная система счисления;

c) цифры Q-ичной позиционной системы счисления;

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

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

1) 5;
2) 6;
3) 7;
4) 8.

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

1) 4;
2) 6;
3) 8.

46. Найти обратное к 5 по модулю 6.

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

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

1) простым расширением кольца **K** с помощью x;
2) простое трансцендентным расширением кольца **K** с помощью x;
3) нет верного ответа.

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

1) полиномом над полем **K;**
2) нормированным полиномом;
3) кольцом полиномов от x над **K.**

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

1) n;

2) a_0, a_1…,a_n;

3) a_n.

a) степень полинома;

b) коэффициенты полинома

c) старший коэффициент полинома

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

1) простым;

2) приводимым;

3) неприводимым.

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

1) неприводимым;

2) нормированным;

3) нет верного ответа.

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

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

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

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

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

1) SSXSSX;

2) SSSXSXX;

3) SXSSSX.

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

1) $x^2x^4x^5x^{10}\ x^{11}\ x^{22}$;
2) $x^2x^3x^6x^7\ x^{14}\ x^{15}$;
3) $x^2x^4x^8x^9\ x^{18}\ x^{19}$.

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

1) SXSXSX;
2) SXSXSS;
3) SSSXSX.

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

1) 5;
2) 6;
3) 8.

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

1) схема Горнера;
2) бинарный метод;
3) метод множителей.

58. Алгоритмом Евклида используется для:

1) вычисления полинома;
2) разложения на множители;
3) нахождения НОД двух полиномов.

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

1) содержанием полинома;

2) примитивной частью полинома;

3) нет верного ответа.

60. Неравенство Ландау-Миньотта позволяет:

1) оценить старшие коэффициенты полиномов;

2) найти границу для коэффициентов НОД двух полиномов;

3) определить количество итераций для вычисления НОД.

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

1) то c:=модулярный_НОД(a,b,p);

2) p:=найти_большое_простое (2*m);

3) m:=граница_Ландау_Миньотта (a,b);

4) то выход c;

5) цикл до бесконечности;

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

7) если делит (c,a) и делит (c,b);

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

1) простым;

2) составным;

3) приводимым.

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

1) 24;

2) 25;

3) 32.

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

1) приведенным;

2) примитивным;

3) нормированным.

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

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

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

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

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

1) коэффициенты полинома равны нулю;

2) полиномы имеют общий делитель положительной степени;

3) нет верного ответа.

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

1) да;

2) нет.

68. Переход от набора значений к его коэффициентам называется:

1) сверткой;

2) интерполяцией;

3) преобразованием Фурье.

69. Быстрый алгоритм интерполяции имеет сложность:

1) $O(n)$;

2) $O(n^2)$;

3) $O(n^3)$.

70. Поставить в соответствие шагам алгоритма их назначение:

1) вычисление значений;

2) интерполяция.

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

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

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

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

1) $w^n=1$;
2) $w^n=-1$;
3) $w=1$.

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

1) по теореме Парсеваля;
2) по теореме Планшереля;
3) по теореме о свертке.

73. Аббревиатура FFT – это:

1) дискретное преобразование Фурье;
2) быстрое преобразование Фурье;
3) нет верного ответа.

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

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

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

3) подкольцом кольца **L**.

75. Если для любых элементов $a_{(i)}$ кольца **K** из равенства $\sum_{(i)\in M} a_{(i)} x_1^{i_1} \ldots x_m^{i_m} = 0$, $M \in N^m$, следует равенство нулю всех коэффициентов $a_{(i)}$, то элементы $x_1,\ldots,x_m$ кольца **L** называются:

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

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

3) нет верного ответа.

76. Произведение степеней переменных это:

1) моном;

2) полином;

3) S-полином.

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

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

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

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

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

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

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

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

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

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

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

d) если элементы $x_1,\ldots,x_m$ 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/cont(p);
3) cont(p).

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

1) содержание полинома p;
2) примитивная часть полинома p;
3) НОД всех коэффициентов полинома p.

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

1) редуцированный полином;
2) S-полином полиномов p и q;
3) наименьшее общее кратное двух полиномов.

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

1) лемму Гаусса;
2) теорему Дирихле;

3) теорему Ламе.

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

1) лексикографическая;

2) общей степени, затем лексикографическая;

3) общей степени, затем обратная лексикографическая.

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

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

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

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

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

1) рекурсивной;

2) распределенной;

3) нет верного ответа.

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

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

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

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

91. Поставить в соответствие.

1) прямой метод;

2) метод Эрмита.

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

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

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

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

a) интегрирования;

b) дифференцирования;

c) нет верного ответа.

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

1) объектом множества B;

2) равным множеству B;

3) подмножеством множества B.

94. Символ $\subset$ называется знаком

1) принадлежности;

2) следствия;

3) включения;

4) тождественности.

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

Поставить в соответствие:

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

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

a) дополнение;

b) объединение;

c) пересечение;

d) разность.

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

1) / (разность);
2) \ (дополнение);
3) $\cap$ (пересечение);
4) $\cup$ (объединение).

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

1) U;
2) A;
3) Ø.

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

1) U;
2) A;
3) Ø.

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

1) симметричным;
2) рефлексивным;
3) транзитивным;
4) антисимметричным.

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

1) антирефлексивно, симметрично и транзитивно на А;

2) рефлексивно, симметрично и транзитивно на А;

3) рефлексивно, антисимметрично и транзитивно на А.

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

1) бинарной операцией;

2) прямым произведением;

3) нет верного ответа.

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

1) нейтральным;

2) симметричным;

3) регулярным.

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

1) сложение;

2) вычитание;

3) умножение;

4) пересечение;

5) объединение.

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

1) да;

2) нет.

105. Какое из множеств замкнуто относительно сложения и умножения?

1) четных чисел;

2) нечетных чисел;

3) нет верного ответа.

106. Какой тип имеет алгебра целых чисел ?

1) (2,1);
2) (2,0);
3) (2,2).

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

1) полем;
2) кольцом;
3) алгебраической системой;
4) нет верного ответа.

108. Если главные операции удовлетворяют условиям (аксиомам):

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

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

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

1) полем;
2) группой;
3) кольцом;
4) нет верного ответа.

109. Поставить в соответствие. Кольцо называется:

1) коммутативным;
2) нулевым;
3) областью целостности.

a) если $|\ \mathbf{K}\ | = \{0_K\}$;
b) если $a \cdot b = b \cdot a, \ \forall a, b \in K$;
c) если $a \neq 0, b \neq 0$ и $ab = 0$ или $ba = 0$;

 $0_K \neq 1_K$

d) если оно коммутативно, и $\forall a,b \in K\left(a \cdot b = 0 \to a = 0 \vee b = 0\right)$.

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

1) нулевым кольцом;
2) полем;
3) мультипликативным моноидом;
4) нет верного ответа.

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

1) поля;
2) кольца;
3) группы.

112. Поставить в соответствие. Умножение натуральных чисел:

1) ассоциативно;
2) коммутативно;
3) дистрибутивно.

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

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

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

ЗАКЛЮЧЕНИЕ

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

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

В практикуме представлены материалы для изучения курсов «Абстрактная и компьютерная алгебра», «Компьютерная алгебра» и «Теоретические основы информатики и современных информационных технологий».

Для организации самостоятельной работы студентов, обучающихся по направлениям «Педагогическое образование» и «Информационные системы и технологии», в пособии представлены индивидуальные задания и вопросы к тестам.

Пособие может быть использовано при обучении по программам бакалавриата и магистратуры. При изучении дисциплин «Абстрактная и компьютерная алгебра» и «Компьютерная алгебра» используется модульно-рейтинговая система контроля знаний студентов. В приложении приведен пример оценки сформированности компетенций по указанным дисциплинам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аладьев, В.З. Системы компьютерной алгебры Maple: искусство программирования [Текст] /В. З. Аладьев. – М.: Лаб. Базовых Знаний, 2006.
2. Ахо, А. Построение и анализ вычислительных алгоритмов [Текст] /А.Ахо, Дж. Хопкрофт, Дж. Ульман. – М.: Мир, 1979.
3. Бабаш, А.В. Криптография /А.В. Бабаш, Г.П. Шанкин; ред. В.П. Шерстюк, Э.А. Применко. – М.: СОЛОН-ПРЕСС, 2007
4. Бухбергер, Б. Компьютерная алгебра: символьные и алгебраические вычисления [Текст]. – М.: Мир, 1986.
5. Дьяконов, В.П. Mathematica 5/6/7. Полное руководство [Текст]. – М.: ДМК Пресс, 2010.
6. Дэвенпорт, Д. Компьютерная алгебра: Системы и алгоритмы алгебраич. вычислений [Текст] / Дж. Дэвенпорт, И. Сирэ, Э. Турнье; пер. с фр. Е.В. Панкратьева и др. – М.: Мир, 1991
7. Кристалинский, Р.Е. Преобразования Фурье и Лапласа в системах компьютерной математики: учеб. для вузов [Текст] / Р.Е. Кристалинский, В.Р. Кристалинский. – М.: Горячая линия: Телеком, 2006.
8. Кокс, Д. Идеалы, многообразия и алгоритмы [Текст] / Д. Кокс, Дж. Литтл, Д. О'Ши. – М.: Мир, 2000.
9. Кормен, Т. Алгоритмы: построение и анализ [Текст] / Т. Кормен, Ч. Лейзерсон, Р. Ривест. – М.: МЦИМО, 2000.
10. Матрос, Д.Ш. Элементы абстрактной и компьютерной алгебры: учеб. пособие для вузов [Текст] /Д.Ш. Матрос, Г.Б. Поднебесова. – М.: Академия, 2004
11. Поднебесова, Г.Б. Основы компьютерной алгебры: учеб. пособие [Текст] / Г.Б. Поднебесова. – М.: БИНОМ. Лаборатория знаний, 2008

ПРИЛОЖЕНИЯ

Приложение 1

Рабочая (модульная программа)

Модуль 1 **Аналитические вычисления на компьютере. Алгебры** **Цель – знать основные принципы вычислений в системах компьютерной алгебры**		
Содержание раздела		
План лекций	*План лабораторных работ*	*План семинарских занятий*
Лекция № 1. Аналитические вычисления на 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. **Лекция № 2. Алгебры** **Лекция № 3. Основные числовые множества** **Методическое обеспечение лекций** • Презентации лекций хранятся на портале университета. **Список литературы [1, 7]**	1. Работа с математическими объектами в системе Mathematica (2 часа). 2. Длинная арифметика (2 часа)	Не предусмотрены учебным планом

<table>
<tr><td colspan="3">Самостоятельная работа</td></tr>
<tr><td colspan="2">Инвариантная часть</td><td>Вариативная часть</td></tr>
<tr><td colspan="2"></td><td>Сдача индивидуальных заданий досрочно +0,2</td></tr>
<tr><td colspan="3">Паспорт оценочных средств по разделу</td></tr>
<tr><td colspan="2">Код контролируемой компетенции (или ее части) и ее формулировка</td><td>наименование оценочного средства</td></tr>
<tr><td colspan="3">Текущий контроль за выполнением лабораторных работ</td></tr>
<tr><td colspan="3">Раздел 2. Кольцо целых чисел
Цель – рассмотреть вопросы делимости и сравнимости в кольце целых чисел</td></tr>
<tr><td colspan="3">Содержание раздела</td></tr>
<tr><td>План лекций</td><td>План лабораторных работ</td><td>План семинарских занятий</td></tr>
<tr><td>Лекция № 1. Элементы теории делимости в кольце целых чисел.
1. Основная теорема арифметики.
2. Теорема Евклида.
3. Алгоритм Евклида.
4. Теорема Ламе.

Лекция № 2. Позиционные системы счисления.
1. Основные определения.
2. Смешанная система счисления.
3. Перевод чисел из одной системы счисления в другую.

Лекция № 3. Элементы теории сравнений в кольце целых чисел.</td><td>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)
3. Вычисление НОД (2 часа)
4. Модулярная арифметика (2 часа)</td><td>Не предусмотрены учебным планом</td></tr>
</table>

1. Сравнимость по модулю. 2. Вычеты. 3. Классы вычетов. 4. Теоремы Эйлера и Ферма. 5. Китайская теорема об остатках. **Лекция № 4.** Модулярная арифметика. 1. Метод Гарнера-Кнута. 2. Сравнение двух целых чисел. 3. Определение цифр в позиционной системе счисления. **Методическое обеспечение лекций** Презентации лекций хранятся на портале университета. **Список литературы [5, 8, 10]**	– Восстановление произведения двух чисел по их модулярным компонентам 5. Разложение на множители (2 часа) **Методическое обеспечение лабораторных работ** Разработки лабораторных работ хранятся на портале университета	
Самостоятельная работа		
Инвариантная часть	**Вариативная часть**	
Форма отчетности Сдача и защита индивидуального задания в течение 12 учебных дней со дня выдачи. **Методическое обеспечение** Текст заданий, предлагаемых студентам, хранится на портале университета	Сдача индивидуальных заданий досрочно +0,2	
Паспорт оценочных средств по разделу		
Код контролируемой компетенции (или ее части) и ее формулировка	наименование оценочного средства	

<table>
<tr><td colspan="3">Текущий контроль за выполнением лабораторных работ</td></tr>
<tr><td colspan="3">Раздел 3
Полиномы от одной переменной
Цель – научить вычислять полиномы и находить НОД полиномов от одной переменной</td></tr>
<tr><td colspan="3">Содержание раздела</td></tr>
<tr><td>План лекций</td><td>План лабораторных работ</td><td>План семинарских занятий</td></tr>
<tr><td>Лекция № 1. Полиномы от одной переменной.
1. Основные определения.
2. Вычисления полиномов.
3. Неравенство Ландау-Миньотта.
4. Соответствие модулярное – целое.
5. Вычисление НОД.
6. Оценка стоимости алгоритма.

Лекция № 2. Быстрое преобразование Фурье.
1. Основной алгоритм.
2. Анализ Фурье.
3. Методы анализа Фурье.
4. Применение преобразования Фурье.

Методическое обеспечение лекций
Презентации лекций хранятся на портале университета.

Список литературы [2, 3, 6, 8, 10]</td><td>1. Вычисление полиномов (2 часа)
– Бинарный метод и метод множителей.
– Схема Горнера.
2. Нахождение НОД (2 часа)
– Применение неравенства Ландау-Миньотта.
– Вычисление модулярного НОД.

Методическое обеспечение лабораторных работ
Разработки лабораторных работ хранятся на портале университета</td><td>Не предусмотрены учебным планом</td></tr>
</table>

<table>
<tr><td colspan="3">Самостоятельная работа</td></tr>
<tr><td colspan="2">Инвариантная часть</td><td>Вариативная часть</td></tr>
<tr><td colspan="2">Типы заданий, предлагаемых студентам
Индивидуальное задание

Форма отчетности
Сдача и защита индивидуального задания в течение 12 учебных дней со дня выдачи.

Текст заданий, предлагаемых студентам, хранится на портале университета</td><td>Сдача индивидуальных заданий досрочно +0,2</td></tr>
<tr><td colspan="3">Паспорт оценочных средств по разделу</td></tr>
<tr><td colspan="2">Код контролируемой компетенции (или ее части) и ее формулировка</td><td>наименование оценочного средства</td></tr>
<tr><td colspan="3">Текущий контроль за выполнением лабораторных работ</td></tr>
<tr><td colspan="3">Раздел 4
Полиномы от нескольких переменных.
Формальное интегрирование и дифференцирование
Цель – научить находить НОД полиномов от нескольких переменных, вычислять производную и интеграл в системах компьютерной алгебры</td></tr>
<tr><td colspan="3">Содержание раздела</td></tr>
<tr><td>План лекций</td><td>План лабораторных работ</td><td>План семинарских занятий</td></tr>
<tr><td>Лекция № 1. Нахождение НОД.
1. Содержание полинома.
2. Примитивная часть полинома.
3. Лемма Гаусса.
4. Алгоритм вычисления НОД.

Лекция № 2. Кодирование. Криптография.
1. Кодирование информации.</td><td>1. Полиномы от одной и нескольких переменных в пакете Mathematica (2 часа)
– Основные функции для работы с полиномами от одной и нескольких переменных.</td><td>Не предусмотрены учебным планом</td></tr>
</table>

2. Блочное и алфавитное кодирование. 3. Классификация шифров. 4. Системы с закрытым ключом. 5. Системы с открытым ключом. **Лекция № 3.** Интегрирование и дифференцирование 1. Задача интегрирования. 2. Интегрирование рациональных функций. 3. Интегрирование более сложных функций. **Методическое обеспечение лекции** Презентации лекций хранятся на портале университета. **Список литературы [2, 4, 6, 7]**	2. Работа с простыми числами (2 часа) 3. Криптосистема RSA (2 часа)	

Самостоятельная работа	
Инвариантная часть	**Вариативная часть**
Форма отчетности Сдача и защита индивидуального задания в течение 12 учебных дней со дня выдачи. **Текст заданий, предлагаемых студентам,** хранится на портале университета	Сдача индивидуальных заданий досрочно +0,2
Паспорт оценочных средств по разделу	
Код контролируемой компетенции (или ее части) и ее формулировка	наименование оценочного средства
Текущий контроль за выполнением лабораторных работ	

Приложение 2

Содержание самостоятельной работы

Темы для самостоятельного изучения	**Кол-во часов**	**Формы самостоятельной работы**	**Методическое обеспечение**	**Форма отчетности**
Алгоритмы символьных преобразований	16	Дополнение конспекта лекций рекомендованной литературой. Действие в соответствии с методическими указаниями на практическом занятии	ЮУрГГПУ (внутренний портал) > Учебно-методические материалы > IITiMOI > IA > 2k > A_K A	Интеллект-карта
Работа с дробями в системах компьютерной алгебры	20	Дополнение конспекта лекций рекомендованной литературой	ЮУрГГПУ (внутренний портал) > Учебно-методические материалы > IITiMOI > IA > 2k > A_K A	Собеседование по проработанной литературе
Отношение делимости полиномов	14	Действие в соответствии с методическими указаниями	ЮУрГГПУ (внутренний портал) > Учебно-	Индивидуальное задание

		на практическом занятии	методические материалы > IITiMOI > IA > 2k > A_K A	
Операции над большими целыми числами. Извлечение корня из больших целых чисел	19	Действие в соответствии с методическими указаниями на практическом занятии	ЮУрГГПУ (внутренний портал) > Учебно-методические материалы > IITiMOI > IA > 2k > A_K A	Реализация алгоритма

Приложение 3

Рейтинг

Для контроля знаний студентов используется модульно-рейтинговая система. Учебный материал разбит на модули (таблицы 3.1 и 3.2). Каждый модуль содержит индивидуальные и/или практические задания и тест. Модуль может содержать баллы за дополнительные задания.

Таблица 3.1

№	Фамилия Имя	Доп. балл	Тест 1	Модуль 1	Системы счисления	Алгоритм Евклида	Вычисление НОД Лаб.	Модулярная арифметика	Разложение на множители Лаб.	Доп. балл	Тест 2	Модуль 2
1	Чуксина Мария	0,09	0,75	84	1	1,2	1,2	1	1	0,09	0,81	100,8
2	Саратцева Юлия	0,1	0,62	72	1	1	1	0,5	1	0,12	0,63	84
3	Курдюкова Лидия	0,1	0,69	79	1	1,2	1,2	1,4	1	0,09	0,63	98,4
4	Щербаков Саша	0,05	0,7	75	1	1	1	0,8	1	0,05	0,69	87,2
5	Ямаева Регина	0,1	0,69	79	1	1	1	1,2	1	0,1	0,63	91,6
6	Терехов Антон	0,04	0,44	48	1	1	1,2	1,4	1	0,4	0,69	110,8
7	Жирняков Женя	0,05	0,63	68	1	0,8	1	0,8	1	0,04	0,56	79,2
8	Мартыненко Полина	0,04	0,44	48	1	0,8	1	0,8	1	0,04	0,69	84,4
9	Ковалев Дмитрий	0,08	0,44	52	1	1	1	1	1	0,04	0,5	81,6

Таблица 3.2.

Вычисление полиномов	НОД полиномов	Mathematica_1	Доп. балл	Тест 3	Модуль 3	Mathematica_2	Лаб. № 10	Лаб. № 11	RSA	Доп. балл	Тест 4	Модуль 4	Итог	Оценка
1	1	1	0,1	0,53	85,2	1	1	1	1,2	0,08	0,62	91	90,25	Отлично
1	0,5	1	0,09	0,93	90,8	1	1	1	1,2	0,14	0,87	103,4	87,55	Хорошо
1	1	1	0,1	0,93	101,2	1	1	1	1,2	0,13	1	108,2	96,7	Отлично
1	1	1	0,05	0,93	99,2	1	1	1	1,2	0,05	0,73	94,2	88,9	Хорошо
1	1	1	0,1	0,93	101,2	1	1	1	1,2	0,05	1	105	94,2	Отлично
1	1	1	0,08	0,93	100,4	1	1	1	1,2	0,05	0,87	99,8	89,75	Отлично
1	1	1		0,93	97,2	1	1	1	1,2		0,93	100,2	86,15	Хорошо
1	1	1		0,93	97,2	1	1	1	1,2	0,03	0,87	99	82,15	Хорошо
1	1	1		0,86	94,4	1	1	1	1,2	0,04	0,93	101,8	82,45	Хорошо

Для вычисления рейтинга по каждому модулю используется следующее соотношение: тест*60+индивидуальные задания*40. Если индивидуальных заданий несколько, то 40 делится на их количество.

Приложение 4

Работа в системе Mathematica

Запустите пакет Mathematica (в панели задач выбрать кнопку Пуск, затем Программы → Wolfram Mathematica 6.0).

Вычисления в системе Mathematica оформляются в виде *документа*.

Документы Mathematica содержат текстовые комментарии, ячейки с математическими выражениями и результаты вычислений в различной форме, включая табличную, матричную или графическую. Файлы документов имеют формат.nb (блокнот).

Главное окно системы имеет вид:

Меню **Файл** служит для работы с файлами. Открытие нового документа осуществляется командой Новый. Для сохранения и открытия файлов используются команды Сохранить, Сохранить как, Сохранение особо… (запись файлов в специальных форматах) и Открыть, Открыть другой (открытие файлов в специальных форматах). Для печати документов используется команда Печать.

В меню **Редактировать** сосредоточены основные операции редактирования.

Меню **Ячейка** содержит команды для работы с ячейками. Ячейки (Cells) являются основными объектами документов. Ячейки отличаются друг от друга статусом, то есть совокупностью свойств, определяющих тип ячейки

и ее поведение в различных ситуациях. Ячейки, содержащие текстовые надписи-комментарии, не оцениваются и не меняются в ходе пересчета документа. Ячейки ввода оцениваются, их содержимое меняется, и они порождают ячейки вывода с разным содержимым. Статус ячеек постоянно проверяется с помощью операции оценивания в ходе пересчета документа.

Операции форматирования сосредоточены в меню **Формат**. С помощью команды Стиль можно задать различные шрифты, выделения и др. Кроме того имеется возможность управления элементами окна: Отобразить линейку – отображение мерной линейки, Отобразить панель – вывод на экран панели инструментов, Отобразить разрывы страниц – показ линий разрыва страниц, Масштаб – установка (в %) масштаба отображения документа.

Команды ввода содержатся в меню **Ввод**. Среди команд ввода такие, как: ввод координат двумерных графиков (Получить графические координаты), выбор точки обзора трехмерных графиков (Выбрать точку зрения 3D), звукозапись (Записать звук), ввод таблиц, матриц и палитр (Сделать таблицу / матрицу /палитру), вставка гиперссылок (Сделать гиперссылку), ввода редактирование кнопок (Сделать кнопку) и др.

Гиперссылка является объектом класса ButtonBox (кнопка), связанным с некоторым другим объектом, представленным файлом – документом или рисунком.

Меню **Ядро** служит для управления действиями, проводимыми ядром системы, называется ячейками загруженного документа. Управление процессом вычислений (работой ядра) возможно из меню Ядро, подменю Вычисление.

Возможно вычисление выделенных ячеек, выделенного выражения, следующей строки ввода, всех ячеек документа и др. Команда Выйти из ядра служит для прерывания текущих вычислений. Управление показом номеров ячеек можно осуществить командой Показать входные/выходные имена. Она управляет и показом, и скрытием, если она не отмечена галочкой, номеров строк, если она отмечена галочкой. Для удаления всех ячеек вывода можно использовать команду Удалить все входные.

Операции поиска и замены находятся в меню **Найти**.

Работа с окнами осуществляется из меню **Окно**. Возможно каскадное расположение окон – Выстроить окна; расположение мозаикой по высоте – Размножить в ширину; расположение мозаикой по ширине – Размножить в высоту. Команда Messages управляет выводом окна сообщений об ошибках.

Для получения справки выбрать раздел меню **Помощь** опцию Обозреватель помощи (рис. 1).

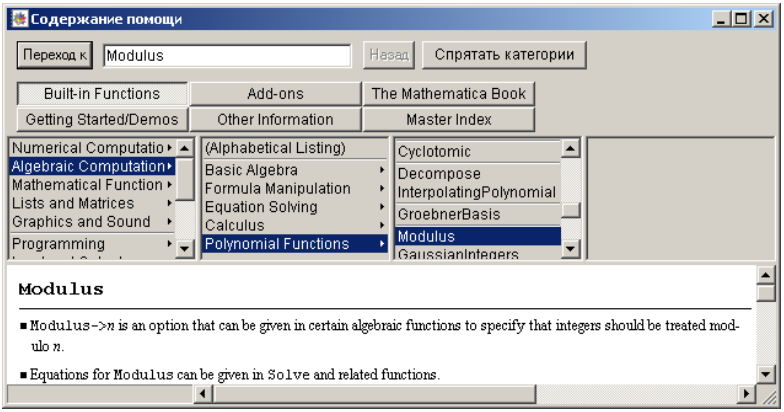


Рис. 1.

В окне браузера справочной системы можно (активизацией соответствующей кнопки) выбрать следующие разделы справок:

Built-in-Functions – встроенные функции;

Add-ons – пакеты расширений;

The Mathematica Book – электронная версия книги «The Mathematica Book»;

Getting Started/Demos – руководство для начинающих и примеры;

Other Information – другая информация;

Master Index – справка по индексу (алфавитный указатель).

Пакеты расширений содержат массу полезных новых функций. Они служат для расширения функциональных возможностей системы в таких областях, как алгебра, геометрия, дискретная математика, теория чисел и др.

По каждой функции приведен ряд примеров, которые открываются при активизации гиперссылки в виде треугольника с надписью Futher Examples.

Справочная система имеет гипертекстовые ссылки (подчеркнутые слова синего цвета).

Для демонстрации возможностей системы, рассчитанный на начальный уровень знакомства с системой, служит электронный учебник.

В разделе Other Information находятся сведения об интерфейсе системы, а также все сведения о командах главного меню, о правилах набора сложных вычислений и др.

Электронная книга является наглядным примером развития электронных книг. В отличие от электронного

учебника она содержит больший объем справочной информации, использует как встроенные функции, так и дополнительные функции из пакетов расширений.

Если команда или функция, которую необходимо найти, известна, то достаточно указать ее в поле у кнопки Переход к … и нажать эту кнопку. Можно осуществить поиск по начальным буквам исконного слова.

2. Для удобства работы в пакете Mathematica существует несколько палитр, в которых находятся пиктограммы ввода математических символов, функций и команд управления системой. Палитры выводятся с помощью меню Файл->Палитры, их всего восемь (рис.2).

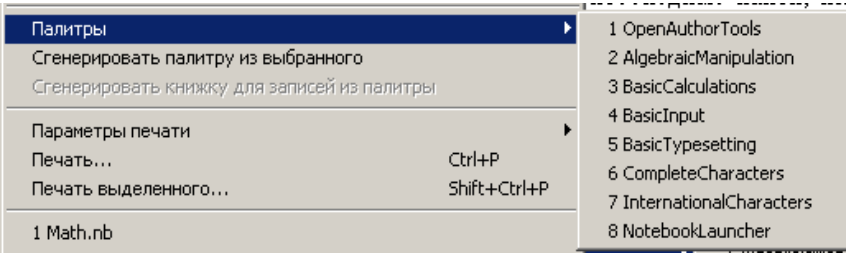


Рис. 2.

В палитре AlgebraicManipulation находятся основные функции компьютерной алгебры, которые можно использовать как шаблоны для вычисления перечисленных функций (рис. 3).

Палитра BasicCalculation содержит семь разделов (рис. 4).

Палитра BasicInput содержит часто используемые математические знаки и греческие буквы (рис. 5).

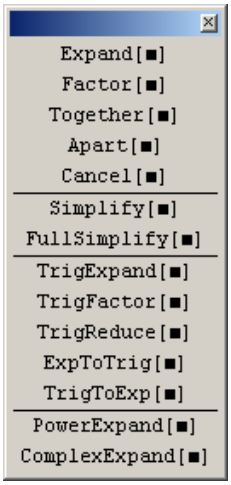


Рис. 3. AlgebraicManipulation

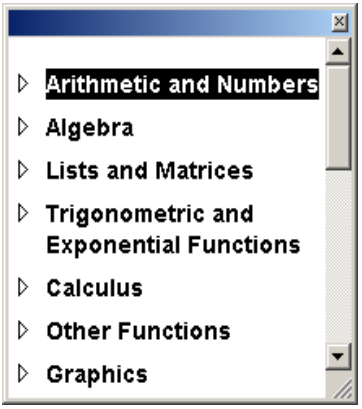


Рис. 4. BasicCalculation

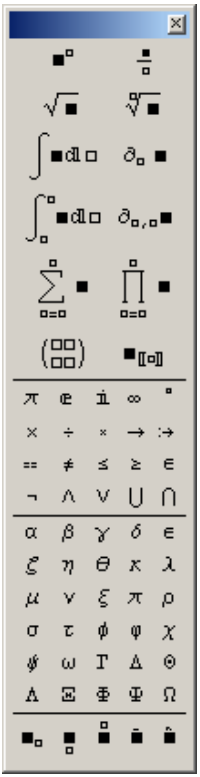


Рис. 5. BasicInput

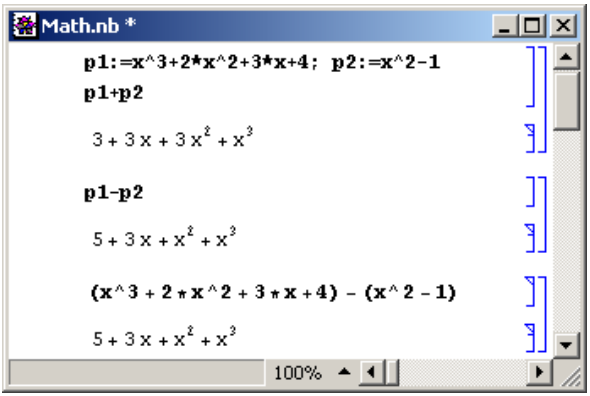
1. Работа с полиномами

1.1. Основные операции над полиномами.

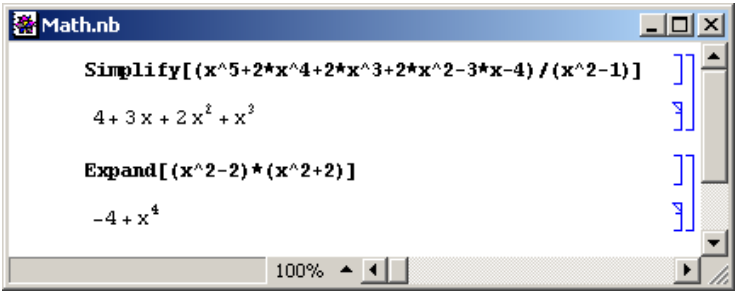
Над полиномами можно выполнять обычные операции сложения, вычитания, умножения и деления. Для получения результата умножения используется функция Expand. Если полиномы делятся друг на друга, то применяется операция Simplify. Для получения результата необходимо нажать Shift + Enter.

Примеры.

1. Найти сумму и разность полиномов (рассмотрены два способа вычисления)



2. Выполнить деление и умножение полиномов, используя функции Simplify и Expand.



1.2. Разложение полиномов

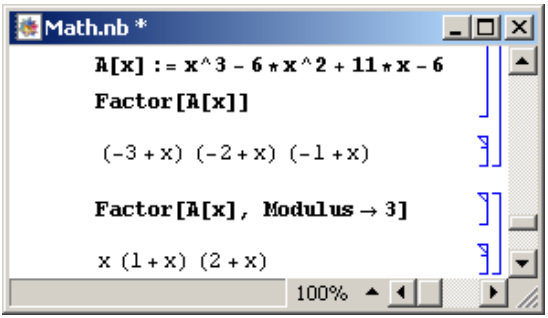
Factor[poly] – выполняет разложение полинома над целыми числами;

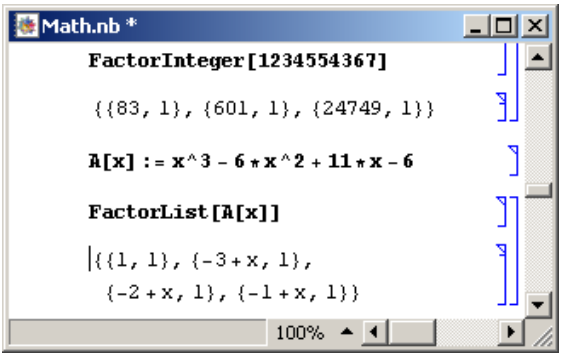
Factor[poly, Modulus->p] – выполняет разложение по модулю простого числа p;

FactorInteger[n] – возвращает список простых множителей числа n вместе с их показателями степени;

FactorList[poly] – возвращает список множителей полинома с их показателями степени.

Пример.





1.3. Функции для работы с полиномами

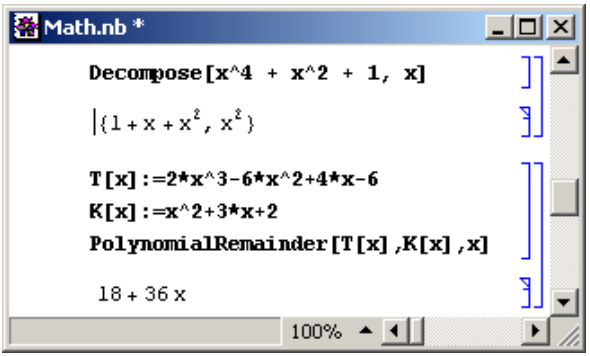
Decompose[poly,x] – выполняет разложение полинома на более простые полиномиальные множители;

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

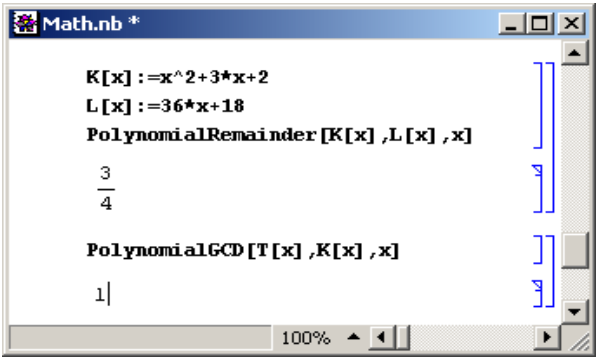
PolynomialGCD[poly1, poly2,….] – возвращает наибольший общий делитель ряда полиномов poly1, poly2,…

С опцией Modulus->p функция возвращает наибольший общий делитель по модулю простого числа p.

Пример 1.



Пример 2.



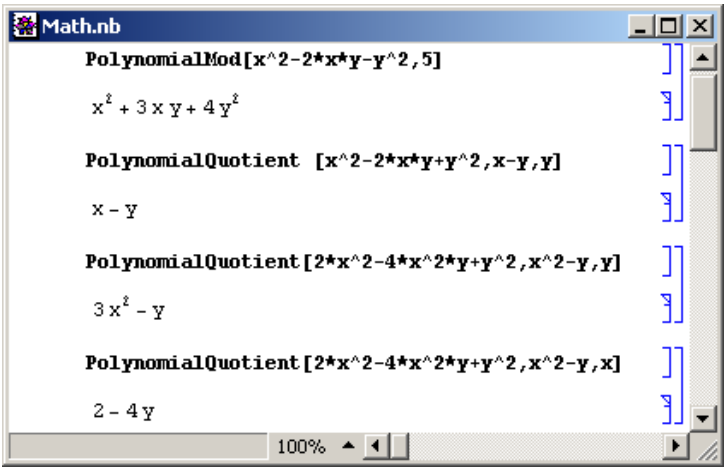
2. Работа с полиномами от нескольких переменных

2.1. Функции для работы с полиномами от нескольких переменных:

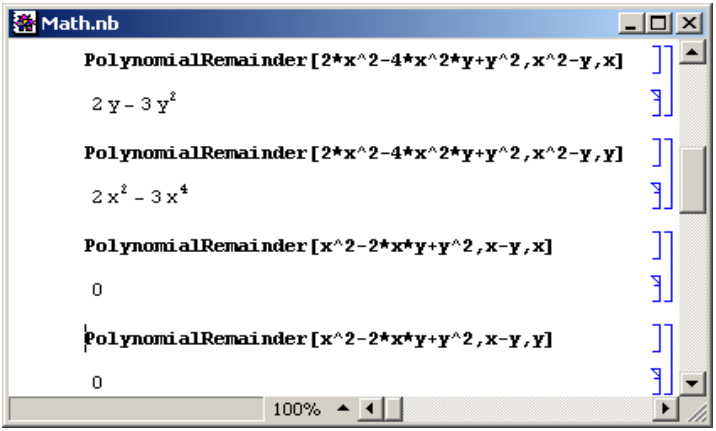
PolynomialMod[poly,m] – возвращает полином poly, приведенный по модулю m;

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

Пример 1.



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



Пример 2.

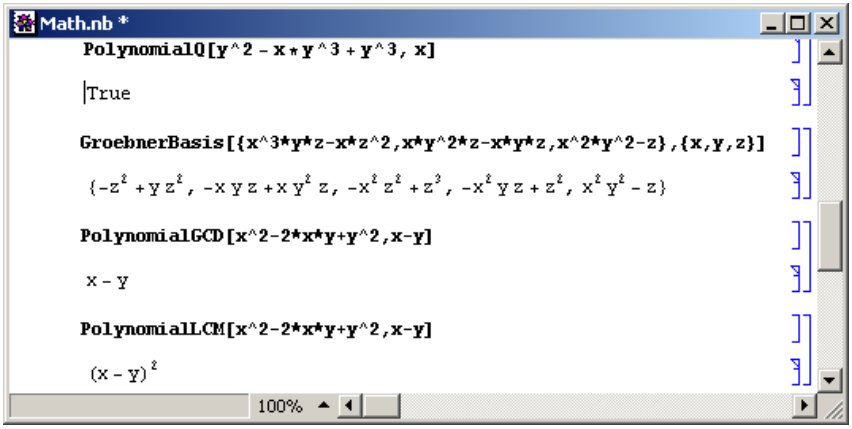
PolynomialQ[expr,var] – проверяет, является ли expr полиномом от var;

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

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

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

Пример 3.

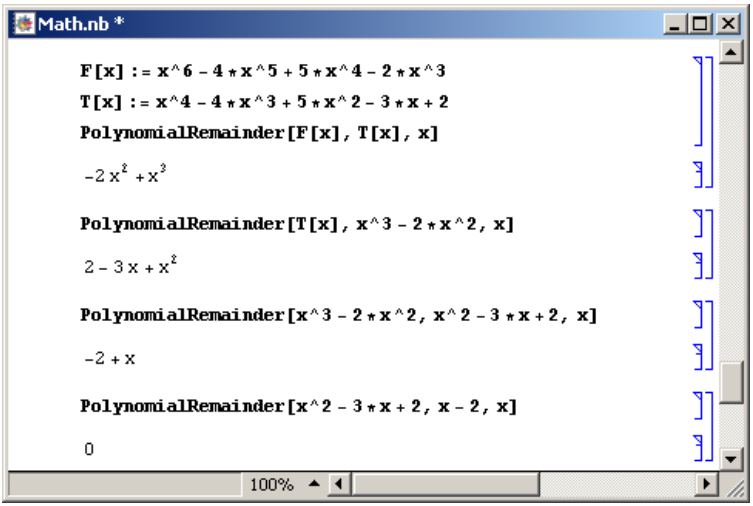


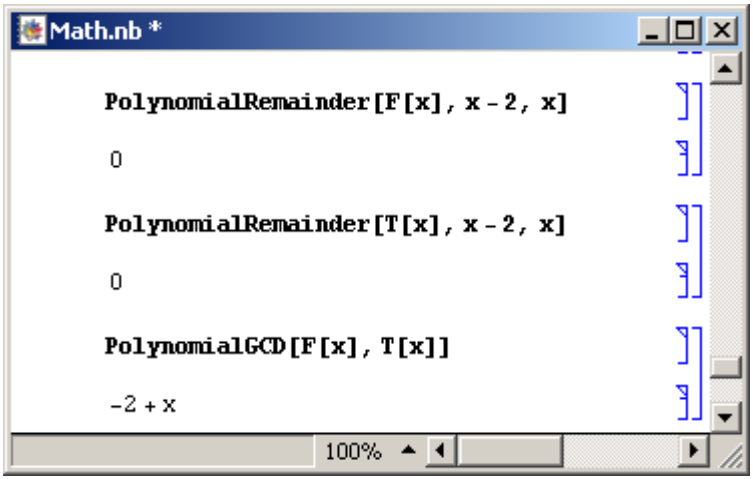
2.2. Нахождение наибольшего общего делителя с помощью функции PolynomialRemainder

Здесь мы продемонстрируем применение алгоритма Евклида для нахождения наибольшего общего делителя двух полиномов.

Пример.

Проверим, является ли полученный полином x-2 наибольшим общим делителем данных полиномов. Используем функции PolynomialRemainder и PolynomialGCD.





Приложение 5

Первые 64 простых числа[1]

2	**3**	5	**7**	**11**	**13**	**17**	**19**
23	**29**	**31**	**37**	**41**	**43**	**47**	**53**
59	**61**	**67**	**71**	**73**	**79**	**83**	**89**
97	**101**	**103**	**107**	**109**	**113**	**127**	**131**
137	**139**	**149**	**151**	**157**	**163**	**167**	**173**
179	**181**	**191**	**193**	**197**	**199**	**211**	**223**
227	**229**	**233**	**239**	**241**	**251**	**257**	**263**
269	**271**	**277**	**281**	**283**	**293**	**307**	**311**

[1] Простые числа 2 и 5 для восстановления чисел с помощью модулярной арифметики не использовать!

Учебное издание

Поднебесова Галина Борисовна

АБСТРАКТНАЯ
И
КОМПЬЮТЕРНАЯ АЛГЕБРА
Практикум

ISBN 978-5-906908-47-6

Работа рекомендована РИСом университета
Протокол № 13 от 19.12.2016. Пункт 18

Издательство ЧГПУ
454080, г. Челябинск, пр. Ленина, 69

Редактор О.В. Максимова
Компьютерная верстка А.Г. Петрова

Подписано в печать 28.04.2017
Объем 2,7 уч.-изд. л. (5,3 п. л.) Формат 60×84/16
Тираж 100 экз. Заказ №

Отпечатано с готового оригинал-макета
в типографии ЧГПУ
454080, г. Челябинск, пр. Ленина, 6