**Лабораторная работа № 1**

**Алгебраические основы. Часть 1 «Теория чисел»**

**Теоретические сведения**

Ниже рассматриваются *N* – множество натуральных чисел, *Z* – множество целых чисел. Множество целых чисел *Z* – счетное, состоит из элементов . На нем определены две алгебраические операции – сложение и умножение. Эти операции обладают следующими свойствами (для любых ):

1) ассоциативность: ; ;

коммутативность: ; ;

2) существует нейтральный элемент – 0 или 1 соответственно: 

3)  – закон дистрибутивности;

4) для каждого целого  существует единственное противоположное целое  такое, что .

**Теорема 1.1 (о делении с остатком).** *Для любых целых чисел a и b*, **, *существуют единственные целые числа q и *, **, *такие, что .*

В этом равенстве  называют остатком, а – частным (неполным частным – при ) от деления  на . При  величины  и  называют делителями или множителями числа . Читатель со школьной скамьи умеет находить частное и остаток методом деления уголком.

*Следствие*. Пусть натуральное число,  Для всякого целого числа  и максимального целого  с условием  существуют единственные целые  такие, что

**

Такое равенство записывают сокращенно  или  (если  известно по контексту) и называют записью числа  в -ичной позиционной системе счисления или системе счисления по основанию  Кажется естественной привычная десятичная позиционная система записи целых чисел . В различных ситуациях более удобными оказываются другие основания. Например, во всех компьютерах на микроуровне вычисления проводятся в двоичной системе счисления. Для перехода к ней с десятичной применяют промежуточную 16-ричную систему счисления.

***Лемма 1.1.*** Если в равенстве  все слагаемые – целые числа и все, кроме может быть одного, делятся на целое , то и это исключенное слагаемое также делится на .

*Определение 1*.*1*.Если целые числа  делятся на целое , то  называют их общим делителем.

В дальнейшем речь идет только о положительных целых делителях.

*Определение 1.2.*Максимальный из общих делителей целых чисел  называется их наибольшим общим делителем и обозначается   
через НОД ().

**Теорема 1.2.** *Если , то *.

Теорема 1.2 позволила Евклиду (примерно 2300 лет тому назад) обосновать следующий факт.

**Теорема 1.3.** *Наибольший общий делитель целых чисел a и b  равен последнему отличному от нуля остатку цепочки равенств*:

**;

**;

*…………………*

* т*. *е*. *.*

*.*

Теорема 1.3 формулирует алгоритм Евклида для нахождения наибольшего общего делителя целых чисел. Его вариантом является следующий (второй способ вычисления наибольшего общего делителя по алгоритму Евклида): вычисляем последовательно разности  до получения последней ненулевой разности, которая и совпадает с **.

***Пример 1.1.*** С помощью алгоритма Евклида найти НОД (72, 26).

*Решение*. В соответствии с теоремой 1.2 ; ; ; . Следовательно, НОД (72, 26) = 2.

**Теорема 1.4*.*** *Если *, *то существуют такие целые  и v*, *что выполняется следующее соотношение* (*соотношение* *Безу*)*: .*

***Пример 1.2.*** Из примера 1.1 следует, что



Такой способ получения соотношения Безу для конкретных целых чисел называется расширенным алгоритмом Евклида. Он состоит из двух этапов: собственно алгоритма Евклида – прогонки вниз и прогонки вверх – и последовательного выражения остатков в каждом из шагов предыдущего этапа (с соответствующим приведением подобных на каждом шаге).

*Определение 1*.*3*. Натуральное число  называется простым, если оно делится только на 1 и на себя.

**Теорема 1.5*.*** *Всякое натуральное число  либо является простым числом*, *либо имеет простой делитель.*

Заметим, что из соотношения  натуральных чисел, больших единицы, следует, что либо , либо  принадлежит отрезку . Легко видеть, что наименьший натуральный делитель  натурального числа  является простым числом. Исторически первый метод проверки натурального числа  на простоту, заключающийся в делении его на простые числа, не превосходящие , носит название «решета Эратосфена». К настоящему времени разработан достаточно большой цикл алгоритмов проверки числа на простоту.

**Теорема 1.6 (теорема Евклида).** *Простых чисел бесконечно много.*

Значение простых чисел в том, что они по теореме 1.5 являются составными кирпичиками всех натуральных чисел.

*Определение 1*.*4*. Целые числа  и называются взаимно простыми, если **.

**Теорема 1.7 (критерий взаимной простоты целых чисел)*.*** *Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v*, *что выполняется равенство .*

*Следствие*.  тогда и только тогда, когда  

Важным в теории чисел и ее приложениях является следующее свойство взаимно простых целых чисел.

***Лемма 1.2.*** Пусть произведение целых чисел  делится на целое число и . Тогда  делится на .

**Теорема 1.8 (основная теорема арифметики).** *Всякое целое число  однозначно раскладывается в произведение простых множителей*

*.*

Если в этом равенстве собрать одинаковые множители, то получим каноническое разложение целого числа .

***Пример 1.3.*** Приведем примеры канонических разложений целых чисел:   
a) 196 = 2⋅98 = 2⋅2⋅49 = 22⋅72; б) 

**Теорема 1.9.** *Пусть  – натуральное число*, * Для любых целых чисел  и  следующие условия равносильны*:

1) * и  имеют одинаковые остатки от деления на *

2) * делится на  т*. *е*. * для подходящего целого *

3) * для некоторого целого *

*Определение 1*.*5*.Целые числа  и  называются сравнимыми по модулю  если они удовлетворяют одному из условий теоремы 1.9. Этот факт обозначают формулой  или  и называют данную формулу сравнением.

***Пример 1.4.*** –57(mod 4) 11(mod 4) 23(mod 4) 3(mod 4).

***Пример 1.5.*** Если  то всякое целое число сравнимо по модулю  со своим остатком от деления на  Это следует из определения 1.5 и второго условия теоремы 1.9. Ведь  делится на 

**Теорема 1.10 (малая теорема Ферма).** *Пусть  – простое число и целое число  не делится на *. *Тогда *.

Теория сравнений и малая теорема Ферма позволяют быстро находить остаток от деления большого числа на простое число.

**Порядок выполнения работы**

Вариант задания на выполнение лабораторной работы выдаётся преподавателем

**Задание 1.1.** Найти канонические разложения чисел 

*Решение.*

  Следовательно, 627 = 3∙11∙19, 399 = 3∙7∙19.

**Задание 1.2.** Найти НОД (627,399), воспользовавшись: а) алгоритмом Евклида; б) разложением чисел на простые множители.

*Решение*. Применим алгоритм Евклида:

627 = 399 ∙ 1 + 228;

399 = 228 ∙ 1 + 171;

228 = 171 ∙ 1 + 57;

171 = 57∙ 3. Следовательно, НОД (627; 399) = 57.

Найдем НОД (*а*, **), воспользовавшись разложением на простые множители чисел  и  полученным в решении задания 1.1:

627 = 3 ∙ 11∙ 19; 399 = 3 ∙ 7 ∙ 19.

Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих как в одно, так и в другое разложения чисел НОД (627; 399) = 3 ∙ 19 = 57.

Найдем НОД (*а*, **) методом вычитаний:

627 – 399 = 228; 399 – 228 = 171; 228 – 171 = 57; 171 – 57 = 114;

114 – 57 = 57; 57 – 57 = 0. Следовательно, НОД (627; 399) = 57.

**Задание 1.3.** С помощью расширенного алгоритма Евклида найти целые числа , удовлетворяющие соотношению Безу: для целых чисел 

*Решение*. Сначала найдем по алгоритму Евклида НОД (110, 48):

110 = 48 ∙ 2 + 14;

48 = 14 ∙ 3 + 6;

14 = 6 ∙ 2 + 2;

6 = 3 ∙ 2. Следовательно, НОД (110, 48) = 2.

Теперь построим соотношение Безу для данных и :

110 = 48 ∙ 2 + 14; поэтому 14 = 110 + 48 ∙ (–2);

48 = 14 ∙ 3 + 6; поэтому 6 = 48 + 14 ∙ (–3);

14 = 6 ∙ 2 +2; поэтому 2 = 14 + 6 ∙ (–2). В это равенство подставим выше полученное выражение для 6 и приведем подобные относительно чисел 48 и 14. Итак 2 = 14 + 6 ∙ (–2) = 14 + (48 + 14 ∙ (–3))( –2) = 14 ∙ 7 + 48 ∙ (–2).

В полученное выражение для НОД (110, 48) = 2 подставим вышеприведенное выражение числа 14. Получим окончательно

2 = 14 ∙ 7 + 48 ∙ (–2) = (110 + 48 ∙ (–2)) 7 + 48 ∙ (–2) = 110 ∙ 7 + 48 ∙ (–16) = 2.

**Индивидуальные задания**

1. Найти канонические разложения чисел *а* и *b*.

2. Найти НОД , воспользовавшись: a) алгоритмом Евклида; б) разложением чисел на простые множители.

3. С помощью расширенного алгоритма Евклида найти целые *u*, *v*,

удовлетворяющие соотношению Безу: 

**Вариант 1.**

1–3. 101398751, 326147777.

**Вариант 2.**

1–3. 5999801, 48685811.

**Вариант 3.**

1–3. 660422941,  36481301.

**Вариант 4.**

1–3.  9002242397, 433817903.

**Вариант 5.**

1–3.  9118515943,  3386496689.

**Вариант 6.**

1–3. 5336161097, 196210799.

**Вариант 7.**

1–3.  7049964661,  168687989.

**Вариант 8.**

1–3.  83748733,  73435591.

**Вариант 9.**

1–3.  16254559,  1029073.

**Вариант 10.**

1–3.  6099377,  9568217.

**Вариант 11.**

1–3.  7957549,  23118553.

**Вариант 12.**

1–3.  16088437,  18216949.

**Вариант 13.**

1–3.  244604911,  61875907.

**Вариант 14.**

1–3.  356216713,  31238065.

**Вариант 15.**

1–3.  7409621,  6793883.

**Лабораторная работа № 2**

**Алгебраические основы. Часть 2 «Конечные поля»**

**Теоретические сведения**

Полем называют множество элементов, на котором определены две операции. Одна из них называется сложением и обозначается *a* + *b*, а другая – умножением и обозначается *a* · *b*, даже если эти операции не являются обычными операциями сложения и умножения чисел. Для того чтобы множество элементов, на котором заданы операции сложения и умножения, было полем, необходимо, чтобы по каждой из этих операций выполнялись все групповые аксиомы, а также выполнялся дистрибутивный закон, т. е. для трех любых элементов поля *а*, *b*, *с* были справедливы равенства

*а* · (*b* + *с*) = *а* · *b* + *а* ·*с* и (*b* + *с*) ·*а* = *b* ·*а* + *с* ·*а*.

Кроме того, по каждой операции группа должна быть коммутативной, т. е. должно выполняться *а + b = b + a и а* · *b* = *b* · *а*. Групповые свойства по операции умножения справедливы для всех ненулевых элементов поля.

Поля с конечным числом элементов *q* называют полями Галуа по имени их первого исследователя Эвариста Галуа и обозначают *GF*(*q*).

Число элементов поля *q* называют порядком поля. Конечные поля используются для построения большинства известных кодов и их декодирования.

В зависимости от значения *q* различают простые или расширенные поля. Поле называют простым, если *q* – простое число. Для обозначения простых чисел будем использовать символ *p*. Простое поле образуют числа по модулю *p*: 0, 1, 2,.., *p*–1, а операции сложения и умножения выполняются по модулю *p*.

Наименьшее число элементов, образующих поле, равно 2. Такое поле должно содержать 2 единичных элемента: **0** относительно операции сложения и **1** относительно операции умножения. Это поле *GF*(2), или двоичное. Правила сложения и умножений для элементов *GF*(2) приводятся рис.1.

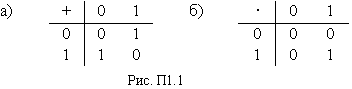


Рис.1

*GF*(3) – троичное поле с элементами 0, 1, 2. Для него правила сложения и умножения приводятся на рис.2.

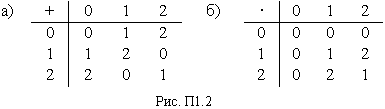


Рис.2

Формирование таблиц производится приведением результата сложения или умножения чисел, записанных во главе строк или столбцов, по модулю *p*, т. е. в качестве результата операции принимается остаток от деления полученного числа на *p*.

Анализируя состав таблиц, легко убедиться, что 0 и 1 как единичные элементы по операции сложения и умножения не изменяют значения других элементов поля по соответствующей операции. Кроме того, видно, что для каждого элемента по операции сложения и для ненулевых элементов по операции умножения имеются обратные.

Для поля *GF*(5) с элементами 0, 1, 2, З, 4 правила сложения и умножения приводятся на рис.3.

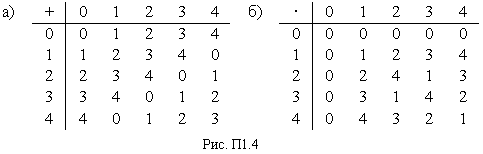
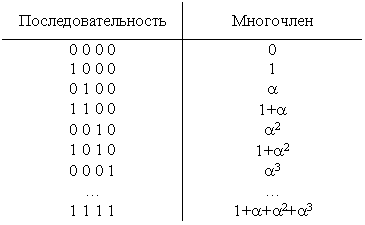


Рис.3

Изучим возможность построения полей с элементами в виде последовательностей чисел.

Определим условия, при которых последовательности длины *m* с элементами из поля *GF*(*p*) образуют поле.

Рассмотрим последовательности длины 4 с элементами из GF(2). Такие последовательности можно складывать как векторы, и нулевым элементом по операции сложения является 0000. Для задания операции умножения сопоставим каждой последовательности многочлен от :



Умножение таких многочленов может дать степень, большую чем 3, т. е. последовательность, не принадлежащую рассматриваемому множеству.

Например, (1101) · (1001)  (1++3) · (1+3) = 1++4+6. Для того чтобы свести ответ к многочлену степени не более 3, положим, что α удовлетворяет уравнению степени 4, например,

*p*() = 1++4 = 0,

или

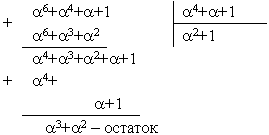
4 = 1+.

Тогда

5 =+2, 6 =2+3;

1++4+6 = 1++1++2+3 = 2+3.

Это эквивалентно делению на многочлен 1++4 и нахождению остатка от деления:



Таким образом, имеет место аналогия при формировании поля из чисел и последовательностей чисел (многочленов). Эта аналогия распространяется и на то, что для обратимости введенной операции умножения (чтобы система элементов в виде последовательностей длины *m* или многочленов степени меньшей *m*, образовывала поле) многочлен Π() должен быть неприводим над полем своих коэффициентов.

Поле, образованное многочленами над полем *GF*(*р*) по модулю неприводимого многочлена *p*(*x*) степени *m*, называется расширением поля степени *m* над *GF*(*p*) или расширенным полем. Оно содержит *pm* элементов и обозначается GF(*pm*).

Поле, образованное шестнадцатью двоичными последовательностями длины 4, или многочленами степени 3 и менее с коэффициентами из *GF*(2) по модулю многочлена *x*4+ *x*+1, неприводимого над *GF*(2), является примером расширенного поля *GF*(24), которое может быть обозначено также *GF*(16)

Важнейшим свойством конечных полей является следующее. Множество всех ненулевых элементов конечного поля образует группу по операции умножения, т. е. мультипликативную группу порядка *q*–1. Рассмотрим совокупность элементов мультипликативной группы, образованную некоторым элементом a и всеми его степенями 2,3 и т. д. Так как группа конечна, должно появиться повторение, т. е. *i* = *j*. Умножая это равенство на (*i*)–1 = (–1)*i*, получим 1 = *j*-*i*. Следовательно, некоторая степень равна 1.

Наименьшее положительное число *e*, такое, что *e*= 1, называется порядком элемента . Совокупность элементов 1, , 2,…,*e*–1 образует подгруппу, поскольку произведение любых двух элементов принадлежит этой совокупности, а элемент, обратный *j*, равен *e*–*j* и тоже входит в эту совокупность.

Группа, которая состоит из всех степеней одного из ее элементов, называется циклической группой.

Из рассмотренного свойства конечных полей вытекают два важных следствия. Первое из них утверждает, что многочлен *xq*–1–1 имеет своими корнями все *q*–1 ненулевых элементов поля *GF*(*q*), т. е.

http://dvo.sut.ru/libr/opds/i287ohor/Image20.gif

В поле *GF*(*q*) элемент a, имеющий порядок *e* = *q*–1, называется примитивным. Отсюда следует, что любой ненулевой элемент *GF*(*q*) является степенью примитивного элемента. Второе следствие из рассмотренного свойства утверждает, что любое конечное поле *GF*(*q*) содержит примитивный элемент, т. е. мультипликативная группа *GF*(*q*) является циклической.

В табл. 1 представлены различными способами элементы *GF*(24).

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Последовательность длины 4** | **Многочлен** | **Степень** | **Логарифм** |
| 1 | 2 | 3 | 4 |
| 0000 | 0 | 0 | – |
| 1000 | 1 | 1 | 0 |
| 0100 |  |  | 1 |
| 0010 | 2 | 2 | 2 |
| 0001 | 3 | 3 | 3 |
| 1100 | 1+ | 4 | 4 |
| 0110 | +2 | 5 | 5 |
| 0011 | 2+3 | 6 | 6 |
| 1101 | 1++3 | 7 | 7 |
| 1010 | 1+2 | 8 | 8 |
| 0101 | +3 | 9 | 9 |
| 1110 | 1++2 | 10 | 10 |
| 0111 | +2+3 | 11 | 11 |
| 1111 | 1+ +2+3 | 12 | 12 |
| 1011 | 1+2+3 | 13 | 13 |
| 1001 | 1+3 | 14 | 14 |

Поле *GF*(24), представленное в табл.1, построено по модулю *x*4+*x*+1. Примитивный элемент поля a является корнем этого многочлена. Многочлен, корнем которого является примитивный элемент, называется примитивным многочленом. Если в качестве *p*(*x*) выбрать примитивный неприводимый многочлен степени *m* над полем *GF*(2),то получим поле *GF*(2*m*) из всех 2*m* двоичных последовательностей длины *m*.

Поле *GF*(4) нельзя представить в виде совокупности чисел 0, 1, 2, 3. Построим его как расширенное поле по модулю многочлена *p*(*x*) = *x*2+*x*+1 .

В табл. 2 элементы этого поля представлены различными способами. Здесь принято, что примитивный элемент α является корнем *p*(α), т. е. 2++1 = 0.

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Последовательность длины 2** | **Многочлен** | **Степень** | **Логарифм** |
| 00 | 0 | 0 | – |
| 10 | 1 | 1 | 0 |
| 01 |  |  | 1 |
| 11 | 1+ | 2 | 2 |

Правила сложения и умножения в этом поле приведены на рис. 5.

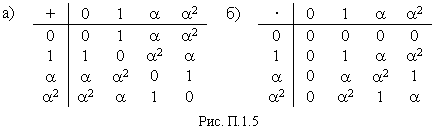


Рис.5

Формирование первой строки, первого столбца и диагональных элементов таблицы сложения, а также двух первых строк и двух первых столбцов таблицы умножения не вызывает затруднения. Поясним формирование других элементов:

1+ = 2, 1+2 = , +2 = 1;

·2 =3 =· (1+) = +2 = 1

на основе соотношения для примитивного элемента 2++1 = 0.

**Порядок выполнения работы**

Вариант задания на выполнение лабораторной работы выдаётся преподавателем

**Задание 2.1.** Сформировать поле из восьми элементов 

*Решение.* Поскольку  число простое, то над полем из двух элементов все неприводимые полиномы третьей степени являются примитивными. Зафиксируем неприводимый полином степени 3, например . Обозначим через α его корень, принадлежащий  Тогда  (так как характеристика поля  равна 2, то ). Тогда , , , , .

Следовательно, поле  можно задать в виде таблицы из двух столбцов: в левом столбце запишем все различные степени , в правом – соответствующие этим степеням суммы вида 

Таблица элементов поля :

α-∞| 0

α1 | α

α2 | α2

α3 | α+1

α4 | 

α5 | α2+α+1

α6 | α2+1

α7 | 1.

**Индивидуальные задания**

1. Составить таблицы сложения и умножение в поле *GF* (*p*).

2. Сформировать поле Галуа с 32-мя элементами (варианты 1 – 12) и с   
16-ю элементами (варианты 13 – 15), а также с примитивным полиномом 

**Вариант 1.**

1. *р* = 7 2. 

**Вариант 2.**

1. *p* = 11 2. 

**Вариант 3.**

1. *p* = 13 2. 

**Вариант 4.**

1. *p* = 17 2. 

**Вариант 5.**

1. *p* = 19 2. 

**Вариант 6.**

1. *p* = 23 2. 

**Вариант 7.**

1. *p* = 29 2. 

**Вариант 8.**

1. *p* = 31 2. 

**Вариант 9.**

1. *p* = 31 2. 

**Вариант 10.**

1. *p* = 7 2. 

**Вариант 11.**

1. *p* = 11 2. 

**Вариант 12.**

1. *p* = 13 2. 

**Вариант 13.**

1. *p* = 17 2. 

**Вариант 14.**

1. *p* = 23 2. 

**Вариант 15.**

1. *p* = 29 2. 