МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Практическая работа №6**

по дисциплине «Основы информационной безопасности»

на тему: Теория чисел

Выполнил студент 2 курса 7 группы специальность ПОИБМС Володькин Никифор Дмитриевич

(Ф.И.О.)

Преподаватель Ржеутская Надежда Викентьевна

(Ф.И.О.)

**Цель: получение основных сведений из курса теории чисел.**

**Теоретические сведения**

Ниже рассматриваются: *N* – множество натуральных чисел, *Z* – множество рациональных чисел. Множество целых чисел *Z* – счетное, состоит из элементов 0; ±1; ±2; …; ± *n*,…. На нем определены две алгебраические операции – сложение и умножение. Эти операции обладают следующими свойствами (для любых ):

1. ассоциативность: ; ;

2. коммутативность: ; ;

3. существует нейтральный элемент – 0 и 1 соответственно:



4.  – закон дистрибутивности;

5. для каждого целого  существует единственное противоположное, то есть такое целое *b*, что *a* + *b* = *b* + *a* = 0.

*Теорема 2.1* (*О делении с остатком*). Для любых целых чисел *a* и *b*, , существует единственные целые числа *q* и  , такие, что .

В этом равенстве  называют остатком, а  – частным (неполным частным – при ) от деления *a*  на  При *r* = 0 величины *b* и *q* называют делителями или множителями числа *а*. Читатель со школьной скамьи умеет находить частное и остаток методом деления уголком.

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

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

*Лемма 2.1.* Если в равенстве  все слагаемые – целые числа и все, кроме может быть одного, делятся на целое , то и это исключенное слагаемое делится на .

**Определение 2.1*.***Если целые числа  делятся на целое , то *d*  называют их *общим делителем*.

В дальнейшем речь идет только о положительных целых делителях.

**Определение 2.2.** Максимальный из общих делителей целых чисел  называется их *наибольшим общим делителем* и обозначается через НОД ().

*Теорема 2.2.* Если *,* то НОД *(a, b)*=НОД *(b, c).*

Теорема 2.2 позволила Евклиду (примерно 2300 лет тому назад) обосновать следующий факт.

*Теорема 2.3.* Наибольший общий делитель целых чисел  *a* и *b*   равен последнему отличному от нуля остатку цепочки равенств:

*;*

*;*

*…………………*

**

**

то есть  *=* НОД *.*

Теорема 2.3 формулирует алгоритм Евклида 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 НОД *(a, b).*

**Определение 2.3.** Натуральное число ** называется *простым*, если оно делится только на1 и на себя.

*Теорема 2.5.* Всякое натуральное число ** либо является простым числом, либо имеет простой делитель.

Заметим, что из соотношения  натуральных чисел, больших единицы, следует, что, либо *p,* либо *q* принадлежит отрезку . Легко видеть, что наименьший натуральный делитель ** натурального числа ** является простым числом. Исторически первый метод проверки натурального числа ** на простоту заключается 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 2.6 (Евклид).* Простых чисел бесконечно много.

Значение простых чисел в том, что они по теореме 2.5 являются составными кирпичиками всех натуральных чисел.

**Определение 2.4.** Целые числа *a*  и  *b* называются *взаимно простыми,* еслиНОД .

*Теорема 2.7* (*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.** НОД** тогда и только тогда, когдаНОД иНОД .

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

*Лемма 2.2.* Пусть произведение целых чисел *ab* делится на целое число *с* и НОД . Тогда *b*  делится на  *с*.

*Теорема 2.8**(Основная теорема арифметики)*. Всякое целое число ** однозначно раскладывается в произведение простых множителей

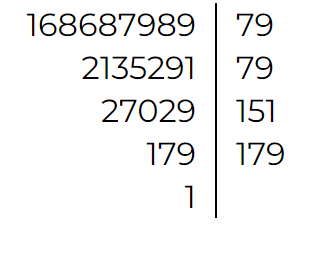
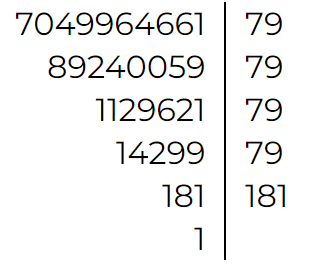
*.*

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

**Определение 2.5.**Целые числа *а* и *b* называются сравнимыми по модулю *m*, если они удовлетворяют одному из условий теоремы 2.9.Этот факт обозначают формулой ** илии называют данную формулу сравнением.

**Выполнение работы**

**Было найдено каноническое разложение чисел а = 7049964661, b = 168687989:**



Следовательно, **7049964661=794 ∙ 181**; **168687989=792 ∙ 151 ∙ 179**.

**Был найден НОД(a, b) алгоритмом Евклида:**

**7049964661 = 168687989 ∙ 41 + 133757112,**

**168687989 = 133757112 ∙ 1 + 34930877,**

**133757112 = 34930877 ∙ 3 + 28964481,**

**34930877 = 28964481 ∙ 1 + 5966396,**

**28964481 = 5966396 ∙ 4 + 5098897,**

**5966396 = 5098897 ∙ 1 + 867499,**

**5098897 = 867499 ∙ 5 + 761402,**

**867499 = 761402 ∙ 1 + 106097,**

**761402 = 106097 ∙ 7 + 18723,**

**106097 = 18723 ∙ 5 + 12482,**

**18723 = 12482 ∙ 1 + 6241,**

**12482 : 6241 = 2.**

Следовательно, **НОД(a, b) = 6241.**

**Был найден НОД(a, b) разложением чисел на простые множители:**

Т. к. **7049964661=794 ∙ 181**; **168687989=792 ∙ 151 ∙ 179**, то **НОД(a, b) = 79 ∙ 79 = 6241.**

**С помощью расширенного алгоритма Евклида были найдены целые u, v, удовлетворяющие соотношению Безу: au + bv = НОД(a, b):**

Составим соотношение Безу:

7049964661 = 168687989 ∙ 41 + 133757112, поэтому 133757112 = 7049964661 – 168687989 (-41)

168687989 = 133757112 ∙ 1 + 34930877, поэтому 34930877 = 168687989 + 133757112 (-1)

133757112 = 34930877 ∙ 3 + 28964481, поэтому 28964481 = 133757112 + 34930877(-3)

34930877 = 28964481 ∙ 1 + 5966396, поэтому 5966396 = 34930877 + 28964481(-1)

28964481 = 5966396 ∙ 4 + 5098897, поэтому 5098897 = 28964481 + 5966396 (-4)

5966396 = 5098897 ∙ 1 + 867499, поэтому 867499 = 5966396 + 5098897(-1)

5098897 = 867499 ∙ 5 + 761402, поэтому 761402 = 5098897 + 867499(-5)

867499 = 761402 ∙ 1 + 106097, поэтому 106097 = 867499 + 761402 (-1)

761402 = 106097 ∙ 7 + 18723, поэтому 18723 = 761402 + 106097(-7)

106097 = 18723 ∙ 5 + 12482, поэтому 12482 = 106097 + 18723(-5)

18723 = 12482 ∙ 1 + 6241, поэтому 6241 = 18723 + 12482(-1)

**Тогда 6241 = 18723 + 12482(-1) = 18723 + (106097 + 18723(-5))(-1) = 18723 ∙ 6 + 106097(-1)**

**Тогда 6241 = 18723 ∙ 6 + 106097(-1) = (761402 + 106097 (-7)) ∙ 6 + 106097(-1) = 761402 ∙ 6 + 106097(-43)**

**Тогда 6241 = 761402 ∙ 6 + 106097(-8) = 761402 ∙ 6 + (867499 + 761402(-1) )(-43) = 761402 ∙ 49 + 867499(-43)**

**Тогда 6241 = 761402 ∙ 49 + 867499(-43) = (5098897 + 867499(-5)) ∙ 49 + 867499(-43) = 867499(-288) + 5098897 ∙ 49**

**Тогда 6241 = 867499(-288) + 5098897 ∙ 49 = (5966396 + 5098897(-1))(-288) + 5098897 ∙ 49 = 5098897 ∙ 337 + 5966396(-288)**

**Тогда 6241 = 5098897 ∙ 337 + 5966396(-288) = (28964481 + 5966396(-4)) ∙ 337 + 5966396(-288) = 5966396(-1636) + 28964481 ∙ 337**

**Тогда 6241 = 5966396(-1636) + 28964481 ∙ 337 = (34930877 + 28964481(-1))(-1636) + 28964481 ∙ 337 = 28964481 ∙ 1973 + 34930877(-1636)**

**Тогда 6241 = 28964481 ∙ 1973 + 34930877(-1636) = (133757112 + 34930877(-3)) ∙ 1973 + 34930877(-1636) = 133757112 ∙ 1973 + 34930877(-7555)**

**Тогда 6241 = 133757112 ∙ 1973 + 34930877(-7555) = 133757112 ∙ 1973 + (168687989 + 133757112 (-1))(-7555) = 133757112 ∙ 9528 + 168687989(-7555)**

**Тогда = 133757112 ∙ 9528 + 168687989(-7555) = (7049964661 – 168687989 (-41)) ∙ 9528 + 168687989(-7555) = 7049964661 ∙ 9528 = 168687989(-398203)**

Следовательно, **7049964661 ∙ 9528 + 168687989** **∙** (**-398203) = 6241.**

**Был найден остаток от деления 19972004 на 17:**

1997 делится на 17 с остатком 8, 19972 делится на 17 с остатком 13. При дальнейшем возведении 1997 в степень остатки от деления будут чередоваться 8, 13, 8, 13, 8, … . Значит, в силу четности степени 2004 остаток от деления требуемого числа на 17 будет равен **13**.

**Вывод: получены основные сведения из курса теории чисел.**