Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Дисциплина «Основы защиты информации»

Отчёт по практическому занятию №6

Студент: Коренчук А.В.

ФИТ 2 курс 4 группа

Преподаватель: Ржеутская Н.В.

Минск 2022 г.

**Практическое занятие №6**

**«Криптографическая защита информации»**

Цель: получение основных сведений из курса теории чисел.

**Теоретическое введение**

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).*

Основные свойства сравнений:

**1.** Пусть *.* Тогда  для всякого целого *c*, то есть к обеим частям сравнения можно добавить (или вычесть из обеих частей) одно и то же число.

**2.** Сравнения можно почленно складывать и вычитать: если **, *,* то  

**3.** Сравнения можно почленно перемножать: если ** *,* то **.

**4.** Сравнения можно почленно возводить в любую натуральную степень: если *,* то **.

**5.** Если в сравнении ** числа *a*, *b*, *m* имеют общий множитель *d*, то на него сравнение можно сократить: **.

**6.** Сравнение можно сократить на общий множитель, взаимно простой с модулем: если **, НОД (*d*, *m*) = 1, то из сравнения  следует сравнимость  и  по модулю .

**7.** Сравнение можно умножить на любой целый множитель: если **, то  для всякого целого *t*.

**8.** Рефлексивность: ** для любого целого *а* и всякого натурального *m* >1.

**9.** Симметричность: если **, то **.

**10.** Транзитивность: если **, **, то .

*Теорема 2.10*(*Малая теорема Ферма*). Пусть *p –* простое число и целое число *a* не делится на . Тогд*а .*

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

# **Индивидуальное задание**

*Вариант 12.*

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

а = 16088437, b = 18216949.

**Решение.**

Следовательно, **16088437**= 2412 ∙ 277,

**18216949**=241 ∙ 269 ∙ 281.

2. Найти НОД  пользуясь a) алгоритмом Евклида, б) разложением чисел на простые множители.

**Решение.**

А) *Применим алгоритм Евклида:*

* 18216949 : 16088437 = 1 (остаток 2128512), так как 18216949 = 16088437 ∙ 1 + 2128512,
* 16088437 : 2128512 = 7 (остаток 1188853), так как 16088437 = 2128512 ∙ 7 + 1188853,
* 2128512 : 1188853 = 1 (остаток 939659), так как 2128512 = 1188853 ∙ 1 + 939659,
* 1188853 : 939659 = 1 (остаток 249194), так как 1188853 = 939659 ∙ 1 + 249194,
* 939659 : 249194 = 3 (остаток 192077), так как 939659 = 249194 ∙ 3 + 192077,
* 249194 : 192077 = 1 (остаток 57117), так как 249194 = 192077 ∙ 1 + 57117,
* 192077 : 57117 = 3 (остаток 20726), так как 192077 = 57117 ∙ 3 + 20726,
* 57117 : 20726 = 2 (остаток 15665), так как 57117 = 20726 ∙ 2 + 15665,
* 20726 : 15665 = 1 (остаток 5061), так как 20726 = 15665 ∙ 1 + 5061,
* 15665 : 5061 = 3 (остаток 482), так как 15665 = 5061 ∙ 3 + 482,
* 5061 : 482 = 10 (остаток 241), так как 5061 = 482 ∙ 10 + 241,

482 : 241 = 2 (остаток 0), так как 482 = 241 ∙ 2 + 0, равен нулю, значит НОД равен предыдущему остатку от деления.

Ответ: НОД (16088437; 18216949) = 241.

Б) *Найдём НОД чисел, воспользовавшись разложением на простые множители:*

Разложим числа на простые множители и подчеркнем общие множители чисел:

16088437 = 241 · 241 · 277

18216949 = 241 · 269 · 281

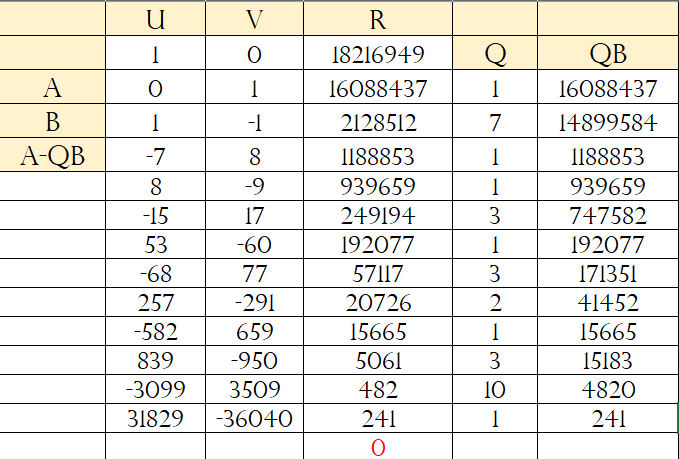
Общие множители чисел: 241

Следовательно, НОД (16088437; 18216949) = 241.

3. С помощью расширенного алгоритма Евклида найти целые *u*, *v*, удов летворяющие соотношению Безу: *au* + *bv* = НОД .

**Решение.**

НОД (16088437; 18216949) = 241



где **ui+1=ui-1-q·ui**;**vi+1=vi-1-q·vi**;

Следовательно, 18216949·31829+16088437·(-36040) =241

4 Найти остаток от деления 1997 2004 на 16.

4. Найти остаток от деления на 17.

1997 делится на 17 с остатком 8.

19972делится на 17 с остатком 13.

19973делится на 17 с остатком 2.

19974делится на 17 с остатком 16.

19975делится на 17 с остатком 9.

19976делится на 17 с остатком 4.

19977делится на 17 с остатком 15.

19978делится на 17 с остатком 1.

19979делится на 17 с остатком 8.

Получили один из предыдущих остатков, значит «зациклились». Число 19979 дает тот же остаток деления на 17, что и 19971. Значит, длина цикла равна 8. 2004 = 250 \* 8 + 4. Число 19972004 дает тот же остаток от деления на 17, что и 19974, то есть 16.

**Вывод:** в ходе работы были получены основные сведения из курса теории чисел**.**