Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студент: Костюкова А.О.

ФИТ 2 курс 4 группа

Преподаватель: Буснюк Н. Н.

Минск 2020

**Практическое занятие №8**

**Тема «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.

**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.

*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 .

*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.

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

**2.3. Индивидуальные задания к ПЗ №8 “Теория чисел”**

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

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

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

6. Найти остаток от деления данного числа на простое.

**Вариант 14**

1-3. *а* = 356216713, *b* = 31238065.

6. Найти остаток от деления  на 19.

**Задание 1.** Найти канонические разложения чисел *а* = 356216713, *b* = 31238065.

**Решение.**

|  |  |
| --- | --- |
| 356216713 | 47 7579079 | 47  161257 | 47 3431 | 47 73 | 73 1 | 31238065 | 5  6247613 | 6247613  1 |

Следовательно, 356216713=47\*47\*47\*47\*73, 31238065=5\*6247613.

**Задание 2.** Найти НОД (356216713*,* 31238065) пользуясь а) алгоритмом Евклида, б) разложением чисел на простые множители.

**Решение.** Применим алгоритм Евклида.

356216713 = 31238065\*11 + 12597998; 31238065 = 12597998\*2 +6042069;

12597998 = 6042069\*1 + 513860; 6042069 = 513860\*11 + 389609; 513860 = 389609\*1+ 124251; 389609 = 124251\*3 + 16856; 124251 = 16856\*7 + 6259;

16856 = 6259\*2 + 4338; 6259 = 4338\*1 + 1921; 4338 = 1921\*2 + 496;

1921 = 496\*3 + 433; 496 = 433\*1 + 63; 433 = 63\*6 + 55; 63 = 55\*1 + 8;

55 = 8\*6 + 7; 8 = 7\*1 + 1; 7 = 7\*1.

Следовательно, НОД (356216713*,* 31238065) = 1.

Найдём НОД (*a, b*), воспользовавшись разложением на простые множители чисел *a* и *b*, полученным в решении предыдущего задания: 356216713=47\*47\*47\*47\*73; 31238065=5\*6247613. Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел: НОД (356216713*,* 31238065) = 1.

**Задание 3.** С помощью расширенного алгоритма Евклида найти целые числа *u*,*v*, удовлетворяющие соотношению Безу:  для целых чисел *а* = 356216713, *b* = 31238065.

**Решение.** Сначала найдем по алгоритму Евклида НОД (356216713*,* 31238065).

356216713 = 31238065\*11 + 12597998; 31238065 = 12597998\*2 + 6042069;

12597998 = 6042069\*1 + 513860; 6042069 = 513860\*11 + 389609;

513860 = 389609\*1+ 124251; 389609 = 124251\*3 + 16856;

124251 = 16856\*7 + 6259; 16856 = 6259\*2 + 4338;

6259 = 4338\*1 + 1921; 4338 = 1921\*2 + 496;

1921 = 496\*3 + 433; 496 = 433\*1 + 63;

433 = 63\*6 + 55; 63 = 55\*1 + 8;

55 = 8\*6 + 7; 8 = 7\*1 + 1; 7 = 7\*1.

Следовательно, НОД (356216713*,* 31238065) = 1.

Теперь построим соотношение Безу для данных *a* и *b.*

356216713 = 31238065\*11 + 12597998; поэтому 12597998 = 356216713 + 31238065∙(-11);

31238065 = 12597998\*2 + 6042069; поэтому 6042069 = 31238065 + 12597998∙(-2);

12597998 = 6042069\*1 + 513860; поэтому 513860 = 12597998 + 6042069\*(-1);

6042069 = 513860\*11 + 389609; поэтому 389609 = 6042069 + 513860\*(-11);

513860 = 389609\*1+ 124251; поэтому 124251 = 513860 + 389609\*(-1);

389609 = 124251\*3 + 16856; поэтому 16856 = 389609 + 124251\*(-3);

16856 = 6259\*2 + 4338; поэтому 4338 = 16856 + 6259\*(-2);

6259 = 4338\*1 + 1921; поэтому 1921 = 6259 + 4338\*(-1);

…

55 = 8\*6 + 7; поэтому 7 = 55 + 8\*(-6);

1 = 8\*6 + 7 = 356216713\*(-3967768) + 31238065\*45245609 = 1.

**Задание 4.**

а)Найти остаток от деления  на 19.

**Решение.**

Метод сравнений 