Учреждение образования

«Белорусский государственный технологический университет»

**Практическое занятие №6**

**«Криптографическая защита информации»**

Выполнил:

Студент 2 курса 1 группы ФИТ

Палазник Арсений Викторович

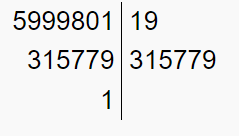
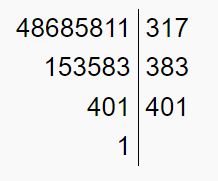
Цель: получение основных сведений из курса теории чисел.

**Вариант 17**

а = 5999801, b = 48685811.

Найти остаток от деления  на 17.

**Задание 1.** Найти канонические разложения чисел *a* и *b*.

5999801 = 19 \* 311577948685811 = 317 \* 383 \* 401

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

а) Нужно отсортировать числа в порядке возрастания: (48685811; 5999801)

Возьмем наименьшее число (48685811) как делитель

48685811 = 5999801 \* 8 + 687403

5999801 = 687403 \* 8 + 500577

687403 = 500577 \* 1 + 186826

500577 = 186826 \* 2 + 126925

186826 = 126925 \* 1 + 59901

126925 = 59901 \* 2 + 7123

59901 = 7123 \* 8 + 2917

7123 = 2917 \* 2 + 1289

2917 = 1289 \* 2 + 339

1289 = 339 \* 3 + 272

339 = 272 \* 1 + 67

272 = 67 \* 4 + 4

67 = 4 \* 16 + 3

4 = 3 \* 1 + 1

3 = 3 \* 1 + 0

НОД (48685811; 5999801) = 1

б) Разложим числа на простые множители и подчеркнем общие множители чисел:

5999801= 19 \* 315779\* 148685811= 317 \* 383 \* 401 \* 1

Общие множители чисел: 1

НОД (48685811; 5999801) = 1 \* 1 = 1

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

*Дано:*

а = 5999801, b = 48685811

НОД (5999801; 48685811) = 1

*Решение:*

Построим соотношение Безу для данных a и b:

48685811 = 5999801 \* 8 + 687403, поэтому 687403 = 48685811 + 5999801 \* (-8)

5999801 = 687403 \* 8 + 500577, поэтому 500577 = 5999801 + 687403 \* (-8)

687403 = 500577 \* 1 + 186826, поэтому 186826 = 687403 + 500577 \* (-1)

500577 = 186826 \* 2 + 126925, поэтому 126925 = 500577 + 186826 \* (-2)

186826 = 126925 \* 1 + 59901, поэтому 59901 = 186826 + 126925 \* (-1)

126925 = 59901 \* 2 + 7123, поэтому 7123= 126925 + 59901 \* (-2)

59901 = 7123 \* 8 + 2917, поэтому 2917= 59901 + 7123 \* (-8)

7123 = 2917 \* 2 + 1289, поэтому 1289= 7123 + 2917 \* (-2)

2917 = 1289 \* 2 + 339, поэтому 339= 2917 + 1289 \* (-2)

1289 = 339 \* 3 + 272, поэтому 272= 1289 + 339 \* (-3)

339 = 272 \* 1 + 67, поэтому 67= 339 + 272 \* (-1)

272 = 67 \* 4 + 4, поэтому 4= 272 + 67 \* (-4)

67 = 4 \* 16 + 3, поэтому 3= 67+ 4 \* (-16)

4 = 3 \* 1 + 1, поэтому 1 = 4 + 3 \* (-1)

3 = 3 \* 1 + 0, поэтому 0 = 3 + 3 \* (-1)

Проведем вычисления в обратном порядке

3 = 4 + 3 \* (-1) = 4 + (67 + 4 \* (-16)) \* (-1) =

= 5999801 *\* 12350872 +* 48685811 *\* (-1522061)*

Т.е. 1 = 5999801 *\* u +* 48685811 *\* v,*

*т.к.* 1 = 5999801 *\* 12350872 +* 48685811 *\* (-1522061)*

*где u = 12350872, v = -1522061*

**Задание 6****.** Найти остаток от деления  на 17.

2005 делится на 17 с остатком 16.

20052 делится на 17 с остатком 1.

20053 делится на 17 с остатком 16.

20054 делится на 17 с остатком 1.

Получили один из предыдущих остатков, значит «зациклились». Число 20053 дает тот же остаток деления на 17, что и 2005. Значит, длина цикла равна 2. Число 20052003 дает тот же остаток от деления на 7, что и 2005, то есть 16.