Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**Практическое занятие №8**

Криптографическая защита информации

Выполнил:

Студент 2 курса 7 группы ФИТ

Жуховцов Владислав Сергеевич

Проверил:

Барковский Евгений Валерьевич

**Минск 2022 г.**

**Цель работы**: Получение основных сведений из курса теории чисел

**Задание**

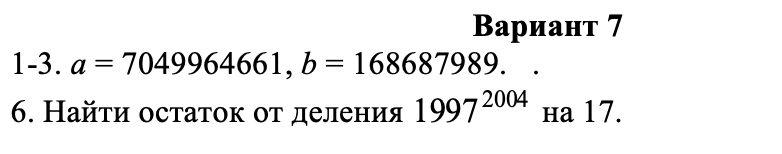
1.Найти канонические разложения чисел *а* и *b*.

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

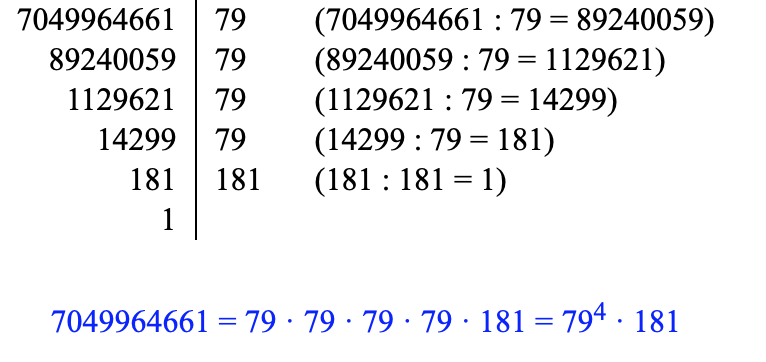
3. С помощью расширенного алгоритма Евклида найти целые *u*, *v*, удовлетворяющие соотношению Безу: *au* + *bv* = НОД(a, b).

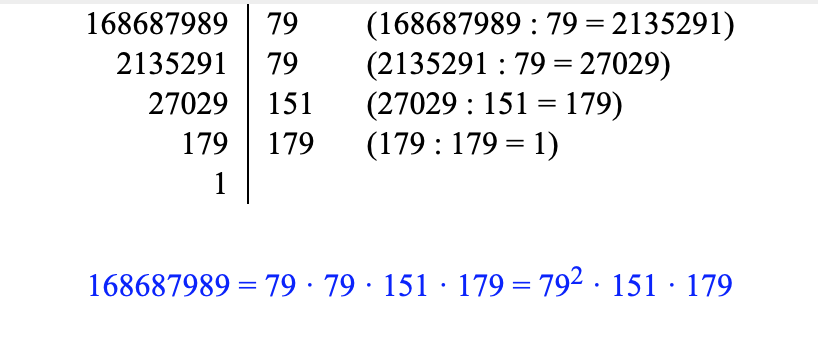
6. Найти остаток от деления данного числа на простое.

***Вариант 7***



1. **Каноническое разложение чисел a и b**





1. **Найти НОД пользуясь**

**А)** 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 + 0

Остаток от деления = 0, следовательно, НОД = 6241

**Б)** Разложением на простые множители

7049964661 = 79\*79\*79\*79\*181

168687989 = 79\*79\*151\*179

Общий множитель чисел: 79

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

По алгоритму Евклида НОД равен 6241.

7049964661 = 1686879893 \* 4 + 302445089 поэтому 302445089 = 704996466 + 168687989 \* (-4)

1686879893 = 302445089 \* 5 + 174654448 поэтому 174654448 = 1686879893 + 302445089 \* (-5)

302445089 = 174654448 \* 1 + 127790641 поэтому 127790641= 302445089 + 174654448 \* (-1)

174654448 = 127790641 \* 1 + 46863807 поэтому 46863807= 174654448 + 127790641 \* (-1)

127790641 = 46863807 \* 2 + 34063027 поэтому 34063027= 127790641 + 46863807 \* (-2)

46863807 = 34063027 \* 1 + 12800780 поэтому 12800780= 46863807 + 34063027 \* (-1)

34063027 = 12800780 \* 2 + 8461467 поэтому 8461467 = 34063027 + 12800780 \* (-2)

12800780 = 8461467 \* 1 + 4339313 поэтому 4339313= 12800780 + 8461467 \* (

-1)

8461467 = 4339313 \* 1 + 4122154 поэтому 4122154 = 8461467 + 4122154 \* (-1)

4339313 = 4122154 \* 1 + 217159 поэтому 217159 = 4339313 +4122154 \* (-1)

4122154 = 217159 \* 18 + 213292 поэтому 213292 = 4122154 + 217159 \* (-18)

217159 = 213292 \* 1 + 3867 поэтому 217159 = 217159 + 213292 \* (-1)

213292 = 3867 \* 55 + 607 поэтому 607 = 213292 + 3867 \* (-55)

3867 = 607 \* 6 + 225 поэтому 225 = 3867 + 607 \* (-6)

607 = 225 \* 11 + 1 поэтому 1 = 225 + 607 \* (-11)

225 = 1 \* 224 + 1 поэтому 1 = 225 + 2254\* (-1)

1 = 225 + 2254\* (-1)= 225 + (225 + 607 \* (-11))\*(-2) и т.д.

Получим 1 = (9528) \* 7049964661 + 1686879893 \* (-398203)

U = 9528

V = -398203

1. **Найти остаток от деления**

на 17

1997 делится на 17 с остатком 8.

1997^2 делится на 17 с остатком 13.

1997^3 делится на 17 с остатком 2.

1997^4 делится на 17 с остатком 16.

1997^5 делится на 17 с остатком 13.

Число 1997^5 дает тот же остаток деления на 17, что и 1997^2. Значит, длина цикла равна 3. 1997=665\*3+2. 1997 делим на длину цикла, получаем целое число и остаток. Число дает тот же остаток от деления на 17, что и 1997^3, то есть 2.

(mod 17) = 2

**Вывод:** в ходе практической работы я получил основные сведения из курса теории чисел.