Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Отчет

К практической работе №8:

Основы защиты информации

«Криптографическая защита информации»

Выполнил:

Студент 2 курса 2 группы ФИТ

Радивил Данила Юрьевич

**Минск 2022**

**Практическое занятие №8**

**«Криптографическая защита информации»**

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

**Задания для аудиторной работы**

**Задание 1.** Найти канонические разложения чисел 

**Решение.**

Следовательно, 627=3∙11∙19 399=3∙7∙19.

**Задание 2.** Найти НОД (627*,* 399) пользуясь а) алгоритмом Евклида, б) разложением чисел на простые множители.

**Решение.** Применим алгоритм Евклида.

627=399∙1 + 228; 399 = 228∙1 + 171; 228 = 171∙1 + 57; 171 = 57∙3.

Следовательно, НОД (627; 399) = 57.

Найдём НОД (*a, b*), воспользовавшись разложением на простые множители чисел *a* и *b*, полученным в решении предыдущего задания: 627=3∙11∙19; 399=3∙7∙19. Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел: НОД (627;399) = 3∙19 = 57.

Найдём НОД(*а, *) методом вычитаний:

627–399 = 228; 399–228 = 171; 228–171= 57; 171–57 = 114;

114–57 = 57; 57–57 = 0. Следовательно, НОД (627; 399) = 57.

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

**Решение.** Сначала найдем по алгоритму Евклида НОД (110, 48).

110 = 48∙2 + 14; 48 = 14∙3 + 6; 14 = 6∙2 + 2; 6 = 3∙2.

Следовательно, НОД (110, 48) = 2.

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

110 = 48∙2 + 14; поэтому 14 = 110 + 48∙(-2);

48 = 14∙3 + 6; поэтому 6 = 48 + 14∙(-3);

14 = 6∙2+2; поэтому 2 = 14 + 6∙(-2). В это равенство подставим выше полученное выражение для 6 и приведем подобные относительно чисел 48 и 14. Итак, 2 = 14+6∙(-2) = 14+(48+14∙(-3))(-2) = 14∙7+48∙(-2). В полученное выражение для НОД(110, 48) = 2 подставим вышеприведенное выражение числа 14. Получим окончательно

2 = 14∙7+48∙(-2) = (110+48∙(-2))7+48∙(-2)=110∙7+48∙(-16) = 2.

    .

**Задание 4.**

а)Найти остаток от деления 2100 на 3.

**Решение.** 2 делится на 3 с остатком 2, 22 делится на 3 с остатком 1. При дальнейшем возведении двойки в степень остатки от деления будут чередоваться 2, 1, 2, 1, 2, … . Значит, в силу четности степени 100 остаток от деления требуемого числа на 3 будет равен 1.

2-й способ – методом сравнений, по аналогии с примером 1.6. 

б) Найти остаток от деления  на 7.

**Решение.** Заменим каждое число на его остаток от деления на 7:

\_1989 | 7 \_1990 | 7 1991 = 7 ∙ 284 + 3;

14 | 284 14 | 284

\_58 \_59 1992 = 7 ∙ 284 + 4.

56 56

\_29 \_30

28 28

1 2

1∙2∙3+43 = 6 + 64 = 70. 70:7 = 10. Следовательно, остаток равен нулю.

в) Найти остаток от деления  на 8.

**Решение.** Заменим 9 на его остаток 1 от деления на 8. Имеем . Значит, остаток от деления  на 8 равен 1.

г) Найти остаток от деления  на 7.

**Решение.** 3 делится на 7 с остатком 3.  делится на 7 с остатком 2. Далее достаточно на 3 умножить только остаток и делать выводы. делится на 7 с остатком 6,  делится на 7 с остатком 4,  делится на 7 с остатком 5,  делится на 7 с остатком 1,  делится на 7 с остатком 3. Получили один из предыдущих остатков, значит «зациклились». Число дает тот же остаток деления на 7, что и 31. Значит, длина цикла равна 6. . Число  дает тот же остаток от деления на 7, что и , то есть 6.

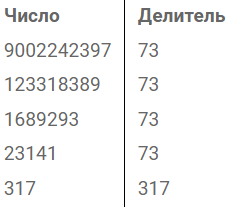
**2.3. Индивидуальные задания к ПЗ №8 “Теория чисел”**

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

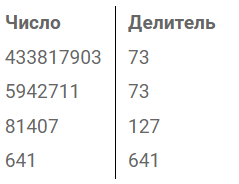
**Задание 1.** Найти канонические разложения чисел а = 9002242397, b = 433817903

**Решение.**

**Число а**

****

**Число b**

****

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

**Задание 2**

**Алгоритм Евклида**

****

9002242397 = 433817903 \* 20 + 325 884 337

433 817 903 = 325 884 337 \* 1 + 107 933 566

325 884 337 = 107 933 566 \* 3 + 2 083 639

107 933 566 = 2 083 639 \* 51 + 1 667 977

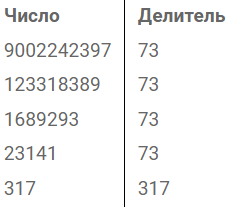
2 083 639 = 1 667 977 \* 1 + 415 662

1 667 977 = 415 662 \* 4 + 5329

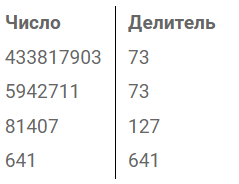
415 662 = 5329 \* 78

НОД чисел a и b = 5329;

**Разложение на простые множители**

****

**Число b**

****

**Общие множители 73 и 73, тогда НОД = 73 \* 73 = 5329;**

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

**Задание 3.** С помощью расширенного алгоритма Евклида найти целые числа *u*,*v*, удовлетворяющие соотношению Безу:  для целых чисел *а* = 9002242397, *b* = 433817903.

**Решение.** Сначала найдем по алгоритму Евклида НОД (9002242397, 433817903).

НОД = 5329;

9002242397 = 433817903 \* 20 + 325 884 337

433 817 903 = 325 884 337 \* 1 + 107 933 566

325 884 337 = 107 933 566 \* 3 + 2 083 639

107 933 566 = 2 083 639 \* 51 + 1 667 977

2 083 639 = 1 667 977 \* 1 + 415 662

1 667 977 = 415 662 \* 4 + 5329

415 662 = 5329 \* 78



5329 = 9 002 242 397 \* (-1041) + 433 817 903 \* 21602;

6. Найти остаток от деления данного числа на простое.

Найти остаток от деления  на 19.

**Задание 4.**

Найти остаток от деления  на 19.

**Решение.** Заменим 2004 на его остаток 9 от деления на 19. Имеем 92998 = 9. Значит, остаток от деления 20042998 на 19 равен 9.

**Вариант 18**

1-3. *а* = 9002242397, *b* = 433817903.

Найти остаток от деления  на 19.

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