Учреждение образования

«Белорусский государственный технологический университет»

**Отчеты по практическим работам**

По дисциплине: «Основы защиты информации»

Студентки 2 курса 1 группы ФИТ

Шимчёнок Елизаветы Константиновны

**2022 г.**

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

**Вариант 12**

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

а = 16088437, b = 18216949

16088437 | 241

66757 | 241

277 | 1

1

18216949 | 241

75589 | 269

281 | 1

1

16088437 = 241 \* 241 \* 1;

18216949 = 241 \* 269 \* 1.

**Задание 2.** Найти НОД (a, b) пользуясь:

а = 16088437, b = 18216949

1. алгоритмом Евклида

Расположим числа в порядке возрастание (18216949, 16088437)

В соответствии с теоремой 2.2

18216949 = 16088437\*1+2128512,

16088437 = 2128512\*7+1188853,

2128512 = 1188853\*1+939659,

1188853 = 939659\*1+249194,

939659 = 249194\*3+192077,

249194 = 192077\*1+57117,

192077 = 57117\*3+20726,

57117 = 20726\*2+15665,

20726 = 15665\*1+5061,

15665 = 5061\*3+482,

5061 = 482\*10+241,

482 = 241\*2+0;

НОД (16088437, 18216949) = 241;

1. разложением чисел на простые множители

Найдём НОД (a, b), воспользовавшись разложением на простые множители чисел a и b, полученным в решении предыдущего задания:

16088437=241\*241\*1,

18216949=241\*269\*1.

Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел: НОД (16088437; 18216949) = 241.

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

а = 16088437, b = 18216949

Сначала найдем по алгоритму Евклида НОД (16088437, 18216949).

18216949 = 16088437\*1+2128512,

16088437 = 2128512\*7+1188853,

2128512 = 1188853\*1+939659,

1188853 = 939659\*1+249194,

939659 = 249194\*3+192077,

249194 = 192077\*1+57117,

192077 = 57117\*3+20726,

57117 = 20726\*2+15665,

20726 = 15665\*1+5061,

15665 = 5061\*3+482,

5061 = 482\*10+241,

482 = 241\*2+0;

НОД (16088437, 18216949) = 241.

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).

18216949=16088437\*1+2128512,

поэтому 2128512= 18216949+ 16088437 ∙ (-1);

16088437=2128512\*7+1188853,

поэтому 1188853= 16088437+ 2128512 ∙ (-7);

2128512=1188853\*1+939659,

поэтому 939659= 2128512+ 1188853 ∙ (-1);

1188853=939659\*1+249194,

поэтому 249194= 1188853+ 939659 ∙ (-1);

939659=249194\*3+192077,

поэтому 192077= 939659+ 249194 ∙ (-3);

249194=192077\*1+57117,

поэтому 57117= 249194+ 192077 ∙ (-1);

192077=57117\*3+20726,

поэтому 20726= 192077+ 57117 ∙ (-3);

57117=20726\*2+15665,

поэтому 15665= 57117+ 20726 ∙ (-2);

20726=15665\*1+5061,

поэтому 5061= 20726+ 15665 ∙ (-1);

15665=5061\*3+482,

поэтому 482= 15665+ 5061 ∙ (-3);

5061=482\*10+241,

поэтому 241= 5061+ 482 ∙ (-10);

482=241\*2+0;

В это равенство подставим выше полученное выражение для 241 и приведем подобные относительно чисел 482, 5061, 15664, 20726, 57117, 191077, 249194, 939659, 1188853, 2128512, 16088437.

241= 5061+ 482(-10) =

= 5061 + (15665 + 5061(-3))(-10) =

= 5061 + 15665(-10) + 5061(30) =

= 5061(31) + 15665(-10) =

= (20726 + 15665(-1))(31) + 15665(-10) =

= 20726(31) + 15665(-31) + 15665(-10) =

= 15665(-41)+20726(31) =

= (57117 + 20726(-2))(-41) + 20726(31) =

= 57117(-41) + 20726(82) + 20726(31) =

= 20726(113) + 57117(-41) =

= (192077 + 57117(-3))(113) + 57117(-41) =

= 192077(113) + 57117(-339) + 57117(-41) =

= 192077(113) + 57117(-380) =

= 192077(113) + (249194 + 192077(-1))(-380) =

= 192077(113) + 249194(-380) + 192077(380) =

= 249194(-380) + 192077(493) =

= 249194(-380) + (939659 + 249194(-3))(493) =

= 249194(-380) + 939659(493) + 249194(-1479) =

= 939659(493) + 249194(-1859) =

= 939659(493) + (1188853+ 939659(-1))(-1859) =

= 939659(493) + 1188853(-1859) + 939659(1859) =

= 939659(2352) + 1188853(-1859) =

= (2128512 + 1188853(-1))(2352) + 1188853(-1859) =

= 2128512(2352) + 1188853(-2352) + 1188853(-1859) =

= 2128512(2352) + 1188853(-4211) =

= 2128512(2352) + (16088437 + 2128512(-7))(-4211) =

= 2128512(2352) + 16088437(-4211) + 2128512(29477) =

= 2128512(31829) + 16088437(-4211) =

= (18216949 + 16088437(-1))(31829) + 16088437(-4211) =

= 18216949(31829) + 16088437(-31829) + 16088437(-4211) =

= 18216949(31829) + 16088437(-36040).

    .

**Задание 6.** Найти остаток от деления 19952004 на 16.

1995 делится на 16 с остатком 11,

19952 делится на 16 с остатком 9,

19953 делится на 16 с остатком 3,

19954 делится на 16 с остатком 1,

19955делится на 16 с остатком 11.

Получили один из предыдущих остатков, значит «зациклились». Число 19955 дает тот же остаток деления на 16, что и 19951.

Значит, длина цикла равна 4.

2004=501 \* 4.

Число 19952004 дает тот же остаток от деления на 16, что и 19950, то есть 1.

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