**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

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

**Задание 1.** Найти канонические разложения чисел 

**Решение.**

|  |  |  |  |
| --- | --- | --- | --- |
| 5999801 | 19 | 48685811 | 317 |
| 315779 | 315779 | 153583 | 383 |
| 1 |  | 401 | 401 |
|  |  | 1 |  |

Следовательно, 5999801=19∙315779 48685811=317∙383∙401.

**Задание 2.** Найти НОД (48685811*,* 5999801) пользуясь а) алгоритмом Евклида, б) разложением чисел на простые множители.

**Решение.** Применим алгоритм Евклида.

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 = 16∙4 + 3;

16 = 3∙5 + 1;

3 = 1∙3.

Следовательно, НОД (48685811*,* 5999801) = 1.

Найдём НОД (*a,b*), воспользовавшись разложением на простые множители чисел *a* и *b*, полученным в решении предыдущего задания: 48685811=317∙383∙401; 5999801=19∙315779. Наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел. Так как общие множители больше 1 у чисел отсутствуют, то НОД (48685811*,* 5999801) = 1.

Найдём НОД(*а,*) методом вычитаний:

48685811 – 5999801 = 42686010;

42686010 – 5999801 = 36686209;

36686209 – 5999801 = 30686408;

30686408 – 5999801 = 24686607;

24686607 – 5999801 = 18686806;

18686806 – 5999801 = 12687005;

12687005 – 5999801 = 6687204;

6687204 – 5999801 = 687403;

5999801 – 687403 = 5312398;

5312398 – 687403 = 4624995;

4624995 – 687403 = 3937592;

3937592 – 687403 = 3250189;

3250189 – 687403 = 2562786;

2562786 – 687403 = 1875383;

1875383 – 687403 = 1187980;

1187980 – 687403 = 500577;

687403 – 500577 = 186826;

500577 – 186826 = 313751;

313751 – 186826 = 126925;

186826 – 126925 = 59901;

126925 – 59901 = 67024;

67024 – 59901 = 7123;

59901 – 7123 = 52778;

52778 – 7123 = 45655;

45655 – 7123 = 38532;

38532 – 7123 = 31409;

31409 – 7123 = 24286;

24286 – 7123 = 17163;

17163 – 7123 = 10040;

10040 – 7123 = 2917;

7123 – 2917 = 4206;

4206 – 2917 = 1289;

2917 – 1289 = 1628;

1628 – 1289 = 339;

1289 – 339 = 950;

950 – 339 = 611;

611 – 339 = 272;

339 – 272 = 67;

272 – 67 = 205;

205 – 67 = 138;

138 – 67 = 71;

71 – 67 = 4;

67 – 4 = 63;

63 – 4 = 59;

59 – 4 = 55;

55 – 4 = 51;

51 – 4 = 47;

47 – 4 = 43;

43 – 4 = 39;

39 – 4 = 35;

35 – 4 = 31;

31 – 4 = 27;

27 – 4 = 23;

23 – 4 = 19;

19 – 4 = 15;

15 – 4 = 11;

11 – 4 = 7;

7 – 4 = 3;

4 – 3 = 1;

3 – 1 = 2;

2 – 1 = 1;

1 – 1 = 0;

Следовательно, НОД (48685811*,* 5999801) = 1.

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

**Решение.** Из предыдущего задания по алгоритму Евклида НОД (48685811*,* 5999801) = 1.

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).

В это равенство подставим выше полученное выражение для 3 и приведем подобные относительно чисел 4 и 67:

1 = 4+3∙(-1) = 4 + (67 + 4∙(-16))∙(-1) = 4∙17+67∙(-1).

Проделаем ещё несколько таких операций:

1 = 4∙17 + 67∙(-1) = (272 + 67∙(-4)) ∙17 + 67∙(-1) = 272∙17 + 67∙(-69);

1 = 272∙17 + 67∙(-69) = 272∙17 + (339 + 272∙(-1))∙(-69) = 339∙(-69) + 272∙86;

1 = 339∙(-69) + 272∙86 = 339∙(-69) + (1289 + 339∙(-3))∙86 = 1289∙86 + 339∙(-327);

1 = 1289∙86 + 339∙(-327) = 1289∙86 + (2917 + 1289∙(-2))∙(-327) = 2917∙(-327) + 1289∙740;

1 = 2917∙(-327) + 1289∙740 = 2917∙(-327) + (7123 + 2917∙(-2))∙740 = 7123∙740 + 2917∙(-1807);

1 = 7123∙740 + 2917∙(-1807) = 7123∙740 + (59901 + 7123∙(-8))∙(-1807) = 59901∙(-1807) + 7123∙(15196);

1 = 59901∙(-1807) + 7123∙(15196) = 59901∙(-1807) + (126925 + 59901∙(-2))∙(15196) = 126925∙15196 + 59901∙(-32199);

1 = 126925∙15196 + 59901∙(-32199) = 126925∙15196 + (186826 + 126925∙(-1))∙(-32199) = 186826∙(-32199) + 126925∙47395;

1 = 186826∙(-32199) + 126925∙47395 = 186826∙(-32199) + (500577 + 186826∙(-2))∙47395 = 500577∙47395 + 186826∙(-126989);

1 = 500577∙47395 + 186826∙(-126989) = 500577∙47395 + (687403 + 500577∙(-1))∙(-126989) = 687403∙(-126989) + 500577∙174384;

1 = 687403∙(-126989) + 500577∙174384 = 687403∙(-126989) + (5999801 + 687403∙(-8))∙174384 = 5999801∙174384 + 687403∙(-1522061);

Получим окончательно

1 = 5999801∙174384 + 687403∙(-1522061) = 5999801∙174384 + (48685811 + 5999801∙(-8))∙(-1522061) = 48685811∙(-1522061) + 5999801∙12350872 = 1.

.

**Задание 4.**

а)Найти остаток от деления  на 17.

**Решение**. 2005 делится на 17 с остатком 16, 20052 делится на 17 с остатком 1. При дальнейшем возведении двойки в степень остатки от деления будут чередоваться 17, 1, 17, 1, 17, … . Значит, в силу нечетности степени 2003 остаток от деления требуемого числа на 17 будет равен 16.

**2-й способ:** В силу свойства 4 сравнений:



Таким образом, остаток от деления  на 17 равен 16.

**Вывод.** В ходе данного практического занятия были изучены основные сведения из курса теории чисел. Были приобретены навыки канонического разложения чисел, нахождения НОД с помощью алгоритма Евклида, разложения чисел на простые множители, поиска целых чисел удовлетворяющих соотношению Безу с помощью расширенного алгоритма Евклида. Также были изучены и применены способы нахождения остатка от деления больших целых чисел.

12x≡1mod (779)

Поскольку НОД(12,779)=1, следовательно данное сравнение имеет 1 решение.

Используем свойство сравнений: a\*d ≡ b\*c (mod n) при a ≡ b (mod n) и d ≡ c (mod n)

12x≡1mod (779)

65 ≡ 65 (mod 779)

Умножим обе части сравнения на 65:

12\*65x ≡ 1\* 65 (mod 779)

780x ≡ 65 (mod 779)

779x ≡ 0 (mod 779)

Отсюда получим:

X ≡ 65