МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «Белорусский государственный технологический университет»

Кафедра информационных технологий

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

Выполнила:

Студентка 2 курса, 7 группы

Курносенко Софья Андреевна

Проверил:

Барковский Евгений Валерьевич

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

**2.1. Необходимые теоретические сведения**

Ниже рассматриваются: *N* – множество натуральных чисел, *Z* – множество рациональных чисел. Множество целых чисел *Z* – счетное, состоит из элементов 0; ±1; ±2; …; ± *n*,…. На нем определены две алгебраические операции – сложение и умножение. Эти операции обладают следующими свойствами (для любых ):

1. ассоциативность: ; ;

2. коммутативность: ; ;

3. существует нейтральный элемент – 0 и 1 соответственно:



4.  – закон дистрибутивности;

5. для каждого целого  существует единственное противоположное, то есть такое целое *b*, что *a* + *b* = *b* + *a* = 0.

*Теорема 2.1* (*О делении с остатком*). Для любых целых чисел *a* и *b*, , существует единственные целые числа *q* и  , такие, что .

В этом равенстве  называют остатком, а  – частным (неполным частным – при ) от деления *a*  на  При *r* = 0 величины *b* и *q* называют делителями или множителями числа *а*. Читатель со школьной скамьи умеет находить частное и остаток методом деления уголком.

*Следствие.* Пусть  – натуральное число,  Для всякого целого числа *a*  и максимального целого  с условием  существуют единственные целые  такие, что 

Такое равенство записывают сокращённо  или  (если *b* известно по контексту) и называют записью числа *a* в *b* – ичной позиционной системе счисления или системе счисления по основанию *b*. Нам кажется естественной привычная десятичная позиционная система записи целых чисел . В различных ситуациях более удобными оказываются другие основания. К примеру, во всех компьютерах на микроуровне вычисления проводятся в двоичной системе счисления. Для перехода к ней с десятичной применяют промежуточную – 16 - ричную систему счисления.

*Лемма 2.1.* Если в равенстве  все слагаемые – целые числа и все, кроме может быть одного, делятся на целое , то и это исключенное слагаемое делится на .

**Определение 2.1*.***Если целые числа  делятся на целое , то *d*  называют их *общим делителем*.

В дальнейшем речь идет только о положительных целых делителях.

**Определение 2.2.** Максимальный из общих делителей целых чисел  называется их *наибольшим общим делителем* и обозначается через НОД ().

*Теорема 2.2.* Если *,* то НОД *(a, b)*=НОД *(b, c).*

Теорема 2.2 позволила Евклиду (примерно 2300 лет тому назад) обосновать следующий факт.

*Теорема 2.3.* Наибольший общий делитель целых чисел  *a* и *b*   равен последнему отличному от нуля остатку цепочки равенств:

*;*

*;*

*…………………*

**

**

то есть  *=* НОД *.*

Теорема 2.3 формулирует алгоритм Евклида нахождения наибольшего общего делителя целых чисел. Его вариантом является следующий – второй способ вычисления наибольшего общего делителя по алгоритму Евклида – вычисляем последовательно разности  до получения последней ненулевой разности, которая и совпадает с НОД *(a, b).*

**Пример 2.1.** помощью алгоритма Евклида найти НОД (72, 26).

**Решение**. В соответствии с теоремой 2.2   ; . Следовательно, НОД (72, 26) = 2.

*Теорема 2.4.* Если *d* = НОД *(a, b)*, то существуют такие целые *u*  и *v*, что выполняется следующее соотношение (Безу): *d = au+ bv.*

**Пример 2.2.** Из примера 2.1 следует, что



Такой способ получения соотношения Безу для конкретных целых чисел называется расширенным алгоритмом Евклида. Он состоит из двух этапов: собственно алгоритма Евклида - прогонки вниз и прогонки вверх – последовательного выражения остатков в каждом из шагов предыдущего этапа (с соответствующим приведением подобных на каждом шаге).

**Определение 2.3.** Натуральное число ** называется *простым*, если оно делится только на1 и на себя.

*Теорема 2.5.* Всякое натуральное число ** либо является простым числом, либо имеет простой делитель.

Заметим, что из соотношения  натуральных чисел, больших единицы, следует, что, либо *p,* либо *q* принадлежит отрезку . Легко видеть, что наименьший натуральный делитель ** натурального числа ** является простым числом. Исторически первый метод проверки натурального числа ** на простоту заключается в делении его на простые числа, не превосходящие , носит название “решета Эратосфена”. К настоящему времени разработан достаточно большой цикл алгоритмов проверки числа на простоту.

*Теорема 2.6 (Евклид).* Простых чисел бесконечно много.

Значение простых чисел в том, что они по теореме 2.5 являются составными кирпичиками всех натуральных чисел.

**Определение 2.4.** Целые числа *a*  и  *b* называются *взаимно простыми,* еслиНОД .

*Теорема 2.7* (*Критерий взаимной простоты целых чисел*). Целые числа  *a* и *b* взаимно просты тогда и только тогда, когда существуют такие целые u и v, что выполняется равенство .

**Следствие.** НОД** тогда и только тогда, когдаНОД иНОД .

Важным в теории чисел и ее приложениях является следующее свойство взаимно простых целых чисел.

*Лемма 2.2.* Пусть произведение целых чисел *ab* делится на целое число *с* и НОД . Тогда *b*  делится на  *с*.

*Теорема 2.8**(Основная теорема арифметики)*. Всякое целое число ** однозначно раскладывается в произведение простых множителей

*.*

Если в этом равенстве собрать одинаковые множители, то получим каноническое разложение целого числа: .

**Пример 2.3.** Приведем примеры канонических разложений целых чисел:

а) 196 = 2⋅98 = 2⋅2⋅49 = 22⋅72;

б) 212-1 = 4095 = 32⋅5⋅7⋅13.

*Теорема 2.9.* Пусть *-* натуральное число*,* . Для любых целых чисел *a* и *b* следующие условия равносильны:

*1) a и b имеют одинаковые остатки от деления на *

*2) a – b делится на m, то есть a – b = mq для подходящего целого q;*

*3) a = b + mq для некоторого целого q.*

**Определение 2.5.**Целые числа *а* и *b* называются сравнимыми по модулю *m*, если они удовлетворяют одному из условий теоремы 2.9.Этот факт обозначают формулой ** илии называют данную формулу сравнением.

**Пример 2.4.** -57(mod 4) 11(mod 4) 23(mod 4) 3(mod 4).

**Пример 2.5.** Если  то всякое целое число сравнимо по модулю *m* со своим остатком от деления на *m*. Это следует из определения 2.5 и второго условия теоремы 2.9. Ведь *a*–*r* делится на *m*.

Основные свойства сравнений:

**1.** Пусть *.* Тогда  для всякого целого *c*, то есть к обеим частям сравнения можно добавить (или вычесть из обеих частей) одно и то же число.

**2.** Сравнения можно почленно складывать и вычитать: если **, *,* то  

**3.** Сравнения можно почленно перемножать: если ** *,* то **.

**4.** Сравнения можно почленно возводить в любую натуральную степень: если *,* то **.

**5.** Если в сравнении ** числа *a*, *b*, *m* имеют общий множитель *d*, то на него сравнение можно сократить: **.

**6.** Сравнение можно сократить на общий множитель, взаимно простой с модулем: если **, НОД (*d*, *m*) = 1, то из сравнения  следует сравнимость  и  по модулю .

**7.** Сравнение можно умножить на любой целый множитель: если **, то  для всякого целого *t*.

**8.** Рефлексивность: ** для любого целого *а* и всякого натурального *m* >1.

**9.** Симметричность: если **, то **.

**10.** Транзитивность: если **, **, то .

*Теорема 2.10*(*Малая теорема Ферма*). Пусть *p –* простое число и целое число *a* не делится на . Тогд*а .*

Теория сравнений и малая теорема Ферма позволяют быстро находить остаток от деления большого числа на простое число.

**Пример 2.6.** Найдем остаток от деления  на 31.

**Решение.** **. Поэтому в силу свойства 4 сравнений . Двоичная запись: 29=11101. Следовательно, для любого натурального *a* величина . Далее, . Поэтому . Тогда . Следовательно, . Таким образом, остаток от деления  на 31 равен 4.

**2.2. 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*.

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

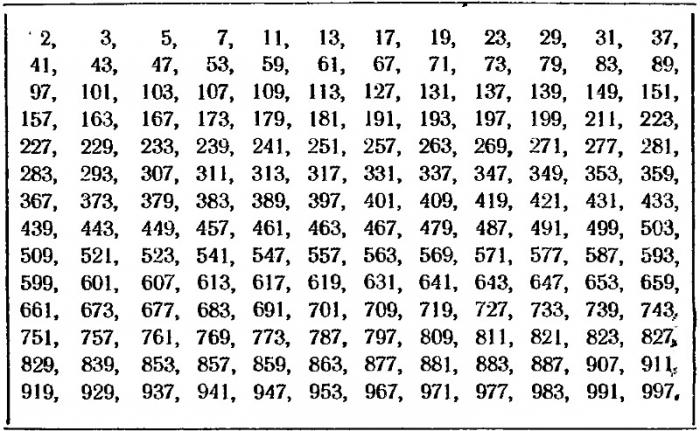
3. С помощью расширенного алгоритма Евклида найти целые *u*, *v*, удовлетворяющие соотношению Безу: *au* + *bv* = НОД .

4. Найти остаток от деления данного числа на простое.

**Вариант 8**

1-3. *а* = 83748733, *b* = 73435591.

4. Найти остаток от деления  на 11.



**Выполнение заданий**

**Задание 1.** Найти канонические разложения чисел *а* = 83748733, *b* = 73435591.

**Решение.**

|  |  |
| --- | --- |
| 83748733 | 89  940997 | 89  10573 | 97  109 | 109  1 | 73435591 | 73  1005967 | 89  11303 | 89  127 | 127  1 |

83748733 = 892 \* 97 \* 109

73435591 = 73 \* 892 \* 127

**Задание 2.** Найти НОД (83748733*,* 73435591) пользуясь а) алгоритмом Евклида, б) разложением чисел на простые множители.

**Решение.**

а) Применим алгоритм Евклида.

Для нахождения наибольшего общего делителя двух чисел нужно соблюдать такой порядок действий:

1. Большее число поделить на меньшее.
2. Меньшее число поделить на остаток, который получается после деления.
3. Первый остаток поделить на второй остаток.  
   Второй остаток поделить на третий и т. д.
4. Деление продолжается до тех пор, пока в остатке не получится нуль. Последний делитель и есть наибольший общий делитель.

83748733 = 73435591\*1 + 10313142

73435591 = 10313142\*7 + 1243597

10313142 = 1243597\*8 + 364366

1243597 = 364366\*3 + 150499

364366 = 150499\*2 + 63368

150499 = 63368\*2 + 23763

63368 = 23763\*2 + 15842

23763 = 15842\*1 + 7921

15842 = **7921**\*2

Таким образом, НОД (83748733*,* 73435591) = 7921

б) найдем НОД (83748733*,* 73435591) разложением чисел на простые множители

Найдём НОД (*a, b*), воспользовавшись разложением на простые множители чисел *a* и *b*, полученным в решении предыдущего задания: 83748733 = 892 \* 97 \* 109; 73435591 = 73 \* 892 \* 127. Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел: НОД (83748733*,* 73435591) = 892 = 7921

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

**Решение.**

Алгоритм Евклида был использован в пункте «а» задания 2, теперь построим соотношение Безу на основании данных оттуда.

Выразим остатки:

83748733 = 73435591\*1 + 10313142 => 10313142 = 83748733 –73435591\*1

73435591 = 10313142\*7 + 1243597 => 1243597 = 73435591 – 10313142\*7

10313142 = 1243597\*8 + 364366 => 364366 = 10313142 – 1243597\*8

1243597 = 364366\*3 + 150499 => 150499 = 1243597 – 364366\*3

364366 = 150499\*2 + 63368 => 63368 = 364366 – 150499\*2

150499 = 63368\*2 + 23763 => 23763 = 150499 – 63368\*2

63368 = 23763\*2 + 15842 => 15842 = 63368 – 23763\*2

23763 = 15842\*1 + 7921 => 7921 = 23763 – 15842\*1

15842 = **7921**\*2

Далее идет обратный ход алгоритма Евклида.

В обратном ходе алгоритма Евклида используем все равенства из прямого хода, двигаясь от последнего к первому.

Выражение для первого остатка с конца:

7921 = 23763 – 15842\*1

На место 15842 (второго остатка с конца) запишем выражение для 15842:

7921 = 23763 – (63368 – 23763\*2)\*1 = 23763 – 63368 + 23763\*2 =

23763\*3 – 63368

На место 23763 запишем соответствующее выражение:

23763\*3 – 63368 = (150499 – 63368\*2)\*3 – 63368 = 150499\*3 – 63368\*2\*3 – 63368 = 150499\*3 – 63368\*7

На место 63368 запишем соответствующее выражение:

150499\*3 – 63368\*7 = 150499\*3 – (364366 – 150499\*2)\*7 = 150499\*3 – 364366\*7 + 150499\*2\*7 = 150499\*17 – 364366\*7

На место 150499 запишем соответствующее выражение:

150499\*17 – 364366\*7 = (1243597 – 364366\*3)\*17 – 364366\*7 = 1243597\*17 – 364366\*3\*17 – 364366\*7 = 1243597\*17 – 364366\*58

На место 364366 запишем соответствующее выражение:

1243597\*17 – 364366\*58 = 1243597\*17 – (10313142 – 1243597\*8)\*58 = 1243597\*17 –10313142\*58 + 1243597\*8\*58 = 1243597\*481 –10313142\*58

На место 1243597 запишем соответствующее выражение:

1243597\*481 –10313142\*58 = (73435591 – 10313142\*7)\*481 –10313142\*58 = 73435591\*481 – 10313142\*7\*481 –10313142\*58 = 73435591\*481 – 10313142\*3425

На место 10313142 запишем соответствующее выражение:

73435591\*481 – 10313142\*3425 = 73435591\*481 – (83748733 –73435591\*1)\* 3425 = 73435591\*481 – 83748733\*3425 + 73435591\*1\*3425 = **73435591\*3906 – 83748733\*3425**

Таким образом,

*au* + *bv* = 83748733\*(─ 3425) + 73435591\*3906

**Задание 4.** Найти остаток от деления  на 11.

**Решение с применением теоремы Эйлера.**

Пусть x 19962003(mod 11)

1. Найдем НОД основания степени и модуля, т.е. (1996, 11).

1996 = 22 \* 499

11 = 11

Значит НОД(1996, 11) = 1

1. Заменим x на некоторое число, тем самым упростив основание степени.

Воспользуемся следующими теоремами:

▪ Пусть *-* натуральное число*,* . Для любых целых чисел *a* и *b* справедливо следующее условие:

a – b делится на m, то есть a – b = mq для подходящего целого q.

Тогда:

a = 1996

b = 5

m = 11

q = 181

19962003 = (11\*181 +5) 2003 => 19962003 – 52003 = 11\*1812003

Итак: 52003 19962003(mod 11)

▪ Сравнения можно почленно возводить в любую натуральную степень: если *,* то **.

Возведем в степень значения a и b:

5 1996 (mod 11)

1. Упростим показатель степени.

3.1) Функция Эйлера φ(n) определяется как количество натуральных чисел, не превосходящих n и взаимно простых с n.

Разложение 11 на простые множители:

11 = 111

Тогда: φ(11) = 110\*(11–1) = 10

3.2) Составим сравнение числа 2003 (степень) и y по модулю 10:

2003 y (mod 10)

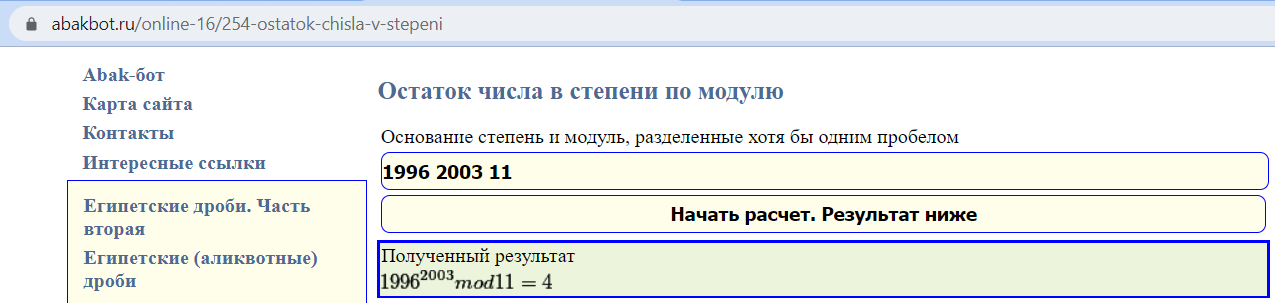
Получается: 2003 3 (mod 10) (см. пункт 2 этого задания)

3.3) x 53 = 125(mod 11)

4  125 (mod 11)

Таким образом, остаток от деления 19962003 на 11 равен 4.

Проверка:



**По способу решения задания 4(г)**

1996 делится на 11 с остатком 5.

19962 делится на 11 с остатком 3.

19963 делится на 11 с остатком 4.

19964 делится на 11 с остатком 9.

19965 делится на 11 с остатком 1.

19966 делится на 11 с остатком 5.

Зациклились (получили один из предыдущих остатков), длина цикла равна 5. 2003 = 400\*5 + 3. Число 19962003 дает тот же остаток от деления на 11, что и 19963, то есть 4.

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