Учреждение образования “Белорусский государственный технологический yниверситет”

Практическая работа №8 «Криптографическая защита информации»

Выполнила:

студентка 2 курса, 7 группы

Колядко Яна Дмитриевна

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 все 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 *- н*атуральное 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.

**Индивидуальные задания**

Вариант 6, a = 5336161097, b = 196210799.

* 1. Найти канонические разложения чисел *a* и *b.* Алгоритм нахождения такой: начиная с первого простого числа, 2, пробуем делить наше число n на эти простые числа без остатка. В случае если делится, делим, пока делиться нацело. Если нет – подбираем следующее простое число.

5336161097 = 794 · 137

196210799 = 792 · 149 · 211

5336161097 79

67546343 79

855017 79

10823 79

137 137

1

196210799 79

2483681 79

31439 79

211 211

137 137

1

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

а) Алгоритм Евклида состоит в делении с остатком большего числа на меньшее из a и b. Если остаток 0 – это наш НОД. Если не ноль, то делим делитель на остаток и так далее, пока не будет 0.

НОД (5336161097, 196210799).

5336161097 mod 196210799 = 38469524

196210799 mod 38469524 = 3863179

38469524 mod 3863179 = 3700913

3863179 mod 3700913 = 162266

3700913 mod 162266 = 131061

162266 mod 131061 = 31205

131061 mod 31205 = 6241

31205 mod 6241 = 0

6241 – наш искомый НОД.

б) Возьмём разложение чисел a и b из первого задания на простые множители и найдем совпадающие. Таким образом, получили 792 = 6241.

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

u = 7519; v = -204487.

a = bq1 + r1; b = bq2 + r2

5336161097 = 196210799 \* 27 + 38469524

196210799 = 38469524 \* 5 + 3863179

38469524 = 3863179 \* 9 + 3700913

3863179 = 3700913 \* 1 + 162266

3700913 = 162266 \* 22 + 131061

162266 = 161061 \* 1 + 31205

131061 = 31205 \* 4 + 6241

31205 = 6241 \* 5

6241 = 131061 – 31205 \* 4 = 131061 – (162266 - 131061) \* 4 = 131061 – 162266 \* 4 + 131061 \* 4 = 131061 \* 5 – 162266 \* 4 = (3700913 – 162266 \* 22) \* 5 – 162266 \* 4 = 3700913 \* 5 – 162266 \* 110 – 162266 \* 4 = 3700913 \* 5 - 162266 \* 114 = 3700913 \* 5 – (3863179 - 3700913) \* 144 = 3700913 \* 5 – 3863179 \* 144 + 3700913 \* 144 = 3700913 \* 149 – 3863179 \* 144 = (38469524 – 3863179 \* 9) \* 149 -3863179 \* 144 = 3856524 \* 149 – 3863179 \* 149 – 3863179 \* 1341 = 38469524 \* 149 – 1490 \* 3863179 = 38469524 \* 149 – (196210799 – 38469524 \* 5) \* 1490 = 38469524 \* 149 – 196210799 \* 1490 + 38469524 \* 7450 = 38469524 \* 7599 – 196210799 \* 1490 = (5336161097 – 196210799 \* 27) \* 7599 – 196210799 \* 1490 = 5336161097 \* 7519 – 196210799 \* 205173 – 196210799 \* 1490 = 5336161097 \* 7519 – 196210799 \* 204487

* 1. Найти остаток от деления 19982001 на 19

a = 19982001 mod 19

19981 mod 19 = 3; a (1) = 3;

19982 mod 19 = 7; a (2) = 7;

19983 mod 19 = 8; a (3) = 8;

19984 mod 19 = 5; a (4) = 5;

19985 mod 19 = 17; a (5) = 17;

19986 mod 19 = 10; a (6) = 10;

19987 mod 19 = 9; a (7) = 9;

19988 mod 19 = 11; a (8) = 11;

19989 mod 19 = 3; a (9) = 3.

Видно, что деление на остаток образует чередующийся цикл. Число 19989 дает тот же остаток деления на 19, что и 19981. Таким образом, чтобы получить нужное значение, нужно получить остаток от деления 2001 на 9 = 3. 2001 = 222 \* 9 + 3. Число 19982001 дает тот же остаток от деления на 19, что и 19983. Таким образом, остаток от деления 19982001 на 19 = 8.

Вывод**:** в данной лабораторной работе былиполучены основные сведения из курса теории чисел.