Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Дисциплина «Основы информационной безопасности»

Отчёт по практическому занятию №6

**Теория чисел**

Студент: Жук С.С.

ФИТ 2 курс 2 группа

Преподаватель: Ржеутская Н.В.

**Практическое занятие №6**

**«Теория чисел»**

Цель: получение основных сведений из курса теории чисел.

**Теоретическое введение**

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.

|  |
| --- |
|  |

**Задание для выполнения.**

1. Найти канонические разложения чисел а и b.
2. Найти НОД  пользуясь:

a) алгоритмом Евклида,

б) разложением чисел на простые множители.

1. С помощью расширенного алгоритма Евклида найти целые u, v, удовлетворяющие соотношению Безу: au + bv = НОД .
2. Найти остаток от деления данного числа на простое.

Вариант индивидуального задания:

|  |  |
| --- | --- |
|  | 1-3. *а* = 6099377, *b* = 9568217.  4. Найти остаток от деления  на 17 числа. |

**Ответы на вопросы**

1. **Сформулируйте алгоритм Евклида нахождения наибольшего общего делителя целых чисел.**

* Пусть у нас есть два числа a и b.
* Вычисляем остаток от деления a на b: r = a % b.
* Если r равно 0, то НОД равен b, и мы завершаем алгоритм.
* В противном случае, заменяем a на b и b на r, затем возвращаемся к первому шагу.

1. **Что значит расширенным алгоритмом Евклида?**

Расширенный алгоритм Евклида - это модифицированная версия алгоритма Евклида, которая помимо нахождения НОД также находит коэффициенты x и y, удовлетворяющие линейному уравнению: au + bv = НОД(a, b).

1. **Какие числа называются взаимно простыми?**

Два целых числа a и b называются взаимно простыми, если их наибольший общий делитель (НОД) равен 1. Это означает, что у них нет общих положительных делителей, кроме единицы.

1. **Объясните малую теорему Ферма?**

Малая теорема Ферма - это важное утверждение в теории чисел. Она гласит, что если p - простое число и a - целое число, не делящееся на p, то a^(p-1) при делении на p дает остаток 1, то есть:

**

**Исполнительская часть**

**Задание 1.** Найти канонические разложения чисел a = 6099377 и b = 9568217.

|  |
| --- |
|  |
| 6099377 | 137 | (6099377 : 137 = 44521) |
| 44521 | 211 | (44521 : 211 = 211) |
| 211 | 211 | (211 : 211 = 1) |
| 1 |  |  |

|  |  |  |
| --- | --- | --- |
| 9568217 | 137 | (9568217 : 137 = 69841) |
| 69841 | 211 | (69841 : 211 = 331) |
| 331 | 331 | (331 : 331 = 1) |
| 1 |  |  |

Следовательно, 6099377 = 137 · 211 · 211 = 137 · 2112  и 9568217 = 137 · 211 · 331.

**Задание 2.** Найти НОД(6099377, 9568217) пользуясь а) алгоритмом Евклида, б) разложением чисел на простые множители.

**Решение.** Применим алгоритм Евклида.

9568217 = 6099377∙1 + 3468840;

6099377= 3468840∙1 + 2630537;

3468840 = 2630537∙1 + 838303;

2630537 = 838303∙3 + 115628;

838303 = 115628∙7 + 28907;

115628 = 28907∙4.

Следовательно, НОД (6099377; 9568217) = 28907.

Найдём НОД (*a, b*), воспользовавшись разложением на простые множители чисел *a* и *b*, полученным в решении предыдущего задания: 6099377=137∙211∙211; 399=137∙331∙211. Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел: НОД (6099377;9568217) = 137∙211 = 28907.

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

**Решение.**

Воспользуемся найденным НОД (6099377; 9568217) = 28907 из предыдущих заданий.

28907 = 838303 – 115628 \* 7 = 838303 – (2630537 – 838303 \* 3) \* 7 = 838303 \* 22 – 2630537 \* 7 = (3468840 – 2630537) \* 22 – 2630537 \* 7 = 3468840 \* 22 – 2630537 \* 29 = 3468840 \* 22 – (6099377 – 3468840) \* 29 = 3468840 \* 51 – 6099377 \* 29 = (9568217 – 6099377) \*51 – 6099377 \* 29 = 9568217 \* 51 – 6099377 \* 80 = 9568217 \* 51 + 6099377 \* (-80) = 28907

a = 9568217, u = 51, b = 6099377, v = -80.

**Задание 4.** Найти остаток от деления  на 17 числа.

**Решение.**

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

2006 = 118 mod 17.

P = 17. Применим малую теорему Ферма:

20061999 = 118 1999 (mod 17).

Поскольку 17 – простое число, то 17 – 1 =16, и по малой теореме Ферма:

11816 = 1 (mod 17)

Теперь выразим 118 1999 через 11816:

118 1999 = (11816)124 \* 11815 (mod 17)

Поскольку 11816 = 1 (mod 17), то

(11816)124 = 1124 = 1 (mod 17)

Теперь осталось найти 11815 (mod 17). Можно разложить 118 на множители:

118 = 17 \* 6 +16

Тогда, 118 = 16 (mod 17)

Можно выразить 11815 = 1615 (mod 17)

Теперь найдем 1615 (mod 17). Можно возвести 16 в степень 15 и взять остаток от деления на 17:

1615 = 1 073 741 824

1615 = 1 073 741 824 (mod 17) = 12 (mod 17)

Итак, получили, что 11815 = 12 (mod 17)

Теперь, объединяя все результаты, получили остаток от деления  на 17:

20061999 = 1 \* 12 (mod 17) = 12 (mod 17)

Итак, остаток от деления  на 17 равен 12.

**Вывод: В ходе работы были получены основные сведения из курса теории чисел. А также изучен алгоритм для нахождения НОД чисел. А с помощью малой теоремы Ферма можно найти остаток от деления больших чисел.**