Практическое занятие №8

ТЕОРИЯ ЧИСЕЛ

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель работы:**  
Изучить основные понятия теории чисел, освоить методы вычисления наибольшего общего делителя (НОД) с использованием алгоритма Евклида и его расширенной версии, а также применить понятие сравнений по модулю и малую теорему Ферма для решения задач, связанных с разложением чисел на простые множители и поиском остатков от деления.

**Краткие теоретические сведения:**

1. **Арифметические операции и свойства целых чисел:**
   * Множество целых чисел ℤ содержит 0, положительные и отрицательные числа.
   * На ℤ определены операции сложения и умножения, обладающие свойствами ассоциативности, коммутативности, дистрибутивности, а также наличием нейтральных элементов (0 и 1).
2. **Деление с остатком и позиционные системы счисления:**
   * Теорема о делении с остатком утверждает, что для любых целых чисел a и b (b ≠ 0) существуют единственные числа q и r, такие что a = b⋅q + r, где 0 ≤ r < |b|.
   * Это основание для записи чисел в позиционных системах счисления, где число представляется в виде суммы цифр, умноженных на соответствующие степени основания.
3. **Наибольший общий делитель (НОД) и алгоритм Евклида:**
   * НОД(a, b) – наибольший общий делитель чисел a и b.
   * Алгоритм Евклида позволяет найти НОД посредством последовательного вычисления остатков от деления, а его расширенная версия даёт возможность выразить НОД через линейную комбинацию a и b (соотношение Безу).
4. **Простые числа и каноническое разложение:**
   * Простое число p > 1 делится только на 1 и на себя.
   * Теорема о бесконечности простых чисел (Евклида) утверждает, что простых чисел бесконечно много.
   * Каждое натуральное число n > 1 может быть представлено в виде произведения простых множителей (каноническое разложение).
5. **Сравнения по модулю и малая теорема Ферма:**
   * Два целых числа называются сравнимыми по модулю m, если они дают одинаковый остаток при делении на m (записывается как a ≡ b (mod m)).
   * Малая теорема Ферма утверждает, что если p — простое число и a не делится на p, то a^(p–1) ≡ 1 (mod p). Это свойство позволяет быстро находить остатки от деления больших чисел на простые.

**Условие задания**

1. Найдите канонические разложения чисел а и b.

2. Найдите НОД (а, b) пользуясь:

a) алгоритмом Евклида;

б) разложением чисел на простые множители.

3. С помощью расширенного алгоритма Евклида найдите целые u, v, удовлетворяющие соотношению Безу: au + bv = НОД(а, b).

4. Найдите остаток от деления данного числа на простое.

|  |  |
| --- | --- |
| Номер варианта | Задание |
| 4 | 1–3. а = 9002242397, b = 433817903.  4. Найти остаток от деления 20042998 на 19 |

**Исполнительная часть**

1. a = 9 002 242 397 = 73 \* 123 318 389 = 732 \* 1 689 293 = 733 \* 23 141 =

= 734 \* 317

b = 433 817 903 = 73 \* 5 942 711 = 732 \* 81 407 = 732 \* 127 \* 641

1. а)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | u | v | r |  |
| a | 1 | 0 | 9 002 242 397 | q |
| b | 0 | 1 | 433 817 903 | 20 |
| a - bq |  |  | 325 884 337 | 1 |
|  |  |  | 107 933 566 | 3 |
|  |  |  | 2 083 639 | 51 |
|  |  |  | 1 667 977 | 1 |
|  |  |  | 415 662 | 4 |
|  |  |  | 5 329 | 78 |
|  |  |  | 0 |  |

(9 002 242 397, 433 817 903) = 5329

б) (9 002 242 397, 433 817 903) = 73 \* 73 = 5329

3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | u | v | r |  |
| a | 1 | 0 | 9 002 242 397 | q |
| b | 0 | 1 | 433 817 903 | 20 |
| a - bq | 1 | -20 | 325 884 337 | 1 |
|  | -1 | 21 | 107 933 566 | 3 |
|  | 4 | -83 | 2 083 639 | 51 |
|  | -205 | 4254 | 1 667 977 | 1 |
|  | 209 | -4337 | 415 662 | 4 |
|  | -1041 | 21602 | 5 329 | 78 |
|  |  |  | 0 |  |

a\*u + b\*v = r

9 002 242 397 \* (-1041) + 433 817 903 \* 21602 = 5 329

5 329 = 5 329

u = -1041

v = 21602

4

X ≡ 20042998 (mod 19)

2004 ≡ 9(mod 19)

X ≡ 92998 (mod 19) 9ф(m) ≡ 1 (mod m)

Ф(19) = 18 918 ≡ 1 (mod 19)

2998≡ 1 (mod 19)

X ≡ (918 )166 \* 910(mod 19)

X ≡ 910(mod 19)

X ≡ 81 \* 81 \* 81 \* 81 \* 81(mod 19) 81≡ 5 (mod 19)

X ≡ 5 \* 5 \* 5 \* 5 \* 5(mod 19)

X ≡ 55(mod 19)

X ≡ 252 \* 5(mod 19) 25≡ 6 (mod 19)

X ≡ 62 \* 5(mod 19)

X ≡ 36\* 5(mod 19) 36≡ 17 (mod 19)

X ≡ 17\* 5(mod 19)

X ≡ 85 (mod 19)

X ≡ 9 (mod 19)

Ответ: остаток от деления = 9.

**Используемая литература**

1. Лабораторный практикум «Основы информационной безопасности», Н. В. Ржеутская, О. А. Нистюк, Н. И. Уласевич, 2024.
2. ЭЛЕКТРОННЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «Математические основы криптографии» для специальности 1 - 98 01 03 «Программное обеспечение информационной безопасности мобильных систем», И.К. Асмыкович, Е.И. Ловенецкая, БГТУ.