Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Лабораторная работа № 2

по дисциплине: «Теоретико-числовые методы в криптографии»

на тему: «Остаток от деления»

Выполнил

обучающийся гр. ВКБ41

Якушевский Сергей Сергеевич

Проверила:

Ст. пр. Артамонова Е.А.

Лабораторная работа №

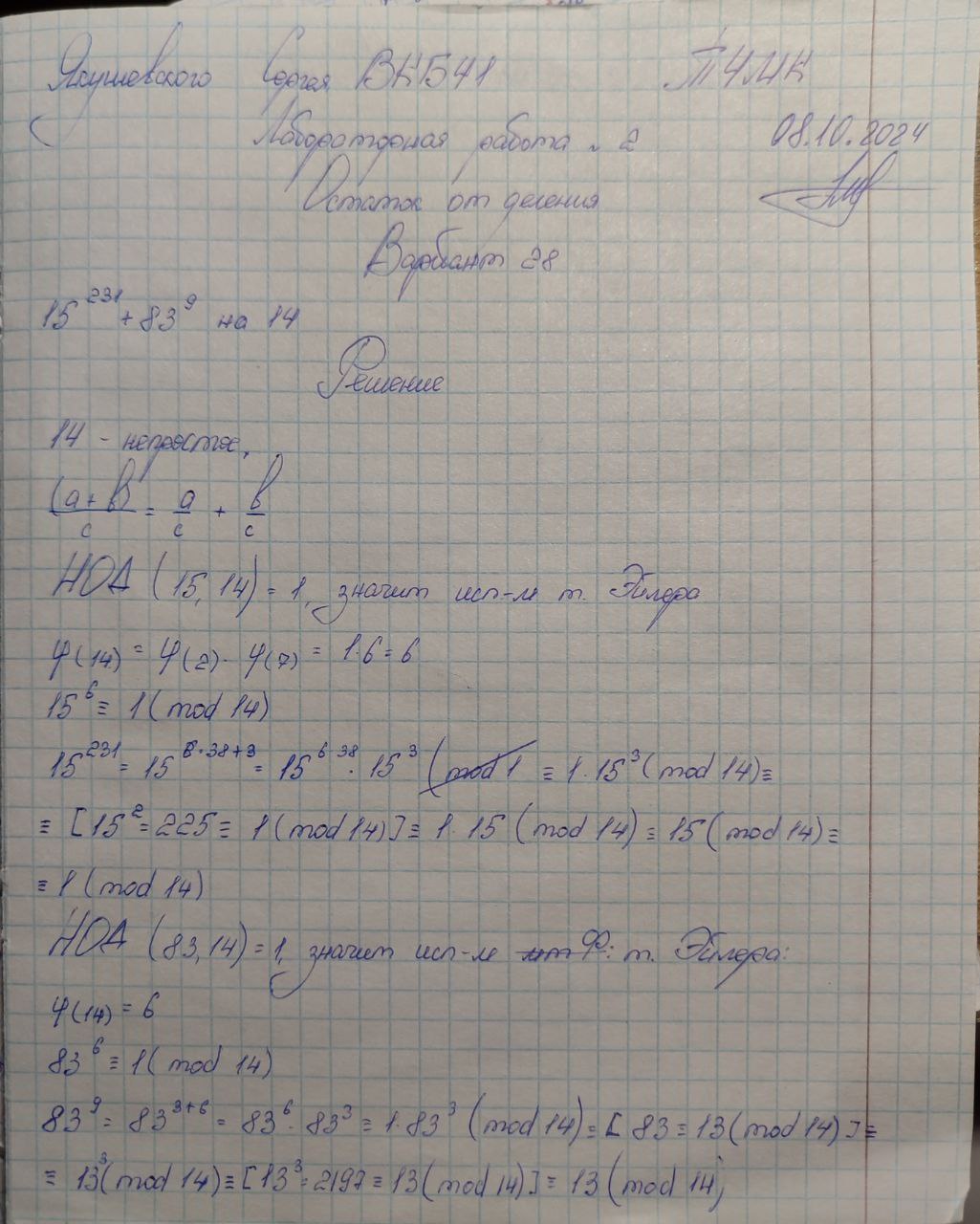
«Остаток от деления»

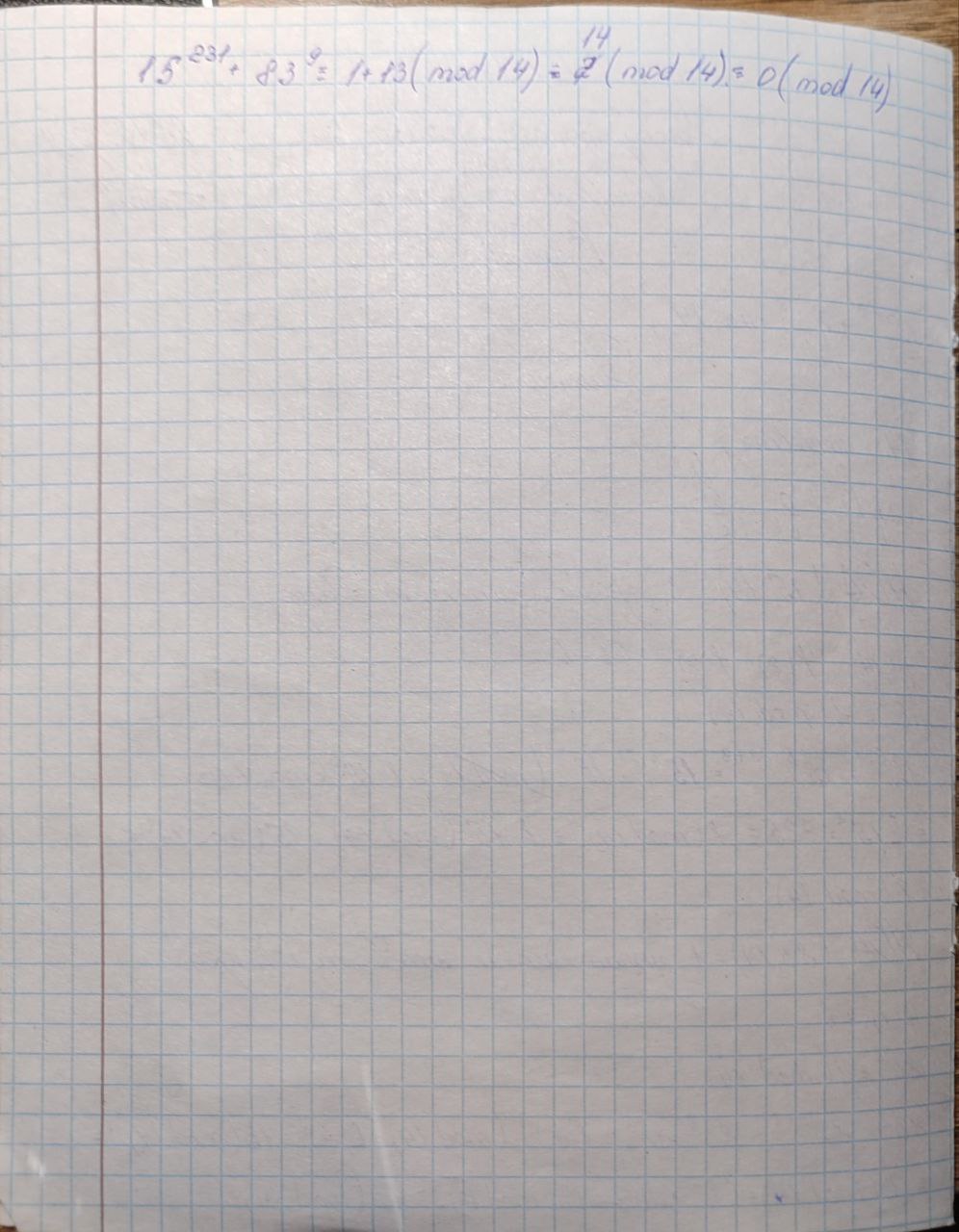
Вариант № 28

Задание.

Найти остаток от деления, используя теорему Эйлера или малую теорему Ферма. Написать программу, реализующую нахождение остатка.

## Ручная реализация.





## Входные данные.



## Результат.

## 

## Листинг программы.

## 

EulerTheorem

package dstu.csae.theorems;  
  
import mathutils.MathUtils;  
  
import java.util.Optional;  
  
public class EulerTheorem {  
  
 public static boolean matches(int number, int degree, int field) {  
 if(field < 1){  
 return false;  
 }  
 return MathUtils.*getGCD*(number, field) == 1;  
 }  
  
 public static Optional<Integer> getResult(int number, int degree, int field) {  
 if(!*matches*(number, degree, field)){  
 return Optional.*empty*();  
 }  
 int phi = MathUtils.*getEulerFunction*(field);  
 degree %= phi;  
 return Optional.*of*(MathUtils.*powMod*(number, degree, field));  
 }  
}

FermatsTheorem

package dstu.csae.theorems;  
  
import dstu.csae.Main;  
import mathutils.MathUtils;  
  
import java.util.Optional;  
  
public class FermatsTheorem {  
  
 public static boolean matches(int number, int degree, int field){  
 if(!MathUtils.*isPrime*(field)){  
 return false;  
 }  
 return MathUtils.*getGCD*(number, field) == 1;  
 }  
  
 public static Optional<Integer> getResult(int number, int degree, int field){  
 if(!*matches*(number, degree, field)){  
 return Optional.*empty*();  
 }  
 degree %= (field - 1);  
 return Optional.*of*(MathUtils.*powMod*(number, degree, field));  
 }  
  
}

Main

package dstu.csae;  
  
import dstu.csae.theorems.EulerTheorem;  
import dstu.csae.theorems.FermatsTheorem;  
  
import java.util.Arrays;  
import java.util.Optional;  
import java.util.Scanner;  
  
public class Main {  
  
 public static final String *INPUT\_TEMPLATE* = "(\\+?\\d+(\\^\\d+)?)+\\(mod\\d+\\)";  
  
 public static void main(String[] args) {  
 System.*out*.println("Лабораторная работа № 2");  
 String input = "";  
 Scanner scan = new Scanner(System.*in*);  
 while (!input.matches(*INPUT\_TEMPLATE*)){  
 System.*out*.print("Введите выражение в формате a^b + c^d (mod m): ");  
 if(scan.hasNextLine()){  
 input = scan.nextLine().replaceAll("\\s", "");  
 }  
 }  
 scan.close();  
 String fieldStr = input.substring(input.indexOf("(mod") ).replaceAll("\\D", "");  
 int field = Integer.*parseInt*(fieldStr);  
 input = input.substring(0, input.indexOf("(mod"));  
 String[] tokens = input.split("[+\\-\*/]");  
 int sum =Arrays.*stream*(tokens)  
 .map(token -> token.split("\\^"))  
 .map(token -> {  
 int number = Integer.*parseInt*(token[0]);  
 int degree = Integer.*parseInt*(token[1]);  
 if (EulerTheorem.*matches*(number, degree, field)){  
 return EulerTheorem.*getResult*(number, degree, field);  
 }  
 return FermatsTheorem.*getResult*(number, degree, field);  
 })  
 .filter(Optional::isPresent)  
 .map(Optional::get)  
 .mapToInt(Integer::*valueOf*)  
 .sum() % field;  
 System.*out*.println("Результат: " + sum);  
 }  
  
}

## Вывод по работе.

В ходе выполнения лабораторной работы были изучены теоретические сведения о способах нахождения остатка от деления, а также были получены навыки в практическом применении теоремы Эйлера и малой теоремы Ферма для решения задач нахождения остатка от деления.