Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Лабораторная работа № 1

по дисциплине: «Теоретико-числовые методы в криптографии»

на тему: «алгоритм Евклида»

Выполнил

обучающийся гр. ВКБ41

Якушевский Сергей Сергеевич

Проверила:

Ст. пр. Артамонова Е.А.

Лабораторная работа № 1

«алгоритм Евклида»

Вариант № 28

## Задание.

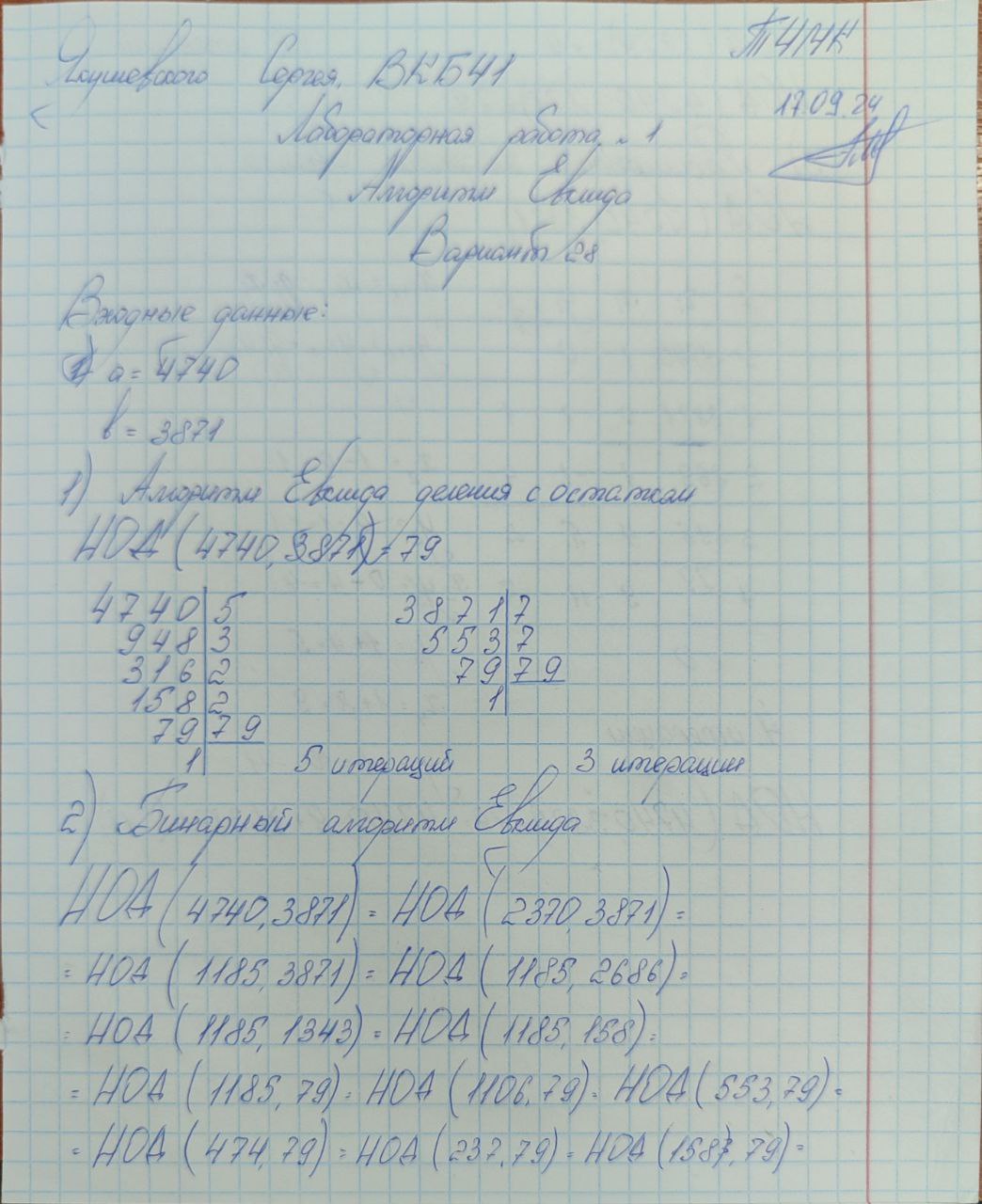
Вычислить при помощи:

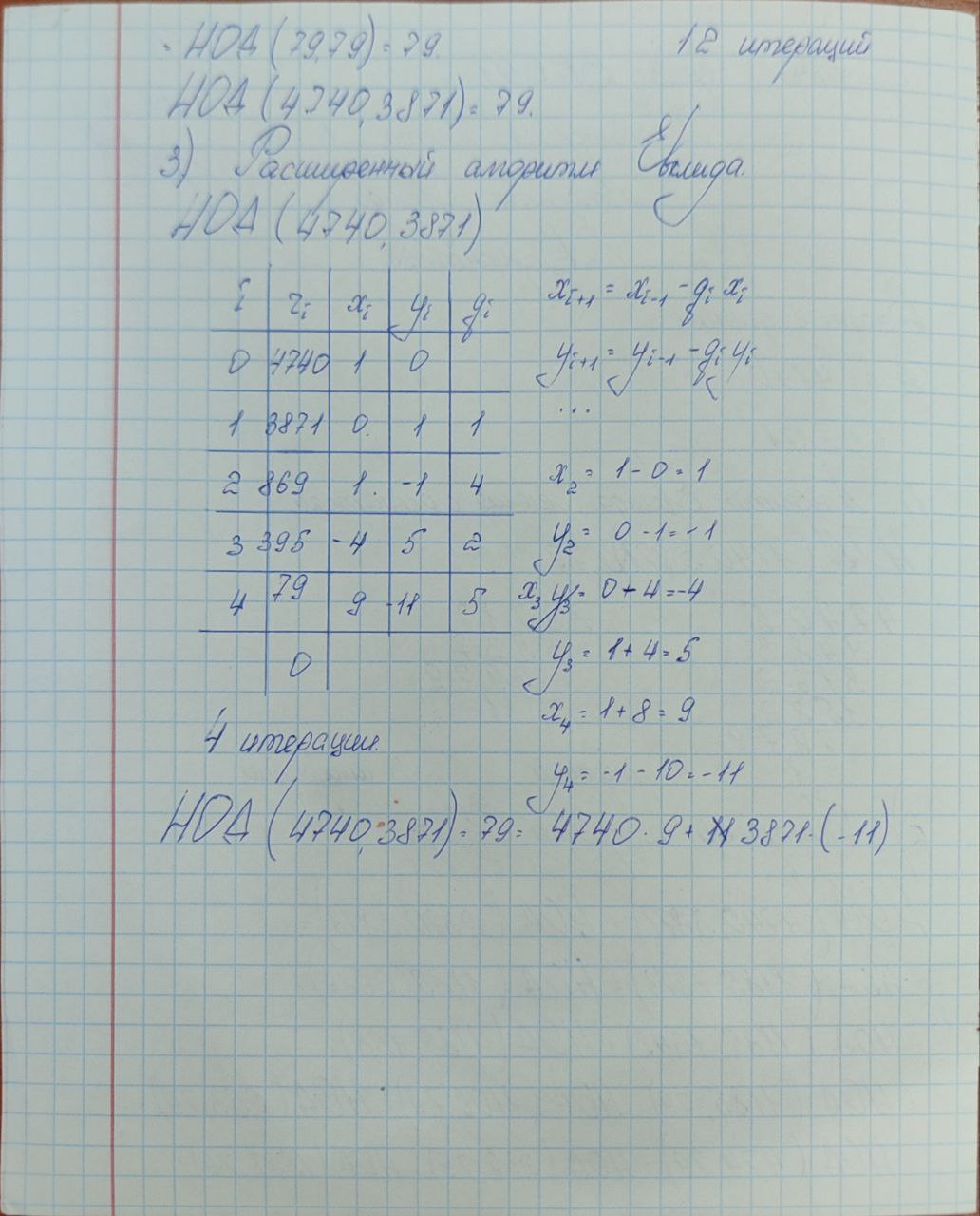
1. алгоритма Евклида с делением с остатком
2. бинарного алгоритма Евклида
3. расширенного алгоритма Евклида

Сравнить количество итераций.

Написать программу, реализующую бинарный алгоритм Евклида.

## Ручная реализация.





## Входные данные.

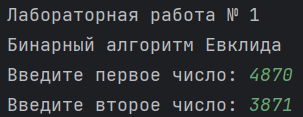


Рисунок Входные данные для нахождения НОД(a, b) бинарным алгоритмом Евклида

## Результат.

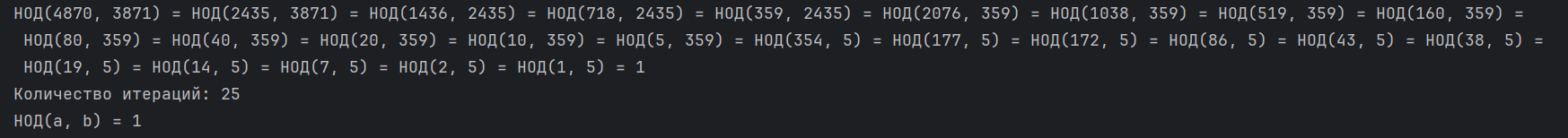


Рисунок Результат выполнения бинарного алгоритма Евклида

## Листинг программы.

package main.java;  
  
import java.util.Scanner;  
  
public class Main {  
  
 static String *introduction* = "Лабораторная работа № 1\n" +  
 "Бинарный алгоритм Евклида";  
  
 public static void main(String[] args) {  
 System.*out*.println(*introduction*);  
 int a = *input*("Введите первое число: ");  
 int b = *input*("Введите второе число: ");  
 int LCD = *getLCD*(a, b);  
 System.*out*.println("НОД(a, b) = " + LCD);  
 }  
  
 static int input(String output){  
 Scanner scanner = new Scanner(System.*in*);  
 int num = -1;  
 while(num == -1){  
 System.*out*.print(output);  
 if(!scanner.hasNextInt()){  
 System.*out*.println("Вы ввели не число. Повторите попытку");  
 scanner.next();  
 continue;  
 }  
 num = Math.*abs*(scanner.nextInt());  
 }  
 return num;  
 }  
  
 static int getLCD(int a, int b){  
 int iterationCount = 1;  
 while(a != b){  
 System.*out*.printf("НОД(%d, %d) = ", a, b);  
 if(a == 1){  
 break;  
 }  
 if(a % 2 == 0 && b % 2 == 0){  
 a /= 2;  
 b /= 2;  
 System.*out*.print("2 \* ");  
 }else if(a % 2 == 0){  
 a /= 2;  
 }else if (b % 2 == 0) {  
 b /= 2;  
 }else{  
 int c = Math.*min*(a, b);  
 a = Math.*max*(a, b) - c;  
 b = c;  
 }  
 iterationCount++;  
 }  
 System.*out*.println(a);  
 System.*out*.printf("Количество итераций: %d \n", iterationCount);  
 return a;  
 }  
  
}

## Вывод по работе.

В ходе выполнения лабораторной работы были закреплены теоретические сведения и практические навыки о различных вариациях нахождения наименьшего общего делителя (НОД) методом Евклида: алгоритм деления с остатком, бинарным алгоритмом и расширенным алгоритмом. На практике было установлено, что для решения заданного варианта оптимальным оказался расширенный алгоритм Евклида, т.к. для его выполнения потребовалось всего 4 итерации.