Государственное образовательное учреждение

«Белорусский государственный технологический университет»

Отчет

*по лабораторной работе №8*

ТЕМА ЗАНЯТИЯ: ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ

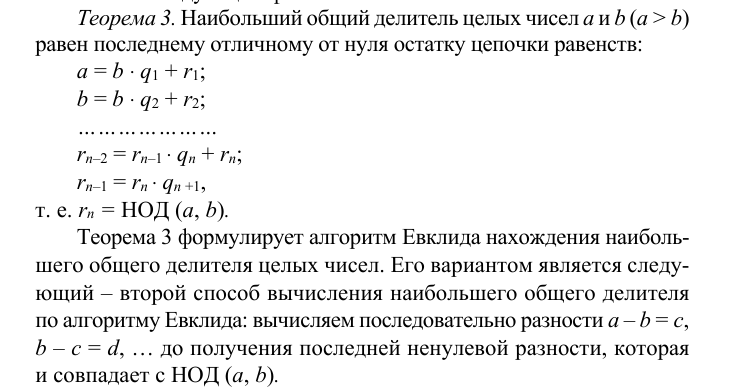
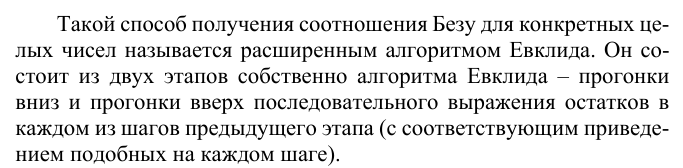
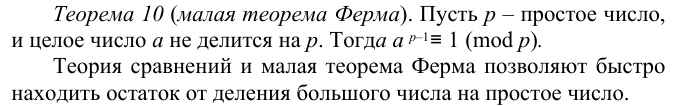
|  |  |
| --- | --- |
|  | **Исполнитель:**  Студента (-ка) группы 2  Специальность\_\_\_\_ИСиТ\_\_\_  Гулевич Никита Максимович  (Ф.И.О.) |
|  | **Преподаватель**:  Ржеутская Н. В. |

Минск, 2025

Цель: изучить и закрепить умение реализации электронноцифровой подписи на примере RSA.

**Задание для выполнения.**

Ответить на следующие вопросы:

1. Сформулируйте алгоритм Евклида нахождения наибольшего общего делителя целых чисел.
2. Что значит расширенный алгоритм Евклида?
3. Какие числа называются взаимно простыми?
4. Объясните малую теорему Ферма.
5. 
6. 
7. 
8. 

Каноническое разложение

a=356216713=47^4 \* 73

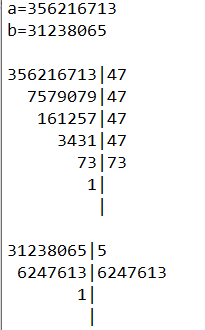
b=31238065=5 \* 6247613

НОД

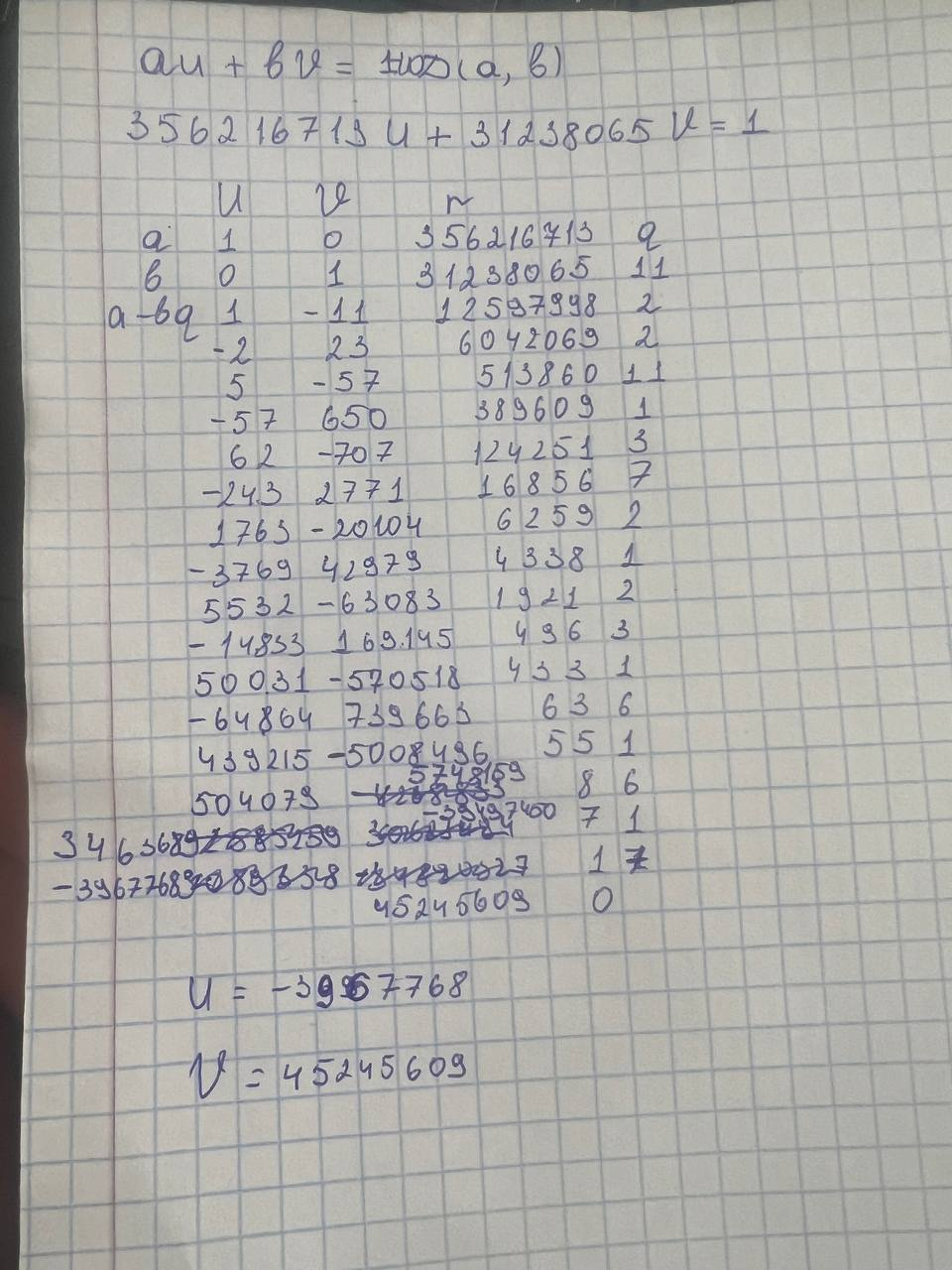
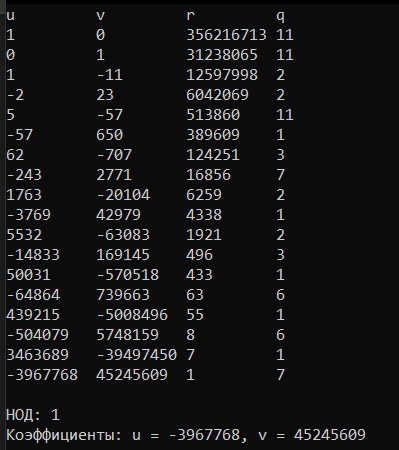
По каноническому разложению

НОД(a,b) = 1

По алгоритму Евклида



Расширенный алгоритм евклида

Найти остаток от деления  на 19.

