Учреждение образования

«Белорусский государственный технологический университет»

**Основы информационной безопасности**

**Лабораторная работа №8**

**«Теория чисел»**

Выполнил:

Студент 2 курса 2 группы ФИТ

Мойсеёнок Денис

Преподаватель:

Ржеутская Надежда Викентьевна

Минск 2025

**Цель:** получить основные сведения из курса теории чисел.

**Вопросы:**

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

Алгоритм Евклида – это эффективный метод для нахождения наибольшего общего делителя (НОД) двух целых чисел.

1. Если *b* = 0, то НОД (*a*, *b*) = *a*. Алгоритм завершен.

2. Иначе, вычисляем остаток от деления *a* на *b*: *r* ≡ *a* (mod *b*).

3. Присваиваем *a* = *b*, *b* = *r*

4. Возвращаемся к шагу 1.

2. Что значит расширенный алгоритм Евклида?

Расширенный алгоритм Евклида не только находит НОД двух целых чисел *a* и *b*, но и находит такие целые числа *u* и *v*, что выполняется следующее уравнение: *au* + *bv* = НОД (*a*, *b*)

3. Какие числа называются взаимно простыми?

Целые числа *a* и *b* взаимно просты тогда и только тогда, когда существуют такие целые *u* и *v*, что выполняется равенство *a* ⋅ *u* + *b* ⋅ *v* = 1.

4. Объясните малую теорему Ферма.

Пусть *p* – простое число, и целое число *a* не делится на *р*. Тогда .

**Задания:**

1. Найдите канонические разложения чисел *а* и *b*.

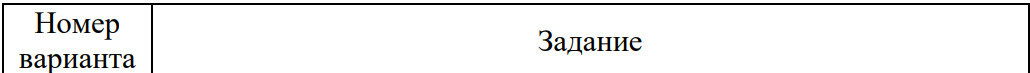
2. Найдите НОД (*а*, *b*) пользуясь:

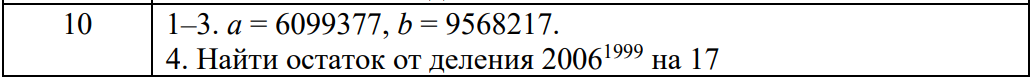
a) алгоритмом Евклида;

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.





1.

|  |  |
| --- | --- |
| 6099377 | 137 |
| 44521 | 211 |
| 211 | 211 |
| 1 |  |

|  |  |
| --- | --- |
| 9568217 | 137 |
| 69841 | 211 |
| 331 | 331 |
| 1 |  |

6099377 = 137 ⋅ 211­2

9568217 = 137 ⋅ 211 ⋅ 331

2. a) 9568217 = 6099377 ⋅ 1 + 3468840

6099377 = 3468840 ⋅ 1 + 2630537

3468840 = 2630537 ⋅ 1 + 838303

2630537 = 838303 ⋅ 3 + 115628

838303 = 115628 ⋅ 7 + 28907

115628 = 28907 ⋅ 4

НОД (6099377, 9568217) = 28907

б) 6099377 = 137 ⋅ 211 ⋅ 331

9568217 = 137 ⋅ 211 ⋅ 331

НОД (6099377, 9568217) = 137 ⋅ 211 = 28907

3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | *u* | *v* | *r* |  |
| *a* | 1 | 0 | 9568217 | *q* |
| *b* | 0 | 1 | 6099377 | 1 |
| *a* - *bq* | 1 | -1 | 3468840 | 1 |
|  | -1 | 2 | 2630537 | 1 |
|  | 2 | -3 | 838303 | 3 |
|  | -7 | 11 | 115628 | 7 |
|  | 51 | -80 | 28907 | 4 |
|  |  |  | 0 |  |

28907 = 9568217 ⋅ 51 + 6099377 ⋅ (-80)

4. 20061999 на 17

2006 ≡ 0 (mod 17)

20061999 ≡ 0 (mod17)