МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КУБГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**Отчет**

**по практическому заданию №5**

**по курсу**

**«КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»**

Работу выполнила

Студентка 49 группы

Шестак В. А.

Преподаватель:

Крамаренко А. А.

Краснодар 2025

**Цель работы:** Изучение алгоритмов факторизации и тестов на простоту.

**Теория:**

1. Простые числа Мерсена

**Теория:** Простые числа Мерсена — это простые числа вида Mp=2^p−1, где p также является простым числом. Примеры простых чисел Мерсена включают M2=3, M3=7, M5=31, M7=127, и M13=8191M13=8191[1](https://nsportal.ru/ap/library/nauchno-tekhnicheskoe-tvorchestvo/2024/03/13/chisla-mersena)[3](https://www.wolfram.com/language/11/algebra-and-number-theory/mersenne-primes-and-perfect-numbers.html.ru).

1. Простые числа Ферма

**Теория:** Простые числа Ферма имеют вид Fn=2^2^n+1, где n — неотрицательное целое число. Примеры простых чисел Ферма включают F0=3, F1=5, F2=17, и F3=257. Однако только первые пять чисел Ферма (F0 до F4) являются простыми; все остальные известные числа Ферма являются составными.

1. Тест Ферма

**Теория:** Тест Ферма — это вероятностный тест простоты, основанный на малой теореме Ферма. Для простого числа p, если a^p−1≡1mod  p для любого целого числа a, не кратного p, то p является вероятно-простым.

1. Испытание квадратным корнем

**Теория:** Испытание квадратным корнем не является стандартным методом проверки простоты. Однако, если вы имеете в виду проверку, является ли число квадратом, то для простых чисел 23 и 41 это не применимо, поскольку они не являются идеальными квадратами.

1. Тест Миллера-Рабина

**Теория:** Тест Миллера-Рабина — это вероятностный тест простоты, который улучшает тест Ферма. Он проверяет, является ли число n составным, выполняя несколько итераций теста, основанного на свойстве, что если n простое, то для любого a, не кратного n, либо a^n−1≡1mod  n, либо существует d такое, что a^2^d≡−1mod   n.

1. Метод Ферма разложения на множители

**Теория:** Метод Ферма разложения на множители основан на представлении числа N как разности двух квадратов: N=a^2−b^2=(a+b)(a−b). Этот метод эффективен для чисел, которые близки к идеальным квадратам.

1. (p-1) метод Полларда

**Теория:** (p-1) метод Полларда — это метод факторизации, который эффективен для чисел, у которых один из множителей имеет относительно небольшую функцию Эйлера ϕ(p−1). Он основан на теореме Эйлера и требует знания факторизации p−1.

1. РО (Rho) метод Полларда

**Теория:** РО метод Полларда — это вероятностный метод факторизации, который использует функцию f(x)=(x^2+1)mod  n для нахождения циклов в последовательности, что может привести к факторизации n.

1. Квадратичное решето

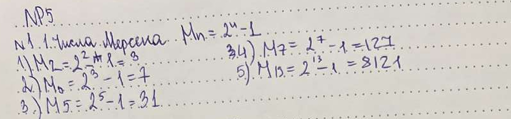
**Теория:** Квадратичное решето - это метод факторизации, который использует квадратичные уравнения для нахождения факторов числа. Он эффективен для больших чисел и основан на нахождении двух квадратов, которые конгруэнтны по модулю n.

1. Решето поля чисел

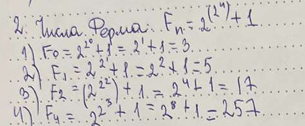
**Теория:** Решето поля чисел — это метод факторизации, который использует алгебраические числа для нахождения факторов. Он является более сложным и эффективным методом для больших чисел, но требует глубоких знаний алгебры.

**Ход работы:**

1. Привести пример пяти простых чисел Мерсена

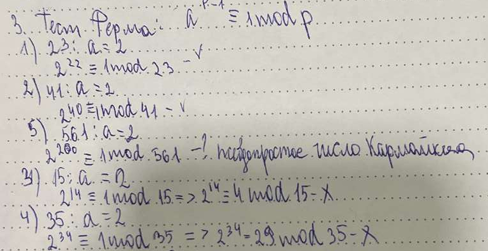


1. Привести пример четырех простых чисел Ферма.

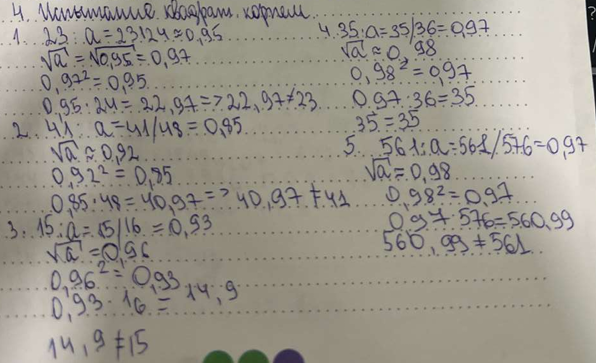


1. Провести тест Ферма для чисел 23, 41, 15, 35, 561 Каково название

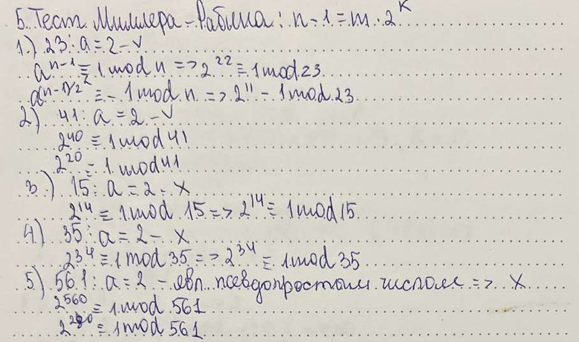
последнего числа?



1. Провести испытание квадратным корнем для чисел 23, 41, 15, 35, 561

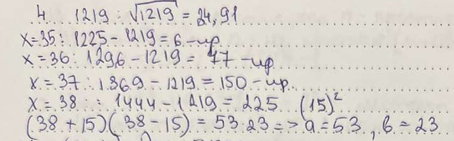
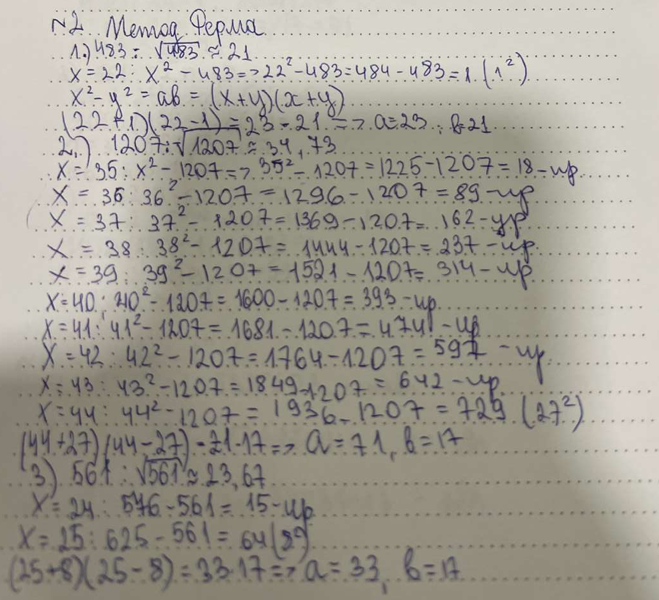


1. Провести тест Миллера-Рабина для чисел 23, 41, 15, 35, 561



1. Применить метод Ферма разложения на множители для чисел 483, 1207,

561, 1219



1. Решение разных задач Фороузана.

