|  |  |
| --- | --- |
| **Российский университет транспорта (МИИТ)**  **Институт транспортной техники и систем управления**  **Кафедра «Управление и защита информации»** | |
| **Отчет**  **по практическому заданию**  **по теме «Возведение в степень по модулю числа»**  **по дисциплине «Криптографические методы защиты информации»** | |
|  | Выполнил:  Студент группы ТКИ-342  Белов С.В.  Проверил:  Доцент кафедры УиЗи, к.т.н., с.н.с.  Михалевич И.Ф. |
| Москва 2023 | |

**Оглавление**

[Задание 2](#_Toc1099027345)

[Исходные данные 3](#_Toc1182135674)

[1. Вычисление простого числа 4](#_Toc1703362445)

[1.1 Теоритическая часть 5](#_Toc2121914341)

[1.2 Реализация методов 7](#_Toc1221597029)

[1.3 Проверка 7](#_Toc1367584568)

[2. Проверка чисел на взаимную простоту 7](#_Toc720652766)

[2.1 Теоритическая часть 8](#_Toc1454251693)

[2.2 Реализация методов 10](#_Toc2031654324)

[2.3 Формирования групп взаимно простых чисел 10](#_Toc469382826)

[3. Метод Эль-Гамаля 10](#_Toc330372196)

[4. Реализация метода Эль-Гамаля 10](#_Toc1597716265)

[4.1 Реализация метода в Эксель 10](#_Toc716337031)

[4.2 Реализация методов с помощью программы 10](#_Toc636692704)

[5. Область применения метода Эль-Гамаля 10](#_Toc571502504)

[Заключение 11](#_Toc8745050)

# Задание

Номер варианта: 2.

1. Вычислить простое число p (привести описание трех или более методов проверки простоты, реализовать один или более, проверить число на простоту).
2. Проверить числа l и (b+ f) на взаимную простоту (привести описание методов проверки взаимной простоты чисел, реализовать один или более, проверить, являются ли числа l и (b+ f) взаимно простыми).
3. Описать метод (дать общую характеристику исследуемого метода).
4. Реализовать метод в Эксель и программно.
5. Описать области применения метода (привести примеры).

# Исходные данные

– восьмиразрядное число, отражающее день рождения студента в формате дмг(день, месяц, год полностью).

– восьмиразрядное число, образованное суммой чисел 10 и двухразрядного номера студента в списке группы, дополненное шестью нулями справа.

– простое число, ближайшее меньшее к числу

при

– шестиразрядное число, образованное исключением первого и третьего разрядов слева из числа .

при

Распределение заданий:

N – порядковый номер студента в списке группы, n – номер задания:

При – исследуется метод RSA.

# 1. Вычисление простого числа

## 1.1 Теоритическая часть

Натуральное число называется простым, если оно имеет только два делителя: единицу и само себя. Задача поиска простых чисел не дает покоя математикам уже очень давно. Долгое время прямого практического применения эта проблема не имела, но все изменилось с появлением криптографии с открытым ключом. Далее рассматривается несколько способов поиска простых чисел.

**Решето Эратосфена**

[Решето Эратосфена](https://ru.wikipedia.org/wiki/Решето_Эратосфена) — алгоритм, предложенный древнегреческим математиком Эратосфеном. Этот метод позволяет найти все простые числа меньше заданного числа *n*. Суть метода заключается в следующем. Возьмем набор чисел от 2 до *n*. Вычеркнем из набора (отсеим) все числа делящиеся на 2, кроме 2. Перейдем к следующему «не отсеянному» числу — 3, снова вычеркиваем все что делится на 3. Переходим к следующему оставшемуся числу — 5 и так далее до тех пор пока мы не дойдем до *n*. После выполнения вышеописанных действий, в изначальном списке останутся только простые числа.

Алгоритм можно несколько оптимизировать. Так как один из делителей составного числа *n* обязательно , алгоритм можно останавливать, после вычеркивания чисел делящихся на .

Сложность алгоритма составляет , при этом, для хранения информации о том, какие числа были вычеркнуты требуется  памяти.

Существует ряд оптимизаций, позволяющих снизить эти показатели. Прием под названием «[wheel factorization](https://en.wikipedia.org/wiki/Wheel_factorization)» состоит в том, чтобы включать в изначальный список только числа [взаимно простые](https://ru.wikipedia.org/wiki/Взаимно_простые_числа) с несколькими первыми простыми числами (например меньше 30). В теории предлагается брать первые простые примерно до. Это позволяет снизить сложность алгоритма в раз. Помимо этого для уменьшения потребляемой памяти используется так называемое сегментирование. Изначальный набор чисел делится на сегменты размером и для каждого сегмента решето Эратосфена применяется по отдельности. Потребление памяти снижается до .

**Теорема Ферма и тест Миллера-Рабина**

Простых чисел Мерсенна известно не очень много, поэтому для криптографии с открытым ключом необходим другой способ поиска простых чисел. Одним из таким способов является [тест простоты Ферма](https://ru.wikipedia.org/wiki/Тест_Ферма). Он основан на малой теореме Ферма, которая гласит, что если *n* — простое число, то для любого *a*, которое не делится на *n*, выполняется равенство .

Тест простоты Ферма — вероятностный тест, который заключается в переборе нескольких значений *a*, если хотя бы для одного из них выполняется неравенство , то число *n* — составное. В противном случае, *n* — вероятно простое. Чем больше значений *a* использовано в тесте, тем выше вероятность того, что *n* — простое.

К сожалению, существуют такие составные числа *n*, для которых сравнение  выполняется для всех *a* взаимно простых с *n*. Такие числа называются [числам Кармайкла](https://ru.wikipedia.org/wiki/Число_Кармайкла). Составные числа, которые успешно проходят тест Ферма, называются псевдопростыми Ферма. Количество псевдопростых Ферма бесконечно, поэтому тест Ферма — не самый надежный способ определения простых чисел.

**Тест Миллера-Рабина**

Более надежных результатов можно добиться комбинируя малую теорему Ферма и тот факт, что для простого числа *p* не существует других корней уравнения , кроме 1 и -1. Тест Миллера-Рабина перебирает несколько значений *a* и проверяет выполнение следующих условий.

Пусть *p* — простое число и , тогда для любого *a* справедливо хотя бы одно из условий:

1. Существует целое число *r < s* такое, что

По теореме Ферма , а так как  из свойства о корнях уравнения  следует что если мы найдем такое *a*, для которого одно из условий не выполняется, значит *p* — составное число. Если одно из условий выполняется, число *a* называют свидетелем простоты числа *n* по Миллеру, а само число *n* — вероятно простым.

Чем больше свидетелей простоты найдено, тем выше вероятность того, что *n* — простое. Согласно теореме Рабина вероятность того, что случайно выбранное число *a* окажется свидетелем простоты составного числа составляет приблизительно 1/4.

Следовательно, если проверить *k* случайных чисел *a*, то вероятность принять составное число за простое .

Сложность работы алгоритма , где *k* — количество проверок.

Благодаря быстроте и высокой точности тест Миллера-Рабина широко используется при поиске простых чисел. Многие современные криптографические библиотеки при проверке больших чисел на простоту используют только этот тест.

## 1.2 Реализация методов

## 1.3 Проверка

# 2. Проверка чисел на взаимную простоту

## 2.1 Теоритическая часть

**Взаимно простые числа**

Два целых числа a и b называются взаимно простыми, если их наибольший общий делитель равен единице — то есть НОД (a, b) = 1.

Из определения взаимно простых чисел можно сделать вывод, что у двух взаимно простых чисел может быть только один положительный общий делитель, который равен единице. А всего общих делителей у двух взаимно простых чисел два — это 1 и -1.

Приведем примеры взаимно простых чисел.

Числа 13 и 16 взаимно простые потому, что их положительный общий делитель — единица, что подтверждает взаимную простоту чисел 13 и 16. Заметим, что два простых числа всегда являются взаимно простыми. Однако, два числа не обязательно должны быть простыми, чтобы быть взаимно простыми.

Приведем пример.

Два составных числа 8 и -9 являются взаимно простыми. Сначала найдем НОД этих чисел.

Делители 8: ±1, ±2, ±4, ±8.

Делители -9: ±1, ±3, ±9.

Из этого следует, НОД (8, -9) = 1, поэтому, по определению 8 и -9 — два взаимно простых числа.

Так же это работает, когда у нас не два числа, а больше.

Взаимно простыми целые числа будут тогда, когда они имеют наибольший общий делитель, равный 1.

Иными словами, если у нас есть набор некоторых чисел с наибольшим положительным делителем, большим 11, то все эти числа не являются по отношению друг к другу взаимно обратными.

Возьмем несколько примеров. Так, целые числа −99, 17 и −27 – взаимно простые. Любое количество простых чисел будет взаимно простым по отношению ко всем членам совокупности, как, например, в последовательности 2, 3, 11, 19, 151, 293 и 667. А вот числа 12, −9, 900 и −72 взаимно простыми не будут, потому что кроме единицы у них будет еще один положительный делитель, равный 33. То же самое относится к числам 17, 85 и 187: кроме единицы, их все можно разделить на 17.

Обычно взаимная простота чисел не является очевидной с первого взгляда, этот факт нуждается в доказательстве. Чтобы выяснить, будут ли некоторые числа взаимно простыми, нужно найти их наибольший общий делитель и сделать вывод на основании его сравнения с единицей.

Рассмотрим два основных метода нахождения НОД двумя основными способами: с использованием алгоритма Евклида и путем разложения на простые множители.

**Алгоритм Евклида**

Алгоритм Евклида помогает найти НОД через последовательное деление.

Алгоритм Евклида заключается в следующем: если большее из двух чисел делится на меньшее — наименьшее число и будет их наибольшим общим делителем. Использовать метод Евклида можно легко по формуле нахождения наибольшего общего делителя.

Формула НОД:

НОД (a, b) = НОД (b, с), где с — остаток от деления a на b.

Для нахождения наибольшего общего делителя двух чисел нужно соблюдать такой порядок действий:

1. Большее число поделить на меньшее.
2. Меньшее число поделить на остаток, который получается после деления.
3. Первый остаток поделить на второй остаток.
4. Второй остаток поделить на третий и т. д.

Деление продолжается до тех пор, пока в остатке не получится нуль. Последний делитель и есть наибольший общий делитель.

Пример. Найти наибольший общий делитель чисел 140 и 96:

140 : 96 = 1 (остаток 44)

96 : 44 = 2 (остаток 8)

44 : 8 = 5 (остаток 4)

8 : 4 = 2

Последний делитель равен 4 — это значит: НОД (140, 96) = 4.

Ответ: НОД (140, 96) = 4

**Разложение на множители**

Для того, чтобы найти наибольший общий делитель двух чисел методом разложения на множители, необходимо перемножить все простые множители, которые получаются при разложении этих двух чисел и являются для них общими.

Пример.

Если мы разложим числа 220 и 600 на простые множители, то получим два произведения: 220=2⋅2⋅5⋅11 и 600=2⋅2⋅2⋅3⋅5⋅5. Общими в этих двух произведениях будут множители 2,2 и 5. Это значит, что НОД(220, 600)=2⋅2⋅5=20.

## 2.2 Реализация методов

## 2.3 Формирования групп взаимно простых чисел

# 3. Метод Эль-Гамаля

# 4. Реализация метода Эль-Гамаля

## 4.1 Реализация метода в Эксель

## 4.2 Реализация методов с помощью программы

# 5. Область применения метода Эль-Гамаля

# Заключение