**Задание №1**

Для каждой пары чисел найти наибольший общий делитель и его линейное представление, используя следующие алгоритмы:

1. Расширенный алгоритм Евклида.
2. Расширенный бинарный алгоритм Евклида.
3. Расширенный алгоритм Евклида с «усечёнными» остатками.

**В отчете привести** все итерации алгоритмов (последовательность остатков и две последовательности коэффициентов линейного представления). При числе итераций больше 20 привести первые 5 и последние 5 элементов каждой последовательности. Итерации должны быть пронумерованы.

При получении различных линейных представлений одного и того же наибольшего общего делителя обосновать корректность полученных результатов. Привести формулу для вычисления линейных представлений.

В отчете привести сравнение быстродействия реализованных алгоритмов и объяснить полученные результаты.

**ДЕДЛАЙН: 27.10.2025**

**Задание №2**

Каждое из указанных чисел проверить на простоту с помощью тестов: Ферма, Соловэя-Штрассена, Рабина-Миллера.

**В отчёте привести:**

1. Результат проверки каждым из тестов для каждого числа - "вероятно простое" или "составное".
2. Для составного числа - основание, для которого нарушается условие простоты; показать какое именно условие нарушается.
3. Для простого числа - 5 оснований, для которых условие простоты выполняется; показать выполнимость этого условия.
4. Для каждого из тестов привести пример двух-трех чисел Кармайкла (не менее 30 десятичных знаков каждое; указать источник) и признаки того, что данное число Кармайкла является "простым" и составным. Привести разложение чисел Кармайкла.

**ДЕДЛАЙН: 10.11.2025**

**Задание №3**

Каждое из указанных чисел разложить на множители:

1. ро-методом Полларда.
2. (p-1)-методом Полларда.
3. Методом квадратичного решета.
4. Методом непрерывных дробей.

**В отчёте привести:**

1. **В случае результативного завершения работы программы: результат разложения.**
2. **Для ро-метода Полларда:**
   1. Параметры алгоритма (использованное отображение, начальное значение (несколько, если их пришлось менять)).
   2. При результативном завершении работы – первые 5 и последние 5 значений a, b, НОД(a – b, n), число итераций, время работы программы, выводы (объяснение результативного завершения).
   3. При работе программы более нескольких часов – первые 5 и последние (на момент прерывания программы) 5 значений a, b, НОД(a – b, n), число выполненных итераций, время, затраченное на их выполнение, расчетное время, оставшееся до завершения работы (через оценку сложности алгоритма), выводы (объяснение нерезультативного завершения).
3. **Для (p-1)-метода Полларда:**
   1. Базу разложения (первоначальную, измененную (если потребовалось изменение, обосновать необходимость изменения)).
   2. Значения показателей l\_i.
   3. При результативном завершении работы – основание a, при котором выполнено разложение (несколько, если потребовалось изменять основание).
   4. При невозможности найти разложение более нескольких часов – основание a, при котором выполнено разложение (несколько, если потребовалось изменять основание), число выполненных итераций (одна итерация – прогон алгоритма с одним основанием a), время, затраченное на их выполнение, расчетное время, оставшееся до завершения работы (через оценку сложности алгоритма), выводы (объяснение нерезультативного завершения).
4. **Для метода непрерывных дробей:**
   * 1. При результативном завершении работы:
     2. Базу разложения (первоначальную, измененную (если потребовалось изменение, обосновать необходимость изменения)), при большом объеме базы – число элементов в базе и ее последний элемент, критерии исключения элементов из базы.
     3. Числители P\_i подходящих дробей, использованных при разложении, для D-гладких значений (P\_i)^2 (mod n), при большом объеме данных – 5 значений Pi и (P\_i)^2 (mod n).
     4. Векторы показателей для D-гладких значений (P\_i)^2 (mod n), при большом объеме данных – 5 векторов, соответствующих значениям (P\_i)^2 (mod n) из предыдущего пункта.
     5. Метод, использованный для поиска линейно-зависимых векторов (если была использована готовая процедура – указать, из какой библиотеки).
     6. Значения s и t.
     7. При невозможности найти разложение более нескольких часов:
   1. Данные по пп. 4.1.1–4.1.3 на момент прерывания программы.
   2. Расчетное необходимое число гладких чисел (P\_i)^2 (mod n) и время, необходимое для их поиска.
      1. Выводы (объяснение результатов работы).
5. **Для метода квадратичного решета**
6. При результативном завершении работы:
   * 1. Базу разложения (первоначальную, измененную (если потребовалось изменение, обосновать необходимость изменения)), при большом объеме базы – число элементов в базе и ее последний элемент, критерии исключения элементов из базы.
     2. Использованный диапазон значений x, результат процедуры просеивания.
     3. Значения x и соответствующие им D-гладкие значения f(x), при большом объеме данных – по 5 значений x и f(x).
     4. Векторы показателей для D-гладких значений f(x), при большом объеме данных – 5 векторов, соответствующих значениям f(x) из предыдущего пункта.
     5. Метод, использованный для поиска линейно-зависимых векторов (если была использована готовая процедура – указать, из какой библиотеки).
     6. Значения s и t.
7. При невозможности найти разложение более нескольких часов:
   * 1. 4.2.1. Данные по пп. 5.1.1–5.1.4 на момент прерывания программы.
     2. 4.2.2. Расчетное необходимое число гладких чисел f(x) и время, необходимое для их поиска.
8. Выводы (объяснение результатов работы).

**ДЕДЛАЙН: 08.12.2025**

**Задание №4**

Элемент a имеет порядок q по модулю p. Найти дискретный логарифм x - такое целое число 1<x<q, что a^x = b (mod p):

1. ро-методом Полларда.
2. Методом Гельфонда;
3. Методом базы разложения.

**В отчёте привести:**

1. **В случае результативного завершения работы программы: результат дискретного логарифмирования - число x.**
2. **Для метода Гельфонда:**
   1. Значение s.
   2. Базу данных вида {k, b\*a^(-k s) (mod p)}, отсортированную по первой координате. При большом объёме базы - первые 5 и последние 5 её элементов.
   3. Значение t, для которого a^t = b\*a^(-k s) (mod p) для некоторого k. Уравнение для вычисления логарифма x. Метод решения уравнения.
   4. При невозможности найти дискретный логарифм более нескольких часов – значение t, до которого построена последовательность a^t (mod p), время, затраченное на построение второй последовательности, расчетное время, оставшееся до завершения работы (через оценку сложности алгоритма), выводы (объяснение нерезультативного завершения).
3. **Для метода базы разложения:**
4. При результативном завершении работы:
   * 1. Базу разложения B (первоначальную, измененную (если потребовалось изменение, обосновать необходимость изменения)), при большом объеме базы – число элементов в базе и ее последний элемент.
     2. B-гладкие значения a^(u\_i) (mod p), соответствующие им показатели u\_i, при большом объеме данных – по 5 указанных значений
     3. Векторы показателей для B-гладких значений a^(u\_i) (mod p), при большом объеме данных – 5 векторов, соответствующих значениям a^(u\_i) (mod p) из предыдущего пункта.
     4. Показатель v, для которого значение b^v (mod p) является B-гладким, соответствующий вектор показателей.
     5. Метод, использованный для исключения переменных (если была использована готовая процедура – указать, из какой библиотеки).
     6. Метод, использованный для решения линейного сравнения относительно неизвестного x.
5. При невозможности найти дискретный логарифм более нескольких часов:
   * 1. Данные по пп. 4.1.1–4.1.3 на момент прерывания программы.
     2. Расчетное необходимое число гладких чисел a^(u\_i) (mod p) и время, необходимое для их поиска.
     3. Показатель v, для которого значение b^v (mod p) является B-гладким, соответствующий вектор показателей.
6. **Для ро-метода Полларда:**
7. Параметры алгоритма (использованное отображение, начальное значение (несколько, если их пришлось менять)).
8. При результативном завершении работы – первые 5 и последние 5 значений c, d, log\_a\_(c), log\_a\_(d), число итераций, время работы программы, выводы (объяснение результативного завершения).
9. При работе программы более нескольких часов – первые 5 и последние (на момент прерывания программы) 5 значений c, d, log\_a\_(c), log\_a\_(d), число выполненных итераций, время, затраченное на их выполнение, расчетное время, оставшееся до завершения работы (через оценку сложности алгоритма), выводы (объяснение нерезультативного завершения).

**ДЕДЛАЙН: 22.12.2025**