



Задания, ответы и критерии оценивания

**Требования к оформлению заданий.** При проверке заданий учитывается не только ответ, но и само решение. Важно оформлять решения во всех заданиях. Ответы без решения оцениваются не более чем в 1 балл.

**Задача 1** (Максимум 10 баллов)

Найдите все тройки натуральных чисел  $(x, y, z)$ , такие что  $5^x + 5^y = z^2$  и  $x, y < 10, z \leq 50$

**Ответ:** Решений в натуральных числах нет.

**Решение:** Для решения этой задачи нам нужно найти все тройки натуральных чисел  $(x, y, z)$ , удовлетворяющие условию  $5^x + 5^y = z^2$ , при этом  $x, y < 10$  и  $z \leq 50$ .

Мы можем решить эту задачу, перебрав все возможные значения  $x$  и  $y$  в диапазоне от 1 до 9 (поскольку они меньше 10) и проверив, удовлетворяет ли соответствующее значение  $z$  условию  $z^2 = 5^x + 5^y$  и  $z \leq 50$ .

1. Для каждой пары  $x$  и  $y$ , вычислить  $z^2 = 5^x + 5^y$ .
2. Проверить, является ли  $z$  целым числом, и удовлетворяет ли оно условию  $z \leq 50$ .

Таких троек не окажется.

Объяснение следующее:

При  $x > 1$  и/или  $y > 1$  сумма двух чисел оканчивается на 30 или 50. Натуральный квадрат с нулем на конце может быть только квадратом круглого числа, но в таком случае он будет заканчиваться на 00, из чего следует отсутствие натуральных решений в указанном диапазоне.

**Критерии оценивания**

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	3	Ученик понимает задачу и определяет ограничения для $x, y$ и $z$ , правильно формулирует уравнение $5^x + 5^y = z^2$ и понимает его математический смысл.
3	7	Ученик показывает отсутствие решений путем полного перебора всех вариантов без указания свойств суммы и квадрата числа.
4	10	Ученик указывает свойства совпадения суммы и квадрата числа, получив вывод с отсутствием ответа в натуральных числах.

## Задание 2 (Максимум 20 баллов)

Решите в натуральных числах уравнение  $17m - 5n = 1$ , где  $m$  и  $n$  лежат в пределах от 1 до 100

**Ответ:**

1. (3,10)
2. (8,27)
3. (13,44)
4. (18,61)
5. (23,78)
6. (28,95)

**Решение:**

Диофантово уравнение вида  $ax - by = c$ , где  $a, b, c$  — известные целые числа, а  $x, y$  — неизвестные, которые нужно найти.

Если предположить, что ваше уравнение должно выглядеть как  $17m - 5n = 1$ , где  $m$  и  $n$  — натуральные числа, лежащие в пределах от 1 до 100, тогда мы можем решить его, перебирая значения  $m$  и  $n$  и проверяя, удовлетворяют ли они уравнению.

### Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	10	Ученик понимает задачу и может правильно записать уравнение, понимает концепцию линейного диофантова уравнения и методы его решения.
3	15	Ученик применяет метод перебора или другой подход для нахождения частичного решения задачи.
4	20	Ответ полностью совпадает. Правило описано.

## Задание 3 (Максимум 20 баллов)

Дана последовательность  $s_n$ , где  $s_n$  - последняя цифра суммы квадратов первых  $n$  натуральных чисел, т.е.  $s_n$  - последняя цифра числа  $1^2 + 2^2 + 3^2 + \dots + n^2$ . Определите периодичность этой последовательности. Создайте первую перестановку из последовательных уникальных цифр  $s_n$  и определите, образуют ли последующие перестановки периодическую последовательность.

**Ответ:** НЕ ОБРАЗУЕТ ПЕРИОДИЧЕСКУЮ ПОСЛЕДОВАТЕЛЬНОСТЬ

**Решение:**

Для определения периодичности последовательности  $s_n$ , которая является последней цифрой суммы квадратов первых  $n$  натуральных чисел, нам нужно

вычислить эти суммы для различных значений  $n$  и наблюдать за поведением последних цифр этих сумм.

Последовательность задается как  $1^2+2^2+3^2+\dots+n^2$  (мы рассматриваем только последнюю цифру этой суммы).

решить эту задачу вручную, следуя следующим шагам:

1. Вычислить последние цифры сумм квадратов для первых нескольких  $n$ , например, от 1 до 50.
2. Наблюдать за последовательностью этих цифр и искать периодичность.
3. Определить уникальные цифры в начале этой последовательности (первая перестановка).
4. Следить за повторением этой перестановки в дальнейшем.

### Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	5	Ученик понимает задачу и может правильно описать последовательность $S_n$ . Ученик корректно вычисляет последние цифры сумм квадратов для первых нескольких $n$ и начинает анализировать последовательность.
3	10	Ученик выявляет уникальные цифры в начале последовательности и формирует первую перестановку.
4	15	Ученик анализирует последовательность на предмет периодичности и частично определяет её, но делает некоторые ошибки или не полностью исследует периодичность.
5	20	Ученик полностью и правильно решает задачу, определяя периодичность последовательности и полностью исследуя её свойства.

### **Практическое задание.** (Максимум 50 баллов)

Необходимо разработать и описать алгоритм с выбранными входными параметрами шифра RSA, один из основных методов асимметричного шифрования. Задача включает в себя три основных этапа: генерацию ключей, шифрование и дешифрование сообщений. Вы должны продемонстрировать понимание математических принципов, лежащих в основе RSA, а также умение применять эти принципы на практике.

RSA (названный в честь его создателей Рональда Ривеста, Ади Шамира и Леонарда Адлемана) является одним из первых и наиболее широко используемых алгоритмов асимметричного шифрования. Асимметричное шифрование означает использование

различных ключей для шифрования и расшифровки данных. В RSA используются два ключа: открытый ключ для шифрования и закрытый ключ для расшифровки.

Процесс работы RSA включает в себя следующие шаги:

#### Генерация ключей

1. Выбор двух больших простых чисел ( $p$  и  $q$ ): Эти числа генерируются и хранятся в секрете.
2. Вычисление произведения ( $n = p * q$ ): Число  $n$  используется как часть обоих ключей и определяет длину ключа RSA.
3. Вычисление функции Эйлера ( $\varphi(n) = (p-1) * (q-1)$ ): Эта функция используется для генерации ключей.
4. Выбор открытого ключа ( $e$ ): Число  $e$  должно быть взаимно простым с  $\varphi(n)$  и обычно выбирается из набора стандартных значений (например, 65537).
5. Вычисление закрытого ключа ( $d$ ): Число  $d$  вычисляется как мультипликативно обратное к  $e$  по модулю  $\varphi(n)$ , т.е. такое, что  $d * e \equiv 1 \pmod{\varphi(n)}$ .

После этого открытый ключ ( $e, n$ ) может быть распространен, а закрытый ключ ( $d, n$ ) должен быть сохранен в секрете.

#### Шифрование и расшифровка

1. Шифрование: Чтобы зашифровать сообщение  $M$ , отправитель использует открытый ключ получателя. Сообщение преобразуется в число  $m$ , меньшее  $n$  (например, с использованием кодировки ASCII). Затем зашифрованное сообщение  $C$  вычисляется по формуле:  $C = m^e \pmod n$ .
2. Расшифровка: Чтобы расшифровать сообщение  $C$ , получатель использует свой секретный ключ ( $d$ ). Оригинальное сообщение  $m$  восстанавливается путем вычисления:  $m = C^d \pmod n$ . После этого  $m$  преобразуется обратно в текст сообщения.

#### Решение:

##### 1. Разработка Алгоритма Генерации Ключей:

- Выбор двух больших простых чисел  $p$  и  $q$ .
- Вычисление модуля  $n=p \times q$ , который будет частью обоих ключей.
- Вычисление функции Эйлера:  $\varphi(n)=(p-1) \times (q-1)$ .
- Выбор открытой экспоненты  $e$ , которая взаимно проста с  $\varphi(n)$ .
- Вычисление закрытой экспоненты  $d$ , такой что  $d \times e$  дает остаток 1 при делении на  $\varphi(n)$ .

##### 2. Реализация Алгоритмов Шифрования и Дешифрования:

- Шифрование: Преобразование сообщения в число и возведение его в степень  $e$  по модулю  $n$ .
- Дешифрование: Возведение зашифрованного числа в степень  $d$  по модулю  $n$ .

## Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	10	Правильный выбор простых чисел. Корректность вычисления открытого и закрытого ключей.
3	15	Ученик выявляет уникальные цифры в начале последовательности и формирует первую перестановку.
4	25	Правильность алгоритма шифрования, включая применение открытого ключа.
5	50	Ученик полностью и правильно решает задачу.