1:

Целое число - это число, которое не имеет дробной части и может быть положительным, отрицательным или нулём.

Натуральное число - это положительное целое число, которое используется для счёта. Примеры натуральных чисел: 1, 2, 3, 4, 5, ...

Делимость чисел - это свойство двух чисел, когда одно число (делитель) равномерно делится на другое число (делимое) без остатка.

Собственный делитель - это положительный делитель целого числа, который не равен самому числу. Например, собственные делители числа 6 - 1, 2 и 3, т.к. они делят число 6 без остатка, но не равны ему самому.

НОД - Наибольшее целое число, которое делит без остатка числа a и b, называется наибольшим общим делителем этих чисел – НОД (a, b)

2:

Основная теорема арифметики, примеры

Любое целое число > 1 может быть представлено в виде произведения простых множителей. Прим: 6 = 2\*2\*2

3.

Сущность проблемы факторизации и её связь с прикладной криптографией

Проблема факторизации заключается в том, что для больших целых чисел сложно найти их простые множители. Например, для числа с 300 цифрами найти его простые множители классическими методами может занять слишком много времени и ресурсов. Эта проблема становится особенно актуальной в контексте криптографии, где безопасность системы шифрования основана на сложности факторизации больших целых чисел.

В криптографии используется множество алгоритмов, которые основаны на принципе сложности факторизации. Например, одним из наиболее известных алгоритмов является RSA (Rivest-Shamir-Adleman), который используется для защиты передаваемых сообщений. Для создания ключей в алгоритме RSA необходимо выбрать два больших простых числа и вычислить их произведение, которое будет использоваться в качестве открытого ключа. Затем, для шифрования сообщений используется открытый ключ, а для расшифровки - закрытый ключ, который является приватной информацией. Надежность шифрования в алгоритме RSA основана на сложности факторизации больших целых чисел, которые являются частью открытого ключа.

Таким образом, проблема факторизации имеет большое значение в криптографии, и её решение может оказать серьезное влияние на безопасность систем шифрования.\

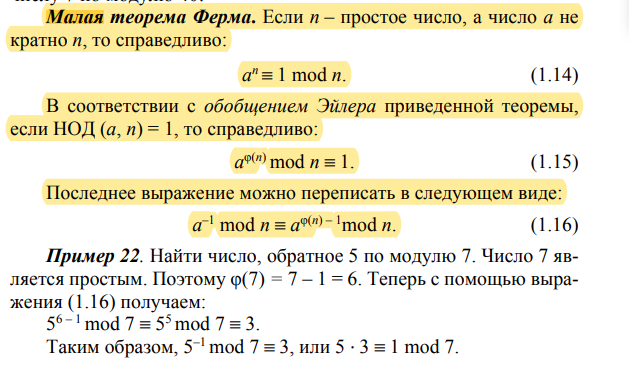
**Каноническое разложение**

Каноническое разложение числа - это представление числа в виде произведения простых множителей с учётом их степеней.

**Безу**

Соотношение Безу утверждает, что для любых целых чисел a и b, не оба равных нулю, существуют такие целые числа x и y, что ax + by = НОД(a,b), где НОД(a,b) - наибольший общий делитель чисел a и b.

**Малая теорема Ферма:**



Основные свойства модулярной арифметики:

Свойство 1 **собственного делителя**: положительный наименьший собственный делитель составного числа n не превосходит √n

Свойство 2 **собственного делителя**. Положительный наименьший собственный делитель составного числа n есть простое число.

Свойство 2. Любое составное число представляется уникальным образом в виде произведения простых чисел; иначе еще говорят, что разложение числа на простые множители однозначно

Свойство 4. Наименьший простой делитель составного числа n не превышает √n, поэтому для проверки простоты числа достаточно проверить его делимость на 2 и на все нечетные (а еще лучше простые) числа, не превосходящие √n; как видим, данное свойство коррелирует со свойством 1 собственного делителя.

Свойство 4. Любое четное число, большее 2, представимо в виде суммы двух простых чисел, а любое нечетное, большее 5, представимо в виде суммы трех простых чисел.

Свойство 5. Для любого натурального n, большего 1, существует хотя бы одно простое число на интервале от n до 2n.