

Домашнее задание 26.

1. Предположим, что $\text{НОК}(a, b, c) = \text{НОК}(\text{НОК}(a, b), c)$ и аналогично для НОД.¹ Докажите, что

$$\text{НОК}(x, y, z) = \frac{xyz \cdot \text{НОД}(x, y, z)}{\text{НОД}(x, y) \cdot \text{НОД}(x, z) \cdot \text{НОД}(y, z)}$$

для любых положительных x, y, z .

2. Пусть число $p > 3$ простое. Тогда $24 \mid (p^2 - 1)$.

3. Докажите, что не существует арифметической прогрессии $\{a_k\}_{k \in \mathbb{N}}$ (с ненулевой разностью), т. ч. числа a_1, \dots, a_n попарно взаимно просты для всех $n > 0$.

4. Докажите, что дробь $\frac{n^2 - n + 1}{n^2 + 1}$ несократима при любом целом $n > 0$.

5. Один из вариантов криптоалгоритма RSA таков. Выбирают два (больших) различных простых числа p и q , для которых вычисляют $n = pq$ и $m = (p - 1)(q - 1)$; затем фиксируют некоторое $e \in \{2, \dots, m - 2\}$, т. ч. $\text{НОД}(e, m) = 1$, и находят число d со свойством $ed \equiv 1 \pmod{m}$. Пара (e, n) является *ключом зашифровывания* и публикуется, а пара (d, n) — это *ключ расшифровывания*, который держат в секрете.

Всякий, зная публичный ключ, может зашифровать некоторое сообщение (открытый текст представляют в виде числа $P \in \{1, \dots, n - 1\}$), получая шифротекст $C = \text{остаток}(P^e, n)$. Адресат сообщения, зная секретный ключ, расшифровывает открытый текст $P' = \text{остаток}(C^d, n)$. Докажите, что:

- а) по данным e и m всегда можно найти число $d \in \{2, \dots, m - 2\}$, причем для этого есть алгоритм, лучший² полного перебора;
- б) расшифровка корректна, т. е. $P' = P$ для *любого* открытого текста P .
6. Если число $a^{10} + b^{10} + c^{10} + d^{10} + e^{10} + f^{10}$ кратно 11, то $abcdef$ делится на 11^6 .

¹Это легко проверить исходя из определения НОК нескольких чисел, которое было на лекции, и аналогичного ему определения НОД.

²Это свойство не нужно доказывать.