

Примеры решений задач

1. Разделить с остатком. Записать неполное частное и остаток.

741 на 37

$$741 = 37 * 20 + 1$$

Ответ: Неполное частное 20, остаток 1

2. С помощью алгоритма Евклида найти наибольший общий делитель чисел.

Для любых натуральных чисел x и y ($x \leq y$) выполнено

$$\text{НОД}(x, y) = \text{НОД}(x, r),$$

где r есть остаток от деления y на x .

На этом основан алгоритм Евклида нахождения $\text{НОД}(x, r)$

$$4158 = 3 * 1056 + 990$$

$$1056 = 1 * 990 + 66$$

$$990 = 15 * 66 + 0$$

Ответ: $\text{НОД}(4158, 1056) = 66$

3. Являются ли числа взаимно простыми?

4159 и 1056

$$4159 = 3 * 1056 + 991$$

$$1056 = 1 * 990 + 65$$

$$991 = 15 * 65 + 16$$

$$65 = 16 * 4 + 1$$

$\text{НОД}(4159, 1056) = 1$ - числа взаимно простые

4. Найти какие-либо множители Безу для чисел

81 и 26

$$81 = 3 * 26 + 3$$

$$26 = 8 * 3 + 2$$

$$3 = 1 * 2 + 1$$

$$1 = 3 - 1 * 2 =$$

$$= 3 - 1 * (26 - 8 * 3) = 9 * 3 - 1 * 26 =$$

$$= 9 * (81 - 3 * 26) - 1 * 26 =$$

$$= 9 * 81 - 28 * 26$$

Множители Безу: 9 и 28

5. Найти $k^{-1} \bmod n$
 $3^{-1} \bmod 5$

Вычислять $x^{-1} \bmod n$ можно, используя множители Безу.

Выражения $x^{-k} \bmod n$ подсчитываются с помощью очевидных равенств $x^{-k} = (x^{-1})^k$

$$1 = 2 \cdot 3 - 1 \cdot 5, \quad 2 \cdot 3 = 1 + 1 \cdot 5, \quad 2 \cdot 3 = 1 \pmod{5}$$
$$3^{-1} = 2 \pmod{5}$$

6. Шифр RSA

Пусть $p = 47$ и $q = 71$, тогда $n = 3337$.

Ключ e не должен иметь общих множителей с

$$(p-1) \cdot (q-1) = 46 \cdot 70 = 3220;$$

Принимаем $e = 79$, тогда

$$d = 79^{-1} \bmod 3220 = 1019.$$

Пусть сообщение имеет следующий вид: $M = 688232687$ и длина блока равна 3:

$$m_1 = 688, \quad m_2 = 232, \quad m_3 = 687.$$

Зашифрование: $c_1 = 688^{79} \bmod 3337 = 1570$ и т. д.

Расшифрование: $m_1 = 1570^{1019} \bmod 3337 = 688$ и т. д.

Для возведения в степень больших чисел можно воспользоваться онлайн калькулятором: Модулярная арифметика
https://planetcalc.ru/8326/?language_select=ru