

1)

$$x^2 \equiv 219 \pmod{383}$$

Чтобы это сравнение было разрешимо, необходимо, чтобы  $\left(\frac{219}{383}\right)$  был равен 1

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right) \cdot \left(\frac{73}{383}\right) = 1 \cdot \left(\frac{73}{383}\right), \text{ т.к. } (383 \equiv -1 \pmod{12})$$

$$\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right) \cdot (-1)^{6876} = \left(\frac{18}{73}\right) = 1 \cdot \left(\frac{2}{73}\right) = (-1)^{(73^2-1)/2} = 1$$

Сравнение разрешимо.

2)

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) (-1)^{\frac{p-1}{2}}$$

Рассмотрим все остатки по модулю 5

a)

$$p \equiv 1 \pmod{5}$$

$$1 \cdot (-1)^0 = 1$$

b)

$$p \equiv 4 \equiv 29 \pmod{5}$$

$$1 \cdot (-1)^{18} = 1$$

c)

$$p \equiv 2 \equiv 7 \pmod{5}$$

$$\left(\frac{2}{5}\right) \cdot (-1)^3 = -1$$

d)

$$p \equiv -2 \equiv 13 \pmod{5}$$

$$\left(\frac{3}{5}\right) \cdot (-1)^6 = -1$$

3)

$$x^2 + 2x + 72 \equiv \pmod{128 \cdot 151 \cdot 199}$$

По каждому из модулей 151, 199 (Символ Лежандра по каждому из этих чисел равен 1 с соответствующим знаменателем 80 и 128) сравнение имеет по 2 решения.

Теперь рассмотрим сравнение  $(x + 1)^2 \equiv 57 \pmod{128}$

Найдем обратное по модулю (128) к числу 57

$$57^{64} \equiv 1 \pmod{128} \leftrightarrow 57^{63} \equiv 9 \pmod{128}$$

Теперь имеем:

$$9(x + 1)^2 \equiv 1 \pmod{128} \equiv (3x + 3)^2$$

Это сравнение имеет 4 решения ( $7 > 3$ ).

Так как каждое сравнение имеет решение, то общее количество решений равно  $2 \cdot 2 \cdot 4 = 16$

5)

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^{q-1} \equiv 1 \pmod{q}$$

Применим малую теорему Ферма:  $2^{q-1} \equiv 1 \pmod{q}$ :  $2^{2p} \equiv 1 \pmod{q}$  (используя  $q = 2p + 1$ )  $2^p \equiv 1 \pmod{q}$  (поделим обе стороны на  $2^p$ )

Теперь рассмотрим числа Мерсенна  $M_p = 2^p - 1$ :  $2^p \equiv 1 \pmod{q}$

$$2^p - 1 \equiv 0 \pmod{q}$$

Таким образом, мы видим, что  $2^p - 1$  делится на  $q$ . это означает, что  $2^p - 1$  имеет делитель, отличный от 1 и  $2^p - 1$ . Следовательно,  $2^p - 1$  не является простым, за исключением случая  $p = 3$  (где  $q = 2p + 1 = 7$ ). Таким образом, числа Мерсенна  $M_p = 2^p - 1$  являются простыми только при  $p = 3$ .