

問2. 12

(1)①

$$2^{-1} \equiv 2^{16-1} \pmod{17}$$

$$\equiv (2^4)^3 2^3 \pmod{17}$$

$$\equiv (-1)^3 8 \pmod{17} \quad (\because 2^4 = 16 \equiv -1 \pmod{17})$$

$$\equiv -8 \pmod{17}$$

$$\equiv 9 \pmod{17}.$$

(1)②

割り算の計算は、表記困難のため、省略.

$$n = 17, a = 2, r_1 = 1 \text{ とすると,}$$

$$\gcd(a, n) = r_1 = -8a + n = -8 \times 2 + 17.$$

よって,

$$2^{-1} \equiv -8 \equiv 9 \pmod{17}.$$

(2)①

$$3^{-1} \equiv 3^{70-1} \pmod{71}$$

$$\equiv (3^4)^{17} 3 \pmod{71}$$

$$\equiv 10^{17} \times 3 \pmod{71} \quad (\because 3^4 = 81 \equiv 10 \pmod{71})$$

$$\equiv (10^3)^5 \times 3 \times 10^2 \pmod{71}$$

$$\equiv 6^5 \times 2^4 \pmod{71} \quad (\because 10^3 = 1000 \equiv 6 \pmod{71}, 3 \times 10^2 = 300 \equiv 16 = 2^4 \pmod{71})$$

$$\equiv (3^2 \times 2^3)^2 \times 3 \times 2^3 \pmod{71}$$

$$\equiv 1 \times 24 \pmod{71} \quad (\because 3^2 \times 2^3 = 72 \equiv 1 \pmod{71})$$

$$\equiv 24 \pmod{71}.$$

(1)②

割り算の計算は、表記困難のため、省略.

$$n = 71, a = 3, r_1 = 2, r_2 = 1 \text{ とすると,}$$

$$\gcd(a, n) = r_2 = a - r_1 = a - (n - 23a) = 24a - n = 24 \times 3 - 71.$$

よって,

$$3^{-1} \equiv 24 \pmod{71}.$$

問2. 13

$N = 3 \times 7 = 21, L = 2 \times 6 = 12$ である.

(1)

$$e = 5^{-1}$$

$$\equiv 5^{\varphi(12)-1} \pmod{12}$$

$$\equiv 5^3 \pmod{12}$$

$$\equiv 5^2 \times 5 \pmod{12}$$