cryptography

$x^{-1} \bmod y$

1000 bit — 1000 bit

$24^{-1} \bmod 16$

$24 \times a = 1 \bmod 16$

$\gcd(99, 78) = ?$ gcd: 3

$\Downarrow$ b, a ≥ b

$\gcd(78, 21) = ?$ gcd: 3

$\Downarrow$

$\gcd(21, 15) = ?$ gcd: 3

$\Downarrow$

$\gcd(15, 6) = ?$ gcd: 3

$\Downarrow$

$\gcd(6, 3) = ?$

$\Downarrow$

$\gcd(3, 0) = ?$ → gcd = 3

$99 \cdot (-11) + 78 \cdot (+14) = 3$

$78 \cdot 3 + 21 \cdot (-11) = 3$

$21 \cdot (-2) + 15 \cdot (3) = 3$

$15 \cdot (1) + 6 \cdot (-2) = 3$

$6 \cdot 0 + 3 \cdot 1 = 3$

$3x + 0y = 3$

$x_0 = 1 \quad y_0 = 0$

$3 - \left\lfloor \frac{91}{78} \right\rfloor (-11)$ (1)

$-2 - \left\lfloor \frac{78}{21} \right\rfloor \cdot 3$

$y_3 = x_2 - \left\lfloor \frac{21}{15} \right\rfloor \cdot y_2$

$y_2 = x_1 - \left\lfloor \frac{15}{6} \right\rfloor \cdot y_1 = 1 - 1 \cdot (-2) = 1 + 2 = 3$

$= 0 - 2 \cdot 1 = -2$

$x_2 = y_1 = 1$

$x_1 = y_0$

$y_1 = x_0 - \left\lfloor \frac{6}{3} \right\rfloor \cdot y_0$

$x = y_1 \quad y = x_1 - \left\lfloor \frac{a}{b} \right\rfloor \cdot y_1$