Modular inverses

EG $3 \cdot 7 \equiv 1 \pmod{10}$

$\Rightarrow 3^{-1} \equiv 7 \pmod{10}$ $\quad \frac{1}{3} = 3^{-1}$

also: $7^{-1} \equiv 3$

EG Solve $3x \equiv 4 \pmod{10}$.

$x \equiv 3^{-1} \cdot 4 \equiv 28 \equiv 8 \pmod{10}$

$3^{-1} \equiv 7$, $8 \equiv -2$

verify: $3 \cdot 8 \equiv 4 \pmod{10}$

$3 \cdot (-2) \equiv 4$

EG $4^{-1} \equiv ? \pmod{13}$

brute-force: try $1, 2, 3, \ldots, 10$, $4 \cdot 10 \equiv 1$ $\Rightarrow 4^{-1} \equiv 10 \pmod{13}$

clever: $4 \cdot 3 \equiv -1 \pmod{13}$ $\Rightarrow 4^{-1} \equiv -3 \equiv 10 \pmod{13}$

Bezout's identity: $4r + 13s = 1$ $\quad \gcd(4, 13)$

find r, s using Euclid

here: $r = 10$, $s = -3$

$4r \equiv 1 \pmod{13}$

$\Rightarrow 4^{-1} \equiv r \equiv 10 \pmod{13}$

LEM $a^{-1} \pmod{n}$ exists $\iff \gcd(a, n) = 1$

Pf $1 \equiv ax \pmod{n}$

$\iff 1 = ax + ny$

if $\gcd(a, n) = 1$ then find x, y using Euclid

if $\gcd(a, n) > 1$ then has no integer sol

NOTE mod p (prime): all residues (nonzero) are invertible