Enclidean Alg. a > b > 0then QCD(a,b) = QCD(b,amodb) GCD(55,22) = GCD(22,11) = GCD(11.6) = 11GCD(18,12) = GCD(12,6) = 6

$$ADD(11, 10) = ACD(10, 1) = 1$$
e.g. $a = 710$, $b = 310$.

$$0. 71.0 = 2 \times 310 + 90$$

$$0. 310 = 3 \times 90 + 40$$

$$0. 40 = 2 \times 40 + 10$$

$$9ed(10, 0) = 10 = gcd(710, 310).$$

$$9cd(a, b) = 9cd(1al, 1bl).$$

$$9cd(a, 0) = 1al$$

Extended Euclidean Alg.

given a, b integers $exists \quad x, \quad y. \quad int. \quad s.t.$ gcd(a,b) = d = ax + by.

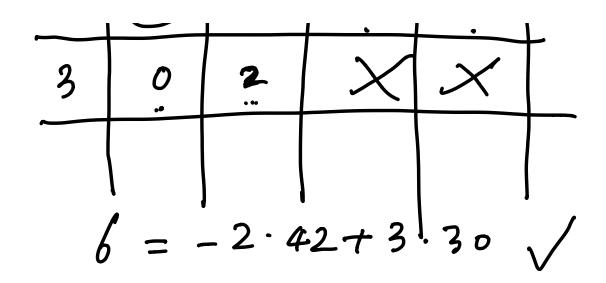
If a, b are rel. prime.

$$gcd(a,b)=1 = ax+by$$
.

 $multiplicative inverse of b mod a$
 $1 = ax + by$) mod $a = by mod a$
 $y = b^{-1} mod a$.

 $y = b^{-1} mod a$.

 $y = ax + by$
 $y = ax$



prime numbers

im. a >1.

$$91 = 7 \times 13.$$
 $66 = 2 \times 3 \times 5 = 4 \times 15$
 $11011 = 7 \times 11^{2} \times 13$

$$a = P_1 \times P_2 \dots \times P_n$$

$$P_1 < P_2 \times \dots < P_n$$
are prime # s

 $Q_i > 0$ fundamental theorem of arithmetic