The Euclidean Algorithm

gcd (a, b) prime factorization → inefficient

Lemma $\gcd(a,b) = \gcd(b, \underbrace{a \bmod b}_{r})$ $a \geq b$

$a = b \cdot q + r$, $d = \gcd(a,b)$

$d \mid a \quad d \mid b \quad d \mid r$

ex $\gcd(10266, 986)$

$\equiv \gcd(986, 406)$

$\equiv \gcd(406, 174)$

$\equiv \gcd(174, 58)$

$\equiv 58$

10266 / 986 = 10, 10266 − 9860 = 406

986 / 406 = 2, 986 − 812 = 174

406 / 174 = 2, 406 − 348 = 058

174 / 58 = 3, 174 − 174 = 0

$58 = 406 - 174 \cdot 2$

$58 = 406 - (986 - 406 \cdot 2) \cdot 2$

$= 406 - 2 \cdot 986 + 4 \cdot 406$

$= 5 \cdot (10266 - 10 \cdot 986) - 2 \cdot 986$

$= 5 \cdot 10266 - 50 \cdot 986 - 2 \cdot 986$

$= 5 \cdot 10266 - 52 \cdot 986$

Bezout's coefficients.

---

gcd (a, b)
x = a y = b
while y ≠ 0
  r = x mod y
  x = y
  y = r
return x

\# divisions $O(\log b)$

Thm If a and b are positive integers, then there exists integers s and t such that

$\gcd(a,b) = a \cdot \underline{s} + b \cdot \underline{t}$ } Bezout's identity

Bezout's coefficients.

Proof Euclid's algorithm

$$\underset{a}{r_0} = \underset{b}{r_1} \cdot q_1 + r_2$$
$$r_1 = r_2 \cdot q_2 + r_3$$

$$r_2 = r_0 - r_1 \cdot q_1$$
$$* \; r_i = r_{i-2} - r_{i-1} \cdot q_{i-1}$$

$$\vdots$$

$r_{n-2} = r_{n-1} q_{n-1} + r_n \to$ the last non-zero remainder $\gcd(a,b)$

$$r_{n-1} = r_n \cdot q_n + 0$$

$$\gcd(a,b) = r_n = r_{n-2} - r_{n-1} \cdot q_{n-1}$$
$$= r_{n-4} - r_{n-3} \cdot q_{n-3} - (r_{n-3} - r_{n-2} \cdot q_{n-2}) \cdot q_{n-1}$$

replace & reorganize

$$= s \cdot \underset{a}{r_0} + t \cdot \underset{b}{r_1}$$

$\blacksquare$

Ex Prove that $\boxed{\dfrac{\gcd(m,n)}{n} \binom{n}{m}}$ is an integer

$$\binom{n}{m} = \frac{n!}{m!\,(n-m)!} \quad \text{is an integer}$$

$$\Rightarrow \quad \gcd(m,n) = x \cdot m + y \cdot n \quad \text{for some integers } x, y$$

$$\frac{x \cdot m + y \cdot n}{n} \binom{n}{m} = \frac{x \cdot m}{n} \binom{n}{m} + \underbrace{\frac{y \cdot n}{n} \cdot \binom{n}{m}}_{\text{integer}}$$

$$\frac{x \cdot m}{n} \binom{n}{m} = \frac{x \cdot m}{n} \cdot \frac{n!\,(n-1)!}{m!\,(n-m)!\,(m-1)!}$$

$$= \frac{x \cdot (n-1)!}{(m-1)!\,(n-m)!} = \underbrace{x}_{\text{integer}} \underbrace{\binom{n-1}{m-1}}_{\text{integer}}$$

Def Integers $a_1, \dots, a_n$ are relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \le i < j \le n$.

Lemma $\underset{\text{prime}}{p} \mid a_1 \cdot a_2 \cdot \dots \cdot a_n$ then $p \mid a_i$ for some i

Lemma $a, b, c \in \mathbb{Z}_+$ $\gcd(a,b) = 1$ $a \mid b.c$

then $a \mid c$.

proof By Bezout's thm $a.s + b.t = 1$

$a.s.c + b.t.c = c$

$a \mid a.s.c$

$a \mid b.t.c$ (since $a \mid bc$)

then $a \mid c$

Thm Let $m \in \mathbb{Z}_+$, $a, b, c \in \mathbb{Z}$

If $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$ then

$a \equiv b \pmod m$

Proof $m \mid ac - bc$

$4 \mid 2(8^6 - 2)$

$m \mid c(a-b)$ by lemma since $\gcd(c, m) = 1$

$m \mid a-b \implies a \equiv b \pmod m$

By defn. of congruence relation