Euclidean Algorithm for GCD

Division Algorithm

Lemma Given $a \in \mathbb{Z}$ & a +ve integer b, $\exists! q \in \mathbb{Z}$ and a unique r s.t. $a = bq + r$, $0 \leq r < b$

- q: quotient
- r: remainder.

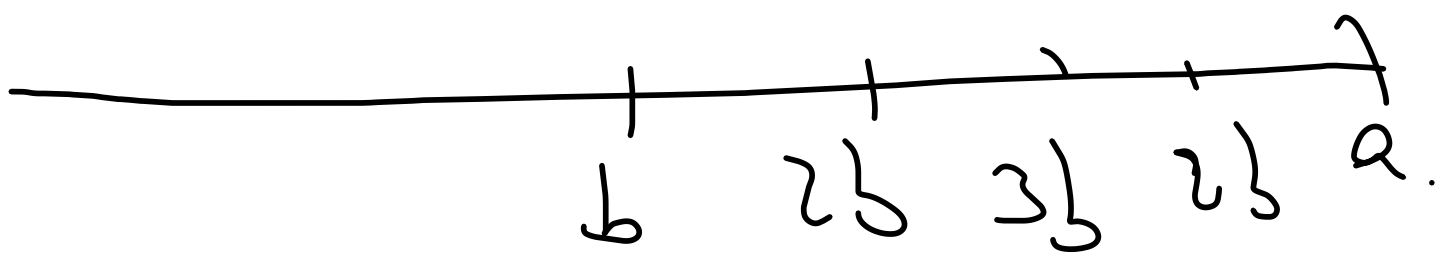
pf WLOG assume a non-negative

If $a = 0$, then take $q = 0$, $r = 0$.

Assume $a > 0$. If $a < b$, take

$q = 0$ & $r = a$.

Assume $a \geq b > 0$.



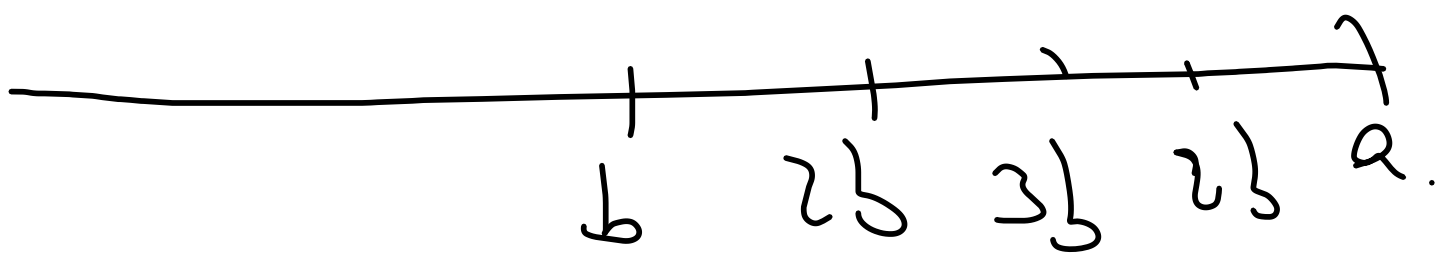
pf WLOG assume a non-negative

If $a = 0$, then take $q = 0$, $r = 0$.

Assume $a > 0$. If $a < b$, take

$q = 0$ & $r = a$.

Assume $a \geq b > 0$.



Let $S = \{a \in \mathbb{Z}^+ : qb \leq a\}$

$S \neq \phi$ & finite.

Let $q = \max S$.

$qb \leq a$.

Set $r = a - qb$.

Defn Let $a, b \in \mathbb{Z}$. Then $GCD(a,b) = d$ if

(1) d is a common divisor of a & b

(2) $d' \mid a$ & $d' \mid b \Rightarrow d' \mid d$.

Set $GCD(0,0) = 0$

Since $GCD(a,b) = GCD(|a|,|b|)$,
w.l.s. we assume $a,b \geq 0$. Let $GCD(a,b) = d$.
If one of a,b, say $b=0$, then
$GCD(a,b) = a$. Assume both $a,b > 0$.
W.l.s. assume $a > b > 0$.
Set $r_0 = a$ & $r_1 = b$.
By the Division Alg.

Obtain integers q_1 & r_2 s.t.

$$r_0 = r_1 q_1 + r_2, \quad \text{where } 0 \le r_2 < r_1$$

Again by Division Alg. $\exists\ q_2, r_3$ s.t.

$$r_1 = r_2 q_2 + r_3, \quad \text{where } 0 \le r_3 < r_2$$

$$\vdots$$

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

Obtain integers q_1 & r_2 s.t.

$$r_0 = r_1 q_1 + r_2, \quad \text{where } 0 \le r_2 < r_1$$

Again by Division Alg. $\exists\ q_2, r_3$ s.t.

$$r_1 = r_2 q_2 + r_3, \quad \text{where } 0 \le r_3 < r_2$$

$$\vdots$$

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

Claim $d = GCD(r_0, r_{i+1})$ $\forall i \geq 2$ $< n$.

Clearly, $d = GCD(a, b) = GCD(r_0, r_1)$

Let $d' = GCD(r_1, r_2)$

(1) $\boxed{r_0 = r_1 q_1 + r_2}$

Since $d \mid r_0$ & $d \mid r_1$, d divides r_2

Hence d is a common divisor of r_1 & r_2

Hence $d \mid GCD(r_1, r_2) = d'$

$d' \mid r_1$ & $d' \mid r_2$. Hence by (1), $d' \mid r_0$.

Hence d' is a common divisor of $r_0, r_1 \therefore d' \mid d$.

Hence $d = GCD(r_n, r_{n-1}) = r_n$.

$r_{n-1} = r_n q_n$.

Euclid (a, b).

Input : a pair of non-negative integers

Output GCD(a, b).

1. If b := 0

2. then return (a)

3. Else return Euclid(b, a mod b)

Ex. Suppose Euclid(a, b) makes
k recursive calls, then show
that $a \geq F_{k+2}$ & $b \geq F_{k+1}$, where
$\{F_n\}$ is the Fibonacci seq.

Lemma Given $a, b \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}$ s.t. integer

$$a = bq + r \quad \& \quad |r| \leq b/2$$

If $\exists$ $r \leq \frac{b}{2}$ Then done.

$\nexists$ $r > b/2$

$$a = bq + r.$$

$$= b(q+1) - (b - r).$$

q'

Extended Euclidean Algorithm.

Thm For any pair of integers $a, b \in \mathbb{Z}$

$\exists$ integers λ and μ s.t.

$$GCD(a,b) = d = \lambda a + \mu b.$$

If WLOG assume $a, b \geq 0$.

We have

$$r_0 = r_1 q_1 + r_2, \quad r_2 < r_1$$
$$r_1 = r_2 q_2 + r_3, \quad r_3 < r_2$$
$$\vdots$$
$$r_{n-1} = r_n q_n$$

Claim Each r_i is a linear combination of a, b. More precisely, for each i

$\exists$ integers λ_i & μ_i s.t.

$$\boxed{r_i = \lambda_i a + \mu_i b.} \qquad i = 0, \ldots, n-1$$

Pf By induction on i. True for $i=0$ & $i=1$

Assume the result is true for integer $\leq i$

$$r_{i-1} = r_i q_i + r_{i+1} \quad , \quad r_{i+1} < r_i$$

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_i q_i \\ &= (\lambda_{i-1} a + \mu_{i-1} b) - (\lambda_i a + \mu_i b) q_i \\ &= (\lambda_{i-1} - \lambda_i q_i) a + (\mu_{i-1} + \mu_i q_i) b. \end{aligned}$$

Set $\lambda_{i+1} = \lambda_{i-1} - \lambda_i q_i$

$\mu_{i+1} = \mu_{i-1} - \mu_i q_i$

Hence the claim. In particular

$$G(1)(a,b) = \gamma_n = \boxed{\lambda_n a + \mu_n b.}$$

λ_n, μ_n are obtained by the following recursion

$\lambda_0 = 1$ $\quad \mu_0 = 0$

$\lambda_1 = 0$ $\quad \mu_1 = 1$

$\lambda_{i+1} = \lambda_{i-1} - q_i \lambda_i$

$\mu_{i+1} = \mu_{i-1} - q_i \mu_i$

Extended-Euclid (a, b)

Input A pair of non-negative integers

Output A triplet of the form (d, λ, μ)

where $d = GCD(a, b)$ & $\boxed{d = \lambda a + \mu b.}$

1. If $b := 0$

   then return $(a, 1, 0)$.

   else $(d', \lambda', \mu') := \text{Extended-Euclid}(b, a \bmod b)$

   $(d, \lambda, \mu) = (d', \mu', \lambda' - \lfloor \frac{a}{b} \rfloor \mu')$.

   return (d, λ, μ)

Correctness

By induction hypothesis if

$(d', \lambda', \mu') = \text{Extended-Euclid}(b, a \bmod b)$

then $d' = GCD(b, a \bmod b)$ &

$d = d' = \lambda' b + \mu' \; a \bmod b$

$= \lambda' b + \mu' \left[a - \left\lfloor \frac{a}{b} \right\rfloor b \right]$

$= \mu' a + \left(\lambda' - \left\lfloor \frac{a}{b} \right\rfloor \mu' \right) b$

$= \lambda a + \mu b$

$\therefore \; d = d' = \lambda' b + \mu' \; a \bmod b$

Correctness

By induction hypothesis if

$$(d', \lambda', \mu') = \text{Extended-Euclid}(b, a \bmod b)$$

Then $\boxed{d' = GCD(b, a \bmod b)}$ &

$$\boxed{d' = \lambda' b + \mu' \, a \bmod b}$$

$$\therefore d = d' = \lambda' b + \mu' \, a \bmod b.$$

$$= \lambda' b + \mu' \left[a - \left\lfloor \frac{a}{b} \right\rfloor b \right]$$

$$= -\mu' \left\lfloor \frac{a}{b} \right\rfloor b + \left(\lambda' - \left\lfloor \frac{a}{b} \right\rfloor \mu' \right) b$$

$$= \lambda a + \mu b.$$

Thm Suppose $GCD(a, n) = 1$.

Then $\exists$ an integer b s.t.

$$\boxed{ab \equiv 1 \mod n.}$$

b is called the "multiplicative inverse of a modulo n".

Pf By Extended- Euclid, $\exists \lambda, \mu$

s.t. $a\lambda + n\mu = 1$

$\Rightarrow a\lambda \equiv 1 \mod n$.

Cor $\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n : GCD(a, n) = 1 \}$.

is a multiplicative group.

Chinese Remainder Theorem (CRT)

Let $n_1, n_2, \cdots, n_k$ be +ve integers which are pairwise co-prime.

Let $n = n_1 n_2 \cdots n_k$.

Then the following system of congruences.

$$X \equiv a_1 \bmod n_1$$
$$X \equiv a_2 \bmod n_2$$
$$\vdots$$
$$X \equiv a_k \bmod n_k$$

has a unique solution modulo n for X.

pf Uniqueness. Suppose X, Y are 2 solutions

then

$$X \equiv Y \bmod n_1 \Rightarrow n_1 \mid X - Y$$

$$X \equiv Y \bmod n_2 \Rightarrow n_2 \mid X - Y$$

$$\vdots \qquad\qquad \vdots$$

$$X \equiv Y \bmod n_r \qquad n_r \mid X - Y$$

$\Big\}$ $\underbrace{n_1 \cdots n_r}_{n} \mid X - Y$

$X \equiv Y \bmod n$

Existence.

Define $m_i' = \frac{n}{n_i}$. (clearly $GCD(m_i, n_i) = 1$)

Hence $\exists\ \tilde{m}_i$ s.t. $\boxed{m_i \tilde{m}_i \equiv 1 \bmod n_i}$

Take $X = a_1 m_1 \tilde{m}_1 + a_2 m_2 \tilde{m}_2 + \cdots + a_k m_k \tilde{m}_k$

Clearly $X \bmod n_1 = a_1 m_1 \tilde{m}_i \bmod n_1$

$\equiv a_1 \bmod n_1$

Euler's φ-fn.

$$\varphi(n) = \begin{cases} 1 & \text{if } n = 1 \\ \#\text{ of +ve integers } < n \text{ which are co-prime to } n & \text{o.w.} \end{cases}$$

$\varphi(6) = 2.$

1, ~~2~~, ~~3~~, ~~4~~, 5

Thm φ satisfies the following

① $\varphi(p^\alpha) = p^\alpha\left(1-\frac{1}{p}\right)$, where p is prime.

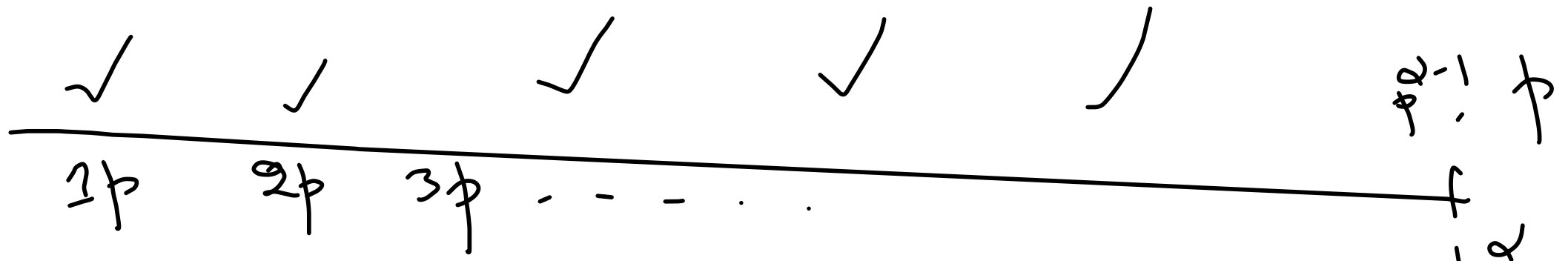
② If $GCD(m,n)=1$, then

$$\varphi(mn) = \varphi(m)\varphi(n)$$

③ If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Then

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

pf



We shall count all +ve integers $\leq p^\alpha$ that are not co-prime to p^α.

# of such integers is $p^{\alpha-1}$

$$\therefore \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$$