Number Theory

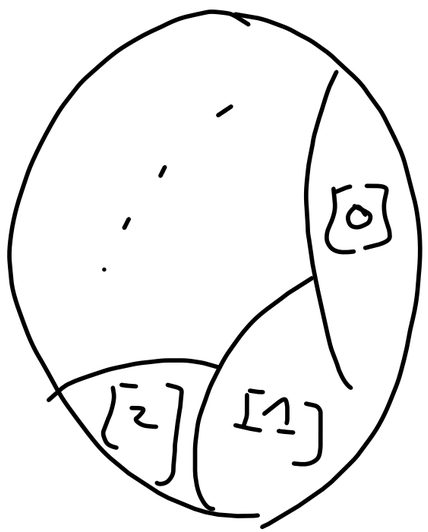
Defn Let $a, b \in \mathbb{Z}$. Fix a +ve integer n. We say ~~that~~

$$a \equiv b \bmod n$$

if $n \mid a - b$.

Equivalences classes $[0], [1], [2], \ldots [n-1]$

$\mathbb{Z}$



$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

Define two operations + and $\times$ on $\mathbb{Z}_n$ as follows:

Let $a, b \in \mathbb{Z}_n$

Let c be the unique element in $\mathbb{Z}_n$ s.t. $a + b \equiv c \bmod n$.

We define $\boxed{a + b = c}$ in $\mathbb{Z}_n$.

Let $d \in \mathbb{Z}_n$ be the unique element s.t. $a \cdot b = d \bmod n$.

We define $\boxed{a \cdot b = d}$ in $\mathbb{Z}_n$

Clearly (Check), $(\mathbb{Z}_n, +, \times)$ is a ring.

Division Algorithm

Let $a \in \mathbb{Z}$ and b a +ve integer.

Then $\exists$ a unique q (quotient) and a unique r (remainder) s.t.

$$\boxed{a = qb + r \quad \text{with } 0 \le r < b.}$$

ff t.

Defⁿ Let $a, b \in \mathbb{Z}$.

The greatest common divisor (GCD) of a and b is the largest integer d s.t. $d|a$ and $d|b$. More formally:

$GCD(a,b) = d$ if

(i) $d|a$ & $d|b$.

(ii) If $c|a$ & $c|b$ then $c|d$.

We define $GCD(a,0) = 0$.

Euclidean Algorithm.

Let $a, b \in \mathbb{Z}$. Since $GCD(a,b) = GCD(|a|, |b|)$ we assume $a, b \geq 0$. W.l.g. assume $a > b \geq 0$.

If $b = 0$, $GCD(a,b) = a$. So assume $a > b \geq 1$.

Set $r_0 = a$ & $r_1 = b$.

By the division algorithm, $\exists\, q_1$ and r_2 s.t.

$$\boxed{r_0 = q_1 r_1 + r_2}, \quad 0 \le r_2 < r_1.$$

If $r_2 > 0$, then by D.A, we obtain.

q_2 and r_3 s.t.

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

$$\vdots$$

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

Claim $GCD(r_i, r_{i+1}) = GCD(a,b) = d$.

$\forall\, i = 0, \dots, n-1$

We prove the claim by induction on i. True for $i = 0$

Assume true for $i-1$

Let $d' = GCD(r_i, r_{i+1})$.

(*) $r_{i-1} = q_i r_i + r_{i+1}, \quad 0 \le r_{i+1} < r_i$

By ind. hyp, $d \mid r_{i-1}$ & $d \mid r_i \Rightarrow d \mid r_{i+1}$

Hence $d \mid d'$

By (2) $d' \mid r_i$, $d' \mid r_{i+1}$ & hence

$d' \mid r_{i-1}$

So $d' \mid r_{i-1}$ and $d' \mid r_i$.

Hence $d' \mid GCD(r_{i-1}, r_i) = d$.

Hence $d = d'$

Hence the claim holds.

$$d = GCD(r_i, r_{i+1}) = GCD(r_{n-1}, r_n)$$
$$= r_n.$$

Euclid(a, b).

Input : Non-neg. integers a, b.

Output : GCD(a, b).

1. If b = 0, then
   return a

2. Else Euclid(b, a mod b).

Complexity. Assume that Euclid(a, b) makes R recursive calls. Then

$a \geq F_{K+2}$ and $b \geq F_{K+1}$, where.

$\{F_n\}$ is the Fibonacci seq:

We shall prove this by induction on k.

$F_0 = 1, F_1 = 1$

$F_2 = F_0 + F_1 = 2.$

For $k=0$, $b=1$.

Hence $a \geq 2 = F_2$.

$a \geq F_1$

Assume that the result holds for $k-1$

First recursive call is

Euclid(b, a mod b)

⋮ } k-1 recursive calls.

By ind. hyp.

$b \geq F_{(k-1)+2} = F_{k+1}$

$a \bmod b \geq F_{(k-1)+1} = F_k$.

$b \geq F_{k+1}$

$a \bmod b \geq F_k$.

By division algorithm.

$$a = qb + a \bmod b.$$

$$\geq b + a \bmod b.$$

$$\geq \overline{f}_{k+1} + \overline{f}_k = \overline{f}_{k+2}$$

Complexity of Euclid is $O(\log b)$.

Ex Show that Euclid (F_{k+1}, F_k) makes exactly k recursive calls.

Modified Division Alg.

Let $a \in \mathbb{Z}$, $b > 0$. $\exists$ a unique integer q and a unique integer r s.t

$$a = qb + r, \quad 0 \leq |r| \leq \frac{b}{2}$$

pf:

$a = \tilde{q} b + \tilde{r} \quad ; \quad 0 \le \tilde{r} < b$.

If $\tilde{r} \le \frac{b}{2}$ done.

If $\tilde{r} > \frac{b}{2}$, then

$|-(b-\tilde{r})|$

$= b - \tilde{r} < \frac{b}{2}$

$a = (\tilde{q}+1) b - (b - \tilde{r})$

Thm (Extended Euclidean Algorithm)

Let $a, b \in \mathbb{Z}$ & let $d = GCD(a, b)$

Then $\exists$ integers λ and μ s.t.

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

pf:

$$r_0 = r_1 q_1 + r_2, \quad 0 \le r_2 < r_1$$
$$r_1 = r_2 q_2 + r_3, \quad 0 \le r_3 < r_2$$
$$\vdots$$
$$r_{n-1} = r_n q_n$$

Claim: $\exists \lambda_i$ and μ_i s.t.

$$r_i = \lambda_i a + \mu_i b, \quad i = 0, \ldots, n.$$

for $i=0$, set $\lambda_0 = 1$ and $\mu_0 = 0$.

Assume the result for all $j < i$.

$$r_j = \lambda_j a + \mu_j b \quad \text{for all } j < i.$$

Consider the relation.

$$r_{i-2} = r_{i-1} q_{i-1} + r_i \;, \quad 0 \le r_i < r_{i-1}$$

$$r_i = r_{i-2} - r_{i-1} q_{i-1}$$

$$r_i = (\lambda_{i-2}^{a} + \mu_{i-2}^{b}) - (\lambda_{i-1}^{a} + \mu_{i-1}^{b}) q_{i-1}$$

$$= \underbrace{(\lambda_{i-2} - \lambda_{i-1} q_{i-1})}_{\lambda_i} a$$

$$+ \underbrace{(\mu_{i-2} - \mu_{i-1} q_{i-1})}_{\mu_i} b.$$

Extended - Euclid (a, b).

Input Non-negative integers a, b.

Output (d, λ, μ) s.t. GCD(a, b) = d = λa + μb.

1. If b = 0 : Then
   return (a, 1, 0).
2. Else Extended-Euclid (b, a mod b) = (d', λ', μ')
3. Return (d', μ', λ' - ⌊a/b⌋ μ')

By induction hypothesis

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

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

By induction hypothesis

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

Also, $\boxed{d = \lambda' b + \mu' a \bmod b.}$ (*)

Now we have.

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

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

$$= \lambda' b + \mu' \, a \bmod b = d \quad \text{by } (*).$$

Cor 1. Let $GCD(a, n) = 1$. i.e. a is co-prime to n. Then $\exists$ an integer b s.t $\boxed{a.b \equiv 1 \bmod n}$.

pf By Thm $\exists \lambda, \mu$ s.t.

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

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

Cor 2 $\mathbb{Z}_n$ is a field iff

n is prime.

If n is prime, then each element of

$\mathbb{Z}_n^* = \{1, \ldots, n-1\}$ has a multiplicative inverse

& hence $\mathbb{Z}_n^*$ is a multiplicative group

If n is not prime, then

$n = n_1 n_2$, where n_1, n_2 are non trivial factors of n

Hence in $\mathbb{Z}_n$

$$n_1 \cdot n_2 = 0$$

$\mathbb{Z}_n$ has zero divisor.

$\mathbb{Z}_n$ is not a field.

Ex 1. Show that Euclid(F_{k+1}, F_k) makes exactly $k-1$ recursive calls.

Ex 2 Compute (d, x, y) that the call Extended-Euclid(899, 493)

Ex 3 Show that $GCD(a, n) = GCD(a+kn, n)$

Ex 4 What does Extended-Euclid(F_{k+1}, F_k) returns?

Ex: Prove that n_1, n_2, n_3 and n_4 are pairwise co-prime iff

$$GCD(n_1 n_2, n_3 n_4) = GCD(n_1 n_3, n_2 n_4)$$