Jan25

Saturday, January 22, 2022 9:47 AM

Extended Euclidean Algorithm

Fix $a, b \in \mathbb{Z}$.

$g = \gcd(a,b)$

The I can find $u, v \in \mathbb{Z}$ s.t.

$$\boxed{g = au + bv}$$

More properties of $\mathbb{Z}$ (= integers).

Defn A positive integer $p \neq 1$ is prime if its divisors are ± 1 & $\pm p$.

Euclid's Lemma

$a, b \in \mathbb{Z}$. p a prime.

If $p | ab$ then $p | a$ or $p | b$.

Proof

$g = \gcd(a,p)$, so $g | p$ i.e. $g = 1$ ① or $g = p$ ②.

② In particular $p | a$ & we win.

① Euclidean Algorithm $\Longrightarrow$

$\exists\ u, v \in \mathbb{Z}$ s.t.

$$1 = g = au + pv$$

Trick multiply through by b.

$$\underline{b = abu + pbv} \quad *$$

Summarize $p | p \Longrightarrow p | pbv$

$p | ab \Longrightarrow p | \underline{abu}$

HW1 #7 $p \,|\, (\underbrace{abu + pbv}_{= b}).$

Example: It is important that p is prime.

$15 \,|\, 3 \cdot 5$

but $15 \nmid 3$ & $15 \nmid 5$ ...

Exercise

Formulate & prove a converse to Euclid's Lemma.

Corollary (Inductive Euclid's Lemma)

p prime.

$p \,|\, a_1 a_2 a_3 \cdots a_n \qquad (a_i \in \mathbb{Z}).$

Then $p|a_1$ or $p|a_2$ or ... or $p|a_n$.

Proof: Proof by induction.

Base Case (n=1)

$p \mid a \implies p \mid a$ ✓

Inductive Step

Assume it's true for products of $< n$ numbers. Show it's true for products of n numbers.

$$p \mid a_1 a_2 \cdots a_n \Rightarrow p \mid \underbrace{(a_1 a_2 \cdots a_{n-1})}_{} \underbrace{a_n}_{}$$

Euclid's Lemma

$$\longrightarrow \underline{p \mid a_1 a_2 \cdots a_{n-1}} \quad \text{or} \quad p \mid a_n.$$

← We win.

→ By inductive hypothesis

$$p \mid a_1 \text{ or } p \mid a_2 \text{ or} \ldots \text{ or } p \mid a_{n-1}$$

we also win.

The Fundamental Theorem of Arithmetic

Every positive integer $a \geq 1$ can be written as a product of primes

$$a = p_1 p_2 \cdots p_t \qquad (*)$$

Such a factorization is unique up to reordering.

Rmk: (*) Allow primes to repeat. Might see

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$$

Crucial Input (Well ordering principle)

Suppose S = nonempty set of integers & suppose $\exists\, b \in \mathbb{Z}$ s.t. $\forall\, x \in S$, $x \geq b$.

Then S has a smallest element.

Exercise: Prove this formally.

Proof

Existence:

$$S = \left\{ a > 1 \;\middle|\; \begin{array}{l} a \text{ is not the product} \\ \text{of primes} \end{array} \right\}$$

Well ordering says $\exists$ a smallest $z \in S$.

z not prime, so $z = z_1 z_2$ w/

$$1 < z_1, z_2 < z$$

$\uparrow$ Theorem is true for z_1 & z_2

$$z_1 = p_1 p_2 \cdots p_t$$

$$z_2 = q_1 q_2 \cdots q_l$$

So $z = z_1 z_2 = p_1 \cdots p_t q_1 \cdots q_l$ so theorem holds for z.

No smallest elt exists so $S = \emptyset$.

Uniqueness:

$$a = \underline{p_1} p_2 \cdots p_t = \underline{q_1} q_2 \cdots q_l \longleftarrow$$

Assume $l \leq t$. (without loss of generality
WLOG)

Notice $p_1 \mid a \leadsto p_1 \mid q_1 q_2 \cdots q_l$.

Euclid's Lemma $\Longrightarrow$ $p_1 \mid q_i$ some i.

Reorder q_i's so $p_1 \mid q_1$

So $p_1 = q_1$ we can cancel

$$p_2 \cdots p_t = q_2 \cdots q_l$$

$\Big\downarrow$ cancel p_2 & q_2

$$p_3 \cdots p_t = q_3 \cdots q_l$$

$$\vdots$$

$$\underbrace{p_{\ell+1} p_{\ell+2} \cdots p_t}_{} = 1$$

These must all $= 1$.

we win $p_1 = q_1 \quad p_2 = q_2 \ \cdots\cdots \ p_\ell = q_\ell$.

& done!

Modular Arithmetic

Def^n Let $m \in \mathbb{Z}_{\geq 1}$
$a \in \mathbb{Z}$.

HW 1 #8 $a = mq + r$ for unique q, r
w/ $0 \leq r < |m|$

The residue of a modulo m is this number r.

Lemma

$m \in \mathbb{N}$. $a, b \in \mathbb{Z}$.

a and b have the same residue modulo $m \iff m \mid (a-b)$

Def^n If a & b are as in the lemma, we say a is congruent to b modulo m. We write

$$a \equiv b \mod m.$$

Important Exercise

→ ① Prove the lemma.

② Prove $\equiv$ mod m is an equivalence relation. on $\mathbb{Z}$.

Recall (HW1 #6)

Equivalence relations give partitions by passing to equivalence classes.

What are the equivalence classes for $\equiv$?

$a \in \mathbb{Z}$. $m \in \mathbb{N}$

$$[a] = \overline{a} = \{ b \mid b \equiv a \mod m \}$$

Lemma $\rightsquigarrow$ $= \{ b \mid m \text{ divides } b-a \} = (*)$

$$b - a = km \iff b = a + km$$

$$(*) = \{ a, a \pm m, a \pm 2m, a \pm 3m, \ldots \}$$

Example $m = 2$ $a = 8$

$$[8] = \{\ldots, -2, 0, 2, 4, 6, 8, 10, 12, 14, \ldots\}$$

$= \text{Even numbers.}$

Define the following set

$$\mathbb{Z}/m\mathbb{Z} = \{\, \overline{a} \mid a \in \mathbb{Z} \,\}$$

Observation

① $a \equiv b \mod m \iff \overline{a} = \overline{b}$

(HW 1 #6)

② There is a surjective function

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\pi"] & \mathbb{Z}/m\mathbb{Z}. \\ a \arrow[r, mapsto] & \overline{a} \end{tikzcd}$$

③ **Not injective**

⚠ $\pi(a) = \overline{a} \underset{\overset{\uparrow}{?}}{=} \overline{a+m} = \pi(a+m).$

$a \equiv a+m \mod m$

$\overset{?}{\Updownarrow}$

$m \mid (a+m) - a$

$\overset{?}{\Updownarrow}$

$m \mid m$ ✓

④ Let r be the residue of a modulo m. Hw1 #8

$$\underline{a = mq + r \qquad 0 \le r < m}$$

$$\Longrightarrow m \mid a - r$$

$$\Longrightarrow \bar{a} = \bar{r} \leftarrow$$

& $r \in \{\underbrace{0, 1, 2, \ldots, m-1}\}$

$$\mathbb{Z}/m\mathbb{Z} = \{\underbrace{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}}\}$$

In particular,

$\mathbb{Z}/m\mathbb{Z}$ is finite

→ These are all distinct!

Pf/ $0 \le a \le b < m$.

& $\bar{a} = \bar{b}$

$$0 \le b - a < m - a \le m$$

& $m \mid (b-a) \Longrightarrow b - a = 0$

so $b = a$ ∅

Example

$\mathbb{Z}/12\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{11}\}$

$\overline{35} = \overline{11}$

↑

$35 = 24 + 11$

$12 \cdot 2 = 35 - 11 \iff 35 \equiv 11 \mod 12$

"clock arithmetic"

3 hours after 11 is 2

$\rightsquigarrow \overline{11} + \overline{3} = \overline{14} = \overline{2}$

We can define + & × on $\mathbb{Z}/m\mathbb{Z}$.

Lemma $a, a', b, b' \in \mathbb{Z}$. $m \in \mathbb{Z}$

$a \equiv a' \mod m \iff \overline{a} = \overline{a'}$

$b \equiv b' \mod m \iff \overline{b} = \overline{b'}$

The

$a + b \equiv a' + b' \mod m \iff \overline{a+b} = \overline{a'+b'}$

$ab \equiv a'b' \mod m \iff \overline{ab} = \overline{a'b'}$.

Proof Exercise.

In particular, the following is well defined

$$\begin{aligned} + : (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ (\bar{a}, \bar{b}) &\longmapsto \overline{a+b} \end{aligned}$$

$$\bar{a} + \bar{b} = \overline{a+b}$$

$$\begin{aligned} \times : (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) &\longrightarrow (\mathbb{Z}/m\mathbb{Z}) \\ (\bar{a}, \bar{b}) &\longmapsto \overline{ab} \end{aligned}$$

$$\bar{a} \times \bar{b} = \overline{ab}$$

Remark on "well defined"

We're making a choice in how we define the function.

$$a \equiv a' \mod m$$

$$\Longrightarrow \bar{a} = \overline{a'}$$

need
$$\begin{array}{ccc} \bar{a} + \bar{b} & = & \overline{a'} + \bar{b} \\ \| & & \| \\ \overline{a+b} & = & \overline{a'+b} \end{array}$$

↑ by the lemma. (Phew!)

Observations & Examples

$$\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$$

$$* \ \overline{2} \cdot \overline{5} = \overline{2 \times 5} = \overline{10} = \overline{4}$$

$10 = 4 + \underline{\underline{\underline{6}}}$

$\overline{10} = \overline{4}$

$2 \equiv 8 \mod 6$ i.e. $\overline{2} = \overline{8}$

$$* \ \overline{8} \cdot \overline{5} = \overline{8 \times 5} = \overline{40} = \overline{4}$$

40

$= 4 + \underbrace{36}_{6 \times 6}$

(phew!).

Zero divisors

$$\overline{2} \cdot \overline{3} = \overline{2 \cdot 3} = \overline{6} = \overline{0}$$

Multiply nonzero things to get zero

Don't have division in general

$\overline{2} x = \overline{3}$ ($2x \equiv 3 \mod 6$)

has no solution.

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}x$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$

Never get $\overline{3}$.

Sometimes I can divide

$\Longrightarrow 5x \equiv 1 \mod 6$ $\qquad (\overline{5}x = \overline{1})$

By hand:

$$5\cdot 5 = 25 = 24+1 = 6\cdot 4+1$$

$$5\cdot 5 \equiv 1 \mod 6$$

Solve $\quad 5x \equiv 3 \mod 6$

$$\underbrace{5\cdot 5}_{\equiv 1}\cdot x \equiv 5\cdot 3 \mod 6$$

Lemma say $\times\overline{24}$ same as $\times\overline{1}$

$$x \equiv 15 \mod 6$$

$$\equiv 3 \mod 6.$$

Solve equations! (divide by 5).

Fun: $\quad 5^{-1} \equiv 5 \mod 6.$

Exercise

Compute $\frac{1}{2}$ mod 5 ←

Def^n

Consider $\bar{a}x = \bar{1}$ in $\mathbb{Z}/m\mathbb{Z}$.

If $\bar{b}$ is a solution ($ab \equiv 1 \mod m$) then b is a multiplicative inverse to a mod m.

(write $a^{-1} \equiv b \mod m$).

Observe

If a^{-1} exists, then we can solve any equation

$$ax \equiv c \mod m$$

$$\Downarrow$$

$$\underbrace{a^{-1}a}_{=1}x \equiv a^{-1}c \mod m$$

$$x \equiv a^{-1}c \mod m. \quad \varnothing$$

Exercise

Solve $2x \equiv 3 \mod 5$

Question

Which $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ can I divide by?

(When is there a solution to $\bar{a}x = \bar{1}$)

Prop $ax \equiv 1 \mod m$ has a soln

$\iff \gcd\underline{(a,m)} = 1$

Proof

$\Rightarrow$ $ax \equiv 1 \mod m.$

$ax - 1 = mk$

$\underline{\underline{ax + mk = 1}}$

$g = \gcd(a,m).$

$$\left.\begin{aligned} g|a &\Rightarrow g|ax \\ g|m &\Rightarrow g|mk \end{aligned}\right\}$$

HW1 #7 $g | ax+mk \rightsquigarrow g|1$

$\rightsquigarrow g = 1$ ✓

$\Leftarrow$ $g = \gcd(a,m) = 1$

Extended Euclidean Alg. $\exists\ u, v \in \mathbb{Z}$

s.t. $au + mv = 1$

So $au = 1 - mv$

$\equiv 1 \mod m$

Letting $x = u$ gives soln. $\varnothing$

Summary TFAE ← (The following are equivalent)

① $\bar{a}$ has inverse in $\mathbb{Z}/n\mathbb{Z}$.

② $\bar{a}x = \bar{1}$ has soln. in $\mathbb{Z}/m\mathbb{Z}$.

③ $ax \equiv 1 \mod m$ has soln in $\mathbb{Z}$.

④ $\gcd(a, m) = 1$

Corollary

All nonzero elements of $\mathbb{Z}/m\mathbb{Z}$ have multiplicative inverses $\iff$ m is prime.

$\implies$ Ex

$\impliedby$ ✓

Defn (Multiplicative Group of $\mathbb{Z}/m\mathbb{Z}$).

$$(\mathbb{Z}/m\mathbb{Z})^\times = \text{mult gp of } \mathbb{Z}/m\mathbb{Z}$$

$$= \{\bar{a} \in \mathbb{Z}/m\mathbb{Z} \mid \bar{a} \text{ has inverse}\}$$

$$= \{\bar{a} \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1\}$$

Ex Compute $(\mathbb{Z}/12\mathbb{Z})^\times$

Next Time Groups. Explain why this is a group.