Math 403. Lecture 3
Equivalence Relations and Modular Arithmetic

Def Let S be a set. An equivalence relation on S is a subset $R \subseteq S \times S$ satisfying following axioms.

(1) (Reflexive) For all $a \in S$, $(a,a) \in R$;

(2) (Symmetric) $(a,b) \in R \Rightarrow (b,a) \in R$;

(3) (Transitive) $(a,b) \in R$, $(b,c) \in R \Rightarrow (a,c) \in R$.

Rmk (1) We like to write $a \underset{R}{\sim} b$ or $a \underset{R}{\equiv} b$ or just $a \sim b$ or $a \equiv b$ if $(a,b) \in R$. Sometimes people also write aRb.

(2) Equivalence relations are a generalization of equality.

Ex (1) Let S be a set. Define $\Delta \subseteq S \times S$ by $\Delta = \{(a,a) : a \in S\}$. Then Δ is an equivalence relation, and $a \underset{\Delta}{\equiv} b \Leftrightarrow a = b$.

Pf Clearly $a \underset{\Delta}{\equiv} b \Leftrightarrow a = b$. So clearly reflx, sym, trans and $=$ is. This is an equiv. rel.

Ex 2 Define a relation on numbers $a \in \mathbb{Z}_{>1}$ by aRb if a and b have a prime factor in common

- Reflex ✓
- Sym ✓
- Tran ~~3R6~~ $3R6$, $6R2$ by $(3,2) \notin R$. So

X

Ex 3 Let $S = \mathbb{Z}$ and $n \in \mathbb{Z}$. Define R_n

$$R_n = \{(a,b) : n \mid b-a\}.$$

Then R_n defines an equiv. relation.

If $a \underset{R_n}{\sim} b$ we write

$$a \equiv b \pmod{n}$$

— or just —

$$a \equiv b \ (n)$$

and say that a is congruent to b modulo n.

Pf (reflex) $a \equiv a \ (n)$ since $n \mid 0$, since

$$0 = 0 \cdot n.$$

(sym) Suppose $a \equiv b \ (n)$. Then $a - b = nk$ for some $k \in \mathbb{Z} \Rightarrow b - a = n(-k) \Rightarrow n \mid b-a \Rightarrow b \equiv a \ (n)$

(trans) Suppose $a \equiv b \ (n)$ and $b \equiv c \ (n)$.

Then $a - b = nk$, $b - c = nj$ for some $k, j \in \mathbb{Z}$.

$\Rightarrow a - c = (a-b) + (b-c) = n(k+j)$

$\Rightarrow n \mid a - c \Rightarrow a \equiv c \ (n)$.

Prop Let $f: S \to T$ be a function. Then define

$$R = R_f = \{(a,b) \in S \times S : f(a) = f(b)\}.$$

Then R defines an equivalence relation.

Pf (reflex) $f(a) = f(a)$ obv.

(symm) $f(a) = f(b) \Rightarrow f(b) = f(a)$ obv.

(trans) $f(a) = f(b)$, $f(b) = f(c) \Rightarrow f(a) = f(c)$.

Def Suppose R is an ~~equiv~~ equivalence rel. on a set S, and $a \in S$. The equivalence class of a is the subset

$$[a] = \{x \in S : (a,x) \in R\}.$$

The quotient of S by R is the set

$$S/R := \{[a] : a \in S\}.$$

The quotient map is the map

$$\pi: S \to S/R \quad \text{given by}$$

$$a \mapsto [a]$$

Lemma Suppose R is an equivalence rel. on a set S. Then for $a, b \in S$

$$[a] = [b] \iff a \in [b].$$

Pf ($\Rightarrow$) Since $a \sim a$ by refl., $a \in [a]$.
So $[a] = [b] \Rightarrow a \in [b]$.

($\Leftarrow$) Suppose $a \in [b]$. Then $b \sim a$. So by sym.) $a \sim b$. Thus $b \in [a]$. Now suppose $c \in [a]$. Then $a \sim c$ and $b \sim a$, so $b \sim c$, So $c \in [b]$. Since this holds for any $c \in [a]$, we have $[a] \subseteq [b]$. But since $b \in [a]$ as well we have $[b] \subseteq [a]$. So $[a] = [b]$.

Cor We have $[a] \cap [b] = \emptyset$ unless $[a] = [b]$.

Pf Suppose $c \in [a] \cap [b]$. Then $[a] = [c] = [b]$.

Modular Arithmetic

Prop Suppose $n \in \mathbb{Z}_+$. Then

① For each $a \in \mathbb{Z}$, there exists a unique $r \in \{0, 1, \ldots, n-1\}$ such that $a \equiv r \pmod{n}$

② If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$ then

$$a + b \equiv c + d \pmod{n}$$

— and —

$$ab \equiv cd \pmod{n}.$$

③ If $ab \equiv ac$ and $(a, n) = 1$ then $b \equiv c$

Pf ① Write $a = nd + r$ using division alg.

Since $n \mid a - r$, we have $a \equiv r \pmod{n}$.

By div alg. $0 \le r < n$. If $0 \le r_1 < r_2 < n$, then

$a \equiv r_1 \Rightarrow$, $a \equiv r_2 \Rightarrow n \mid r_2 - r_1$. But since $0 \le r_2 - r_1 < n$ this is impossible.

② Suppose $a = c + nx$
$b = d + ny$ for $x, y \in \mathbb{Z}$.

Then $a + b = c + d + n(x + y) \Rightarrow n \mid (a + b) - (c + d)$

$$\Rightarrow a + b \equiv c + d \pmod{n}$$

$$ab = cd + cny + dnx + n^2xy$$

$$= cd + n(cy + dx + nxy)$$

$$\Rightarrow n \mid ab - cd \Rightarrow ab \equiv cd \pmod{n}$$

③ $ab \equiv ac \Rightarrow n \mid a(b - c)$
$\Rightarrow n \mid b - c$
since $(a, n) = 1$

Suppose $n \in \mathbb{Z}^+$.

Def $\mathbb{Z}/n = \mathbb{Z}/R_n$ where $R_n = \{(a,b) \in \mathbb{Z}^2 : n \mid a-b\}$.

Prop $\mathbb{Z}/n$ has exactly n elements: $[0], [1], \ldots, [n-1]$.

Pf ✅ For each $[a] \in \mathbb{Z}/n$ show $[a] = [r]$ with r unique integer in $\{0,1,\ldots,n-1\}$.

Def ~~Define~~ Let $0 \le r, s < n$. ~~Define~~ Set

$$[r] + [s] = [r+s]$$

$$[r][s] = [rs].$$

Prop For all $a, b \in \mathbb{Z}$ show

$$[a] + [b] = [a+b]$$

$$[a][b] = [ab].$$

Pf ~~Suppose~~ $a, b \in \mathbb{Z}$. Find $r, s \in \{0,1,\ldots,n-1\}$ s.t. $a \equiv r \pmod n$, $b \equiv s \pmod n$. So

~~So $[a] = [r]$, $[b] = [s]$.~~

~~Thus $[a] + [b] = [r+s]$. Since $r+s \equiv a+b \pmod n$~~

show $[r+s] = [a+b]$.

So ~~Def~~ $a+b \equiv r+s \pmod n \Rightarrow [a+b] = [r+s]$

$ab \equiv rs \pmod n \Rightarrow [ab] = [rs]$.

$\Rightarrow$ ~~$[a+b] = [r+s]$~~

$$[a] + [b] = [r] + [s] = [r+s] = [a+b]$$

$$[a][b] = [r][s] = [rs] = [ab].$$

Nice Properties of $\mathbb{Z}/n$

Prop Suppose $a, b, c \in \mathbb{Z}$. Then, in $\mathbb{Z}/n$,

(1) $[0] + [a] = [a]$

(2) $[a] + ([b] + [c]) = ([a] + [b]) + [c]$

(3) $[a] + [b] = [b] + [a]$.

(4) $[a] + [-a] = 0$.

Pf

(1) $[0] + [a] = [0 + a] = a$

(2) $[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c]$

$= [a + b] + [c] = ([a] + [b]) + [c]$

(3) (3-4) Same idea.

Bottom line We can treat $\mathbb{Z}/n$ in much the same way we treat regular numbers.

Prop Suppose $(a, n) = 1$. Then $\exists\ b \in \mathbb{Z}$ st $[ab] = 1$.
The class $[b]$ is unique.

Pf Can find b, c st $ab + cn = 1$. So $[a][b] = 1$.
$ab \equiv 1 \ (n) \Rightarrow [a][b] = 1$.
Suppose $ab = ab' \equiv 1$. Since $(a, n) = 1$ $b = b'$ by previous prop
So $[b] = [b']$.

Modular Exponentiation

Suppose $n \in \mathbb{Z}_+$ and we want to compute $a^d \bmod n$ where $a, d \in \mathbb{Z}$, $d > 0$.

Here's a way to do it which is fast.

1) Write d in binary. So write

$$d = d_k 2^k + d_{k-1} 2^{k-1} + \cdots + d_0$$

where $d_i \in \{0,1\}$ for all i.

2) Compute $\lceil a \rceil$, $\lceil a^2 \rceil = \lceil a \rceil^2$, $\lceil a^4 \rceil = (\lceil a \rceil^2)^2$,

$\lceil a^8 \rceil = \lceil a^4 \rceil^2$, etc.

3) Now $\lceil a^d \rceil = \lceil a \rceil^d = \lceil a \rceil^{d_k 2^k} \cdot \lceil a \rceil^{d_{k-1} 2^{k-1}} \cdots \lceil a \rceil^{d_0}$.

Ex Compute $7^{305} \pmod{91}$.

Sol (1) Have

$305 = 256 + 32 + 16 + 1$

$= 2^8 + 2^5 + 2^4 + 1$

$305 - 256$

$305 - 256 - 32 - 16$

$305 - 256 - 32 - 16 - 1$

(2) $\lceil 7^2 \rceil = \lceil 49 \rceil$, $\lceil 7^4 \rceil =$