Recall a relation R on a set A is defined as a subset of $A \times A$: $R \subseteq A \times A$

An equivalence relation R is one that satisfies the 3 properties:

1) $\forall x \in A$, xRx ~~transitiv~~ reflexivity
2) $\forall x, y \in A$, $xRy \rightarrow yRx$ symmetry
3) $\forall x, y, z \in A$, $(xRy \wedge yRz) \rightarrow xRz$ transitivity

We looked at how to check / verify these properties

Ex: Let $A = \mathbb{R}$ and $R = \{(a,b) \in \mathbb{R} \times \mathbb{R} \mid \exists k \in \mathbb{Z} \text{ s.t. } a-b = 2k\pi\}$

1) Reflexivity: $a - a = 0 = 2 \cdot 0 \cdot \pi$ ✓ $0 \in \mathbb{Z}$

$\Rightarrow (a,a) \in R \Rightarrow R$ reflexive

2) Symmetry: suppose $(a,b) \in R$

$\Rightarrow \exists k \in \mathbb{Z}$ s.t. $a - b = 2k\pi$

$\Rightarrow b - a = -2k\pi = 2(-k)\pi$

$\Rightarrow -k \in \mathbb{Z}$

$\Rightarrow (b-a) \in R \Rightarrow R$ symmetric

3) if $(a,b) \in R$ and $(b,c) \in R$, $\exists k, n \in \mathbb{Z}$ s.t.

$a - b = 2k\pi$

$b - c = 2n\pi$

Adding

$\Rightarrow a - c = 2k\pi + 2n\pi = 2(k+n)\pi$

with $(k+n) \in \mathbb{Z} \Rightarrow (a,c) \in R$

$\Rightarrow R$ transitive

Ex $R = \{(x,y) \in \mathbb{Q} \times \mathbb{Q}$

Let R be the set of ordered pairs $(x,y) \in \mathbb{Q} \times \mathbb{Q}$ such that when x and y are represented by fractions in lowest terms, these fractions have the same denominator.

Proof

Let $x, y, z \in \mathbb{Q}$

$\Rightarrow \exists\ m, n, p, q, j, k$ s.t. $\gcd(m,n) = 1$

$\gcd(p,q) = 1$

$\gcd(j,k) = 1$

$x = \frac{m}{n} \quad y = \frac{p}{q} \quad z = \frac{j}{k}$

clearly

$\Rightarrow n = n$ so R is reflexive

Suppose $(x,y) \in R$, then $n = q \rightarrow q = n$ so $(y,x) \in R$

so R is symmetric

Suppose $(x,y) \in R$ and $(y,z) \in R$

$\Rightarrow n = q$ and $q = k$

$\Rightarrow n = k \Rightarrow (x,z) \in R$

and R is transitive.

We defined Congruence modulo n

$$a \equiv b \pmod{n} \iff n \text{ divides } a-b$$
$$\iff \exists k \in \mathbb{Z} \text{ s.t. } nk = a-b$$

And showed that congruence mod n defined an equivalence relation

We defined equivalence classes as the set of all elements related to an element a [the equivalence class of a]

$$[a]_R = \{ s \mid (a,s) \in R \}$$

if $b = [a]_R$ then b is called the representative of the equivalence class.

For congruence classes (the equivalence classes for congruence mod n) partition $\mathbb{Z}$. The set of all congruence classes is denoted $\mathbb{Z}_n$

<u>Fact</u> There are exactly n equivalence classes mod n

$$[0], [1], \ldots, [n-1]$$

The <u>set of least residues</u> (for fixed n) is defined by $\{0, 1, \ldots, n-1\}$. Every element in the set of least residues attached to one of the equivalence classes.

Closure of Relations

$\forall x \in R,$

$\forall x,y \in S,\ x \circ y \in S$

Reflexive Closure

Consider a relation

$R = \{(1,1), (2,2), (2,3)\}$ on set $A = \{1,2,3\}$

$\Rightarrow R$ not reflexive $(3 \in A$ but $3 \not R 3 \iff (3,3) \notin R)$

$\Rightarrow$ Smallest reflexive relation that contains R must include ordered pair $(3,3)$.

$\Rightarrow R_r^+ = \{(1,1), (2,2), (3,3), (2,3)\}$

Def The reflexive closure of binary relation R on a set A is the smallest reflexive relation on A that contains R.

$$R_r^+ = R \cup \{(a,a) \mid a \in A\}$$

Symmetric Closure of a binary relation on a set A that contains R is the smallest symmetric relation on set A that contains R

$$R_s^+ = R \cup \{(b,a) \mid (a,b) \in R\}$$

Ex: $R = \{(0,1), (1,1), (1,2), (2,0), (2,2), (3,0)\}$ $A = \{0,1,2,3$

$\Rightarrow (1,0), (0,2), (2,1), (0,3)$

$R_s^+ = R \cup \{(1,0), (2,1), (0,2), (0,3)\}$

__Transitive Closure__ of a binary relation R on a set A is the smallest transitive relation on A that contains R

$$R_t^+ = R \cup \{(a,c) \mid (a,b) \in R \text{ and } (b,c) \in R\}$$

__Ex__ $A = \{1,2,3\}$ $R = \{(1,1),(2,3),(3,1)\}$

$$R_t^+ = R \cup \{(2,1)\}$$

__Def__ A relation R on set A is a __partial ordering__ if

it is 1) reflexive $\forall x \in A,\ xRx$

2) antisymmetric $\forall x,y \in A,\ (xRy \text{ and } yRx) \to x=y$

3) transitive $\forall x,y,z \in A,\ (xRy \wedge yRz) \to xRz$

A set together with a partial ordering R is called a partially ordered set (or poset) and denoted $(A,R$

Ex: $\mathbb{Z}, \geq$

$\mathbb{Z}_{+}, \mid$

Solving

Linear Congruence

$ax \equiv b \pmod n$

How to solve?

1) a is invertible mod n iff $\gcd(a,n)=1$

$\Rightarrow ax + ny = 1 \iff ax \equiv 1 \bmod n$

x is a^{-1}

$\Rightarrow ax \equiv 1 \pmod n$

So might as well call x a^{-1}

2) $ca \equiv cb \pmod n \iff a \equiv b \bmod \frac{n}{\gcd(c,n)}$

i.e. we can cancel the c but we don't end in the same modular space

3) $ax \equiv b \pmod n$ has a solution iff $\gcd(a,n) \mid b$

4) if $\cancel{ax}$ $ax \equiv b \pmod n$ has a soln

i.e. $\gcd(a,n) \mid b$

then there are $\gcd(a,n)$ solutions

separated by $\frac{n}{\gcd(a,n)}$

Ex Solve $12x \equiv 16 \pmod{32}$

$ax \equiv b \pmod n$

1) IS the $\gcd(a,n) = 1$?

$\gcd(12,32) = 4 \neq 1$

$\Rightarrow$ Cannot just find multiplicative inverse $x = a^{-1}$

3) Does $\gcd(a,n) \mid b$?

$\gcd(12,32) = 4$ and $4 \mid 16$

$\Rightarrow$ There is a solution

4) $\Rightarrow$ There are $\gcd(a,n) = \gcd(12,32) = 4$ solutions

separated by $\frac{n}{\gcd(a,n)} = \frac{32}{4} = 8$

To solve, factor out a

$4(3x) \equiv 4 \cdot 4 \pmod{32}$

2) $3x \equiv 4 \bmod \frac{32}{\gcd(32,4)}$

$3x \equiv 4 \bmod \left(\frac{32}{4}\right) \Leftrightarrow 3x \equiv 4 \pmod 8$

$\Rightarrow$ 1) is $\gcd(a,n) = 1$?

$\gcd(3,8) = 1$

$\Rightarrow$ 3 has an inverse modulo 8

Can use extended Euclidean algorithm to find the inverse, but can also guess since 8 small

$3 \times 2 \not\equiv 1 \bmod 8 \quad 3 \times 2 \equiv 1 \bmod 8$

$3x \equiv 4 \pmod 8$

$3 \times 2 = 6$ which is not congruent to $1 \bmod 8$

$3 \times 3 = 9$ which is congruent to $1 \bmod 8$

$\Rightarrow \quad 3 \times (3x \equiv 4 \bmod 8)$

$$x \equiv 12 \bmod 8$$

$$\boxed{x \equiv 4 \bmod 8}$$

$$\left.\begin{aligned} x &\equiv 4 \bmod 32 \\ x &\equiv 12 \bmod 32 \\ x &\equiv 20 \bmod 32 \\ x &\equiv 28 \bmod 32 \end{aligned}\right\} \text{our four solutions}$$

~~Inverses mod n~~

~~Q: when can we find $a, b \in \mathbb{Z}$, $ab \equiv 1 \pmod n$?~~

~~Ex $n = 9$ $\quad 0, 1, 2, 3, 4, 5, 6, 7, 8$ these are remainders / residues modulo 9~~

~~1 has an inverse mod 9 since $1 \cdot 1 \equiv 1 \bmod 9$ $\Rightarrow$ 1 always has an inverse always~~

Inverses Mod n

When can we find $a, b \in \mathbb{Z}$, $ab \equiv 1 \pmod{n}$?

Ex $n = 9$, 0, 1, 2, 3, 4, 5, 6, 7, 8 are minimal residues modulo 9

1 has an inverse mod 9 b/c

$1 \cdot 1 \equiv 1 \pmod 9 \Rightarrow$ 1 will always have an inverse mod n for any n $\Rightarrow 1^{-1} = 1$

If we multiply 2 by any of the residues do we ever get 1?

$2 \times 3 = 6 \not\equiv 1 \bmod 9$

$2 \times 4 = 8 \not\equiv 1 \bmod 9$

$2 \times 5 = 10 \equiv 1 \bmod 9 \Rightarrow 2^{-1} \equiv 5 \bmod n \Rightarrow 5^{-1} \equiv 2 \bmod 9$

$3 \Rightarrow 3 \times 0$ no, 3×1 no, 3×2, 3×3, 3×4 not $\equiv 1 \bmod 9$

$\Rightarrow 3x \not\equiv 1 \bmod 9$ for all x

$\Rightarrow$ 0, 3 do not have inverses

$4 \Rightarrow 4 \times 4$ no, 4×5 no, ..., $4 \times 7 \equiv 1 \bmod 9 \Rightarrow 4^{-1} \equiv 7 \bmod 9$

$7^{-1} \equiv 4 \bmod 9$

$6 \Rightarrow 6x \not\equiv 1 \bmod 9$ for all x

$\cancel{0}, \underline{1}, \underline{2}, \cancel{3}, \underline{4}, \underline{5}, \cancel{6}, \underline{7},$

$8 \Rightarrow 8 \cdot 8 \equiv 1 \bmod 9 \Rightarrow 8^{-1} = 8$ $\Rightarrow$ All have inverses, all relatively prime to 9

Prop $a \in \mathbb{Z}$ is invertible (mod n) iff $\gcd(a,n)=1$

proof $\Rightarrow$ Suppose a invertible mod n

Forward Direction $\Rightarrow$ $\exists b \in \mathbb{Z}$ s.t $a \cdot b \equiv 1 \bmod n$

$\Rightarrow \quad n \mid (ab-1)$

$\Rightarrow \exists k$ s.t $nk = ab-1$

$\Rightarrow \quad ab - nk = 1$

but from before, we know that $ab-nk = l \times \gcd(a,n)$

all linear combinations of a and n are multiples of the gcd

$\Rightarrow ab-nk = l \cdot \gcd(a,n)$

$\Rightarrow \gcd(a,n) \mid 1$

$\Rightarrow \gcd(a,n) = 1$

Suppose $\gcd(a,n)=1$, $\exists x,y \in \mathbb{Z}$ s.t $ax+ny=1$

$ax = 1-ny$ which is the same as saying

$\Rightarrow \quad ax \equiv 1 \bmod n$

This number x that we get from the Extended Euclidean Algorithm

is the inverse of a modulo n

$x = a^{-1}$

... look at an example of finding modular inverses

<u>Ex</u> Find all inverse pairs (mod 20)

$\Rightarrow$ Everything relatively prime to 20

$\{1, 3, 7, 9, 11, 13, 17, 19\}$

$1^{-1} \equiv 1 \bmod 20$ (1 is always its own inverse)

$3 \times 7 = 21 \Rightarrow 3^{-1} \equiv 7 \bmod 20 \Leftrightarrow 7^{-1} \equiv 3 \bmod 20$

$9 \times 9 = 81 \Rightarrow 9^{-1} \equiv 9 \bmod 20$ (9 is its own inverse)

$11 \times 11 = 121 \Rightarrow 11^{-1} \equiv 11 \bmod 20$

$19 \equiv -1 \bmod 20 \Rightarrow 19 \times 19 \equiv (-1)^2 \equiv 1 \bmod 20$

$19^{-1} \equiv 19 \pmod{20}$

Trick: we can work with negative numbers, which simplify the arithmetic since they are smaller

$17 \equiv -3 \bmod 20 \Rightarrow$

$13 \equiv -7 \bmod 20 \Rightarrow$

$17 \times 13 \equiv (-3)(-7) \equiv 21 \equiv 1 \pmod{20}$

$\Rightarrow 13^{-1} \equiv 17 \bmod 20$

13, 17 are inverse pairs

with a small n, possible to guess and check inverses

$34^{-1} \bmod 143$

$\Rightarrow$ Use the fact that $\exists\, x,y$ s.t. $34x + 143y = \gcd(34,143)$

i.e. we haven't checked that 34 and 143 are relatively prime

but we will see this along the calculation!

$$143 = 4\times 34 + 7 \Rightarrow 7 = 143 - 4\times 34$$

$$34 = 4\times 7 + 6 \Rightarrow 6 = 34 - 4\times 7 = 34 - 4\times(143 - 4\times 34)$$

$$= 17\times 34 - 4\times 143$$

$$7 = 1\times 6 + 1 \Rightarrow 1 = 7 - 1\times 6$$

$$\Rightarrow (143 - 4\times 34) - (17\times 34 - 4\times 143)$$

$$6 = 6\cdot 1 + 0 \qquad \Rightarrow 1 = 5\times 143 - 21\times 34$$

$\gcd(143, 34) = 1$

which is a requirement for inverse to exist

$$34(-21) = 1 - 5(143)$$

$$34(-21) = 1 - 5(143) \equiv 1 \bmod 143$$

$$\Rightarrow 34^{-1} \equiv -21 \bmod 143$$

If we don't want to deal with negative numbers, can add a multiple of 143

$$34^{-1} \equiv 122 \bmod 143$$

Chinese Remainder Thm

Suppose $n_1, \ldots, n_k \in \mathbb{N}$ w/ $\gcd(n_i, n_j) = 1$

(Seq of natural numbers that are pairwise relatively prime)

and $b_1, \ldots, b_k \in \mathbb{Z}$.

Given that setup, we have a system of linear congruences

$$x \equiv b_1 \pmod{n_1}$$
$$\vdots$$
$$x \equiv b_k \pmod{n_k}$$

has a unique solution modulo $n_1 \cdots n_k = \prod_{i=1}^{k} n_i$

__Proof__ here is constructive, meaning we will first

Let $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k = \prod_{i=1}^{k} n_i$

$N_i = N / n_i$ (prod of all little n's except for n_i)

Claim: $\gcd(N_i, n_i) = 1$

Proof: Sps $d \mid n_i$ and $d \mid N_i$. Since all of the n_j relatively prime, d must divide one of the little n_j's not n_i

$$\Rightarrow d \mid n_j \text{ for } j \neq i$$

$$\Rightarrow d \mid \underbrace{\gcd(n_j, n_i)}_{=1} \Rightarrow d = 1$$

$\gcd(N_i, n_i) = 1 \Rightarrow N_i$ has an inverse modulo n_i called x_i

Let x_i be $N_i x_i \equiv 1 \bmod n_i$. Possible b/c $\gcd(N_i, n_i) = 1$

a) $x_i N_i \equiv 1 \pmod{n_i}$

b) $x_i N_i \equiv 0 \bmod n_j$ for $i \neq j$

b/c ~~$N_i \neq n_i$~~

N_i was defined as the product of all the n_j's except for n_i

$$N_i = \prod_{j \neq i} n_j$$

therefore N_i is a multiple of n_j

$\Rightarrow$ ~~N_i is congruent to N_j~~ $N_i \equiv 0 \bmod n_j$

Consider $x = x_1 N_1 b_1 + x_2 N_2 b_2 + \dots + x_k N_k b_k$

Modulo n_i

$\Rightarrow$

every term where the subscript is not equal to i will be 0 for b and 1 for a

$$x \equiv 0 + \dots 0 + x_i N_i b_i + 0 + \dots 0 \pmod{n_i}$$

but $x_i N_i \equiv 1 \bmod n_i$ from a $\Rightarrow$ $x \equiv b_i \pmod{n_i}$ $\quad 1 \leq i \leq k$

The $N_i b_i$ are inverse pairs modulo n_i.

That is existence, what about uniqueness?

Pf Sps x, y are sols $\Rightarrow x \equiv b_i \bmod n_i \quad y \equiv b_i \bmod n_i$

$\Rightarrow x - y \equiv 0 \pmod{n_i} \quad 1 \leq i \leq k$

$n_i \mid x - y \quad 1 \leq i \leq k \Rightarrow x - y = c \cdot n_i$

but n_i relatively prime

$\Rightarrow N \mid x - y \Rightarrow x \equiv y.$