Congruences

Definition: Let $m \in \mathbb{N}$ be fixed, $a, b \in \mathbb{Z}$. Then ~~a is congruent to~~ b modulo m if $m \mid (a-b)$.

Notation: $a \equiv b \pmod{m}$. Otherwise, $a \not\equiv b \pmod{m}$.

Alternatively: $a - b = km$ for some $k \in \mathbb{Z}$
$a = b + km$

Example: $m = 7$ $2 \equiv 9 \pmod 7$ $7 \mid (2-9)$
$1 \not\equiv 9 \pmod 7$ $7 \nmid (1-9)$
$59 \equiv 31 \pmod 7$ $7 \mid (59-31)$

For which m is $59 \equiv 31 \pmod m$
$m \mid 28 \Rightarrow m = 1, 2, 4, 7, 14, 28$

Definition: A relation $\sim$ is an equivalence relation if it is reflexive, symmetric, and transitive.

Proposition: $\equiv$ is an equivalence relation. Let $m \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$. Then
1. (reflexive) $a \equiv a \pmod m$
2. (symmetric) if $a \equiv b \pmod m$, then $b \equiv a \pmod m$
3. (transitive) if $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$

Proof:
1. $a - a = 0$ and $m \mid 0$. So $a \equiv a \pmod m$
2. Since $m \mid (a-b)$, $m \mid -(a-b)$, so $m \mid (b-a)$. So $b \equiv a \pmod m$
3. Since $a \equiv b \pmod m$, $m \mid (a-b)$
   Since $b \equiv c \pmod m$, $m \mid (b-c)$
   By div of int comb, $m \mid [(a-b)+(b-c)]$, so $m \mid (a-c)$.
   So $a \equiv c \pmod m$. □

If $\sim$ is an equivalence relation, the universe can be partitioned into "equivalence classes" where within a class, every pair of elements is related, and elements in different classes are not related.

For $\equiv \pmod 5$, the integers congruent to 0 are
$\ldots -10, -5, 0, 5, 10, 15, 20, \ldots$
Any 2 are congruent

$-5 \equiv 0 \pmod 5$
$0 \equiv 20 \pmod 5$
$\Big] \Rightarrow -5 \equiv 20 \pmod 5$

Define $[0] = \{5n \mid n \in \mathbb{Z}\}$
$[1] = \{5n+1 \mid n \in \mathbb{Z}\} = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$
$[2] = \{5n+2 \mid n \in \mathbb{Z}\}$
$[3] = \{5n+3 \mid n \in \mathbb{Z}\}$
$[4] = \{5n+4 \mid n \in \mathbb{Z}\}$

Example: Define $A \heartsuit B$ if A, B are in the same eng. class
This is an eq. rel.
Equivalence classes: eng depts.

Arithmetic

Proposition: Let $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then
① $a+b \equiv a'+b' \pmod{m}$
② $a-b \equiv a'-b' \pmod{m}$
③ $ab \equiv a'b' \pmod{m}$

Proof: Since $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, so $m \mid (a-a')$ and $m \mid (b-b')$
① By div. of int. comb., $m \mid [(a-a')+(b-b')]$, So $m \mid [(a+b)-(a'+b')]$
So $a+b \equiv a'+b' \pmod{m}$
② Same approach as ① but put in $-$ instead of $+$
③ There exists $k, \ell \in \mathbb{Z}$ such that $a-a' = km$ and $b-b' = \ell m$.
Then $ab = (a'+km)(b'+\ell m)$
$= a'b' + a'\ell m + b'km + k\ell m^2$
So $ab - a'b' = m(a'\ell + b'k + k\ell m)$, hence $m \mid (ab-a'b')$
So $ab \equiv a'b' \pmod{m}$

Division: Does $ac \equiv bc \pmod{m}$ $(c \neq 0) \Rightarrow a \equiv b \pmod{m}$? Not always

Proposition: Let $m \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$ then $a \equiv b \pmod{m}$

Proof: We have $m \mid (ac-bc)$, so $m \mid c(a-b)$. By CAD, since $\gcd(c, m) = 1$, $m \mid (a-b)$. So $a \equiv b \pmod{m}$.

Proposition: Let $m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$
Proof: In the assignment

Congruence and remainders

Proposition: Let $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{m}$ <u>if and only if</u> a, b have the same remainder when divided by m.

Proof: Using the division algorithm, there exists $k, \ell, r, s \in \mathbb{Z}$ such that $a = km + r$, $b = \ell m + s$ where $0 \leq r, s \leq m-1$
Then $a-b = m(k-\ell) + (r-s)$ where $-(m-1) \leq r-s \leq m-1$.

($\Leftarrow$) Assume $r=s$. Then $a-b=m(k-\ell)$, so $m \mid (a-b)$.
So $a \equiv b \pmod m$

($\Rightarrow$) Assume $a \equiv b \pmod m$. Suppose by way of contradiction $r \neq s$. Since $m \mid (a-b)$, by div of int. comb., $m \mid [(a-b)-m(k-\ell)]$
So $m \mid (r-s)$. Since $r-s \neq 0$, then using BBD, $m \leq |r-s|$.
But $|r-s| \leq m-1$, this is a contradiction. So $r=s$.

Examples: Find the remainder of 2^{31415} divided by 7.

$2^2 \equiv 4 \pmod 7$
$2^3 \equiv 8 \equiv 1 \pmod 7$
$(2^3)^k \equiv 1^k \pmod 7$

$31415 = 3 \cdot 10471 + 2$
$2^{31415} \equiv 2^{3 \cdot 10471 + 2} \equiv (2^3)^{10471} \cdot 2^2 \pmod 7$
$\equiv 1 \cdot 4 \equiv 4 \pmod 7$

So the remainder is 4.

Example: Find the remainder of 20^{31415} divided by 9.

$20 \equiv 2 \pmod 9$
So $20^{31415} \equiv 2^{31415} \pmod 9$
$2^2 \equiv 4 \pmod 9$
$2^3 \equiv 8 \equiv -1 \pmod 9$

$2^{31415} \equiv (2^3)^{10471} \cdot 2^2$
$\equiv (-1)^{10471} \cdot 4$
$\equiv -4 \pmod 9$
$\equiv 5 \pmod 9$

$\therefore$ remainder is 5.

Note: Every int is congruent to exactly one of $0, 1, 2, \ldots, m-1 \pmod m$

Modular arithmetic

Definition: The <u>congruence class modulo m</u> of an integer a is the set $[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod m\}$

The set of <u>integer modulo m</u> is

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$$

Example: $m=5$ $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$

$[0] = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 5\} = \{5n \mid n \in \mathbb{Z}\}$
$[1] = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 5\} = \{5n+1 \mid n \in \mathbb{Z}\}$
$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$

Definition of operations: For $a, b \in \mathbb{Z}$, define

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

$$[a] \cdot [b] = [ab]$$

Example: $m=5$ $[2]+[3]=[5]=[0]$ $a\equiv 2 \pmod 5$

$=\{a+b \mid a\in[2], b\in[3]\}$ $b\equiv 3 \pmod 5$

$=a+b=2+3=0 \pmod 5$

$=[0]$

Proposition: $[a]=[b]$ if and only if $a\equiv b \pmod m$ in $\mathbb{Z}_n$

Proof Exercise:

Additive identity: $[0]=\mathbb{Z}_n$ $[a]+[0]=[a]$

Additive inverse: inverse of $[3]$ is $[2]$ since $[3]+[2]+[0]$ (add identity

Multiplicative identity: $[1]$ in $\mathbb{Z}_m$. Since $[a]\cdot[1]=[a]$

Multiplicative inverse: $[a]^{-1}$ is the element in $\mathbb{Z}_m$ such that

$[a]\cdot[a]^{-1}=[1]$

Example: $\mathbb{Z}_5$ $[1]^{-1}=[1]$ $[3]^{-1}=[2]$ $\mathbb{Z}_6$ $[5]^{-1}=[5]$

$[2]^{-1}=[3]$ $[4]^{-1}=[4]$ $[3]^{-1}=\times$ dne

$[0]^{-1}=???$ DNE