The integers modulo N

Definition: Fix an integer $N > 0$. We say that two integers a and b are *congruent* modulo N, written

$$\boxed{a \equiv b \pmod{N}}$$

if $a - b$ is a multiple of N.

$N=2$ $\quad a \equiv b \bmod 2$ means $a-b$ is even.

$\Longleftrightarrow$ a,b both even or a,b are both odd.

$a \equiv b \bmod 2 \Longleftrightarrow a$ and b have same parity.

$N=5$

$7 \equiv 2 \bmod 5$ because $7-2$ is divisible by 5

$m = 2+5k$, where $k \in \mathbb{Z}$, then $m \equiv 2 \bmod 5$.

$\{x \mid x \equiv 2 \bmod 5\} = \{-3, -8, -13, \ldots 2, 7, 12, 17, \ldots\}$

Proposition: Congruence is an equivalence relation.

Equiv Relation: symmetric, reflexive and transitive

Reflexive: $a \equiv a \bmod N$ for all $a \in \mathbb{Z}$ because $a - a = 0$ and $N \mid 0$.

Symmetric: $a \equiv b \bmod N$ means $a - b = kN$ for some $k \in \mathbb{Z}$, then $b - a = (-k)N$ so $b \equiv a \bmod N$.

Transitive: if $a \equiv b \bmod N$ and $b \equiv c \bmod N$ then

$a - b = kN$ and $b - c = tN$ for $k, t \in \mathbb{Z}$.

$a - b + b - c = a - c = kN + tN = (k+t)N$

so $a \equiv c \bmod N$.

Congruence classes

Fix an integer N. We know from the division algorithm that every integer a can be divided by N to yield a unique quotient q and remainder r that satisfy

$$a = qN + r$$

where $0 \leq r < N$.

$N=2$

$N=5$

$11 = 2\cdot 5 + 1$

$27 = 5\cdot 5 + 2$

$33 = 6\cdot 5 + 3$

$-11 = -2\cdot 5 + (-1)$

$7 = 3\cdot 2 + 1$

$8 = 4\cdot 2 + 0$

$-11 = -3\cdot 5 + 4$

Since $a - r = qN$, we know that

$$a \equiv r \pmod{N}.$$

$a = qN + r \implies a - r = qN$

so $a \equiv r \mod N$

Every $a \in \mathbb{Z}$ is congruent to a unique integer r between 0 and $N-1$ inclusive.

Congruence classes continued

Therefore every integer a is congruent to *exactly one* integer r that satisfies $0 \leq r < N$.

Equivalence relation R on a set X always partitions X into disjoint subsets

Each subset is of the form

$$[x] = \{ yRx \mid y \in X \}$$

$[x] = [z]$ if and only if xRz

otherwise $[x] \cap [z] = \emptyset$.

The congruence relation partitions the integers into N equivalence classes. We let

$$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{N}\}$$

Fix $N = 5$.

$[0], [1], [2], [3], [4]$

every integer belongs to exactly one of these.

$13 \in [3]$ $\qquad -11 = [4]$

Congruence Arithmetic

We can do arithmetic on congruence classes.

Definition: Fix $N > 0$. We define the sum of congruence classes $[a]$ and $[b]$ by

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

This is *well-defined.*

$N = 2$

$[0]$ $\uparrow$ even

$[1]$ $\uparrow$ odd

even + odd = odd

$[0] + [1] = [1]$

$[0] = [14]$

$[1] = [11]$

$[0] + [1] = [14] + [11] = [25] = [1]$

$N = 5$

$[2] + [1] = [3]$

any number $\equiv 2 \bmod 5$ + any number $\equiv 1 \bmod 5$ = some number $\equiv 3 \bmod 5$

$[2] + [4] = [6] = [1]$

Some special cases

A look at $N = 2$, $N = 3$, and $N = 4$.

$N=2$

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

$\mathbb{Z}/2\mathbb{Z}$

$N=3$

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\mathbb{Z}/3\mathbb{Z}$

$[2]+[2] = [4] = [1]$

$4 \equiv 1 \ (3)$

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

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

$N=5$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\mathbb{Z}/5\mathbb{Z}$

$\underline{[6]} = \underline{[1]}$ in $\mathbb{Z}/5$

$\quad\quad\quad\; \shortparallel$

$\quad\quad\; [-4]$