The integers modulo N

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

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

if a - b is a multiple of N.

Transitive: if
$$A = b \mod N$$
 and $b = C \mod 30$ i.e.
 $a - b = KN$ and $b - c = tN$ (n K, $t \in \mathbb{Z}$.
 $a - b = KN$ and $b - c = tN$ (n K, $t \in \mathbb{Z}$.
 $a - b + b - c = a - c = KN + tN = (k + 1)N$
 $a = c \mod N$.
1

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

	$\underline{a} = qN + r$
where $0 \leq r < N$.	N = 2
N=S	$7 = 3 \cdot 2 + 1$
= 2.5 + 1	g = 4.2 + 0
27 = 5.5 + 2	Ŭ
33= 6.5+3	05+4
$-11 = -2 \cdot 5 + (-1)$	-11 = -3.5 + 4

Since a - r = qN, we know that

$$a \equiv r \pmod{N}$$
.
 $a \equiv r \pmod{N}$.
 $a = q N + r \implies a - r = q N$
so $a \equiv r \mod N$
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 $0 \le r < N$.

Equivalence relation Ron a set X always
partitions X into disjoint subsets
Each subset is of the from
$$[x] = [z]$$
 if and only if xRZ
otherwise $[x] \cap [z] = 0$.

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.

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

every integer belongs to exactly one of them.

$$[3 \in [3] - 1[= [4]]$$

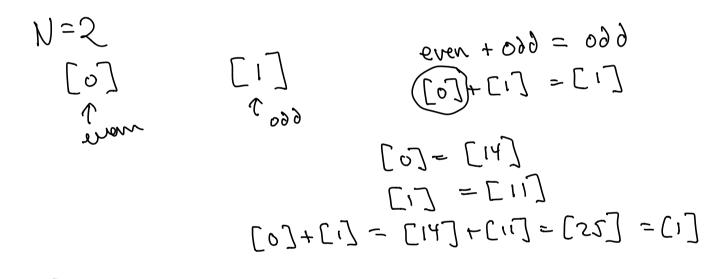
Congruence Arithmetic

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.



$$N=5$$

 $[2] + [1] = [3]$
any number any number some number
 $= 2 \mod 5 + (4) = [6] = [1]$
 $[2] + [4] = [6] = [1]$

Some special cases

A look at
$$N = 2, N = 3$$
, and $N = 4$.
 $N=2$
 $+ \begin{bmatrix} co 3 & Ci 3 \\ \hline co 4 \\ \hline c$