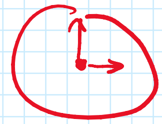
CS 173 Lecture 4: Congruence modulo k

Def: For positive integer k, two integers a & b are congruent modulo k ($a \equiv b \pmod{k}$) if $k \mid (a-b)$.

$15 \equiv 3 \mod 12$



3:00

$-3 \equiv 2 \mod 5$

$2 \equiv -8 \mod 5$

Theorem: For fixed integer $k>0$, for all integers a,b,c,d: if $a \equiv b \mod k$ & $c \equiv d \mod k$, then:

(i) $a+c \equiv b+d \mod k$

(ii) $ac \equiv bd \mod k$.

Scratchwork:
if $\underline{k \mid (a-b)}$ & $k \mid (c-d)$

goal: $k \mid (ac-bd)$ i.e. show $\exists \ell \in \mathbb{Z}$ s.t. $\underline{(ac-bd) = k\ell}$.

Proof: (i) exercise / book

(ii) Fix an integer $k>0$, and let a,b,c,d be integers such that $a \equiv b \mod k$ & $c \equiv d \mod k$.
By definition, $k \mid (a-b)$ & $k \mid (c-d)$, i.e. there exist integers m,n such that $a-b = km$ and $c-d = kn$.
This means $a = b+km$ and $c = d+kn$,
so
$$ac = (b+km)(d+kn)$$
$$= bd + bkn + dkm + k^2mn$$
$$= bd + k(bn+dm+kmn).$$
i.e., $ac - bd = k\ell$, where $\ell = bn+dm+kmn$ is an integer.

i.e., $ac - bd = kl$, where $l = bn + dm + kmn$ is an integer.

So $k \mid ac - bd$, which means that

$$ac \equiv bd \mod k. \qquad \square$$

Define arithmetic operations on <u>equivalence classes</u>.

Definition: Fix integer $k > 0$. The equivalence class $[x]$ is the set of all integers y such that

$$x \equiv y \mod k.$$

If $k = 5$, $[2] = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$

$$= [-3] = [7] = \ldots$$

Define

$$[x] + [y] = [x + y]$$

$$[x] \cdot [y] = [xy]$$

x is a representative of $[x]$

Why does this make sense?

Well suppose that $[a] = [x]$, $[b] = [y]$

$a \equiv x \mod k$, $b \equiv y \mod k$,

so $a + b \equiv x + y \mod k$

i.e. $[a+b] = [x+y]$

similar for product: $ab \equiv xy \mod k$,

so $[ab] = [xy]$.

$\{[0], [1], \ldots, [k-1]\}$ w/ $+, \cdot$ is called "integers mod k", $\mathbb{Z}_k$

Fix $k = 5$, $[2][3] = [2 \cdot 3] = [6] = [1]$

$[2][4] = [2 \cdot 4] = [8] = [3]$.

$$[a]^p = \underbrace{[a] \cdot [a] \cdot [a] \cdots [a]}_{p \text{ of these}}$$

$$\underbrace{}_{p \text{ of these}}$$

$$= [a^p]$$

$$[a]^{p+q} = [a^p][a^q]$$

$[2]^{65}$.

$$[2]^2 = [2\cdot 2] = [4].$$

$$[2]^4 = ([2]^2)^2 = [4]^2 = [4^2] = [16] = \underline{[1]}$$

$$[2]^8 = ([2]^4)^2 = [1]^2 = [1]$$

$$[2]^{16} = [1]$$

$$[2]^{32} = [1]$$

$$[2]^{64} = [1]$$

$$\begin{aligned} [2]^{65} &= [2]^{64}[2] \\ &= [1][2] \\ &= [2]. \end{aligned}$$