CS 173 - Lecture 5

Modular Arithmetic

ex. prove for integers a, b, c, d, k with $k>0$, if $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$, then $ac \equiv bd \pmod{k}$

proof: Let $a, b, c, d, k \in \mathbb{Z}$ s.t $k>0$. Suppose $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$. By definition of congruence, we know $k \mid (a-b)$ and $k \mid (c-d)$. If $k \mid (a-b)$, $k \mid c(a-b) = k \mid (ac-bc)$ because $c \in \mathbb{Z}$. Also, if $k \mid (c-d)$, then $k \mid b(c-d) = k \mid (bc-bd)$ because $b \in \mathbb{Z}$. Then we know $k \mid \big((ac-bc)+(bc-bd)\big) = k \mid (ac-bd)$ $\therefore ac \equiv bd \pmod{k}$

QED

Equivalence/Congruence Classes

ex. $5 \equiv 17 \pmod{12}$ $17 \equiv 5 \pmod{12}$ $29 \equiv 5 \pmod{12}$ $41 \equiv 5 \pmod{12}$ ...

In $\mathbb{Z}_{12}$ means we have 12 different congruent classes

$[0]$ = all integers congruent to $0 \pmod{12}$

congruent class

$= \{0, 12, 24, \ldots\}$

$[1]$ = all integers congruent to $1 \pmod{12}$

$= \{1, 13, -11, \ldots\}$

⋮

$[11]$ = all integers congruent to $11 \pmod{12}$

$= \{11, 23, -1, \ldots\}$

all 12 congruent classes cover every possible integer

each integer falls under exactly one congruence/equivalence class

ex. Compute $\underset{36+5}{41} \times \underset{24+10}{34}$ in $\mathbb{Z}_{12}$

$[5] \cdot [10] = [50]$

$= [2]$

Rules: $[x] \cdot [y] = [x \cdot y]$

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

ex. In $\mathbb{Z}_{11}$, find value of $[8]^{21}$

$[8]^2 = [8] \cdot [8] = [64] = [9]$

$[8]^4 = ([8]^2)^2 = ([9])^2 = [81] = [4]$

$[8]^8 = ([8]^4)^2 = ([4])^2 = [16] = [5]$

$[8]^{16} = ([8]^8)^2 = [5]^2 = [25] = [3]$

$[8]^{21} = [8]^{16} \cdot [8]^4 \cdot [8] = [3] \cdot [4] \cdot [8] = [96] = [8]$

ex. Prove or disprove that $\forall k \in \mathbb{Z}^+$, $(k-1)^2 \equiv 1 \pmod{k}$

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

$(k-1) \equiv -1 \pmod{k}$

what conditions satisfy this?

then $(k-1)(k-1) \equiv (-1)^2 \pmod{k}$

$\equiv 1 \pmod{k}$

$k \in \mathbb{Z}^+$
$\downarrow$
$k \equiv 0 \pmod{k}$

$[x]+[y] \equiv [x+y]$ $\quad$ $[k]+[-1] \equiv [k-1]$

$[0]+[-1] \equiv [k-1]$ $\quad$ $[-1] \equiv [k-1]$

lets us do:

$k \equiv 0 \pmod{k} \rightarrow (k-1) \equiv -1 \pmod{k}$

Proof: Let $k \in \mathbb{Z}^+$. Due to the definition of congruence, $k \equiv 0 \pmod{k}$, and due to modular arithmetic, $k-1 \equiv -1 \pmod{k}$ and also $(k-1)^2 \equiv (-1)^2 \pmod{k}$ which is the same as $(k-1)^2 \equiv 1 \pmod{k}$ QED

Discussion Problems 2.1abcd

2.1 Modular arithmetic

When doing computations in modular arithmetic, organize your work so that intermediate results are kept small. If you're working in base k, your final result should be in the form $[n]$ where $0 \leq n < k$.

(a) In $\mathbb{Z}_{15}$, what are some values in the congruence class of [14].

(b) In $\mathbb{Z}_{15}$, find the value of $[7] + [14] * [3]$.

(c) Find the first six powers of [5] in $\mathbb{Z}_7$. That is compute $[5]^1$, $[5]^2$, and so on up to $[5]^6$.

(d) Calculate the value of $[9]^{12}$ in $\mathbb{Z}_{11}$. (Hint: try repeated squaring.)

a) basically saying $14 \equiv n \pmod{15}$

$n = \{14, 29, -1, 44, -16, \ldots\}$

b) $[7] + [14] \cdot [3] = [7] + [42] = [7] + [12] = [19] = [4]$

c) $[5]^1 = [5]$

$[5]^2 = [25] = [4]$

$[5]^3 = [5]^2 \cdot [5] = [4] \cdot [5] = [20] = [6]$

$[5]^4 = ([5]^2)^2 = [4]^2 = [16] = [2]$

$[5]^5 = [5]^4 \cdot [5] = [2] \cdot [5] = [10] = [3]$

$[5]^6 = [5]^5 \cdot [5] = [3] \cdot [5] = [15] = [1]$

d) $[9]^{12}$ in $\mathbb{Z}_{11}$

$[9]^2 = [81] = [4]$

$[9]^4 = ([9]^2)^2 = [4]^2 = [16] = [7]$

$[9]^8 = ([9]^4)^2 = [7]^2 = [49] = [5]$

$[9]^{12} = [9]^8 \cdot [9]^4 = [5] \cdot [7] = [35] = [2]$