Lecture 28

Handout or Document Camera or Class Exercise

Which of the following satisfies $x \equiv 40 \pmod{17}$?

(Do not use a calculator.)

A) $x = 173$

B) $x = 15^5 + 19^3 - 4$

C) $x = 5 \cdot 18^{100}$

D) $x = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$

E) $x = 17^0 + 17^1 + 17^2 + 17^3 + 17^4 + 17^5 + 17^6$

Solution:

A) $x = 173 \equiv 3 \pmod{17}$

B) $x = 15^5 + 19^3 - 4 \equiv (-2)^5 + 2^3 - 4 \equiv -32 + 8 - 4 \equiv 2 + 4 \equiv 6 \pmod{17}$

C) $x = 5 \cdot 18^{100} \equiv 5(1)^{100} \equiv 5 \pmod{17}$

D) $x = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \equiv 6 \cdot 35 \cdot (-6)(-4) \equiv 6 \cdot 1 \cdot 24 \equiv 6 \cdot 7 \equiv 42 \equiv 8 \pmod{17}$

E) $x = 17^0 + 17^1 + 17^2 + 17^3 + 17^4 + 17^5 + 17^6 \equiv 1 \pmod{17}$

Answer is the second option since $x \equiv 40 \equiv 6 \pmod{17}$.

Instructor's Comments: This is the 5-10 minute mark

Instructor's Comments: Try to make the next exercise only take you to the 10 minute mark.

Example: Show that there are no integer solutions to $x^2 + 4y = 2$.

Proof: Assume towards a contradiction that there exist integers x and y such that $x^2 + 4y = 2$. Reducing modulo 4 yields $x^2 \equiv 2 \pmod 4$. Trying all the possibilities yields

$$(0)^2 \equiv 0 \pmod 4$$
$$(1)^2 \equiv 1 \pmod 4$$
$$(2)^2 \equiv 0 \pmod 4$$
$$(3)^2 \equiv 1 \pmod 4$$

Hence there are no integer solutions. ■

Note: Notice that sometimes, you end up with many solutions. For example, $x^2 \equiv 1 \pmod 8$ has 4 solutions (all the odd numbers work! This is an exercise to check)

Instructor's Comments: Now comes what I think is the hardest to grasp concept in this course; the abstraction of Z/mZ. I personally am going to discuss rings here and take a bit more time here to save a bit of time later on in the course. I will introduce the notion of a ring and field here so that when we get to complex numbers, it will go a bit quicker. This will cause me to spend more time here on topics but I think that's okay.

$\mathbb{Z}_m$ or $\mathbb{Z}/m\mathbb{Z}$ The integers modulo m

Definition: The congruence or equivalence class modulo m of an integer a is the set of integers

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

Note: := means "defined as".

Further, define

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} := \{[0], [1], ..., [m-1]\}$$

Definition: A commutative ring is a set R along with two closed operations $+$ and $\cdot$ such that for $a, b, c \in R$ and

(i) Associative $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

(ii) Commutative $a + b = b + a$ and $ab = ba$.

(iii) Identities: there are [distinct] elements $0, 1 \in R$ such that $a + 0 = a$ and $a \cdot 1 = a$.

(iv) Additive inverses: There exists an element $-a$ such that $a + (-a) = 0$.

(v) Distributive Property $a(b + c) = ab + ac$.

Example: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Not $\mathbb{N}$

Definition: If in addition, every nonzero element has a multiplicative inverse, that is an element a^{-1} such that $a \cdot a^{-1} = 1$, we say that R is a field.

Example: $\mathbb{Q}$, $\mathbb{R}$. Not $\mathbb{N}$ or $\mathbb{Z}$.

Instructor's Comments: This should take you tot he 25-30 minute mark

Definition: We make $\mathbb{Z}_m$ a ring by defining addition and subtraction and multiplication by $[a] \pm [b] := [a \pm b]$ and $[a] \cdot [b] := [ab]$. This makes $[0]$ the additive identity and $[1]$ the multiplicative identity.

Instructor's Comments: Note that the $[a+b]$ means add then reduce modulo m. There is something subtle going on here that might be lost on students.

There is one issue we need to resolve here; the issue of being well defined. How do we know that the above definition does not depend on the representatives chosen for $[a]$ and $[b]$?

Example: For example, in $\mathbb{Z}_6$, is it true that $[2][5] = [14][-13]$?

Instructor's Comments: Note that $[2] = [14]$ and $[5] = [-13]$. To properly prove well-definedness, you would have to do this for all possible representations of $[a]$. Since this will create a notational disaster, I think it's best to try to illustrate the point with a concrete example.

Proof: Note that in $\mathbb{Z}_6$, we have

$$\text{LHS} = [2][5] = [2 \cdot 5] = [10] = [4]$$

and also

$$\text{RHS} = [14][-13] = [14(-13)] = [-182] = [-2] = [4]$$

completing the proof. ∎

Definition: The members $[0], [1], ..., [m-1]$ are sometimes called representative members.

Instructor's Comments: Minimum this is the 35 minute mark.

Instructor's Comments: In practice, this was the 50 minute mark but either way that's okay - hopefully you can squeeze in the addition table.

Addition table for $\mathbb{Z}_4$

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]