PROJECTED WRITTEN NOTES FROM THE M325K LECTURE ON THURSDAY, MARCH 28, 2024, on Sec 8.4 (Epp's 4th Edition) - MODULAR ARITHMETIC: THEOREMS 8.4.1 and 8.4.3, and the Handout, "ALTERNATE VERSIONS OF EXAMPLES..." CLASS #20

Sec 8.5 #32:

It is given that R is an equivalence relation on set A.

To Prove: For all $a, b \in A$,
if bRc and $c \in [a]$, then $b \in [a]$.

Proof: Let $a, b, c \in A$ be given.
Suppose bRc and $c \in [a]$. [NTS: $b \in [a]$].

[Procedural Defn of $[a]$: "$x \in [a] \Leftrightarrow xRa$."]

Since $c \in [a]$, cRa, by defn of $[a]$.

Since bRc and cRa,
bRa, by Transitivity of R.
$\therefore b \in [a]$, by defn of $[a]$.

$\therefore$ For all $a, b, c \in A$, if bRc and $c \in [a]$,
then $b \in [a]$, by Direct Proof.
QED.

Recall the "Congruence (mod n)" relation for a given positive integer n:

For any two integers a and b,

$$a \equiv b \pmod{n} \iff n \mid (a-b)$$

Theorem 8.4.2: For any fixed positive integer n, the relation "Congruence (mod n)" is an equivalence relation.

(You proved this for $n=5$ in HW #9. The general proof is the same.)

The distinct equivalence classes for "Congruence (mod n)" are $[0], [1], \ldots, [n-1]$ (n congruence classes)

THEOREMS 8.4.1 AND 8.4.3 SUMMARY

Thm 8.4.1: a, b, n, k are integers with $k \geq 1$ and $n \geq 1$

The following are EQUIVALENT

(1) $n \mid (a-b)$

(2) $a \equiv b \pmod{n}$

(3) $a = b + nk$ for some integer k

(4) a and b have the same QR Theorem remainder when divided by n

(5) $(a \bmod n) = (b \bmod n)$

THEOREM 8.4.1

Thm 8.4.3: Given that $a \equiv A \pmod{n}$ and $b \equiv B \pmod{n}$ and k is a positive integer,

Then (1) $(a+b) \equiv (A+B) \pmod{n}$

(2) $(a-b) \equiv (A-B) \pmod{n}$

(3) $ab \equiv AB \pmod{n}$

(4) $a^k \equiv A^k \pmod{n}$

Theorem 8.4.1:

This Theorem gives different ways to prove that two integers are congruent to each other (mod n) for a given positive integer n.

Recall $23 \equiv 8 \pmod 5$

because $23 - 8 = 15 = 5 \times 3$

so $5 \mid (23-8)$

$23 - 8 = 5 \times 3$ (Add 8 to both sides)

$23 = 8 + 5 \times 3$

$\therefore 23 \equiv 8 \pmod 5$ by Thm 8.4.1

$$5\overline{)23} \quad 4 \quad 20 \quad 3$$

$$5\overline{)8} \quad 1 \quad 5 \quad 3$$

$(23 \bmod 5) = 3$

$(8 \bmod 5) = 3$

$(23 \bmod 5) = (8 \bmod 5)$

$\therefore 23 \equiv 8 \pmod 5$ by Thm 8.4.1

THEOREMS 8.4.1 AND 8.4.3 SUMMARY

Thm 8.4.1: a, b, n, k are integers with $k \geq 1$ and $n \geq 1$

The following are EQUIVALENT

(1) $n \mid (a-b)$

(2) $a \equiv b \pmod{n}$

(3) $a = b + nk$ for some integer k

(4) a and b have the same QR Theorem remainder when divided by n

(5) $(a \bmod n) = (b \bmod n)$

Thm 8.4.3: Given that $a \equiv A \pmod{n}$ and $b \equiv B \pmod{n}$ and k is a positive integer,

Then (1) $(a+b) \equiv (A+B) \pmod{n}$

(2) $(a-b) \equiv (A-B) \pmod{n}$

(3) $ab \equiv AB \pmod{n}$

(4) $a^k \equiv A^k \pmod{n}$

THEOREM 8.4.3

Thm 8.4.3 in Action (Let $n = 23$)

Let $a = 751$ and $A = 15$

$751 = 15 + 23 \cdot 36$

$\therefore 751 \equiv 15 \pmod{23}$ by Thm 8.4.1

Let $b = 60$ and $B = 14$

$60 = 14 + 23 \times 2$

$\therefore 60 \equiv 14 \pmod{23}$ by Thm 8.4.1

$751 \times 60 = 45,060$ // $15 \times 14 = 210$

$a \times b$ $A \times B$

Is $ab \equiv AB \pmod{23}$?

$45,060 - 210 = (23)(1,950)$

$\therefore 23 \mid (ab - AB)$ s.

$(751)(60) \equiv (15)(14) \pmod{23}$

by 8.4.3.

Focusing on the Handout

"Alternate Versions..."

Always write "K mod n" in Parentheses as "(K mod n)"

So $(2,146 \bmod 17) = 4$.

$(K \bmod n) = 4$ when $K = 3,146$ and $n = 17$.

Alternate Terminology:

$(K \bmod n)$ is "The least (mod n) Residue of K"

$(2,146 \bmod 17)$ is "The least (mod 17) Residue of 2,146"

Alternate Versions of Example 8.4.4 and Example 8.4.5 for use in finding the solution
to Problems 14 and 15 of Section 8.4 of Epp's Fourth Edition

CONVENTION: In this class, always use PARENTHESES for the "mod" function, and so, write " (2,146 mod 17) = 4 " and NOT " 2,146 mod 17 = 4 ".

The DEFINITION of the "MOD" FUNCTION:

Let m and n be integers such that $n > 1$. The integer **(m mod n)** is defined as follows:

(m mod n) = the integer **r** if and only if, for some integer **k** ,

(1) $\mathbf{m = nk + r}$ and (2) $\mathbf{0 \leq r < n}$.

In this handout, we will use the following result from Theorem 8.4.1:

Variables **a** , **b** , and **n** are integers with $\mathbf{n > 1}$. Then, by Theorem 8.4.1,

$\mathbf{a \equiv b \pmod n}$ if and only if, for some integer **k** , $\mathbf{a = nk + b}$.

Here is a SHORTCUT CALCULATOR PROCEDURE for quickly finding (M mod n)
(Illustrated here using M = 20,736 and n = 713 .) :

To compute (20,736 mod 713) on your calculator,

1) Divide M = 20,736 by n = 713 : $20{,}736 \div 713 = 29.08274895$.

Write down (or make note of) the **integer part** 29 .

2) Subtract the whole integer part of the result (here, subtract 29 leaving 0.08274895).

3) Multiply that result by the modulus n (here, multiply by 713)

The result (perhaps after rounding to the nearest integer) is $(0.08274895)(713) = 59.00000135$,
which rounds to 59 . This means that $20{,}736 = (713)(29) + 59$.

We show that (20,736 mod 713) = 59 .

Now, $20{,}736 = (713)(29) + 59$ and $0 \leq 59 < 713$.

Therefore, (20,736 mod 713) = 59 by definition of the "mod" function.

We use the following results from Theorem 8.4.3:

Variables a , b , A , B and n represent integers , with $n > 1$.

Suppose that $a \equiv A \pmod n$ and $b \equiv B \pmod n$.

Then,

$ab \equiv AB \pmod n$; $a + b \equiv A + B \pmod n$; $a - b \equiv A - B \pmod n$;

And, for any positive exponent k , $a^k \equiv A^k \pmod n$.

We will also use the following result from Theorem 8.4.1:

Variables a , b and n represent integers , with $n > 1$. Then, by Theorem 8.4.1,

$a \equiv b \pmod n$ if and only if $(a \bmod n) = (b \bmod n)$

Example 8.4.4: Find the least (mod 713) residue of 144^4 ;

i.e., determine the integer $(144^4 \bmod 713)$.

Solution:

$(144)^2 = 713 \times 29 + 59$. (Check it out: $(144)^2 = 20{,}736 = 713 \times 29 + 59$.)

$\therefore 144^2 \equiv 59 \pmod{713}$, by Theorem 8.4.1 .

$\therefore 144^4 = (144^2)^2 \equiv (59)^2 \pmod{713}$, by Theorem 8.4.3 .

Since $(59)^2 = 713 \times 4 + 629$, $(59)^2 \equiv 629 \pmod{713}$ by Theorem 8.4.1.

$\therefore 144^4 \equiv 629 \pmod{713}$, by transitivity.

$\therefore (144^4 \bmod 713) = (629 \bmod 713)$ by Theorem 8.4.1.

Now, $629 = 713 \times 0 + 629$ and $0 \leq 629 < 713$.

$\therefore (629 \bmod 713) = 629$, by definition of the "mod" function.

$\therefore (144^4 \bmod 713) = 629$, by transitivity.

Example 8.4.5: Determine $(12^{43} \bmod 713)$.

Solution: The exponent 43 can be written as a sum of powers of 2. In fact, $43 = 32 + 8 + 2 + 1$.

$\therefore \quad 12^{43} = 12^{(32+8+2+1)} = (12^{32})(12^{8})(12^{2})(12^{1})$, by rules of algebra.

In the first part of the solution, the goal is this:

For each number of the form 12^{M}, where M is a power of 2, we find the integer K so that

$$12^{M} \equiv K \pmod{713} \quad \text{and} \quad 0 \leq K < 713.$$

Note that $12^{1} = 12$ and that $0 \leq 12 < 713$.

$\therefore$ **$12^{1} \equiv 12 \pmod{713}$**, by the reflexive property of "Congruence (mod 713)".

Now, $12^{2} = 144$ and note that $0 \leq 144 < 713$.

$\therefore$ **$12^{2} \equiv 144 \pmod{713}$**, by the reflexive property of "Congruence (mod 713)".

$\therefore \quad 12^{4} = (12^{2})^{2} \equiv 144^{2} \pmod{713}$, by Theorem 8.4.3.

Since $144^{2} = 713 \times 29 + 59$, $144^{2} \equiv 59 \pmod{713}$, by Theorem 8.4.1.

$\therefore$ **$12^{4} \equiv 59 \pmod{713}$**, by transitivity.

LEARN THIS !

$\therefore \quad 12^{8} = (12^{4})^{2} \equiv 59^{2} \pmod{713}$, by Theorem 8.4.3.

Since $59^{2} = 713 \times 4 + 629$, $59^{2} \equiv 629 \pmod{713}$, by Theorem 8.4.1.

$\therefore$ **$12^{8} \equiv 629 \pmod{713}$**, by transitivity.

$\therefore \quad 12^{16} = (12^{8})^{2} \equiv 629^{2} \pmod{713}$, by Theorem 8.4.3.

Since $629^{2} = 713 \times 554 + 639$, $629^{2} \equiv 639 \pmod{713}$, by Theorem 8.4.1.

$\therefore$ **$12^{16} \equiv 639 \pmod{713}$**, by transitivity.

$\therefore \quad 12^{32} = (12^{16})^{2} \equiv 639^{2} \pmod{713}$, by Theorem 8.4.3.

Since $639^{2} = 713 \times 572 + 485$, $639^{2} \equiv 485 \pmod{713}$, by Theorem 8.4.1.

$\therefore$ **$12^{32} \equiv 485 \pmod{713}$**, by transitivity.

10

Summarizing the results from this page and from the previous page:

$$12^{43} = (12^{32})(12^{8})(12^{2})(12^{1}) \quad \text{and}$$

$12^{1} \equiv 12 \pmod{713}$, $12^{2} \equiv 144 \pmod{713}$, $12^{8} \equiv 629 \pmod{713}$, and $12^{32} \equiv 485 \pmod{713}$.

$\therefore 12^{43} = (12^{32})(12^{8})(12^{2})(12^{1}) \equiv ((485)(629)(144)(12)) \pmod{713}$ by Theorem 8.4.3.

Since $(485)(629) = 713 \times 427 + 614$, $(485)(629) \equiv 614 \pmod{713}$, by Theorem 8.4.1.

Since $(144)(12) = 713 \times 2 + 302$, $(144)(12) \equiv 302 \pmod{713}$, by Theorem 8.4.1.

$\therefore ((485)(629)(144)(12)) \equiv (614)(302) \pmod{713}$, by Theorem 8.4.3 .

$\therefore 12^{43} \equiv (614)(302) \pmod{713}$, by transitivity.

Since $(614)(302) = 713 \times 260 + 48$, $(614)(302) \equiv 48 \pmod{713}$, by Theorem 8.4.1.

$\therefore 12^{43} \equiv 48 \pmod{713}$, by transitivity.

$\therefore (12^{43} \bmod 713) = (48 \bmod 713)$ by Theorem 8.4.1.

Since $48 = 713 \times 0 + 48$ and $0 \leq 48 < 713$,

$(48 \bmod 713) = 48$, by definition of the "mod" function.

$\therefore (12^{43} \bmod 713) = 48$, ~~by Theorem 8.4.1~~ by Substitution . DONE

11

Exploiting the powers of Theorems 8.4.1 and 8.4.3

Problem: Find the least (modulo 12) Residue of

$$62^5 - 37^{27}.$$

[i.e., Find $((62^5 - 37^{27}) \bmod 12)$]

Soln: $62 = 5 \times 12 + 2$, $[a = kn + b]$

$\therefore 62 \equiv 2 \pmod{12}$ by Thm 8.4.1.

$62^5 \equiv 2^5 \pmod{12}$ by Thm 8.4.3

$37 = 3 \times 12 + 1$ $[a = kn + b]$

$\therefore 37 \equiv 1 \pmod{12}$ by Thm 8.4.1.

$37^{27} \equiv 1^{27} \equiv 1 \pmod{12}$ by Thm 8.4.3.

$(62^5 - 37^{27}) \equiv (2^5 - 1) \pmod{12}$ by Thm 8.4.3.

$(62^5 - 37^{27}) \equiv 31 \pmod{12}$ by substitution

$31 = 2 \times 12 + 7$ and $0 \leq 7 < 12$.

$\therefore (31 \bmod 12) = 7$ by def'n of "$(31 \bmod 12)$"

$((62^5 - 37^{27}) \bmod 12) = (31 \bmod 12) = 7$ by Thm 8.4.1 and substitution

$\therefore$ The least (mod 12) Residue of $(62^5 - 37^{27})$ is 7.