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) $\mathbf{m = n\,k + r}$ 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 **n** $>$ 1 . Then, by Theorem 8.4.1,

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

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.

<u>We use the following results from Theorem 8.4.3</u>:

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 , $a^k \equiv A^k \pmod{n}$.

<u>We will also use the following result from Theorem 8.4.1</u>:

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

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

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

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

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

$\therefore$ **$12^{2} \equiv 144 \pmod{713}$** , 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 .

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 . DONE
