HW #11 A, PART I Solutions
M325K SPRING 2014

Section 8.4 (4th Edition)

#32(b)

In the solution to part (a) of #32, assigned, it was determined that 161 is a (mod 660)-inverse of 41.

We verify that 41 and 161 are (mod 660)-inverses of each other: $(161)(41) = 6601 = (10)(660)+1$.
$\therefore [(161)(41)] \equiv 1 \pmod{660}$.

Consider the congruence: $41x \equiv 125 \pmod{660}$.

Multiplying both sides by 161
(where 161 is a (mod 660) inverse of 41), we obtain
$(161)(41x) \equiv (161)(125) \pmod{660}$ by Theorem 8.4.3.
Also, $(161)(41x) \equiv ((161)(41))x \equiv 1 \cdot x \equiv x \pmod{660}$.
$\therefore$ By transitivity, $\underline{x \equiv (161)(125) \equiv 20{,}125 \pmod{660}}$.

Thus, every integer that is congruent to 20,125 modulo 660 is a solution of this congruence.

$$20{,}125 \equiv 20{,}125 \pmod{660}.$$

$\therefore x = 20{,}125$ is one solution.

$\therefore$ (20125 mod 660) is the least non-negative solution.

$20{,}125 = (30)(660) + 325$ and $0 \leq 325 < 660$.
$\therefore$ (20,125 mod 660) $= 325$.

$\therefore x = 325$ is the least positive solution.

The Solution to Problem 32(b) from Section 8.4 of Epp's 4th Edition using the methods presented in class:

The congruence to solve is $41x \equiv 125 \pmod{660}$.
We will need to determine a (mod 660) inverse of 41.

[FINDING a (mod 660) inverse of 41]

$$41 \overline{)660} = 16, \quad 660 - 656 = 4$$
$$4 \overline{)41} = 10, \quad 41 - 40 = 1$$

So; $\gcd(41, 660) = 1$.

Thus, the congruence is a Simple Congruence
$Bx \equiv D \pmod{n}$ with $\gcd(B, n) = 1$

$$4 = (660)(1) - (41)(16)$$
$$1 = (41)(1) - (4)(10)$$
$$1 = (41)(1) - [(660)(1) - (41)(16)](10)$$
$$1 = (41)(1) - (660)(10) + (41)(160)$$
$$1 = (41)(1) - (660)(10) + (41)(160)$$
$$1 = (41)(161) - (660)(10)$$
$$1 = (41)(161) + (660)(-10)$$
$$b = a + nk$$

So, $1 \equiv (41)(161) \pmod{660}$ by Theorem 8.4.1

So, $A = 161$ is a (mod 660) inverse of 41.

It was shown in class that $(161)(125)$ is one solution of the Congruence.
$(161)(125) = 20,125$

Problem # 32(b) continued:

Check: $(41)(20{,}125) = (660)(1250) + 125$,

So, $(41)(20{,}125) \equiv 125 \pmod{660}$ by Thm 8.4.1.

$x_0 = (161)(125) = 20{,}125$ is a solution of the congruence.

The least non-negative solution of this congruence is

$x_1 = (20{,}125 \bmod 660)$.

$20{,}125 = (660)(30) + 325$ and $0 \le 325 < 660$.

So, $(20{,}125 \bmod 660) = 325$

So, the least positive solution of the congruence is $\underline{325}$.

Section 8.4 (FOURTH EDITION)

#37 C ↔ 03 ; O ↔ 15 ; M ↔ 13 ; E ↔ 05.

"C": $M = 3$, $C = \left(3^{43} \bmod 713\right) = \_\_\_\,?$

$3^2 = 9,\ 3^3 = 27,\ 3^4 = 81$

$3^8 = (3^4)^2 \equiv (81)^2 \equiv 144 \pmod{713}$

$3^{16} = (3^8)^2 \equiv (144)^2 \equiv 59 \pmod{713}$

$3^{32} = (3^{16})^2 \equiv (59)^2 \equiv 629 \pmod{713}$

$3^{43} = (3^{32})(3^8)(3^2)(3^1)$

$\equiv (629)(144)(9)(3) \pmod{713}$

$\equiv 675 \pmod{713}$

$\therefore \left(3^{43} \bmod 713\right) = 675$

$\boxed{\text{For } M = 03\ (C),\ C = 675}$

O: $M = 15$, $C = (15^{43} \bmod 713) = \_\_\_$

$15^2 = 225,\ 15^4 = 50{,}675 \equiv 2 \pmod{713}$

$15^8 = (15^4)^2 \equiv 2^2 = 4 \pmod{713}$

$15^{16} = (15^8)^2 \equiv 4^2 = 16 \pmod{713}$

$15^{32} = (15^{16})^2 \equiv 16^2 = 256 \pmod{713}$

$15^{43} = (15^{32})(15^8)(15^2)(15^1)$

$\equiv (256)(4)\underline{(225)(15)} \equiv 89 \pmod{713}$

$(15^{43} \bmod 713) = 89$. $\boxed{\text{For } M = 15\ (O),\ C = 89}$.

SEC. 8.4, #37 (Continued)

M: $M = 13$, $C = (13^{43} \bmod 713) = \_\_\_\_?$

$13^2 = 169$, $13^4 = 28{,}561 \equiv 41 \pmod{713}$

$13^8 = (13^4)^2 \equiv (41)^2 = 1{,}681 \equiv 255 \pmod{713}$

$13^{16} = (13^8)^2 \equiv (255)^2 = 65{,}025 \equiv 142 \pmod{713}$

$13^{32} = (13^{16})^2 \equiv (142)^2 = 20{,}164 \equiv 200 \pmod{713}$

$13^{43} = (13^{32})(13^8)(13^2)(13^1)$

$\equiv (200)(255)(169)(13) \pmod{713}$

$\equiv 476 \pmod{713}$. $\therefore (13^{43} \bmod 713) = 476$

$\boxed{\text{For } M = 13 \text{ ("M")}, C = 476}$

E: $M = 5$, $C = (5^{43} \bmod 713) = \_\_\_\_?$

$5^2 = 25$, $5^4 = 625$.

$5^8 = (5^4)^2 \equiv (625)^2 = 390{,}625 \equiv 614 \pmod{713}$

$5^{16} = (5^8)^2 \equiv (614)^2 = 376{,}996 \equiv 532 \pmod{713}$

$5^{32} = (5^{16})^2 \equiv (532)^2 = 283{,}024 \equiv 676 \pmod{713}$

$5^{43} = (5^{32})(5^8)(5^2)(5^1)$

$\equiv (676)(614)(25)(5) \pmod{713}$

$\equiv 129 \pmod{713}$. $\therefore (5^{43} \bmod 713) = 129$

$\therefore \boxed{\text{For } M = 5 \text{ ("E")}, C = 129}$

$\boxed{\text{The ENCRYPTION: } 675, 089, 476, 129}$