The Solution to Problem 3.1 (a), (c) from Section 8.4 of Epp's 4th Edition using methods presented in class.

3.1(a) We need to find a (mod 13) inverse of 210.

$$\begin{array}{r} 16 \\ 13\overline{)210} \\ \underline{208} \\ 2 \end{array} \qquad \begin{array}{r} 6 \\ 2\overline{)13} \\ \underline{12} \\ 1 \end{array}$$

HW #11 B, M325K
PART II SOLUTIONS
SPRING 2024

$2 = (210)(1) - (13)(16)$

$1 = (13)(1) - (2)(6)$

$1 = (13)(1) - [(210)(1) - (13)(16)](6)$

$1 = (13)(1) - (210)(6) + (13)(96)$

$1 = (13)(97) - (210)(6)$

$1 = (13)(97) + (210)(-6)$

$\therefore 1 \equiv (210)(-6) \pmod{13}$ by Theorem 8.4.1.

$\therefore -6$ is a (mod 13) inverse of 210.

So, -6 is a correct answer, but so is $7 = -6+13$, or $20 = 7+13$, or $-19 = -6-13$.

Any integer x_1 such that $x_1 \equiv -6 \pmod{13}$ is a correct answer.

The solution for 3.1(c) is on the next page.

31(c): The congruence to solve is

$$210x \equiv 8 \pmod{13}.$$

Since $\gcd(210, 13) = 1$, the congruence is a simple congruence $Bx \equiv D \pmod{n}$ with $\gcd(B, n) = 1$.

In the solution to 31(a), it was determined that -6 is a $\pmod{13}$ inverse of 210.

To find a positive solution of this congruence, we need a positive $\pmod{13}$ inverse of 210.

Since $7 = (13)(1) + (-6)$, $7 \equiv -6 \pmod{13}$ by Thm 8.4.1.

Since $7 \equiv -6 \pmod{13}$, 7 is also a $\pmod{13}$ inverse of 210.

Check: $(210)(7) = (13)(113) + 1$

So, $(210)(7) \equiv 1 \pmod{13}$ by Thm 8.4.1. ✓

It was shown in class that $x_0 = (7)(8) = 56$ is one solution of this congruence.

So, the least non-negative solution is

$x_1 = (56 \bmod 13)$.

$56 = (13)(4) + 4$ and $0 \le 4 < 13$

So, $(56 \bmod 13) = 4$ is the least non-negative solution of this congruence.

The next positive solution is $4 + 13 = 17$

Problem 31(c) Continued

To find the greatest negative solution ≤ -300, we need to represent integers t such that $t \equiv 4 \pmod{13}$.

If $t \equiv 4 \pmod{13}$, then there exists an integer k such that $t = 13k + 4$

So, we solve the inequality

$$13k + 4 \leq -300$$
$$13k \leq -304$$
$$k \leq \frac{-304}{13} = -23.3846\ldots$$

Consider $k = -24$, and so $t = (13)(-24) + 4 = -308$

So, $\underline{t = -308}$ is a solution of the congruence and it is the greatest solution that is less than or equal to -300.

Check: $(210)(-308) = (13)(-4976) + 8$

Thus since $(210)(-308) = -64,680$

and $(13)(-4976) = -64,688$

so $(13)(-4976) + 8 = -64,680 = (210)(-308)$.

Since $(210)(-308) = (13)(-4976) + 8)$

$-(210)(-308) \equiv 8 \pmod{13}$ and

$t = -308$ is a solution of this congruence

So, $t = -308$ is the greatest solution less than or equal to -300.

HW #11 B, PART II, Sec 8.4, #31(c) M325K SPRING 2024

(The solution for Section 8.4, #39 is in the back of the book)

This solution for #31(c) uses methods from the Handout "Solving Simple Congruences" SECTION 8.4 (Epp's 4th Edition) SOLUTIONS

#31c. Consider the Congruence

$$210x \equiv 8 \pmod{13}.$$

In 31b, it was discovered that 7 is a (mod 13)-inverse of 210.

We verify that 7 and 210 are (mod 13)-inverses of each other:

$$(7)(210) = 1,470 = (113)(13) + 1,$$

Since $210x \equiv 8 \pmod{13}$, $(7)(210x) \equiv (7)(8) \equiv 56 \pmod{13}$ by Theorem 8.4.3.

Also, $(7)(210x) \equiv ((7)(210))x \equiv 1 \cdot x \equiv x \pmod{13}$, by Theorem 8.4.3.

∴ By transitivity, $x \equiv 56 \pmod{13}$.

Thus, every integer which is congruent to 56 modulo 13 is a solution of this congruence.

$$56 \equiv 56 \pmod{13}.$$

∴ $x = 56$ is one solution. $(56 \bmod 13) = 4$

$(56 \bmod 13) = 4$ since $56 = (4)(13) + 4$ and $0 \le 4 < 13$

(1) The least positive solution is $(56 \bmod 13) = 4$.

(2) The next positive solution is $4 + 13 = 17$.

(3) Every solution is of the form $4 + 13k$ for some integer k.

$-308 = 4 + (13)(-24) < -300 < -295 = 4 + (13)(-23)$

∴ $x = -308$ is the greatest solution less than or equal to -300.

HW #11B; PART II, Sec. 8.4: #36, #39, #40, #42
(continued)

#36 $N = (23)(31) = 713$ $e = 43$

Soln:

LETTER CODES

H ⟷ 08; E ⟷ 05; L ⟷ 12, P ⟷ 16

For "H", $M = 08$; $C \equiv (8^{43} \bmod 713) = \_\_\_\_?$

$8^2 = 64$; $8^4 = 4096 \equiv (4096 \bmod 713) \pmod{713}$.

So, $8^4 \equiv 531 \pmod{713}$

$8^8 = (8^4)^2 \equiv (531^2) \pmod{713} \equiv (531^2 \bmod 713) \pmod{713}$.

So, $8^8 \equiv 326 \pmod{713}$.

$8^{16} = (8^2)^2 \equiv (326^2) \pmod{713} \equiv (326^2 \bmod 713) \pmod{713}$.

So, $8^{16} \equiv 39 \pmod{713}$.

$8^{32} = (8^{16})^2 \equiv 39^2 \pmod{713} \equiv (39^2 \bmod 713) \pmod{713}$.

So, $8^{32} \equiv 95 \pmod{713}$

$43 = 32 + 8 + 2 + 1$.

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

$8^{43} \equiv (95)(326)(64)(8) \pmod{713}$

$(95)(326) \equiv 311 \pmod{713}$ by a simple calculation.

$(64)(8) = 512 \equiv 512 \pmod{713}$ by reflexivity.

$[(95)(326)][(64)(8)] \equiv (311)(512) \pmod{713}$

$8^{43} \equiv (311)(512) \equiv 233 \pmod{713}$ by a simple calculation.

$\therefore (8^{43} \bmod 713) = 233$ For $M = 08$ (H), $C = 233$. 4 MED.

FOR THE REST, SEE THE SOLUTION IN THE BACK OF THE BOOK, and on the following pages:

Sec 8.4 (Epp's 4th Edition) Back of the Book Solutions

Because $27 = 16 + 8 + 2 + 1$, we first perform the following computations:

$13^1 \equiv 13 \pmod{55}$ $\quad 20^1 \equiv 20 \pmod{55}$
$13^2 \equiv 4 \pmod{55}$ $\quad 20^2 \equiv 15 \pmod{55}$
$13^4 \equiv 4^2 \equiv 16 \pmod{55}$ $\quad 20^4 \equiv 15^2 \equiv 5 \pmod{55}$
$13^8 \equiv 16^2 \equiv 36 \pmod{55}$ $\quad 20^8 \equiv 25^2 \equiv 5 \pmod{55}$
$13^{16} \equiv 36^2 \equiv 31 \pmod{55}$ $\quad 20^{16} \equiv 25^2 \equiv 20 \pmod{55}$

$9^1 \equiv 9 \pmod{55}$
$9^2 \equiv 26 \pmod{55}$
$9^4 \equiv 26^2 \equiv 16 \pmod{55}$
$9^8 \equiv 16^2 \equiv 36 \pmod{55}$
$9^{16} \equiv 36^2 \equiv 31 \pmod{55}$

Then we compute

$13^{27} \bmod 55 = (31 \cdot 36 \cdot 4 \cdot 13) \bmod 55 = 7,$
$20^{27} \bmod 55 = (20 \cdot 25 \cdot 15 \cdot 20) \bmod 55 = 15,$
$9^{27} \bmod 55 = (31 \cdot 36 \cdot 26 \cdot 9) \bmod 55 = 4.$

Finally, because 7, 15, and 4 translate into letters as G, O, and D, we see that the message is GOOD.

25. *Hint:* By Theorem 5.2.3, using a in place of r and $n-1$ in place of n, we have $1 + a + a^2 + \cdots + a^{n-1} = \frac{a^n - 1}{a - 1}$. Multiplying both sides by $a - 1$ gives

$$a^n - 1 = (a - 1)(1 + a + a^2 + \cdots + a^{n-1}).$$

26. Step 1: $6664 = 765 \cdot 8 + 544$, and so $544 = 6664 - 765 \cdot 8$
Step 2: $765 = 544 \cdot 1 + 221$, and so $221 = 765 - 544$
Step 3: $544 = 221 \cdot 2 + 102$, and so $102 = 544 - 221 \cdot 2$
Step 4: $221 = 102 \cdot 2 + 17$, and so $17 = 221 - 102 \cdot 2$
Step 5: $102 = 17 \cdot 6 + 0$

Thus gcd(6664, 765) = 17 (which is the remainder obtained just before the final division). Substitute back through steps 4–1 to express 17 as a linear combination of 6664 and 765:

$$17 = 221 - 102 \cdot 2$$
$$= 221 - (544 - 221 \cdot 2) = 221 \cdot 5 - 544 \cdot 2$$
$$= (765 - 544) \cdot 5 - 544 \cdot 2 = 765 \cdot 5 - 544 \cdot 7$$
$$= 765 \cdot 5 - (6664 - 765 \cdot 8) \cdot 7 = (-7) \cdot 6664 + 61 \cdot 765.$$

(When you have finished this final step, it is wise to verify that you have not made a mistake by checking that the final expression really does equal the greatest common divisor.)

28.

a	330	156	18	12	6
b	156	18	12	6	0
r		18	12	6	0
q		2	8	1	2
s	1	0	1	−8	9
t	0	1	−2	17	−19
u	0	1	−8	9	−26
v	1	−2	17	−19	55
$newu$		1	−8	9	−26
$newv$		−2	17	−19	55
$sa + tb$	330	18	−6	6	6

31. a. Step 1: $210 = 13 \cdot 16 + 2$, and so $2 = 210 - 16 \cdot 13$
Step 2: $13 = 2 \cdot 6 + 1$, and so $1 = 13 - 2 \cdot 6$
Step 3: $6 = 1 \cdot 6 + 0$, and so gcd(210, 13) = 1

Substitute back through steps 2–1:

$$1 = 13 - 2 \cdot 6$$
$$= 13 - (210 - 16 \cdot 13) \cdot 6 = (-6) \cdot 210 + 97 \cdot 13$$

Thus $210 \cdot (-6) \equiv 1 \pmod{13}$, and so -6 is an inverse for 210 modulo 13.

b. Compute $13 - 6 = 7$, and note that $7 \equiv -6 \pmod{13}$ because $7 - (-6) = 13 = 13 \cdot 1$. Thus, by Theorem 8.4.3(3), $210 \cdot 7 \equiv 210 \cdot (-6) \pmod{13}$. It follows, by the transitive property of congruence, that $210 \cdot 7 \equiv 1 \pmod{13}$, and so 7 is a positive inverse for 210 modulo 13.

c. This problem can be solved using either the result of part (a) or that of part (b). By part (b) $210 \cdot 7 \equiv 1 \pmod{13}$. Multiply both sides by 8 and apply Theorem 8.4.3(3) to obtain $210 \cdot 56 \equiv 8 \pmod{13}$. Thus a positive solution for $210x \equiv 8 \pmod{13}$ is $x = 56$. Note that the least positive residue corresponding to this solution is also a solution. By Theorem 8.4.1, $56 \equiv 4 \pmod{13}$ because $56 = 13 \cdot 4 + 4$, and so, by Theorem 8.4.3(3), $210 \cdot 56 \equiv 210 \cdot 4 \equiv 9 \pmod{13}$. This shows that 4 is also a solution for the congruence, and because $0 \le 4 < 13$, 4 is the least positive solution for the congruence.

33. *Hint:* If $as + bt = 1$ and $c = au = bv$, then $c = asc + btc = as(bv) + bt(au)$.

35. Proof: Suppose a, n, s and s' are integers such that $as \equiv as' \equiv 1 \pmod{n}$. Consider the quantity $as's$, and note that $as's = (as') \cdot s = (as) \cdot s'$. By Theorem 8.4.3(3), $(as') \cdot s \equiv 1 \cdot s = s \pmod{n}$ and $(as') \cdot s' \equiv 1 \cdot s' = s' \pmod{n}$. Thus by transitivity of congruence modulo n, $s \equiv s' \pmod{n}$. This shows that any two inverses for a are congruent modulo n.

36. The numeric equivalents of H, E, L, and P are 08, 05, 12 and 16. To encrypt these letters, the following quantities must be computed: $8^{43} \bmod 713$, $5^{43} \bmod 713$, $12^{43} \bmod 713$, and $16^{43} \bmod 713$. We use the fact that $43 = 32 + 8 + 2 + 1$.

H: $8 \equiv 8 \pmod{713}$
$8^2 \equiv 64 \pmod{713}$
$8^4 \equiv 64^2 \equiv 531 \pmod{713}$
$8^8 \equiv 531^2 \equiv 326 \pmod{713}$
$8^{16} \equiv 326^2 \equiv 39 \pmod{713}$
$8^{32} \equiv 39^2 \equiv 95 \pmod{713}$
Thus the ciphertext is
$8^{43} \bmod 713$
$= (95 \cdot 326 \cdot 64 \cdot 8) \bmod 713 = 233.$

E: $5 \equiv 5 \pmod{713}$
$5^2 \equiv 25 \pmod{713}$
$5^4 \equiv 625 \pmod{713}$
$5^8 \equiv 625^2 \equiv 614 \pmod{713}$
$5^{16} \equiv 614^2 \equiv 532 \pmod{713}$

Sec 8.4 (Epp's 4th Editin) Back of the Book Solutions

13

#36 Continued

$5^{32} \equiv 532^2 \equiv 676 \pmod{713}$
Thus the ciphertext is
$5^{43} \bmod 713$
$= (676 \cdot 614 \cdot 25 \cdot 5) \bmod 713 = 129.$

L: $12 \equiv 12 \pmod{713}$
$12^2 \equiv 144 \pmod{713}$
$12^4 \equiv 144^2 \equiv 59 \pmod{713}$
$12^8 \equiv 59^2 \equiv 629 \pmod{713}$
$12^{16} \equiv 629^2 \equiv 639 \pmod{713}$
$12^{32} \equiv 639^2 \equiv 485 \pmod{713}$
Thus the ciphertext is
$12^{43} \bmod 713$
$= (485 \cdot 629 \cdot 144 \cdot 12) \bmod 713 = 48.$

P: $16 \equiv 16 \pmod{713}$
$16^2 \equiv 256 \pmod{713}$
$16^4 \equiv 256^2 \equiv 653 \pmod{713}$
$16^8 \equiv 653^2 \equiv 35 \pmod{713}$
$16^{16} \equiv 35^2 \equiv 512 \pmod{713}$
$16^{32} \equiv 512^2 \equiv 473 \pmod{713}$
Thus the ciphertext is
$16^{43} \bmod 713$
$= (473 \cdot 35 \cdot 256 \cdot 16) \bmod 713 = 128.$

Therefore, the encrypted message is 233 129 048 128. (Again, note that in practice, individual letters of the alphabet are grouped together in blocks during encryption so that deciphering cannot be accomplished through knowledge of frequency patterns of letters or words. We kept them separate so that the numbers in the computations would be smaller and easier to work with.)

39. By exercise 38, the decryption key, d, is 307. Hence, to decrypt the message, the following quantities must be computed: $675^{307} \bmod 713$, $89^{307} \bmod 713$, and $48^{307} \bmod 713$. We use the fact that $307 = 256 + 32 + 16 + 2 + 1$.

$675 \equiv 675 \pmod{713}$
$675^2 \equiv 18 \pmod{713}$
$675^4 \equiv 18^2 \equiv 324 \pmod{713}$
$675^8 \equiv 324^2 \equiv 165 \pmod{713}$
$675^{16} \equiv 165^2 \equiv 131 \pmod{713}$
$675^{32} \equiv 131^2 \equiv 49 \pmod{713}$
$675^{64} \equiv 49^2 \equiv 262 \pmod{713}$
$675^{128} \equiv 262^2 \equiv 196 \pmod{713}$
$675^{256} \equiv 196^2 \equiv 627 \pmod{713}$

$89 \equiv 89 \pmod{713}$
$89^2 \equiv 78 \pmod{713}$
$89^4 \equiv 78^2 \equiv 380 \pmod{713}$
$89^8 \equiv 380^2 \equiv 374 \pmod{713}$
$89^{16} \equiv 374^2 \equiv 128 \pmod{713}$
$89^{32} \equiv 128^2 \equiv 698 \pmod{713}$
$89^{64} \equiv 698^2 \equiv 225 \pmod{713}$
$89^{128} \equiv 225^2 \equiv 2 \pmod{713}$
$89^{256} \equiv 2^2 \equiv 4 \pmod{713}$

$48 \equiv 48 \pmod{713}$
$48^2 \equiv 165 \pmod{713}$
$48^4 \equiv 131 \pmod{713}$
$48^8 \equiv 49 \pmod{713}$
$48^{16} \equiv 262 \pmod{713}$
$48^{32} \equiv 196 \pmod{713}$
$48^{64} \equiv 627 \pmod{713}$
$48^{128} \equiv 627^2 \equiv 266 \pmod{713}$
$48^{256} \equiv 266^2 \equiv 169 \pmod{713}$

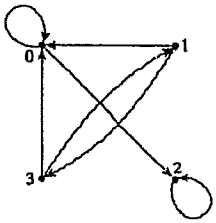
Thus the decryption for 675 is
$675^{307} \bmod 713 = (675^{256+32+16+2+1}) \bmod 713$
$= (627 \cdot 49 \cdot 131 \cdot 18 \cdot 675) \bmod 713 = 3,$ which corresponds to the letter C.
The decryption for 89 is
$89^{307} \bmod 713 = (89^{256+32+16+2+1}) \bmod 713$
$= (4 \cdot 698 \cdot 128 \cdot 78 \cdot 89) \bmod 713 = 15,$ which corresponds to the letter O.
The decryption for 48 is
$48^{307} \bmod 713 = (48^{256+32+16+2+1}) \bmod 713$
$= (169 \cdot 196 \cdot 262 \cdot 165 \cdot 48) \bmod 713 = 12,$ which corresponds to the letter L.
Thus the decrypted message is COOL.

41. a. *Hint:* For the inductive step, assume $p \mid q_1 q_2 \dots q_{s+1}$ and let $a = q_1 q_2 \dots q_s$. Then $p \mid a q_{s+1}$, and either $p = q_{s+1}$ or Euclid's lemma and the inductive hypothesis can be applied.

42. a. When $a = 15$ and $p = 7$, $a^{p-1} = 15^6 = 11390625 \equiv 1 \pmod 7$ because $11390625 - 1 = 7 \cdot 1627232$.

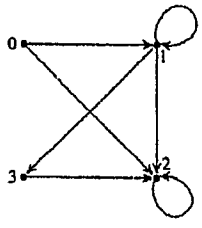
Section 8.5

1. a.



R_1 is not antisymmetric: $1 \, R_1 \, 3$ and $3 \, R_1 \, 1$ and $1 \neq 3$.

b.



R_2 is antisymmetric: There are no cases where $a \, R \, b$ and $b \, R \, a$ and $a \neq b$.

7

From Sec 8.4 (Epp's 4th Ed) #39

$5^{32} \equiv 532^2 \equiv 676 \pmod{713}$
Thus the ciphertext is
$5^{43} \bmod 713$
$= (676 \cdot 614 \cdot 25 \cdot 5) \bmod 713 = 129.$

L: $12 \equiv 12 \pmod{713}$
$12^2 \equiv 144 \pmod{713}$
$12^4 \equiv 144^2 \equiv 59 \pmod{713}$
$12^8 \equiv 59^2 \equiv 629 \pmod{713}$
$12^{16} \equiv 629^2 \equiv 639 \pmod{713}$
$12^{32} \equiv 639^2 \equiv 485 \pmod{713}$
Thus the ciphertext is
$12^{43} \bmod 713$
$= (485 \cdot 629 \cdot 144 \cdot 12) \bmod 713 = 48.$

P: $16 \equiv 16 \pmod{713}$
$16^2 \equiv 256 \pmod{713}$
$16^4 \equiv 256^2 \equiv 653 \pmod{713}$
$16^8 \equiv 653^2 \equiv 35 \pmod{713}$
$16^{16} \equiv 35^2 \equiv 512 \pmod{713}$
$16^{32} \equiv 512^2 \equiv 473 \pmod{713}$
Thus the ciphertext is
$16^{43} \bmod 713$
$= (473 \cdot 35 \cdot 256 \cdot 16) \bmod 713 = 128.$

Therefore, the encrypted message is 233 129 048 128. (Again, note that in practice, individual letters of the alphabet are grouped together in blocks during encryption so that deciphering cannot be accomplished through knowledge of frequency patterns of letters or words. We kept them separate so that the numbers in the computations would be smaller and easier to work with.)

39. By exercise 38, the decryption key, d, is 307. Hence, to decrypt the message, the following quantities must be computed: $675^{307} \bmod 713$, $89^{307} \bmod 713$, and $48^{307} \bmod 713$. We use the fact that $307 = 256 + 32 + 16 + 2 + 1$.

$675 \equiv 675 \pmod{713}$
$675^2 \equiv 18 \pmod{713}$
$675^4 \equiv 18^2 \equiv 324 \pmod{713}$
$675^8 \equiv 324^2 \equiv 165 \pmod{713}$
$675^{16} \equiv 165^2 \equiv 131 \pmod{713}$
$675^{32} \equiv 131^2 \equiv 49 \pmod{713}$
$675^{64} \equiv 49^2 \equiv 262 \pmod{713}$
$675^{128} \equiv 262^2 \equiv 196 \pmod{713}$
$675^{256} \equiv 196^2 \equiv 627 \pmod{713}$

$89 \equiv 89 \pmod{713}$
$89^2 \equiv 78 \pmod{713}$
$89^4 \equiv 78^2 \equiv 380 \pmod{713}$
$89^8 \equiv 380^2 \equiv 374 \pmod{713}$
$89^{16} \equiv 374^2 \equiv 128 \pmod{713}$
$89^{32} \equiv 128^2 \equiv 698 \pmod{713}$
$89^{64} \equiv 698^2 \equiv 225 \pmod{713}$
$89^{128} \equiv 225^2 \equiv 2 \pmod{713}$
$89^{256} \equiv 2^2 \equiv 4 \pmod{713}$

$48 \equiv 48 \pmod{713}$
$48^2 \equiv 165 \pmod{713}$
$48^4 \equiv 131 \pmod{713}$
$48^8 \equiv 49 \pmod{713}$
$48^{16} \equiv 262 \pmod{713}$
$48^{32} \equiv 196 \pmod{713}$
$48^{64} \equiv 627 \pmod{713}$
$48^{128} \equiv 627^2 \equiv 266 \pmod{713}$
$48^{256} \equiv 266^2 \equiv 169 \pmod{713}$

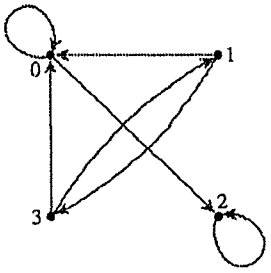
Thus the decryption for 675 is
$675^{307} \bmod 713 = (675^{256+32+16+2+1}) \bmod 713$
$= (627 \cdot 49 \cdot 131 \cdot 18 \cdot 675) \bmod 713 = 3,$ which corresponds to the letter C.
The decryption for 89 is
$89^{307} \bmod 713 = (89^{256+32+16+2+1}) \bmod 713$
$= (4 \cdot 698 \cdot 128 \cdot 78 \cdot 89) \bmod 713 = 15,$ which corresponds to the letter O.
The decryption for 48 is
$48^{307} \bmod 713 = (48^{256+32+16+2+1}) \bmod 713$
$= (169 \cdot 196 \cdot 262 \cdot 165 \cdot 48) \bmod 713 = 12,$ which corresponds to the letter L.
Thus the decrypted message is COOL.

41. a. *Hint:* For the inductive step, assume $p \mid q_1 q_2 \cdots q_{s+1}$ and let $a = q_1 q_2 \cdots q_s$. Then $p \mid a q_{s+1}$, and either $p = q_{s+1}$ or Euclid's lemma and the inductive hypothesis can be applied.

42. a. When $a = 15$ and $p = 7$, $a^{p-1} = 15^6 = 11390625 \equiv 1 \pmod{7}$ because $11390625 - 1 = 7 \cdot 1627232$.

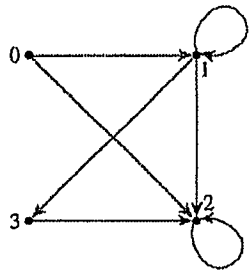
Section 8.5

1. a.



R_1 is not antisymmetric: $1 \, R_1 \, 3$ and $3 \, R_1 \, 1$ and $1 \neq 3$.

b.



R_2 is antisymmetric: There are no cases where $a \, R \, b$ and $b \, R \, a$ and $a \neq b$.

In order to solve problem #39, you needed to FIND an inverse of 43 modulo 660. This is the task in #38

Sec 4: #38 FIND the least positive inverse for 43 modulo 660.

(4e)

$$43\overline{)660}\ (15 \qquad 15\overline{)43}\ (2 \qquad 13\overline{)15}\ (1 \qquad 2\overline{)13}\ (6$$

43 | 30 | 13 | 12

230 | 13 | 2 | 1

215

15

$1 = (13)(1) - (2)(6)$

$2 = (15)(1) - (13)(1)$

$13 = (43)(1) - (15)(2)$

$15 = (660)(1) - (43)(15)$

(Substituting for "2")

$1 = (13)(1) - [(15)(1) - (13)(1)](6)$

$1 = (13)(7) - (15)(6)$

Subst. for 13 →

$1 = [(43)(1) - (15)(2)](7) - (15)(6)$

$1 = (43)(7) - (15)(20)$

Subst. for 15 →

$1 = (43)(7) - [(660)(1) - (43)(15)](20)$

$1 = (43)(307) - (660)(20)$ $= (43)(307) + (660)(-20)$

$\therefore (43)(307) \equiv 1 \pmod{660}$. Since $0 < 307 < 660$, 307 is the least positive inverse of 43 modulo 660.

SECTION 8.4, #40

DECRYPT: 028, 018, 675, 129

and use $N = 713$ and $d = 307$

For a given ciphertext C, the Plaintext is $M = (C^d \bmod 713)$.

For $C = 028$, $m = (28^{307} \bmod 713) = $ ____ ?

$28^2 = 784 \equiv (784 \bmod 713) \pmod{713}$

$28^2 \equiv 71 \pmod{713}$ since $(784 \bmod 713) = 71$, which is true since $784 = 713(1) + 71$ and $0 \le 71 < 713$.

$28^4 = (28^2)^2 \equiv 71^2 \pmod{713} \equiv (71^2 \bmod 713) \pmod{713}$.

So, $28^4 \equiv 50 \pmod{713}$.

$28^8 = (28^4)^2 \equiv 50^2 \pmod{713} \equiv (50^2 \bmod 713) \pmod{713}$.

So, $28^8 \equiv 361 \pmod{713}$.

$28^{16} = (28^8)^2 \equiv (361)^2 \pmod{713} \equiv (361^2 \bmod 713) \pmod{713}$.

So, $28^{16} \equiv 555 \pmod{713}$

$28^{32} = (28^{16})^2 \equiv 555^2 \pmod{713} \equiv (555^2 \bmod 713) \pmod{713}$

So, $28^{32} \equiv 9 \pmod{713}$.

$28^{64} = (28^{32})^2 \equiv 9^2 \pmod{713} = 81$

So, $28^{64} \equiv 81 \pmod{713}$

$28^{128} = (28^{64})^2 \equiv 81^2 \pmod{713} \equiv (81^2 \bmod 713) \pmod{713}$

So, $28^{128} \equiv 144 \pmod{713}$.

$28^{256} = (28^{128})^2 \equiv 144^2 \pmod{713} \equiv (144^2 \bmod 713) \pmod{713}$.

So, $28^{256} \equiv 59 \pmod{713}$.

10

SECTION 8.4, #40 (Continued)

$\therefore 28^{307} = (28^{256})(28^{32})(28^{16})(28^{2})(28^{1})$

$\therefore 28^{307} \equiv (59)(9)(555)(71)(28) \pmod{713}$.

$(59)(9) \equiv 531 \pmod{713}$ by a simple calculation.

$(531)(555) \equiv 236 \pmod{713}$ by a simple calculation.

$(236)(71) \equiv 357 \pmod{713}$ by a simple calculation.

$(357)(28) \equiv 14 \pmod{713}$ by a simple calculation.

$\therefore$ by Transitivity, $28^{307} \equiv 14 \pmod{713}$.

$\therefore (28^{307} \bmod 713) = 14$.

For $C = 028$, $M = 14$, Letter = "N"

For $C = 018$, $M = (18^{307} \bmod 713) =$ _____ ?

$18^{2} \equiv 324 \pmod{713}$ by a simple calculation.

$18^{4} = (18^{2})^{2} \equiv 324^{2} \pmod{713} \equiv (324^{2} \bmod 713) \pmod{713}$.

So, $18^{4} \equiv 165 \pmod{713}$.

$18^{8} = (18^{4})^{2} \equiv 165^{2} \pmod{713} \equiv (165^{2} \bmod 713) \pmod{713}$.

So, $18^{8} \equiv 131 \pmod{713}$

$18^{16} = (18^{8})^{2} \equiv 131^{2} \pmod{713} \equiv (131^{2} \bmod 713) \pmod{713}$.

So, $18^{16} \equiv 49 \pmod{713}$.

$18^{32} = (18^{16})^{2} \equiv 49^{2} \pmod{713} \equiv (49^{2} \bmod 713) \pmod{713}$.

So, $18^{32} \equiv 262 \pmod{713}$

$18^{64} = (18^{32})^{2} \equiv 262^{2} \pmod{713} \equiv (262^{2} \bmod 713) \pmod{713}$.

So, $18^{64} \equiv 196 \pmod{713}$.

SECTION 8.4, #40 (Continued)

$18^{128} = (18^{64})^2 \equiv 196^2 \pmod{713} \equiv (196^2 \bmod 713) \pmod{713}$.

So, $18^{128} \equiv 627 \pmod{713}$.

$18^{256} = (18^{128})^2 \equiv 627^2 \pmod{713} \equiv (627^2 \bmod 713) \pmod{713}$.

So, $18^{256} \equiv 266 \pmod{713}$.

$\therefore 18^{307} = (18^{256})(18^{32})(18^{16})(18^{2})(18^{1})$

$18^{307} \equiv (266)(262)(49)(324)(18) \pmod{713}$

$(266)(262) \equiv 531 \pmod{713}$ by a simple calculation.

$(531)(49) \equiv 351 \pmod{713}$ by a simple calculation.

$(351)(324) \equiv 357 \pmod{713}$ by a simple calculation.

$(357)(18) \equiv 9 \pmod{713}$ by a simple calculation

$\therefore$ By Transitivity, $18^{307} \equiv 9 \pmod{713}$.

$\therefore (18^{307} \bmod 713) = 9$.

For $C = 18$, $m = 9$, LETTER = "I"

For Ciphertext $C = 675$, it was shown in Problem #89 of Section 8.4 that $(675^{307} \bmod 713) = 3$.

So, For $C = 675$, $m = 3$, LETTER = "C".

For $C = 129$, $m = (129^{307} \bmod 713) =$ _____ ?

$129^2 \equiv 242 \pmod{713}$ by a simple calculation.

$129^4 = (129^2)^2 \equiv 242^2 \pmod{713} \equiv (242^2 \bmod 713) \pmod{713}$

$\therefore 129^4 \equiv 98 \pmod{713}$

SECTION 8.4, #40 (Continued)

$129^8 = (129^4)^2 \equiv 98^2 \pmod{713} \equiv (98^2 \bmod 713) \pmod{713}$.

So, $129^8 \equiv 335 \pmod{713}$

$129^{16} = (129^8)^2 \equiv 335^2 \pmod{713} \equiv (335^2 \bmod 713) \pmod{713}$

So, $129^{16} \equiv 284 \pmod{713}$

$129^{32} = (129^{16})^2 \equiv 284^2 \pmod{713} \equiv (284^2 \bmod 713) \pmod{713}$.

So, $129^{32} \equiv 87 \pmod{713}$.

$129^{64} = (129^{32})^2 \equiv 87^2 \pmod{713} \equiv (87^2 \bmod 713) \pmod{713}$

So, $129^{64} \equiv 439 \pmod{713}$

$129^{128} = (129^{64})^2 \equiv 439^2 \pmod{713} \equiv (439^2 \bmod 713) \pmod{713}$

So, $129^{128} \equiv 211 \pmod{713}$.

$129^{256} = (129^{128})^2 \equiv 211^2 \pmod{713} \equiv (211^2 \bmod 713) \pmod{713}$.

So, $129^{256} \equiv 315 \pmod{713}$.

$129^{307} = (129^{256})(129^{32})(129^{16})(129^2)(129^1)$

$129^{307} \equiv (315)(87)(284)(242)(129) \pmod{713}$

$(315)(87) \equiv 311 \pmod{713}$
$(311)(284) \equiv 625 \pmod{713}$
$(625)(242) \equiv 94 \pmod{713}$
$(94)(129) \equiv 5 \pmod{713}$

} by a simple calculation.

∴ By Transitivity, $129^{307} \equiv 5 \pmod{713}$.

$= (129^{307} \bmod 713) = 5$.

So, FOR $C = 129$, $M = 5$, LETTER = E.

Summary:

CIPHERTEXT C:	028	018	675	129
PLAINTEXT M:	14	09	03	05
MESSAGE:	N	I	C	E

Problem #42 from Section 8.4 of Epp's 4th Edition

---

a) We need to verify that, with $p = 7$ and with $a = 15$,

$$a^{p-1} \equiv 1 \pmod{p} \text{ is true.}$$

We must show that $15^6 \equiv 1 \pmod{7}$.

$$15^6 = (7)(1,627,232) + 1,$$

So, by Theorem 8.4.1,

$$15^6 \equiv 1 \pmod{7}$$

---

b) We need to verify that, with $p = 11$ and with $a = 8$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

We must show that $8^{10} \equiv 1 \pmod{11}$.

$$8^{10} = (11)(97,612,893) + 1$$

So, by Theorem 8.4.1,

$$8^{10} \equiv 1 \pmod{11},$$