Michelle Bergin
Discrete Mathematics
HW7
4.4 :: 2, 3, 4, 5, P1, P2
4.6 :: 23($***$), 24, 25, 26, 27, P3, P4

- 4.4 :: 2) Show that 937 is an inverse of 13 modulo 2436
  I am having a hard time in this chapter. But I have been trying to search for help online. From what I understand, 937 is the inverse of 13 modulo 2436 because if you take 937 * 13 % 2436 it equals 1

- 4.4 :: 3) find an inverse of 4 modulo 9
  $3 \cdot 4 = 3 (mod 9)$
  $4 \cdot 4 = 7 (mod 9)$
  $5 \cdot 4 = 2 (mod 9)$
  $6 \cdot 4 = 6 (mod 9)$
  $7 \cdot 4 = 1 (mod 9)$ found it!

- 4.4 :: 4) find an inverse of 2 modulo 17
  $9 \cdot 2 = 1 (mod 17)$ found it

- 4.4 :: 5) find a modulo m

  a. $a = 4, m = 9$
  $9 = 2 \cdot 4 + 1$
  $1 = 9 - 4 \cdot 2$

  b. $a = 19, m = 141$
  $141 = 7 \cdot 19 + 8$
  $19 = 2 \cdot 8 + 3$
  $8 = 2 \cdot 3 + 2$
  $3 = 2 + 1$
  $1 = 3 - 1 \cdot 2$
  $= 3 - 1 \cdot (8 - 2 \cdot 3)$
  $= 3 \cdot 3 - 8$
  $= 3 \cdot (19 - 2 \cdot 8) - 8$
  $= 3 \cdot 19 - 6 \cdot 8 - 8$
  $= 3 \cdot 19 - 7 \cdot 8$
  $= 3 \cdot 19 - 7 \cdot (141 - 7 \cdot 19)$
  $= 3 \cdot 19 - 7 \cdot 141 + 49 \cdot 19$
  $= 52 \cdot 19 - 7 \cdot 141$
  $52 modulo 141$

  c. $a = 55, m = 89$
  $89 = 1 \cdot 55 + 34$
  $55 = 1 \cdot 34 + 21$
  $34 = 1 \cdot 21 + 13$
  $21 = 1 \cdot 13 + 8$
  $13 = 1 \cdot 8 + 5$
  $8 = 1 \cdot 5 + 3$
  $5 = 3 + 2$
  $3 = 2 + 1$
  $1 = 3 - 2$
  $= 3 - 1 \cdot (5 - 3)$
  $= 2 \cdot 3 - 5$
  $= 2 \cdot (8 - 5) - 5$
  $= 2 \cdot 8 - 3 \cdot 5$
  $= 2 \cdot 8 - 3 \cdot (13 - 8)$
  $= 5 \cdot 8 - 3 \cdot 13$
  $= 5 \cdot (21 - 13) - 3 \cdot 13$
  $= 5 \cdot 21 - 8 \cdot 13$
  $= 5 \cdot 21 - 8 \cdot (34 - 21)$
  $= 13 \cdot 21 - 8 \cdot 34$
  $= 13 \cdot (55 - 34) - 8 \cdot 34$

$= 13 \cdot 55 - 21 \cdot 34$
$= 13 \cdot 55 - 21 \cdot (89 - 55)$
$= 34 \cdot 55 - 21 \cdot 89$
$34 modulo 89$

d. $a = 89, m = 232$
$232 = 2 \cdot 89 + 54$
$89 = 54 + 35$
$54 = 35 + 19$
$35 = 19 + 16$
$19 = 16 + 3$
$16 = 5 \cdot 3 + 1$
$1 = 16 - 5 \cdot 3$
$= 16 - 5 \cdot (19 - 16)$
$= 6 \cdot 16 - 5 \cdot 19$
$= 6 \cdot (35 - 19) - 5 \cdot 19$
$= 6 \cdot 35 - 11 \cdot 19$
$= 6 \cdot 35 - 11 \cdot (54 - 35)$
$= 17 \cdot 35 - 11 \cdot 54$
$= 17 \cdot (89 - 54) - 11 \cdot 54$
$= 17 \cdot 89 - 28 \cdot 54$
$= 17 \cdot 89 - 28 \cdot (232 - 2 \cdot 89)$
$= 73 \cdot 89 - 28 \cdot 232$
$73 modulo 232$

- P1)

a. $\phi(3)$
1, 2 :: Total 2

b. $\phi(10)$
1, 3, 7, 9 :: Total 4

c. $\phi(17)$
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 :: Total 16

d. $\phi(6)$
1, 5 :: Total 2

e. $\phi(4)$
1, 3 :: Total 2

f. $\phi(8)$
1, 3, 5, 7 :: Total 4

g. $\phi(7)$
1, 2, 3, 4, 5, 6 :: Total 6

h. $\phi(5)$
1, 2, 3, 4 :: Total 4

i. $\phi(16)$
1, 3, 5, 7, 9, 11, 13, 15 :: Total 8

- P2)

a. $(100010)^7 mod 3$
$2 mod 3$

b. $(10003)^{41} mod 10$
$3 mod 10$

c. $(77)^{83} mod 8$
$5 mod 8$

d. $(77)^{-83} mod 8$
$5 mod 8$

e. $(109457)^{-44409} mod 10$
$7^3 mod 10$
$3 mod 10$

f. $(700*6+5)^{23}mod6$
   $5mod6$

g. $(700*6+5)^{23}mod7$
   5^5mod7
   $3mod7$

h. $(1089438345809)^{4444444444444444}mod10$
   $1mod10$

i. $(1089438345809)^{4444444444444444}mod5$
   $1mod5$

j. $(14)^{-16}mod17$
   1

- 23)

- 24) ATTACK
  a ,b ,c ,d ,e ,f ,g ,h ,i ,j ,k ,l
  00,01,02,03,04,05,06,07,08,09,10,11
  m ,n ,o ,p ,q ,r ,s ,t ,u ,v ,w ,x ,y ,z
  12,13,14,15,16,17,18,19,20,21,22,23,24,25
  $n = 43 \cdot 59 and e = 13$
  001919000210
  229913172117
  Done!

- 25) UPLOAD
  tip: next class use UPGRAYEDD
  $n = 53 \cdot 61 and e = 13$
  201511140003
  254527571211
  Done!

- 26) $17 modulo 52 \cdot 60$
  $3120 = 183 \cdot 17 + 9$
  $17 = 9 + 8$
  $9 = 8 + 1$
  $1 = 9 - 8$
  $\quad = 9 - (17 - 9)$
  $\quad = 2 \cdot 9 - 17$
  $\quad = 2 \cdot (3120 - 183 \cdot 17) - 17$
  $\quad = 2 \cdot 3120 - 367 \cdot 17$
  $2mod3120$
  3185203824602550