Group 2: Kyle, Jesus, Ying, Adam, Mason, Gage, Connor

Group 2 Homework 4

2.18

a) X =31
b) S = 27209
c) No solution because there is not an inverse of 697 mod 451
d) X = 986
e) X = 11733

2.23

a.) square root of 340 mod 437 (roots 19 and 23)

z^2 = 340 mod 19 = 17 mod 19

y^2 = 340 mod 23 = 18 mod 23

(finding the squares)

17 + 19 = 36 = $\mathbf{6^2}$

18 + 23 = 41 X

18 + 23 + 23 = 64 = $\mathbf{8^2}$

X = { 6 mod 19 ; 8 mod 23

19t + 6 = 8 mod 23

19t = 2 mod 23 (find a multiple of 19 such that it is +- 1 from a multiple of 23)

6 * (19t = 2 mod 23) => 114t = 12 mod 23

114 mod 23 = -1 => -t = 12 mod 23 => t = -12 mod 23 => -12 mod 23 => t = 11 mod 23

X = 19(11) + 6 = **215**

b.) square root of 253 mod 3143 (roots 7 and 449)

z squared = 253 mod 7

y squared = 253 mod 449

(finding the squares)

253 mod 7 = 1 so +-1

Group 2: Kyle, Jesus, Ying, Adam, Mason, Gage, Connor

253 + 449 +449 + 449 = 1600 = 40 squared so 40

X = 1 mod 7
X = 40 mod 449

449t + 40 = 1 mod 7

449t = -39 mod 7

449 mod 7 = 1 => t = -39 mod 7 => t = 3

X = 449(3) + 40 = **1387**

c.) 2583 mod 4189 (roots 59 and 71)

z squared = 2853 mod 59 = 1 so roots = +- 1

y squared = 2853 mod 71 = 64 so roots = +- 8

x = 1 mod 59
x = 8 mod 71

59t + 1 = 8 mod 71

6*(59t = 7 mod 71) = > 354t = 42 mod 71

354 mod 71 = -1

-t = 42 mod 71 => t = -42 mod 71 => t = 29

59(29) + 1 = **1712** and a second can be found from 4819 – 1712 = **2477** **1 and 2**

x = -1 mod 59
x = 8 mod 71

59 – 1 = 8 mod 71

6*(59t = 9 mod 71) = > 354t = 54 mod 71

354 mod 71 = -1

-t = 54 mod 71 => t = -54 mod 71 => t = 17

Group 2: Kyle, Jesus, Ying, Adam, Mason, Gage, Connor

59(17) – 1 = **1002** and a second can be found from 4819 – 1002 = **3187** **3 and 4**

d.) square root of 813 mod 868 (roots 4, 31, and 7)

z squared = 813 mod 4 = +- 1 mod 4 (roots)

y squared = 813 mod 7 = +- 1 mod 7 (roots)

w squared = 813 mod 31 = 7 mod 31

$a^{p+1/4} mod\ p = \ 7^{32/4} mod\ 31 = 10\ (root)$

X = $\begin{bmatrix} 1 \bmod 4 \\ 1 \bmod 7 \\ 10 \bmod 31 \end{bmatrix}$

x = 31t + 10 (set equal to second)

31t + 10 = 1 mod 7 => 31t = -9 mod 7

5*(31t = -9 mod 7) => 155t = -45 mod 7

155 mod 7 = 1

t = -45 mod 7 => t = 4 mod 7 => t = 7s + 4 (plug into third)

31t + 10 => 31(7s + 4) + 10 => 217s +134 (set equal to first)

217s + 134 = 1 mod 4

217 mod 4 = 1

s = -133 mod 4 => s = 3 (plug back in)

217(3) + 134 = **785** and we can get a second by 868-785 = **83** **1 and 2**

X = $\begin{bmatrix} -1 \bmod 4 \\ 1 \bmod 7 \\ 10 \bmod 31 \end{bmatrix}$

x = 31t + 10 (set equal to second)

31t + 10 = 1 mod 7 => 31t = -9 mod 7

5*(31t = -9 mod 7) => 155t = -45 mod 7

155 mod 7 = 1

Group 2: Kyle, Jesus, Ying, Adam, Mason, Gage, Connor

t = -45 mod 7 => t = 4 mod 7 => t = 7s + 4 (plug into third)

31t + 10 => 31(7s + 4) + 10 => 217s +134 (set equal to first)

217s + 134 = -1 mod 4

217 mod 4 = 1

s = -135 mod 4 => s = 1 (plug back in)

217(1) + 134 = **351** and a second can be found by 868 – 351 = **517** **3 and 4**

$$X = \begin{cases} -1 \bmod 4 \\ -1 \bmod 7 \\ 10 \bmod 31 \end{cases}$$

x = 31t + 10 (set equal to second)

31t + 10 = -1 mod 7 => 31t = -9 mod 7

5*(31t = -11 mod 7) => 155t = -55 mod 7

155 mod 7 = 1

t = -55 mod 7 => t = 1 mod 7 => t = 7s + 1 (plug into third)

31t + 10 => 31(7s + 1) + 10 => 217s + 41 (set equal to first)

217s + 41 = -1 mod 4

217 mod 4 = 1

s = -42 mod 4 => s = 2 (plug back in)

217(2) + 41 = **475** and a second can be found by 868 – 475 = **393** **5 and 6**

$$X = \begin{cases} 1 \bmod 4 \\ -1 \bmod 7 \\ 10 \bmod 31 \end{cases}$$

x = 31t + 10 (set equal to second)

31t + 10 = -1 mod 7 => 31t = -9 mod 7

5*(31t = -11 mod 7) => 155t = -55 mod 7

155 mod 7 = 1

t = -55 mod 7 => t = 1 mod 7 => t = 7s + 1 (plug into third)

Group 2: Kyle, Jesus, Ying, Adam, Mason, Gage, Connor

$31t + 10 \Rightarrow 31(7s + 1) + 10 \Rightarrow 217s + 41$ (set equal to first)

$217s + 41 = 1 \bmod 4$

$217 \bmod 4 = 1$

$s = -40 \bmod 4 \Rightarrow s = 0$ (plug back in)

$217(0) + 41 =$ **41** and a second can be found by $868 - 41 =$ **827** **7 and 8!**