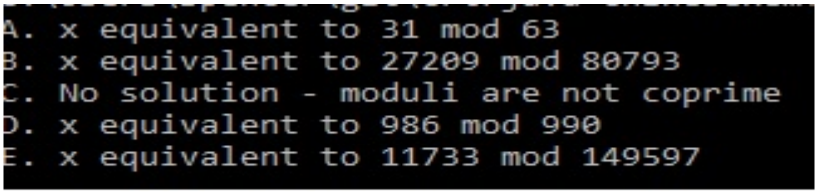
Homework 4

Group 5

David Skinner, Lauren Rainbolt, Daniel Decipulo, Jared Ramirez, Spencer Vaughn

2.18 – The answers to this problem are included in the .java file and image below.



```
A. x equivalent to 31 mod 63
B. x equivalent to 27209 mod 80793
C. No solution - moduli are not coprime
D. x equivalent to 986 mod 990
E. x equivalent to 11733 mod 149597
```

2.23 – Use the method described in Section 2.8.1 to find square roots modulo the following composite moduli.

(a) Find a square root of 340 modulo 437. (Note that 437 = 19 · 23.)

$$z^2 \equiv 340 \; mod \; 19 \equiv 17 \; mod \; 19$$

$$y^2 \equiv 340 \; mod \; 23 \equiv 18 \; mod \; 23$$

$$z = 6 \; and \; y = 8$$

$$6^2 = 36 \equiv 17 \; mod \; 19, 8^2 = 64 \equiv 18 \; mod \; 19$$

$$x \equiv \begin{cases} 6 \; mod \; 19 \\ 8 \; mod \; 23 \end{cases}$$

$$x = 19 + 6$$

$$114 \equiv -1 \; mod \; 23$$

$$\underline{x = 19 * 11 + 6 = 215}$$

(b) Find a square root of 253 modulo 3143.

$$3142 = 7 * 449$$

$$z^2 \equiv 253 \; mod \; 7 \equiv 1 \; mod \; 7$$

$$y^2 \equiv 253 \; mod \; 449$$

$$z = 1 \; and \; y = 40$$

$$x \equiv \begin{cases} 1 \; mod \; 7 \\ 40 \; mod \; 449 \end{cases}$$

$$\underline{449 \equiv 1 \; mod \; 7, x = 449 * 3 + 40 = 1387}$$

(c) Find four square roots of 2833 modulo 4189. (The modulus factors as 4189 = 59 · 71. Note that your four square roots should be distinct modulo 4189.)

$$4189 = 59 * 71$$

$$z^2 \equiv 2833 \; mod \; 59 \equiv 1 \; mod \; 59$$

$$y^2 \equiv 2833 \; mod \; 71 \equiv 64 \; mod \; 71$$

$$z = 1 \; and \; y = 8$$

Chinese Remainder Theorem(CRT)

$$x \equiv \begin{cases} 1 \; mod \; 59 \\ 8 \; mod \; 71 \end{cases}$$

$$354 \equiv -1 \; mod \; 71$$

$$x = 59 * 17 - 1 = 1002$$

$$-1002 \equiv 3187$$

$$4 \; roots: \begin{cases} 1712 \\ 2477 \\ 1002 \\ 3187 \end{cases}$$

(d) Find eight square roots of 813 modulo 868.

$$868 = 4 * 7 * 31$$

$$z_1^2 \equiv 813 \; mod \; 4 \equiv 1 \; mod \; 4$$

$$z_2^2 \equiv 813 \; mod \; 7 \equiv 1 \; mod \; 7$$

$$z_3^2 \equiv 813 \; mod \; 31 \equiv 7 \; mod \; 31$$

CRT

$$x \equiv \begin{cases} 1 \; mod \; 4 \\ 1 \; mod \; 7 \\ 10 \; mod \; 31 \end{cases}$$

$$217s + 134 \equiv 1 \; mod \; 4$$

$$217s \equiv -133 \; mod \; 4$$

$$s \equiv -1 \; mod \; 4$$

$$\underline{x = 217 * 3 + 134 = 785}$$

$$\underline{-785 \equiv 83}$$

$$x \equiv \begin{cases} -1 \; mod \; 4 \\ -1 \; mod \; 7 \\ 10 \; mod \; 31 \end{cases}$$

x = 31(7s+4) +10 = 217s +134

$$217s + 134 \equiv -1 \; mod \; 4$$

$$217s \equiv -135 \; mod \; 4$$

$$s \equiv 1 \; mod \; 4$$

$$\underline{x \;=\; 217 + 134 = 351}$$

$$\underline{-351 \equiv 517}$$

$$x \equiv \begin{cases} -1 \; mod \; 4 \\ -1 \; mod \; 7 \\ 10 \; mod \; 31 \end{cases}$$

$$x \;= 31(7s + 1) + 10 = 217s + 41$$

$$217s + 41 \equiv -1 \; mod \; 4$$

$$217s \equiv -42 \; mod \; 4$$

$$1 \equiv 2 \; mod \; 4$$

$$\underline{x \;=\; 434 + 41 = 475}$$

$$\underline{-475 \equiv 393}$$

$$x \equiv \begin{cases} 1 \; mod \; 4 \\ -1 \; mod \; 7 \\ 10 \; mod \; 31 \end{cases}$$

$$x \equiv \; 40 \; mod \; 868 \; and \; x \equiv 828 \; mod \; 868$$

$$8\ roots\colon \begin{cases} 41 \\ 83 \\ 351 \\ 393 \\ 475 \\ 517 \\ 785 \\ 827 \end{cases}$$