Group 3 Homework 6 Grading by Group 2

Problem 3.8

All of the answers seem correct. They use the same method I used, which is the same one from the book, and got the same answers I received. In conclusion, 100% good job.

Problem 3.12

u = 252426389 correct

v = -496549570 correct

1244183534252426389 \*732959706-496549570 = m mod 1889570071 correct

missing the final step, that is the value of m

Problem 3.14

a) 7 is a witness for 1105 being composite.

b) 7 is a witness for 294409 being composite.

c) All of the results for the Miller-Rabin Test are 1 or -1 so, 294439 is most likely prime as shown.

d) All of the results for the Miller-Rabin Test are 1 or -1 so, 118901509 is probably prime. However, the group stated that 118901509 is prime which the MRT does not show.

e) 11 is a witness for 118901521 being composite as one of the results after the first test is 1.

f) All of the results for the Miller-Rabin Test are 1 or -1 so, 118901527 is probably prime. However, the group stated that 118901527 is prime which the MRT does not show.

g) 11 is a witness for 118915387 being composite.

Problem 3.21

1. 37 \* 47 = 1739

37 and 47 are both prime

37 – 1 = 36 = 22 \* 32 is a product of small primes

**CORRECT**

1. 449 \* 491 = 220459

449 and 491 are both prime

449 – 1 = 448 = 26 \* 7 is a product of small primes

**CORRECT**

1. 6917 \* 6991 = 48356747

6917 and 6991 are both prime

6917 – 1 = 6916 = 22 \* 7 \* 13 \* 19 is a product of small primes

**CORRECT**

Problem 3.25

1. 227
2. 277
3. 499
4. 1637

All answers are correct, however the work seems to be very minimal in order to get these values. There seems to be a lot of steps missing.