Math 580: Quiz 3

Show ALL Work Name **Solutions**

Comment: This quiz does not require a lot of work if you are doing these problems correctly. As a consequence, it will be very difficult to get enough partial credit for an "A" unless you have the correct answers. I also want to see where your answers are coming from. You should check your work to make sure it is clear and easy to follow as well as correct.

1. Calculate the inverse of 43 modulo 4321. Give an answer that is in the set $\{0, 1, 2, \ldots, 4320\}$.

   Inverse of 43 modulo 4321: $\boxed{201}$ (from $\{0, 1, 2, \ldots, 4320\}$)

   Solution. Recall that to get the inverse of a modulo b, we solve $ax + by = 1$ and reduce the equation modulo b. Starting the Euclidean algorithm for obtaining the value of $\gcd(4321, 43)$, we obtain

   $$4321 = 43 \cdot 100 + 21$$

   $$43 = 21 \cdot 2 + 1.$$

   Working backwards now, we see that

   $$1 = 43 - 21 \cdot 2 = 43 - (4321 - 43 \cdot 100) \cdot 2 = 4321(-2) + 43 \cdot 201.$$

   Since $4321 \equiv 0 \pmod{4321}$, this reduces to (that is, implies the congruence)

   $$1 \equiv 43 \cdot 201 \pmod{4321}.$$

   Thus, the inverse of 43 modulo 4321 is 201. $\square$

2. Calculate the inverse of 4321 modulo 43. Give an answer that is in the set $\{0, 1, 2, \ldots, 42\}$. You can use your work for the problem above.

   Inverse of 4321 modulo 43: $\boxed{41}$ (from $\{0, 1, 2, \ldots, 42\}$)

   Solution. From the previous problem, we have

   $$4321(-2) + 43 \cdot 201 = 1.$$

   Since $43 \equiv 0 \pmod{43}$, this equation implies the congruence

   $$4321(-2) \equiv 1 \pmod{43}.$$

   Thus, the inverse of 4321 modulo 43 is $-2 \equiv 41 \pmod{43}$. $\square$