MATH 451
SPRING 2015
EXAM II PROBLEM SET

(1) The multiplicative inverse of 279 in $\mathbb{Z}_{401}$ is 23. Find a number x such that

$$279x \equiv 11 \pmod{401}.$$

(2) Bob has created a linear Caesar cipher of the form $[s] = [2][t] + [5]$. Looking at Bob's cipher, Alice quickly realizes it won't work. Give an argument Alice can use to show Bob the error of his ways. Since Bob is very stubborn this argument should include both a theoretical reason Bob's cipher won't work and specific examples where Bob's cipher fails.

(3) Carefully explain why multiplication is well defined in modular arithmetic.

(4) Find the multiplicative inverse of 3 in $\mathbb{Z}_{11}$.

(5) We know that since 6 and 15 have a common factor that 6 is a zero divisor in $\mathbb{Z}_{15}$. Explain why this is and based on the explanation find all the elements b of $\mathbb{Z}_{15}$ so that $[b][6] = [0]$.

(6) Use the following to facts to find *ALL* solutions to $12x \equiv 9 \pmod{6435}$
   (a) $12 \times 0 \equiv 12 \times 2145 \equiv 12 \times 4290 \equiv 0 \pmod{6435}$
   (b) $12 \times 537 \equiv 9 \pmod{6435}$.

(7) Bob is at it again and has created a new Caesar cipher of the form $[s] = [25][t] + [6]$. He tells Alice that he is going to make it extra hard to break the cipher by applying his cipher twice to every letter. Alice thinks for a moment and realizes that applying the cipher twice does not make it any more difficult to break and even worse, with Bob's choice of Caesar cipher it is a particularly bad idea. Explain why Alice knows
   - applying a Caesar cipher twice does not make the cipher any harder to break, and
   - applying the Caesar cipher Bob is considering twice is a particularly bad idea.

   In the context of modular arithmetic, explain why a number is either a zero divisor or has a multiplicative inverse.

(8) Use a general technique to find the multiplicative inverse of 3 in $\mathbb{Z}_{17}$.

(9) Use the following to facts to find *ALL* solutions to $12x \equiv 9 \pmod{6435}$
   (a) $12 \times 0 \equiv 12 \times 2145 \equiv 12 \times 4290 \equiv 0 \pmod{6435}$
   (b) $12 \times 537 \equiv 9 \pmod{6435}$.

(10) Use the fact that the multiplicative inverse of 398 in $\mathbb{Z}_{451}$ is 17 to find a number x such that

$$398x \equiv 12 \pmod{451}.$$