CMPS/MATH 2170 Discrete Mathematics – Fall 15

11/4/15

8. Homework

Due **11/12/15** at the beginning of the lab

1. **No Inverse (6 points)**
   Use a proof by contradiction to prove that $gcd(a, m) = d > 1$ implies that there is no inverse of a modulo m.
   (Hint: Use that d is a common divisor of a and m.)

2. **Modular Inverse (6 points)**
   Compute an inverse of 288 modulo 1837 by running the Euclidean algorithm and determining the Bézout coefficients.

3. **Solving a Linear Congruence (4 points)**
   Describe all solutions of the linear congruence $7x \equiv 42 \pmod 9$. Show your work.

4. **Decryption (6 points)**
   You intercepted the message 1685 0238 2456 that was sent to Carola. Carola's public key is $(59, 2627)$. (You think is odd because those are some pretty small numbers.) You think you can decrypt the message...

   - Factor n by brute-force trying out small prime numbers.
   - Compute the decryption key d.
   - Just as in class, assume that letters are encoded with 2-digit numbers $A = 00, \ldots, Z = 25$, and that four digits are grouped together to form a message symbol. Decrypt the message.

   Show your work. You can use an online tool such as WolframAlpha to help with modular exponentiation.

5. **Signature (4 points)**
   Alice wants to send the message "AT BEADTREE" to her friends. We know from class that Alice's RSA public key is $(13, 2537)$ and her secret key is $(361, 2537)$. Help Alice by digitally signing the message for her.