

Math 11200/20 homework 7
Due date: Friday, November 18, 2016

Note: You shouldn't need to use a calculator for these problems.

Please present your solutions clearly and in an organized way. Think of it this way: if you show it to another student in this class, he/she should be able to understand it without needing to ask you questions.

Problem 7.1. Exercise 6.4 from the textbook.

Problem 7.2. Exercise 6.5 from the textbook.

Problem 7.3. What is the remainder when you divide the following numbers by 9? By 11? (You don't need a calculator. And you don't actually need to do the divisions!)

- (a) 85,140
- (b) 111,650
- (c) 1,268,904
- (d) 24,248,484

Problem 7.4. Exercise 6.7 from the textbook. We didn't talk about "residue classes," so do the following instead: for (a), find the remainder when $6!$ is divided by 7. Do the same for (b), (c), (d). (Recall $6!$ is "6 factorial" and is equal to $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$.)

Problem 7.5. Recall from the midterm that the solution to $x^4 \equiv 1 \pmod{5}$ is $x \equiv 1, 2, 3, 4 \pmod{5}$. What if we look at the congruence $x^{m-1} \equiv 1 \pmod{m}$ for other values of m ? What do you observe? (You don't need to prove your observations.)

Problem 7.6. Solve these systems of congruences (if possible):

- (a) $x \equiv 0 \pmod{5}$ and $x \equiv 0 \pmod{7}$
- (b) $x \equiv 2 \pmod{5}$ and $x \equiv 8 \pmod{10}$
- (c) $x \equiv 3 \pmod{6}$ and $x \equiv 6 \pmod{7}$
- (d) $x \equiv 4 \pmod{7}$ and $x \equiv 7 \pmod{9}$
- (e) $x \equiv 0 \pmod{4}$ and $x \equiv 3 \pmod{6}$

(If you need help, see the example on page 2 of http://www.cs.xu.edu/math/math302/08f/06_CRT.pdf.)

Problem 7.7.

- (a) Encrypt "THIS IS SECRET" using the encryption function $f(x) = 7x + 1 \pmod{26}$. What is the decryption function g ?
- (b) Encrypt "YOU CANNOT DECODE THIS" using the encryption function $f(x) = 13x + 1 \pmod{26}$. What is the decryption function g ?

Problem 7.8. I used the function $f(x) = 15x + 18 \pmod{26}$ to encrypt a message. The ciphertext is "WNOJRUENSJTO IC PGF" What is the original message?