Homework Sections 4.4

Max's lecture
MATH 55

Due July 11, 2019

Note: All problems are taken from Rosen, Discrete Mathematics and its applications, 8th ed. Have fun, and please feel free to ask each other and me for help!

Exercise 4.4.6bc. Find an inverse of a modulo m for each of these pairs of relatively prime integers using the method followed in Example 2.

(a) $a = 34$ and $m = 89$

(b) $a = 144$ and $m = 233$

Exercise 4.4.8. Show that an inverse of a modulo m, where a is an integer and $m > 2$ is a positive integer, does not exist if $\gcd(a, m) > 1$.

Exercise 4.4.12b. Solve the congruence using the inverse in 6c.

$$144x \equiv 4(\mod 233)$$

Exercise 4.4.16. (a) Show that the positive integers less than 11, except 1 and 10, can be split into pairs of integers such that each pair consists of integers that are inverses of each other modulo 11.

(b) Use part (a) to show that $10! \equiv -1(\mod 11)$

Exercise 4.4.32. Which integers are divisible by 5 but leave a remainder of 1 when divided by 3?

Exercise 4.4.34. Use Fermat's little theorem to find $23^{1002} \mod 41$

Exercise 4.4.38. (a) Use Fermat's little theorem to compute $3^{302} \mod 5$, $3^{302} \mod 7$, and $3^{302} \mod 11$.

(b) Use your resluts from part (a) and the Chinese remainder theorem to find $3^{302} \mod 385$. (Note that 385 is the product of 5,7, and 11)