115 Homework 7

Due Friday November 19

Question 1 (Midterm *déja vu*.) Prove that the system of congruences

$$x \equiv a_1 \bmod m_1 \, , \dots , x \equiv a_r \bmod m_r \, ,$$

has a unique solution modulo $m_1 \dots m_r$ when $m_1, \dots, m_r$ are pairwise relatively prime.

Question 2 (Rosen 6.1.10) What is the remainder when 6^{2000} is divided by 11?

Question 3 (Rosen 6.1.34) Show that if p is prime and $0 < k < p$, then

$$(p-k)!(k-1)! \equiv (-1)^k \bmod p \, .$$

Question 4 (Rosen 6.1.40,41) Utilize the fact that if p is prime and $0 < k < p$ then $p | \binom{p}{k}$ to show that integers a and b obey $(a+b)^p = a^p + b^p \bmod p$. Now give an inductive proof of Fermat's little theorem.

Question 5 (Rosen 6.2.2) Show 45 is pseudoprime base 17 and 19.

Question 6 (Rosen 6.2.20) Show all Carmichael numbers are squarefree.