CS 581 Homework 9

Due on 03/22/2018

Problem 1.

a) Compute $gcd(85, 289)$ using Euclid's extended algorithm.

b) Compute x and y such that $85x + 289y = gcd(85, 289)$. Show your work.

Problem 2.

Use Fermat's little theorem to compute 3^{62} mod 7. Show your work.

Problem 3.

a) Show that $n^7 - n$ is divisible by 42 for every positive integer n.

b) Show that every prime not equal to 2 or 5 divides infinitely many of the numbers 1, 11, 111, 1111, etc.

c) Show that if $p > 3$ is a prime, then $p^2 \equiv 1 \pmod{24}$.

Problem 4.

a) Prove that if p is prime, and $0 < k < p$, then $p \mid \binom{p}{k}$.

b) Prove that for all integers a and b and all primes p,

$$(a + b)^p \equiv a^p + b^p \ (mod\ p) \tag{1}$$

Problem 5.

Let a be 1 in the previous problem, and use its conclusion to prove Fermat's little theorem.