Math 435 Number Theory I
Problem Set 6

Due: Friday October 14:

1) Suppose p is primes.

a) Suppose $\gcd(d, p-1) = 1$. Prove that $[1]$ is the unique congruence class solving $X^d \equiv 1 \pmod{p}$ in $\mathbb{Z}_p$. [Hint: Use the Bezout Property.]

b) Suppose $d|(p-1)$. Prove that $X^d \equiv 1 \pmod{p}$ has d incongruent solutions in $\mathbb{Z}_p$. [Hint: $(X^d - 1)$ divides $(X^{p-1} - 1)$.]

c) Conclude that if p and q are primes, then $X^q \equiv 1 \pmod{p}$ has a unique solution in $\mathbb{Z}_p$ unless $p \equiv 1 \pmod{q}$ in which case there are q solutions in $\mathbb{Z}_p$.

2) Using the methods of §4.3 solve

$$X^5 + X^3 + 1 \equiv 0 \pmod{27}$$

3) Using the methods from §4.3 and the Chinese Remainder Theorem find all solutions to

$$X^2 + 5X + 24 \equiv 0 \pmod{36}$$