Math 115 - Midterm 1+2 Definitions

1. **Theorem 2.25.** If the degree of the congruence $f(x) \equiv 0 \pmod{p}$ is $n \geq p$, then we can reduce the congruence by computing $\frac{f(x)}{x^p - x}$ by long division of polynomials and taking the remainder polynomial $r(x)$ and we get that the solutions to $r(x) \equiv 0 \pmod{p}$ are precisely those of $f(x) \equiv 0 \pmod{p}$. We also note that the degree of $r(x) \equiv 0 \pmod{p}$ will be less than p.

2. **Theorem 2.26.** The congruence $f(x) \equiv 0 \pmod{p}$ of degree n has at most n solutions.

3. **Corollary 2.27.** If $f(x) \equiv 0 \pmod{p}$ has more than n solutions, then p divides each of the coefficients of $f(x)$.

4. **Theorem 2.28.** If $F : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, then there exists an $f \in \mathbb{Z}[x]$ with degree at most $p-1$ such that $F(x) \equiv f(x) \pmod{p}$ for all residue classes $x \pmod{p}$.

5. **Theorem 2.29.** $f(x) \equiv 0 \pmod{p}$ of degree n has precisely n solutions iff $x^p - x = q(x)f(x) + ps(x)$ where $q(x)$ has degree $p - n$ and $s(x)$ is either 0 or has degree less than n.

6. **Corollary 2.30.** If $d \mid (p-1)$, then the congruence $x^d \equiv 1 \pmod{p}$ has precisely d solutions.