# Worksheet 3

1. Assume $n \geq p$ and $n \equiv r \mod (p-1)$, where $1 \leq r \leq p-1$, then $x^n \equiv x^r \mod p$ for all $x$.

2. Use (1) to reduce the polynomial $x^{11} + 2x^8 + x^5 + 3x^9 + 4x^3 + 1 \mod 5$.

3. (High School dream). Prove $(x+y)^p \equiv x^p + y^p \mod p$.

4. Prove that the system of linear congruences in one variable given by

$$x \equiv b_1 \mod m_1$$

$$x \equiv b_2 \mod m_2$$

   is solvable if and only if $\gcd(m_1, m_2) | (b_1 - b_2)$. In this case, prove that the solution is unique modulo $\text{lcm}(m_1, m_2)$.

5. Let $\{r_1, r_2, \cdots r_{\phi(m)}\}$ be a reduced residue system modulo m. Prove that m divides $r_1 + r_2 + \cdots + r_{\phi(m)}$ for $m > 2$.

   Hint: Show $(r_i, m) = 1$, then $(m - r_i, m) = 1$.

   Show $\phi(m)$ is even.