MATH 152: PROBLEM SET 3

DUE OCTOBER 16

1. For any fixed positive integer n show that there are only finitely many solutions to the equation $\phi(x) = n$.

2. Let g be a primitive root $\pmod p$. Show that $(p-1)! \equiv g \cdot g^2 \cdot g^3 \cdot \cdots \cdot g^{p-1} \equiv g^{p(p-1)/2} \pmod p$, and conclude Wilson's theorem.

3. Let k and a be positive integers with $a \geq 2$. Show that $k \mid \phi(a^k - 1)$. (Hint: consider the order of $a \pmod{a^k - 1}$.)

4. Let k be a natural number, and p be a prime. Show that

$$\sum_{n=1}^{p-1} n^k \equiv \begin{cases} -1 \pmod p & \text{if } (p-1)|k \\ 0 \pmod p & \text{if } (p-1) \nmid k. \end{cases}$$

5. Let $p \neq 2, 5$ be a prime. The decimal expansion of $1/p$ will then have a certain number of digits that repeat. Prove that the number of such digits equals the order of $10 \pmod p$.

6. In class we discussed how primitive roots $\pmod p$ are lifted to primitive roots $\pmod{p^2}$. This problem gives a generalization of that strategy. Let f be a polynomial of degree d with leading coefficient 1, and let f' denote its derivative. Let a be a solution to $f(x) \equiv 0 \pmod p$.

(i). If $f'(a) \not\equiv 0 \pmod p$ then show that the solution $a \pmod p$ lifts (or gives rise) to a unique solution $\pmod{p^2}$.

(ii). If $f'(a) \equiv 0 \pmod p$, but $f(a) \not\equiv 0 \pmod{p^2}$ then show that a does not lift to a solution $\pmod{p^2}$.

(iii). If $f'(a) \equiv 0 \pmod p$ and $f(a) \equiv 0 \pmod{p^2}$ show that a gives rise to p solutions $\pmod{p^2}$.