Math 53
Homework 6

due March 6 in class

1. Prove that there are infinitely many primes that are 5 mod6.

2. Follow the following steps to prove that there are infinitely many primes $q \equiv 1 \mod 3$:

   (a) Suppose there are finitely many primes $\equiv 1 \mod 3$, say $p_1, p_2, \ldots, p_k$. Consider $a = 3p_1p_2 \ldots p_k$. Prove that if q is a prime divisor of $N = a^2 + a + 1$, then the order of a mod q is 3.

   (b) Show that $q \equiv 1 \mod 3$.

   (c) Show that therefore $q \mid a$. Show this is a contradiction to the statement that $p_1, p_2, \ldots p_k$ are all the primes $\equiv 1 \mod 3$.

3. Show that if p is an odd prime and $p \mid x^{2^r} + 1$, then $p \equiv 1 \mod 2^{r+1}$. Deduce that there are infinitely many primes congruent to 1 modulo any fixed power of 2.

4. Suppose that p is prime, and that $p \not| a$. Let $\operatorname{ord}_p a = t$ and let $p^z | a^t - 1$ but $p^{z+1} \not| a^t - 1$. Prove that if $p > 2$ or $z > 1$,

$$t_n = \operatorname{ord}_{p^n} a = \begin{cases} t & \text{for } n \leq z, \\ tp^{n-z} & \text{for } n \geq z. \end{cases}$$

5. Primitive Roots modulo p^n for p an odd prime.

   (a) Show that if g is a primitive root of p and $g^{p-1} \not\equiv 1 \pmod{p^2}$ then g is a primitive root of p^n for all n. (Recall that for g to be a primitive root mod m you need $\operatorname{ord}_m g = \phi(m)$.)

   (b) Show that if $g^{p-1} \equiv 1 \pmod{p^2}$, then $(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$.

   (c) Conclude that there is always a primitive root modulo p^n.

6. Show that there is a primitive root mod n if and only if $n = 2, 4, p^k, 2p^k$ for any odd prime p and any $k \geq 1$.