1. Find the number of incongruent roots modulo 13 of each of the following polynomials:
   Hint: All of these can be done without actually finding any roots of the polynomials.

   (a) $x^2 + 1$

   (b) $x^2 - 5$

   (c) $x^6 - 1$

2. Find a complete set of incongruent primitive roots of 13.

3. Show that if p is prime and $p \equiv 1 \mod 4$, then there is an integer x with $x^2 \equiv -1 \mod p$.
   Hint: What does $p \equiv 1 \mod 4$ say about there being elements of order 4 mod p?

4. Suppose that n is a positive integer and a and b are integers relatively prime to n.

   (a) Show that if $ab \equiv 1 \mod n$, then for any positive integer r, $a^r \equiv 1 \mod n$ if and only if $b^r \equiv 1 \mod n$. Conclude that $\text{ord}_n(a) = \text{ord}_n(b)$.

   (b) Now suppose that $\text{ord}_n(a)$ and $\text{ord}_n(b)$ are relatively prime. Show that

$$\text{ord}_n(ab) = \text{ord}_n(a) \cdot \text{ord}_n(b)$$

5. Let p be prime and suppose that $p-1 = q_1^{e_1} \cdots q_g^{e_g}$ where $q_1, \ldots, q_g$ are distinct primes and $e_1, \ldots, e_g \geqslant 1$. In this problem, we construct a primitive root mod p

   (a) Show that there are integers $a_1, a_2, \ldots, a_g$ so that $\operatorname{ord}_p(a_i) = q_i^{e_i}$ for each $1 \leqslant i \leqslant g$

   (b) Use the previous exercise to show that $a_1 a_2 \cdots a_g$ is a primitive root modulo p

(c) Use this procedure to find a primitive root mod 29.

Draft of Homework 5 Problems

1. Suppose that r is a primitive root mod p for an odd prime p. Show that

$$r^{\frac{p-1}{2}} \equiv -1 \mod p$$

   Hint: What happens if you square both sides?

2. Suppose that p is an odd prime and S is a set of $\varphi(p-1)$ primitive roots modulo p. What is the least positive residue of the product of all elements of S modulo p?

3. Suppose that p is prime and $p = 2q + 1$ where q is an odd prime. Show that for any positive integer n with $1 < n < p - 1$, $-n^2$ is a primitive root modulo p.

4. Show that the integer m has a primitive root if and only if the only solutions to the congruence $x^2 \equiv 1 \mod m$ are $x \equiv \pm 1 \mod m$.