Problem Set 7

Due: March 31st, 5pm

1 Formal proofs

For each problem in this section, you must give a complete and rigorous proof. Your arguments should be clear, logically ordered, and written in full sentences.

In particular, state all assumptions explicitly and define all notation. Justify every nontrivial step.

1. (1 point) Let a be a primitive root modulo p. Prove that a^k is also a primitive root modulo p if and only if $\gcd(k, p-1) = 1$.
2. (1 point) Show that if a is a primitive root modulo p, then $a^{(p-1)/2} \equiv -1 \pmod{p}$.
3. (2 points) Let n be a positive integer. By Euler's theorem, for any $a \in \mathbb{Z}_n^\times$, we have $a^{\varphi(n)} \equiv 1 \pmod{n}$, and so $\mathrm{ord}_n(a)$ divides $\varphi(n)$. We say a is a primitive root modulo n if $\mathrm{ord}_n(a) = \varphi(n)$. Prove that if $n = pq$ for distinct odd primes p and q, then there is no primitive root modulo n.

2 Demonstrations

For problems in this section, you still need to give complete mathematical reasoning to support your answers. I should be able to follow and understand your work, but it doesn't have to be organized into a formal proof.

4. (1 point) Let n be a positive integer and $a \in \mathbb{Z}_n^\times$ with $d = \mathrm{ord}_n(a)$. Find a formula for $\mathrm{ord}_n(a^k)$ in terms of d and k, and show that your formula is correct.

3 Explorations

In this section, I'm looking for answers that are supported by evidence, but you don't have to prove your answers. Please **include all code snippets** when using computational tools, failure to do so may result in loss of points.

5. (1 point) Let p be a prime. For each divisor d of $p-1$, make a conjecture as to how many elements of $\mathbb{Z}_p^\times$ have order d. Test your conjecture for primes up to 50. (You may

want to start with the computational part to gather data, and then look for patterns in the data to help you make your conjecture.)

6. (1 point) For each prime $p \leq 100$, find the smallest primitive root modulo p.
   (a) Create a table showing the smallest primitive root for each prime up to 100.
   (b) What is the most common smallest primitive root? How many primes have this value as their smallest primitive root?
   (c) What is the largest value that appears as a smallest primitive root for primes up to 100?
   (d) Do you notice any patterns in your data? For instance, are there primes where the smallest primitive root is unusually large?
7. (1 point) Investigate which positive integers n have primitive roots.
   (a) For each n from 1 to 30, determine whether there exists a primitive root modulo n. (Recall: a is a primitive root modulo n if $\text{ord}_n(a) = \varphi(n)$.)
   (b) Based on your data, make a conjecture about which types of numbers have primitive roots.
   (c) Test your findings for a few values beyond 30, such as $n = 50, 54, 64, 81, 100, 125, 128, 162$.