CPSC 418/MATH 318 Practice Problems

Primitive Roots, Discrete Logarithms

Fermat's Little Theorem states that $a^{p-1} \equiv 1 \pmod{p}$ for all $a \in \mathbb{Z}_p^*$. Recall that a *primitive root* of a prime p is an integer $g \in \mathbb{Z}_p^*$ such that the smallest positive exponent k with $g^k \equiv 1 \pmod{p}$ is $p-1$.

An integer g is a primitive root of p if and only if the powers

$$g^0 \pmod{p}\,,\ g^1 \pmod{p}\,,\ \ldots\,,\ g^{p-2} \pmod{p}$$

are all distinct and make up the entire collection of elements in $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$.

The *discrete logarithm* of an element $a \in \mathbb{Z}_p^*$ (with respect to a primitive root g) is the unique integer $x \in \{0, 1, \ldots, p-2\}$ with $g^x \equiv a \pmod{p}$.

1. True or false? Verify your claims.
   (a) 2 is a primitive root of 7.
   (b) 3 is a primitive root of 7
   (c) 5 is a primitive root of 11.
   (d) 4 is a primitive root of 13.

2. Use trial and error to find a primitive root of 19.

3. Let p be a prime, $g \in \mathbb{Z}_p^*$, and $h \equiv g^2 \pmod{p}$. Can h be a primitive root of p? Why or why not?

4. Let p be a prime and g a primitive root of p.
   (a) Is it always true that $-g$ is a primitive root of p? Prove or give a counterexample.
   (b) Is it always true that the inverse of g modulo p is a primitive root of p? Prove or give a counterexample.

5. (a) Verify that 2 is a primitive root of 11.
   (b) Use trial and error to find the discrete logarithm of 5 with respect to 2 modulo 11.
   (c) Use trial and error to find the discrete logarithm of 7 with respect to 2 modulo 11.

6. Let p be a prime and g a primitive root of p.
   (a) What is the discrete logarithm of 1?
   (b) What is the discrete logarithm of g?
   (c) What is the discrete logarithm of -1 when p is odd?