Assignment 9

True/False questions, not to turn in:

- The order of an element modulo n is always 1 or an even number.
- Let $p > 2$ be a prime. A polynomial of odd degree over $\mathbb{Z}_p$ necessarily has a root.
- If a polynomial $f(x)$ with integer coefficients has no solutions modulo a prime p, then it also has no solution modulo other primes.
- If $\bar{a}$ is a primitive root modulo a prime p, then $\bar{a}$ is also a primitive root modulo other primes.
- If $\bar{a} = \bar{b}^2$ then a cannot be a primitive root.

Questions to turn in:

1. Find a primitive root modulo $p = 53$ using the techniques we learned in class. Use it to find at least 2 more primitive roots.
2. In normal calculus we have the formula: $\log_a(c) = \frac{\log_b(c)}{\log_b(a)}$. Is the same true when discussing discrete logarithms in $\mathbb{Z}_p$? i.e. when a, b are primitive roots modulo p, and $\bar{c}$ is a nonzero element, is it the case that $\log_b(c) = \log_a(c)\log_b(a)$? Either prove or provide a counterexample.
3. Suppose that $f\colon \mathbb{Z}_p^* \to \mathbb{Z}_{p-1}$ is a well-defined, 1-1 function from the set of nonzero residues modulo p to the set of residues modulo $p-1$ that has the property that $f(xy) = f(x) + f(y)$ for all $x, y \in \mathbb{Z}_p^*$. Show that it is in fact a discrete logarithm function for some primitive root. (All discrete logarithms would have those properties). Here are some steps to help you:
    - Show there must be an a such that $f(a) = 1$.
    - Show that a is a primitive root, i.e. that the order of a is $p-1$. The function f and its properties can help you with that.
    - Show that f equals the discrete logarithm with base a.
4. Illustrate the Diffie-Hellman protocol for $p = 53$, using the primitive root you found in question 1. You will need to use two randomly selected numbers between 1 and $51 = 53 - 2$, use the numbers 10 and 14. What is the secret shared key in this instance, and what are the messages that Alice and Bob exchange?
5. According to our theory, the polynomial $x^{13} - 1$ would have exactly 13 roots in $\mathbb{Z}_{53}$ (make sure you understand why). In other words, there are exactly 13 elements in $\mathbb{Z}_{53}$ such that $x^{13} = 1$. Find those elements. Here are some steps to help you:
    - Find one such element that is not 1. Our technique for finding a primitive root should help.
    - Try powers of that element. Explain why they would also have this property.