Math 173A - Discrete Logarithms

1. Let g be a primitive root for $\mathbb{F}_p$.

   (a) Suppose that $x = a$ and $x = b$ are both integer solutions to the congruence $g^x \equiv h \pmod{p}$. Prove that $a \equiv b \pmod{p-1}$. Explain why this means the map

   $$\log_g : \mathbb{F}_p^\times \to \mathbb{Z}/(p-1)\mathbb{Z}$$

   $$g^x \mapsto x \pmod{p-1}$$

   is well-defined.

   (b) Prove that $\log_g(h_1 h_2) \equiv \log_g(h_1) + \log_g(h_2) \pmod{p-1}$ for all $h_1, h_2 \in \mathbb{F}_p^\times$.

   (c) Prove that $\log_g(h^n) \equiv n \log_g(h)$ for all $h \in \mathbb{F}_p^\times$ and $n \in \mathbb{Z}$.

2. This exercise describes a public key cryptosystem that requires Alice and Bob to exchange several messages. We illustrate it with an example using small numbers.

   Alice and Bob publicly agree on a prime $p = 23$. Suppose Alice wants to send Bob the message $m = 11$. She chooses a random exponent $a = 3$ and sends the number $u \equiv m^a \equiv 20 \pmod{23}$ to Bob. Bob chooses a random exponent $b = 9$ and sends $v \equiv u^b \equiv 5 \pmod{23}$ back to Alice. Alice then computes $w \equiv v^{15} \equiv 19 \pmod{23}$ and sends w to Bob. Finally, Bob computes $w^5 \equiv 11 \pmod{23}$ to recover Alice's original message.

   (a) Explain why this system works. In particular, how are Alice's exponents $a = 3$ and 15 related? Likewise, how are Bob's exponents $b = 9$ and 5 related?

   (b) How would you explain this cryptosystem in general? That is, how does it work outside of just this example?

   (c) Can you break this system if you can solve the discrete logarithm problem?