Name: Solutions

Directions: Show all work. No credit for answers without work.

1. **[2 points]** Compute $\log_6(2)$ in $\mathbb{F}_{13}$.

$6^2 = 36 = 36 - 26 = 10$
$6^3 = 10 \cdot 6 = 60 = 60 - 52 = 8$
$6^4 = 8 \cdot 6 = 48 = 48 - 52 = -4 = 9$
$6^5 = 9 \cdot 6 = 54 = 54 - 52 = 2$

x	0	1	2	3	4	5
6^x	1	6	10	8	9	2

So $\log_6(2) = 5$

2. **[2 points]** Suppose that g_1 is a primitive root in $\mathbb{F}_p$ and g_2 is not. What is different between the functions $\log_{g_1}(y)$ and $\log_{g_2}(y)$?

$\log_{g_1}(y)$ is defined for all $y \in \mathbb{F}_p^*$ but $\log_{g_2}(y)$ is defined only on a subset of $\mathbb{F}_p^*$.

3. **[2 parts, 3 points each]** You want to use the Diffie-Hellman protocol to share a private key with your friend. You and your friend agree to use prime $p = 11$ and base $g = 2$.

   (a) You choose the random element 8. What do you send to your friend?

$A = g^a = 2^8 = (2^4)^2 = (16)^2 = 5^2 = 25 = \boxed{3}$

   (b) Your friend responds with the number 5. What is your shared secret?

Shared secret: $g^{ab} = B^a = 5^8 = (5^4)^2 = \left((5^2)^2\right)^2$
$= \left((25)^2\right)^2 = (3^2)^2 = 9^2 = 81 = \boxed{4}$