USS: Introduction to mathematical cryptography
Thursday July 21 problems

1. In this problem we will consider the group $G = (\mathbb{Z}/p\mathbb{Z})^\times$ for p an odd prime, under multiplication. Throughout suppose that g generates this group, and write $\log_g h \equiv a \pmod{p-1}$ if $h \in (\mathbb{Z}/p\mathbb{Z})^\times$ is such that $h \equiv g^a \pmod{p}$.

   (a) Prove that $g^a \equiv g^b \pmod{p}$ if and only if $a \equiv b \pmod{p-1}$, so that the value of $\log_g h$ is indeed well-defined modulo $p-1$ for any $h \in (\mathbb{Z}/p\mathbb{Z})^\times$.

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

   (c) Show that the equation $x^2 \equiv h \pmod{p}$ has a solution if and only if $\log_g(h)$ is even. (Does it even make sense to say that $\log_g(h)$ is even?)

2. This is Trappe and Washington's problem 2 in Section 7.6.

   (a) Compute $6^5 \pmod{11}$.

   (b) It is a fact that $(\mathbb{Z}/11\mathbb{Z})^\times = \langle 2 \rangle$. Let x be such that $2^x \equiv 6 \pmod{11}$. Without computing x, is x odd or even?

3. This is Trappe and Washington's problem 6 in Section 7.6. It is a fact that $(\mathbb{Z}/101\mathbb{Z})^\times = \langle 2 \rangle$, and $\log_2 3 \equiv 69 \pmod{100}$ and $\log_2 5 \equiv 24 \pmod{100}$.

   (a) Using the fact that $24 = 2^3 \cdot 3$, compute $\log_2 24 \pmod{100}$.

   (b) Using the fact that $5^3 \equiv 24 \pmod{101}$, compute $\log_2 24 \pmod{100}$.

4. Find an odd prime p such that $(\mathbb{Z}/p\mathbb{Z})^\times \neq \langle 2 \rangle$.

5. Use the baby steps, giant steps algorithm to solve the problem

$$11^x \equiv 21 \pmod{71}.$$