Chapter 7 Homework 1-3, 6, 7, 10, 11

1.

(a) Let $p = 13$. Compute $L_2(3)$.
We want to find $x \ni 2^x \equiv 3 \pmod{13}$. Since $2^4 = 16 \equiv 3 \pmod{13}$, we have that $x = 4$.

(b) Show that $L_2(11) = 7$.
$2^7 = 128 \equiv 11 \pmod{13}$

2.

(a) Compute $6^5 \pmod{11}$.
$6^5 = 7776 \equiv 10 \pmod{11}$

(b) Let $p = 11$. Then 2 is a primitive root. Suppose $2^x \equiv 6 \pmod{11}$. Without finding the value of x, determine whether x is even or odd.
$\beta^{\frac{p-1}{2}} \equiv 6^{\frac{11-1}{2}} \equiv 6^5 \equiv -1 \pmod{11}$. Since we get -1, x must be odd.

3. It can be shown that 5 is a primitive root for the prime 1223. You want to solve the discrete logarithm problem $5^x \equiv 3 \pmod{1223}$. Given that $3^{611} \equiv 1 \pmod{1223}$, determine whether x is even or odd.
$\beta^{\frac{p-1}{2}} \equiv 3^{611} \equiv 1 \pmod{1223}$. Since we get 1, x must be even.

6. Let $p = 101$, so 2 is a primitive root. It can be shown that $L_2(3) = 69$ and $L_2(5) = 24$.

(a) Using the fact that $24 = 2^3 \cdot 3$, evaluate $L_2(24)$.
we are given that $2^{69} \equiv 3 \pmod{101}$. We want to find $2^x \equiv 24 \pmod{101}$.

$$\begin{aligned} 2^x &\equiv 2^3 \cdot 3 \pmod{101} \\ &\equiv 2^3 \cdot 2^{69} \pmod{101} \\ &\equiv 2^{72} \pmod{101} \end{aligned}$$

So, $x = 72$.

(b) Using the fact that $5^3 \equiv 24 \pmod{101}$, evaluate $L_2(24)$.

$$\begin{aligned} 2^x &\equiv 24 \pmod{101} \\ &\equiv 5^3 \pmod{101} \\ &\equiv (2^{24})^3 \pmod{101} \\ &\equiv 2^{72} \pmod{101} \end{aligned}$$

So again, $x = 72$.

7. Suppose you know that

$$3^6 \equiv 44 \pmod{137} \qquad\qquad 3^{10} \equiv 2 \pmod{137}$$

Find a value of x with $0 \leq x \leq 135$ such that $3^x \equiv 11 (\text{mod } 137)$.

We want

$$3^x \equiv 11 (\text{mod } 137) \Rightarrow L_3(11) = x$$

Now, $11 = \frac{44}{4} = \frac{44}{2^2}$ and $3^{136} \equiv 1 (\text{mod } 137)$. So, using properties of logarithms, we have

$$3^x \equiv 3^{6-2\cdot 10} \equiv 3^{-14} \equiv 3^{-14+136} \equiv 3^{122} (\text{mod } 137)$$

So, $x = 122$.

10. In the Diffie-Hellman key exchange protocol, Alice and Bob choose a primitive root α for a large prime p. Alice sends $x_1 \equiv \alpha^a (\text{mod } p)$ to Bob, and Bob sends $x_2 \equiv \alpha^b (\text{mod } p)$ to Alice. Suppose Eve bribes Bob to tell her the values of b and x_2. However, he neglects to tell her the value of α. Suppose $gcd(b, p-1) = 1$. Show how Eve can determine α from the knowledge of p, x_2 and b.

    Eve knows $x_2 \equiv \alpha^b (\text{mod } p)$. So, if she can find b^{-1} then she needs only to solve $x_2^{b^{-1}} \equiv \alpha (\text{mod } p)$ for α. But, we know b^{-1} exists because $(b, p-1) = 1$. So, for a given b, $\alpha \equiv x_2^{b^{-1}} (\text{mod } p)$.

11. In the ElGamal cryptosystem, Alice and Bob use $p = 17$ and $\alpha = 3$. Bob chooses his secret to be $a = 6$, so $\beta = 15$. Alice sends the ciphertext $(r, t) = (7, 6)$. Determine the plaintext m.

    To decrypt, we use $tr^{-a} \equiv (\text{mod } p)$. Here we have

$$\begin{aligned} m &\equiv 6 \cdot 7^{-6} (\text{mod } 17) \\ &\equiv 6(7^6)^{-1} (\text{mod } 17) \\ &\equiv 6 \cdot (117649)^{-1} (\text{mod } 17) \\ &\equiv 6 \cdot (9)^{-1} (\text{mod } 17) \\ &\equiv 6 \cdot 2 (\text{mod } 17) \\ &\equiv 12 \end{aligned}$$

    So, $m = 12$.