Section 2.2: The Discrete Logarithm Problem (p62)

(2.2A) In their famous paper, Diffie & Hellman described a public key method by which certain material could be securely shared over an insecure channel. This method, called the Diffie-Hellman key exchange (Section 2.3), is based on the assumption that the discrete logarithm problem (DLP) is difficult to solve.

(2.2B) Let \( p \) be a (large) prime. By Thm 1.31 (Primitive Root Thm), there exists a primitive root \( g \) whose powers mod \( p \) generate all the nonzero elements of \( \mathbb{F}_p \). So, each nonzero element of \( \mathbb{F}_p \) is equal to some power of \( g \) mod \( p \).

- In particular, \( g^{p-1} \equiv 1 \pmod p \) by FLT and no smaller power of \( g \) is congruent to 1.
- Note: The textbook uses the notation \( \mathbb{F}_p \) and \( \mathbb{Z}_p \) interchangeably, with equality notation for elements of \( \mathbb{F}_p \) and congruence notation for elements of \( \mathbb{Z}_p \).

(2.2C) \textbf{Def:} Let \( g \) be a primitive root for \( \mathbb{F}_p \) and let \( h \) be a nonzero element of \( \mathbb{F}_p \). The \textbf{Discrete Logarithm Problem (DLP)} is the problem of finding an exponent \( x \) between 0 and \( p - 2 \) such that:

\[ g^x \equiv h \pmod p. \]

- The number \( x \) is called the \textit{discrete logarithm of \( h \) to the base \( g \)} and is denoted \( \log_g(h) \).
- If there is one solution \( x \), then there are infinitely many solutions of the form \( x + k(p-1) \):

\[ g^{x+k(p-1)} = g^x \cdot (g^{p-1})^k = h \cdot 1^k = h \pmod p, \]

where \( k \) is any number.

- In other words, \( \log_g(h) \) is really defined mod(\( p-1 \)).

(2.2D) \textbf{Ex:} \( p = 56509 \) is prime and has \( g = 2 \) as a primitive root. What is the discrete log of \( h = 38679 \)?

\[ 2^{11235} \equiv 38679 \pmod{56509} \]

Exercises: 2.3, 2.4