Assignment 6 - 2021.10.27

Submission deadline: 2021.11.03

1. Let g be a generator for Z_p^*. Suppose that $x = a$ and $x = b$ are both integer solutions to the congruence $g^x \equiv h(mod\ p)$. Prove that $a \equiv b(mod\ p-1)$.

2. Computer the following discrete logarithms. (You can write a simple program to help)
   a). $\log_2(13)$ for the prime p=23.
   b). $\log_{10}(22)$ for the prime p=47.
   c). $\log_{627}(608)$ for the prime p=941

3. The group S3 consists of the following six distinct elements $e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$, where e is the identity element and multiplication is performed using the rules
   $$\sigma^3 = e, \qquad \tau^2 = 1, \qquad \tau\sigma = \sigma^2\tau$$
   Compute the following values in the group S3:
   a) $\tau\sigma^2$
   b) $\tau(\sigma\tau)$
   c) $(\sigma\tau)(\sigma\tau)$
   d) $(\sigma\tau)(\sigma^2\tau)$
   Is S3 a commutative group?

4. Let p be a prime and let q be a prime that divides p-1. Let $a \in Z_p^*$ and let $b = a^{(p-1)/q}$. Prove that either b=1 or else b has order q. (Recall that the order of b is the smallest k such that $b^k = 1$ in Z_p^*.