Homework 12

not graded; hand in by Tuesday, December 3, 11:00 for comments on your solution

Problem 1. Let $m \in \mathbb{N}$ and $r \in \mathbb{Z}_m^\times$ be a primitive root. Show the following properties of the discrete logarithm:

a) $\log_r(\overline{1}) = \overline{0}$,

b) $\log_r(ab) = \log_r(a) + \log_r(b)$ for all $a, b \in \mathbb{Z}_m^\times$,

c) $\log_r(a^k) = k \log_r(a)$ for all $a \in \mathbb{Z}_m^\times$ and $k \in \mathbb{Z}_{\phi(m)}$,

d) If $s \in \mathbb{Z}_m^\times$ is another primitive root, then $\log_s(a) \log_r(s) = \log_r(a)$ and $\log_r(s) \in \mathbb{Z}_{\phi(m)}^\times$,

e) $\log_r(-\overline{1}) = \phi(m)/2$.

Problem 2. In the ElGamal signature algorithm, if Alice uses the same random number $k \in \mathbb{Z}_{\phi(m)}$ to sign two different messages, generating two different signatures, show that Eve can compute k, and even Alice's private key a.

Problem 3. Let p be an odd prime. Show that there exists $x \in \mathbb{Z}_p$ with $x^4 = \overline{-1}$ if and only if $p \bmod 8 = \overline{1}$.

Problem 4. Find all primitive roots in $\mathbb{Z}_{50}$.

Problem 5. Use discrete logarithms to find all integers x solving the equation

a) $4x^6 \bmod 25 = 17 \bmod 25$

b) $3^x \bmod 25 = 7 \bmod 25$

c) $2^x \bmod 13 = x \bmod 13$

d) $x^x \bmod 25 = x \bmod 25$