Math 418/818

Assignment 7

Due 12 November 2015

[6] 1. Let \( n = pq \) be a product of two distinct odd primes and put \( d = \gcd(p - 1, q - 1) \).
   (a) Prove that \( n \) is a pseudoprime to the base \( b \) if and only if \( b^d \equiv 1 \pmod{n} \).
   (b) Conclude (using part (a)) that \( |\mathcal{P}_n| = d^2 \).
   [2*] (c) Prove that if \( n > 0 \) is any odd integer, then \( b \in \mathcal{E}_n \) if and only if \( -b \in \mathcal{E}_n \).

[5] 2. (a) Let \( p = 467 \). Which of the three numbers 111, 127, and 225 are squares in \( \mathbb{F}_p \)?
   Justify your answer. (Do not use the prime factorization your numbers.)
   (b) For which primes \( p \) is 7 a quadratic residue mod \( p \)? (Give your answer in terms of a list of congruence conditions on \( p \).)

[3] 3. (a) Let \( m \) be a squarefree odd integer, and let \( (a, m) = 1 \). Show that \( x^2 \equiv a \pmod{m} \)
   has a solution if and only if \( \left( \frac{a}{p} \right) = 1 \), for all primes \( p | m \).
   [3*] (b)* Extend part (a) to all odd integers \( m \).

   (a) Write a MAPLE program \texttt{encode(m, g, y, p)} to encode a given message \( m \)
   (with \( 0 < m < p \)) by using the ElGamal protocol. Here, \( p \) is a prime, \( g \) an integer
   with \( 0 < g < p \) and \( y(=g^x) \) the public key. (Use MAPLE’s built-in random number
   generator in the range \( 2 \ldots p - 2 \).)
   (b) Write a MAPLE program \texttt{decode(M, g, y, p)} which decodes an encrypted message \( M \)
   produced by the program \texttt{encode} of part (a). (Use MAPLE’s built-in discrete
   log program (\texttt{numtheory[mlog]}) to find the secret key \( x \).)
   (c) Test your programs of parts (a) and (b) by encrypting and decrypting the message
   \( m = 20080919 \) \textit{twice}, using the public key \( (g, y, p) = (2222, 35029140, 112233449) \).