Introduction to Cryptography: Answers to Homework 2

1. Let p be a prime number such that $p\text{-}1=p_1^{e1}p_2^{e2}...p_m^{em}$ ($\forall i$, p_i is prime and $e_i \geq 1$). Prove that $g \in Z_p^*$ is a generator if and only if for all $1 \leq i \leq m$ it holds that $g^{(p-1)/pi} \neq 1 \mod p$. (33 points)

   Answer:
   Suppose that g is a generator of Z_p^*. Then the smallest exponent j such that $g^j=1$ is p-1. Therefore $g^{(p-1)/pi} \neq 1$ for all i.
   Suppose that $g^{(p-1)/pi} \neq 1$ for all i. We need to show that there is no exponent j<p-1 such that $g^j=1$. Suppose that there exists such an exponent j. The Lagrange theorem states that j must divide p-1. Therefore there is an index i such that j=(p-1)/p_i, or that j divides (p-1)/p_i. A as a result, $g^{(p-1)/pi}=1$.

2. The purpose of this exercise is to find an efficient algorithm for computing discrete logarithms in Z_p^*, where p is prime and $p=2^n+1$.
   The discrete logarithm problem is the following:
   Input: a prime p, a generator g of Z_p^*, and a value y in Z_p^*.
   Output: x s.t. $g^x=y \mod p$.

   Let $x=b_{n-1}2^{n-1}+b_{n-2}2^{n-2}+...+b_12^1+b_0$ be the binary representation of x.

   a. Show how to find the least significant bit (b_0) of x (given g,y). (7 points)

   Answer: $y=g^x$. We know that $y^{p-1}=1$, but what about $y^{(p-1)/2} = g^{x(p-1)/2}$? Let's write $x=2x'+b_0$, where b_0 is a bit. Then $y^{(p-1)/2} = g^{x(p-1)/2} = g^{(2x'+b0)(p-1)/2} = g^{x'(p-1) + b0(p-1)/2}$. Note that if $b_0=0$ then the result is 1, otherwise it is $g^{(p-1)/2}=p-1$. Therefore we should compute $y^{(p-1)/2}$ and check whether the result is equal to 1. If it is then $b_0=0$. Otherwise $b_0=1$.

   b. Set $z=y \cdot g^{-b0}$, and show how to use it to find the bit b_1. (10 points)
      Hint: there is an integer i such that $z=g^{4i+2 \cdot b1}$. Recall also that $e=p-1=2^n$ is the smallest exponent s.t. $g^e=1 \mod p$. Use these facts to find b_1.

   Answer: Denote $x'=x-b_0$. Compute $z=y \cdot g^{-b0} = g^{x'}$. Note that x' is an even number. We therefore know that $z^{(p-1)/2}=1$. We test whether it holds that $z^{(p-1)/4}=1$. The result is equal to either 1 or p-1, depending on whether b_1 is equal to 0 or 1 (this is true based on a similar analysis to that performed for the previous question, make sure that you understand it). Therefore we found the bit b_1.

   c. Show how to find the complete binary representation of x. (10 points)

Answer: We repeat the previous process for each bit of x. Namely, we apply the same procedure as in the previous section, but instead of dividing by g^{-b0} - we divide by g raised to the last bit we found, and instead of raising the result to the power of (p-1)/2 or (p-1)/4, we raise it to the power of $(p-1)/2^{(i+1)}$ when we are searching for bit b_i.

d. Explain why this method is only good for a prime modulo *p* that satisfies $p=2^n+1$. (6 points)

Answer: We were able to run this method since we could compute $(p-1)/2^{(i+1)}$ for every i=1…n, since $p=2^n+1$. If p is not of this form, then at some point we will not be able to compute $(p-1)/2^{(i+1)}$ and obtain an integer result.

Note: this algorithm can be generalized for any Z_p^* for which $p-1=p_1^{e1}p_2^{e2}...p_m^{em}$, all p_i are small primes, and the factorization of p-1 is known. (There is not need to prove this fact.)

3. Let *p* be a prime number. Suppose that *g* is a generator of Z_p^* and let $b=g^i$ for an exponent $0 \le i \le p-2$.
   a. Show that the order of *b* is $(p-1)/gcd(p-1,i)$. (17 points)

   Answer: Let's first check $b^{(p-1)/gcd(p-1,i)}$, we need to show that this value is equal to 1, and that there is no smaller exponent of b which is equal to 1. The value is equal to $g^{i\cdot (p-1)/gcd(p-1,i)} = g^{(p-1)\cdot (i/gcd(p-1,i))}$. The value i/gcd(p-1,i) is an integer, and therefore the result is 1.
   Recall that for any two integers, a·b/gcd(a,b) is equal to the least common multiple of a and b, denoted lcm(a,b). This is the smallest number which is divisible by both a and b.

   b. Show that the number of generators in Z_p^* is $\phi(p-1)$. (16 points)

   Answer: Given the previous answer, $b=g^i$ is a generator iff (p-1)/gcd(p-1,i) = p-1. This holds if gcd(p-1,i)=1, i.e. if I is relatively prime to p-1. The number of such numbers is $\phi(p-1)$.