PMAT 4282 – Cryptography — Assignment #6
Winter 2001

1. Prove the following statement:

   If the order of $a \in \mathbb{Z}_n^*$ is t and $a^s \equiv 1 \pmod{n}$, then t divides s.

2. (a) Suppose that α is a generator of $\mathbb{Z}_n^*$. Prove that α^k is also a generator of $\mathbb{Z}_n^*$ if and only if $\mathrm{GCD}(k, \phi(n)) = 1$.

   (b) Provided that $\mathbb{Z}_n^*$ has at least one generator, then how many generators does it have?

   (c) When p is prime, $\mathbb{Z}_p^*$ is known to have a generator. How many generators are there in:

      i. $\mathbb{Z}_{19}^*$
      ii. $\mathbb{Z}_{31}^*$
      iii. $\mathbb{Z}_{181}^*$
      iv. $\mathbb{Z}_{257}^*$
      v. $\mathbb{Z}_{2^t+1}^*$, where $(2^t + 1)$ is prime
      vi. $\mathbb{Z}_{2t+1}^*$, where t and $(2t + 1)$ are prime

3. Algorithm 4.9 on page 162 of the Handbook of Applied Cryptography, is as follows:

   Input: A multiplicative finite group $\mathcal{G}$ of order n, an element $a \in \mathcal{G}$, and the prime factorisation $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.
   Output: The order t of a.

   1 Set $t \leftarrow n$.
   2 For $i = 1, 2, \cdots, k$ do each of the following:
      2.1 Set $t \leftarrow \frac{t}{p_i^{e_i}}$.
      2.2 Compute $b \leftarrow a^t$.
      2.3 While b is not the multiplicative identity do the following: compute $b \leftarrow b^{p_i}$ and set $t \leftarrow tp_i$.
   3 Return t.

   Use this algorithm to determine the order of each of the following elements:

   (a) 5 in $\mathbb{Z}_7^*$
   (b) 12 in $\mathbb{Z}_{25}^*$
   (c) 3 in $\mathbb{Z}_{61}^*$

   Which of these elements are generators?