The University of Sydney
Math3925 Public Key Cryptography

Semester 2	**Exercises for Week 5**	2004

1. Consider the groups $\mathbb{Z}/391\mathbb{Z}^*$, $\mathbb{Z}/437\mathbb{Z}^*$, and $\mathbb{Z}/1001\mathbb{Z}^*$.

a. For each group, find the relations among 2, 3, and 5.

b. Use the relations to express each group G as $G = G_0 \oplus G_1$, where G_0 is the 2-subgroup and G_1 has odd order, and determine generators for each.

c. Find the exponent of G_0, i.e. the smallest m such that $G_0 = G[2^m]$, then determine generators for each group in the chain of subgroups

$$G[2^m] \supset G[2^{m-1}] \supset \cdots \supset G[2].$$

d. For each group G, determine a set of generators and relations for $G/[2](G)$.

2. In this exercise you must prove the primality of several integers. First we state a couple of theorems.

Theorem 1 *Suppose* $n - 1 = \prod_{i=1}^{r} p_i^{n_i}$ *and there exists an integer* a *such that*

$$a^{(n-1)/p_i} \not\equiv 1 \bmod n, \ \textit{for all } 1 \le i \le r,$$

and $a^{n-1} \equiv 1 \bmod n$. *Then* n *is prime.*

Note that the integer a is an element of exact order $n-1$. The conditions of this theorem can be relaxed to allow separate a_i with respect to each prime divisor of $n-1$.

Theorem 2 *Suppose* $n - 1 = \prod_{i=1}^{r} p_i^{n_i}$ *and there exist an integers* a_i *such that*

$$a_i^{(n-1)/p_i} \not\equiv 1 \bmod n \ \textit{for all } 1 \le i \le r,$$

and $a_i^{n-1} \equiv 1 \bmod n$ *for all* $1 \le i \le r$. *Then* n *is prime.*

Use the theorems to prove the primality of the integers $2^{16}+1$, $3^{59}-2^{59}$, and $7^{39}+24$. What is the obstruction to using this method in general for primality proving?