THE UNIVERSITY OF SYDNEY
MATH3925 PUBLIC KEY CRYPTOGRAPHY

Semester 2 | **Exercises and Solutions 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 $G/[2](G)$.

Solution

a. We first consider $\mathbb{Z}/391\mathbb{Z}^*$. The identities $400 = 2^4 5^2 = 3^2 + 391$, $1 + 391 = 2^3 7^2$, $-7 + 391 = 2^7 3$ (hence $7^2 \equiv 2^{14} 3^2 \bmod 391$), and $2 \cdot 7 + 391 = 405 = 3^4 5$, give rise to the matrix of relations

$$\begin{bmatrix} 4 & -2 & 2 & 0 \\ 3 & 0 & 0 & 2 \\ 14 & 2 & 0 & -2 \\ 1 & -4 & -1 & 1 \end{bmatrix},$$

and after eliminating 7,

$$\begin{bmatrix} 4 & -2 & 2 \\ 1 & 8 & 2 \\ 0 & 2 & -10 \end{bmatrix}.$$

Similar identities determine relation matrices for $\mathbb{Z}/437\mathbb{Z}^*$ and $\mathbb{Z}/1001\mathbb{Z}^*$,

$$\begin{bmatrix} 2 & -2 & 6 \\ 1 & -7 & 0 \\ 9 & -1 & -2 \end{bmatrix}, \text{ and } \begin{bmatrix} 6 & 0 & 6 \\ 4 & -4 & -8 \\ 2 & 10 & 2 \end{bmatrix}.$$

b. The determinants of these matrices are $352 = 32 \cdot 11$, $396 = 4 \cdot 99$, $720 = 16 \cdot 45$. With respect to these factorizations $2^t r$, the 2-subgroups G_0 and the odd subgroup G_1 are then $[r](G)$ and $[2^t](G)$, respectively. Assuming the set $\{2, 3, 5\}$ generates $G = \mathbb{Z}/n\mathbb{Z}^*$, a set of generators for G_0 is $\{2^r, 3^r, 5^r\}$ and for G_1 is $\{2^{2^t}, 3^{2^t}, 5^{2^t}\}$. Specfically, we have:

n	G_0	G_1
391	$\langle 93, 24, 45\rangle$	$\langle 35, 307, 239\rangle$
437	$\langle 208, 208, 229\rangle$	$\langle 16, 81, 188\rangle$
1001	$\langle 967, 573, 265\rangle$	$\langle 471, 718, 170\rangle$

This answer is somewhat unsatisfactory, since the group structure is not self-evident from these abstract set of supposed generators.

In order to determine the group structure of G_0 (or G_1), we consider the subgroup of $\mathbb{Z}^3$ generated by the the known relations (the kernel of the homomorphism $\pi : \mathbb{Z}^3 \to G = \mathbb{Z}/n\mathbb{Z}^*$) augmented by r (or 2^t) times the standard basis elements. For G_0 this gives:

$$\begin{bmatrix} 4 & -2 & 2 \\ 1 & 8 & 2 \\ 0 & 2 & -10 \\ 11 & 0 & 0 \\ 0 & 11 & 0 \\ 0 & 0 & 11 \end{bmatrix}, \quad \begin{bmatrix} 2 & -2 & 6 \\ 1 & -7 & 0 \\ 9 & -1 & -2 \\ 99 & 0 & 0 \\ 0 & 99 & 0 \\ 0 & 0 & 99 \end{bmatrix}, \quad \begin{bmatrix} 6 & 0 & 6 \\ 4 & -4 & -8 \\ 2 & 10 & 2 \\ 45 & 0 & 0 \\ 0 & 45 & 0 \\ 0 & 0 & 45 \end{bmatrix}.$$

Basis reduction gives us a matrix of row vectors surjecting onto G_0:

$$\begin{bmatrix} 1 & 0 & 9 \\ 0 & 1 & 6 \\ 0 & 0 & 11 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 86 \\ 0 & 1 & 83 \\ 0 & 0 & 99 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 7 \\ 0 & 3 & 9 \\ 0 & 0 & 15 \end{bmatrix}.$$

These gives generator sets

$$\begin{gathered} \{2 \cdot 5^9, 3 \cdot 5^9, 5^{11}\} = \{45, 346, 160\}, \\ \{2 \cdot 5^{86}, 3 \cdot 5^{83}, 5^{99}\} = \{436, 229, 208\}, \\ \{2 \cdot 3^2 \cdot 5^7, 3^3 \cdot 5^9, 5^{15}\} = \{694, 34, 846\}. \end{gathered}$$

But we can also rewrite the matrices of kernel relations in terms of these generators. For the first group this gives

$$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 2 & 14 \\ 0 & 0 & 16 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 42 \\ 0 & 2 & 166 \\ 0 & 0 & 176 \end{bmatrix} \begin{bmatrix} 1 & 0 & 9 \\ 0 & 1 & 6 \\ 0 & 0 & 11 \end{bmatrix}^{-1}.$$

where the middle matrix is the Hermite form of the relations matrix for $\mathbb{Z}/391\mathbb{Z}^*$. Settting $g_1 = 45$, $g_2 = 346$, and $g_3 = 160$, we can check the identities

$$g_1 g_3^3 = g_2^2 g_3^{14} = g_3^{16} = 1.$$

c. We treat only the first group. From the above relations among g_1, g_2, and g_3, we see that the exponent of the 2-subgroup of $G = \mathbb{Z}/391\mathbb{Z}^*$ is 16. Thus $G_0 = G[16] = \langle g_1, g_2, g_3 \rangle$. Since $g_1^8 = g_2^8 = g_3 = 254$, we find $(g_1 g_2)^8 = (g_2 g_3)^8 = 1$, so $G[8] = \langle g_1 g_2, g_2 g_3, g_3^2 \rangle$. Continuing in this way, we express the preimages of $G[8]$, $G[4]$, and $G[2]$ in $\mathbb{Z}^3$ are spanned by the rows of the matrices:

$$\begin{bmatrix} 1 & 1 & 15 \\ 0 & 1 & 17 \\ 0 & 0 & 22 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 32 \\ 0 & 1 & 39 \\ 0 & 0 & 44 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 32 \\ 0 & 1 & 83 \\ 0 & 0 & 88 \end{bmatrix}.$$

The first row of the latter matrix is in the kernel of $\pi : \mathbb{Z}^3 \to \mathbb{Z}/391\mathbb{Z}^*$, but the second and third give nontrivial 2-torsion elements 137 and 254, respectively. Note that the only group of order 32 and exponent 16 is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, and that the 2-torsion subgroup is the group of order 4 generated by 137 and 254.

d. In each case, the group G is generated by $\{2, 3, 5\}$, and the relations for the quotient $G/[2](G)$ are a set of generators for the group $[2](G) = [2](G_0) + G_1$.

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*

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

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*

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

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?

Solution For the first number n we find the factorization of $n - 1$ to be:

$$2^{16} + 1 - 1 = 2^{16} = 65536,$$

and so we only need to find one element which is not a square, and 3 is a nonsquare, since its 2^{15}-th power is -1:

$$3^{2^{15}} \bmod 2^{16} + 1 = 655236.$$

For the second prime number we find the factorization:

$$\begin{aligned} 3^{59} - 2^{59} - 1 = \; & 2 \cdot 3 \cdot 7 \cdot 59 \cdot 1151 \cdot 58171 \cdot 123930193 \cdot 687216767 \\ & 2 \cdot 3 \cdot 7 \cdot p_4 \cdot p_5 \cdot p_6 \cdot p_7 \cdot p_8 \end{aligned}$$

It turns out that 2 and 3 are 21-st powers, so fail to satisfy the conditions of the first theorem. Similarly 5 is a square, so also fails. However 2 and 5 can be used in the second theorem to prove the primality of n as is verified in the table below.

a	2	5
$a^{\varphi(n)/2}$	14130386091162273752461387578	1
$a^{\varphi(n)/3}$	1	14039524071766095844181052225
$a^{\varphi(n)/7}$	1	7826610972995267547708375 37
$a^{\varphi(n)/p_4}$	11718328150460486086616882272	10636292038180945801879749999
$a^{\varphi(n)/p_5}$	1004037098196704812361815 09	3216430705463480598022736901
$a^{\varphi(n)/p_6}$	6850603673682354674405653 26	13450338895656173387977763600
$a^{\varphi(n)/p_7}$	7762846453032502793085391834	3732507535185619691818435804
$a^{\varphi(n)/p_8}$	14051755362251040487509134380	9167675531100609270057486746

Note that even though we are magically given the factorization of $\varphi(n) = n-1$ by `Magma`, it remains to prove that each of the larger primes $p_4, \ldots, p_8$ is prime.

For the last prime number n, we find the factorization of $n-1$ to be:

$$7^{39} + 24 - 1 = 2 \cdot 3 \cdot 31^2 \cdot 1129 \cdot 10954261 \cdot 12754748402046864529$$

We find that $2^{(n-1)/p} \bmod n$ is 1 for $p = 2$ but for different from 1 for all other prime divisors. On the other hand, $a = 3$ and $a = 5$ give $a^{(n-1)/3} \bmod n = 1$, and give something different from 1 for all other p. We can therefore apply the second theorem.

Note that, as above, the completeness of the factorization must also be proved. This requires proving the primality of all of the factors of $n-1$. To take a specific example, we give one chain $p_1, p_2, \ldots$ of primes p_i with $p_1 | n-1$ and $p_{i+1} | p_i - 1$, together with the full the factorizations of $p_i - 1$.

$$\begin{array}{l}
12754748402046864529 - 1 = 2^4 \cdot 3 \cdot 7 \cdot 139 \cdot 857 \cdot 6269 \cdot 50832179 \\
50832179 - 1 = 2 \cdot 25416089 \\
25416089 - 1 = 2^3 \cdot 17 \cdot 186883 \\
186883 - 1 = 2 \cdot 3 \cdot 31147 \\
31147 - 1 = 2 \cdot 3 \cdot 29 \cdot 179
\end{array}$$

In each such possible chain of prime divisors the primality of each p_i must be proved. Below a certain bound, say 10000, we may assume that the primality of $p < 10000$ is determined by trial division up to $\sqrt{p} < 100$.