THE UNIVERSITY OF SYDNEY
MATH3925 PUBLIC KEY CRYPTOGRAPHY

Semester 2 **Exercises for Week 2** 2004

1. Let G be an abelian group of order $p^n q^m$ for primes p and q. What are the possible dimensions of $G[p]$ and $G[q]$ as vector spaces?

Hint: Show that $G = G_1 \times G_2$ where $G_1 = [q^m](G)$ and $G_2 = [p^n](G)$. Prove that $|G_1| = p^n$ and $|G_2| = q^m$, then consider the possible p-torsion and q-torsion subgroups in each of G_1 and G_2.

2. Let $n = 1547$ and let $g_1 = 2$, $g_2 = 3$, $g_3 = 5$, and $g_4 = 11$ in $\mathbb{Z}/n\mathbb{Z}^*$.

a. Verify the relations $g_1\, g_3 = g_2^5\, g_4^2$, $g_1^3\, g_2 = g_3^3\, g_4^4$, $g_1^6\, g_4^2 = g_2^2$, and $g_1^3\, g_2^5\, g_3^3 = g_4^2$.

b. Let $\phi : \mathbb{Z}^4 \rightarrow \mathbb{Z}/n\mathbb{Z}^*$ be the homomorphism taking the standard basis to the generators $\{g_1, g_2, g_3, g_4\}$. What is the kernel of ϕ?

c. What is the order and what is the exponent of the group $\mathbb{Z}/n\mathbb{Z}^*$?

d. Determine the dimension r of $\mathbb{Z}/n\mathbb{Z}^*[3]$ as a vector space over $\mathbb{F}_3$, and define an isomorphism from $\mathbb{F}_3^r$ with $\mathbb{Z}/n\mathbb{Z}^*[3]$.

3. Let n be the Mersenne number $2^{29} - 1 = 536870911$.

a. Prove that $|\mathbb{Z}/n\mathbb{Z}^*|$ is divisible by 29.

b. What does the following `Magma` code do?

```
Z := Integers();
R := ResidueClassRing(N);
a := (R!3)^29;
for r in [1..80] do
    printf "%3o: %o\n", r, GCD(Z!(a^r-1),N);
end for;
```

c. Now consider the set of 19 generators

$$\{-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61\}$$

inside of the group $\mathbb{Q}^*$, and label them $g_1, \ldots, g_{19}$. These define a map

$$\mathbb{Z}^{19} \longrightarrow \mathbb{Z}/n\mathbb{Z}^*,$$

by the map $(n_1, \ldots, n_{19}) \mapsto g_1^{n_1} \cdots g_{19}^{n_{19}}$, for which we find a matrix of 2-torsion relations

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -4 & 0 & -2 & 0 & 3 & 3 & 4 & 4 & 2 & 2 & 6 & 4 & 4 & 5 & 4 & 7 & 4 & 3 \\ 1 & 1 & -4 & 2 & 2 & 3 & 3 & 5 & 2 & 2 & 6 & 6 & 5 & 5 & 5 & 5 & 5 & 5 & 5 \\ 0 & -2 & -1 & -3 & 3 & 4 & 0 & 4 & 1 & 5 & 5 & 6 & 2 & 2 & 3 & 3 & 3 & 4 & 3 \end{bmatrix}$$

That is, for any row $(n_1, \dots, n_{19})$ we have

$$\prod_{i=1}^{19} g_i^{2n_i} \equiv 1 \bmod n.$$

Suppose that $n = pq$, with $\mathrm{GCD}(p, q) = 1$, so that

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

We hope that a 2-torsion element u satisfies

$$u \equiv 1 \bmod p \text{ but } u \not\equiv 1 \bmod q.$$

If such is the case, then $p \,|\, \mathrm{GCD}(u-1, n) \neq n$ and we have found a nontrivial factorization. In particular, the second line of this relation matrix gives the equality:

$$\left(2^4 5^2\right)^2 \equiv \left(11^3 13^3 17^4 19^4 23^2 29^2 31^6 37^4 41^4 43^5 47^4 53^7 59^4 61^3\right)^2 \bmod n$$

from which we can derive the factorization

$$\mathrm{GCD}(n, 2^4 5^2 - 11^3 13^3 17^4 19^4 23^2 29^2 31^6 37^4 41^4 43^5 47^4 53^7 59^4 61^3) = 1103.$$

Compute the other factorizations determined by the 2-torsion relations.