Semester 2 **Exercises and Solutions 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.

Solution Since G has order $p^n q^m$, it follows that

$$[p^n][q^m] = [q^m][p^n] = [p^n q^m] = [0]$$

on G. In particular $[p^n](G_1) = \{e\}$ and $[q^m](G_2) = \{e\}$, so G_1 and G_2 must therefore have orders p^n and q^m. These subgroups are called the p-subgroup and q-subgroup of G, respectively.

From the classification of finite abelian groups, the only possible group structures for G_1 must therefore be

$$G_1 = \mathbb{Z}/p^{s_1}\mathbb{Z} \times \cdots \mathbb{Z}/p^{s_t}\mathbb{Z},$$

were $s_1 \le \cdots \le s_t$ and $n = s_1 + \cdots + s_t$. Precisely the possibilities range from the cyclic group $\mathbb{Z}/p^n\mathbb{Z}$ at one extreme to the full p-torsion group

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/p\mathbb{Z}^n.$$

The possible p-torsion subgroups $G[p] = G_1[p]$ can therefore be isomorphic to $\mathbb{Z}/p\mathbb{Z}$ in the cyclic case to $\mathbb{Z}/p\mathbb{Z}^n$. So, as $\mathbb{F}_p$-vector spaces, every dimension from 1 to n is possible. The possible structures for $G[q] = G_2[q]$ are analogous.

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 $\phi : \mathbb{Z}^4 \to \mathbb{Z}/n\mathbb{Z}^*$ 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 $\mathbb{Z}/n\mathbb{Z}^*[3]$.

Solution

- **a.** The identities are each easily verified – for instance the first, $2 \cdot 5 = 3^5 \cdot 11^2$ modulo 1547, follows from $3^5 \cdot 11^2 = 2 \cdot 5 + 18 \cdot 1547$.

b. By rearranging the identities to relations of the form $g_1^{n_1} g_2^{n_2} g_3^{n_3} g_4^{n_4} = 1$, we read off elements (n_1, n_2, n_3, n_4) of the kernel. This gives a matrix

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

whose rows are elements of the kernel. The determinant of this matrix is -1152, which is, up to sign, the order of $\mathbb{Z}/1547\mathbb{Z}^* \cong \mathbb{Z}/7\mathbb{Z}^* \times \mathbb{Z}/13\mathbb{Z}^* \times \mathbb{Z}/17\mathbb{Z}^*$. We conclude that the relations give a complete set of generators for the kernel.

c. The group order is 1152, as determined above, and the exponent is the least common multiple of each of the orders of the cyclic factors. These are 6, 12, and 16, so the exponent is 48.

d. Considering again the cyclic factors, there is a contribution to the 3-torsion subgroup from $\mathbb{Z}/7\mathbb{Z}^*$ and from $\mathbb{Z}/13\mathbb{Z}^*$. Thus the dimension of the 3-torsion subgroup is 2. Since 2 generates $\mathbb{Z}/7\mathbb{Z}^*[3]$ and 3 generates $\mathbb{Z}/13\mathbb{Z}^*[3]$, we solve the two sets of Chinese remainder congruences

$$\begin{array}{lll} x = 2 \bmod 7 & x = 1 \bmod 13 & x = 1 \bmod 17 \\ y = 1 \bmod 7 & y = 3 \bmod 13 & y = 1 \bmod 17 \end{array}$$

to find $x = 443$ and $y = 120$. The 3-torsion subgroup of $\mathbb{Z}/1547\mathbb{Z}^*$ is therefore $\{x^i y^j : i, j \in \mathbb{F}_3\}$, so the map

$$\varphi : \mathbb{F}_3^2 \to \mathbb{Z}/1547\mathbb{Z}^*[3]$$

given by $\varphi(i,j) = x^i y^j$ is an isomorphism.

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 $(n_1, \ldots, n_{19})$ 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.

Solution

a. The form of n implies that the element 2 of $\mathbb{Z}/n\mathbb{Z}^*$ has order 29, which must therefore divide the group order.

b. The statement `printf` specifies a formatted printing — three digits of r are printed, then a colon, then the result of the GCD is printed. The GCD will be divisible by p if and only if $a^r = 3^{29r} \equiv 1 \bmod p$. Since $2 \not\equiv 1 \bmod p$ for any prime p, we know that 29 must divide $p - 1 = |\mathbb{Z}/p\mathbb{Z}^*|$ for any prime divisor of n. The GCD picks out the largest divisor m of n for which 3 has order dividing $29r$ in $\mathbb{Z}/m\mathbb{Z}^*$.

The first nontrivial divisor, 233, of n is found with the value $r = 8$. Since $233 - 1 = 8 \cdot 29$, by Fermat's Little Theorem, the equality $3^{8 \cdot 29} \equiv 1 \bmod 233$ holds. The next nontrivial factor, 1103, is found for $r = 19$.

c. The first line is the relation $-1^2 = 1$, which determines no factorization of n, but the the third and fourth lines determine factors 256999 and 2089.