The University of Sydney
Math3925 Public Key Cryptography

Semester 2 **Exercises for Week 3** 2004

The *echelon form* of a matrix $M \in \mathbb{M}_n(R)$ is an upper triangular matrix U such that there exists an invertible matrix T with $U = TM$.

1. Let a homomorphism $\varphi : \mathbb{Z}^{19} \to \mathbb{Z}^{19}$ be given by the following matrix M (as the right operator $v \mapsto vM$):

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

Find the echelon form of this matrix, the determinant, and show that the cokernel $C = \mathbb{Z}^{19}/\varphi(\mathbb{Z}^{19})$ is finite. Find the group structure of the cokernel, and of the two-torsion subgroup $C[2]$.

You can create the matrix M in `Magma` *using the code at the end of the tutorial sheet. The abelian groups $A = \mathbb{Z}^{19}$, $B = \varphi(A)$, and $C = A/B$ are created as follows.*

```
r := 19;
A<[x]> := FreeAbelianGroup(r);
B<[y]>, phi := sub< A | [ A![ M[i,j] : j in [1..r]] : i in [1..r]]>;
C<[z]>, psi := quo< A | B >;
```

2. How do the abelian invariants compare to the diagonal entries of the echelon form of the matrix M? The echelon form U for the matrix M can be created in `Magma` as follows.

```
U, T := EchelonForm(M);
```

What are the determinants of the matrices M, U, and T?

3. Verify that the matrix M in the previous exercise defines the kernel of the homomorphism

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

where n is the Mersenne number $2^{29} - 1$, and the i-th basis element of $\mathbb{Z}^{19}$ maps to the i-th element of the sequence

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

Hint:

```
R := ResidueClassRing(2^29-1);
smbase := [-1] cat [ R | n : n in [1..61] | IsPrime(n) ];
[ &*[ smbase[j]^M[i,j] : j in [1..19] ] : i in [1..19] ];
```

4. Given the factorization $n = 233 \cdot 1103 \cdot 2089$, determine the group structure of $\mathbb{Z}/n\mathbb{Z}^*$ as an additive group of the form $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$ for $m_1 | m_2 | \cdots | m_r$ and as an additive group of the form $\mathbb{Z}/p_1^{s_1}\mathbb{Z} \times \mathbb{Z}/p_2^{s_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{s_t}\mathbb{Z}$ for primes $p_1, p_2, \ldots, p_t$.

5. How would you compute the two-torsion subgroup of $\mathbb{Z}/n\mathbb{Z}^*$ from the matrix M? Compute the two-torsion elements, then using the factorization of n, determine the image of each in the group

$$\mathbb{Z}/233\mathbb{Z}^* \times \mathbb{Z}/1103\mathbb{Z}^* \times \mathbb{Z}/2089\mathbb{Z}^*.$$

Relation matrix M:

```
M := Matrix([
  [2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],
  [1,1,1,-1,1,-1,1,-1,-1,1,0,1,0,1,-1,0,0,1,1],
  [0,1,0,-1,0,0,0,1,0,-1,2,0,0,-1,0,1,2,-1,-1],
  [0,1,2,0,0,0,0,1,0,0,1,1,-2,-1,1,1,0,1,1],
  [1,1,-2,1,1,-1,0,-1,0,0,-1,1,1,1,-1,0,-1,1,-1],
  [0,1,1,1,2,0,0,0,0,1,0,0,0,-1,-2,0,0,-1,-2],
  [0,1,1,0,0,-2,2,-1,-1,0,0,0,0,-1,0,-2,0,-1,0],
  [0,1,-1,0,2,0,0,-1,1,1,-2,0,1,1,1,-1,0,1,0],
  [1,0,0,1,-1,-1,0,0,-1,1,3,1,1,0,0,-1,0,0,-1],
  [0,1,0,0,2,1,0,-1,-2,0,-2,0,-1,0,-1,1,1,1,0],
  [1,1,0,-1,-2,0,0,1,-1,0,-1,1,2,1,1,2,0,0,0],
  [1,1,-2,0,0,1,0,-2,-1,1,-1,-1,0,-1,-1,-1,0,2,0],
  [0,2,0,-2,0,0,-2,0,-1,0,1,-1,1,1,-1,1,1,-2,0],
  [1,2,-1,-1,1,1,0,1,0,-1,2,0,2,1,-2,-1,1,0,1],
  [1,-1,0,2,0,0,0,-3,1,0,1,2,-1,0,0,-2,0,0,1],
  [1,-2,1,1,-1,1,0,0,2,0,3,1,-1,0,1,0,-1,-1,0],
  [0,1,2,-1,0,-1,0,1,1,-1,3,-1,1,0,-1,0,1,-2,-1],
  [0,3,1,0,2,0,0,1,-1,1,0,-1,3,0,-1,1,0,0,0],
  [0,0,0,3,1,-1,3,-2,-1,1,-1,0,-1,-1,-1,-1,0,1,0]
]);
```