The University of Sydney
Math3925 Public Key Cryptography

Semester 2 **Exercises and Solutions 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 >;
```

Solution The determinant of the matrix is -533826432, given by the `Magma` command `Determinant`. The command `EchelonForm` returns an upper triangular matrix with diagonal entries:

$$[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 58, 2088, 4408],$$

so the order of the cokernel C is $58 \cdot 2088 \cdot 4408 = 533826432$.

From the echelonized row relations, we conclude that all generators can be expressed in terms of the last three generators, and these satisfy relations among themselves given by the lower right-hand block

$$\begin{bmatrix} 58 & 1566 & 3596 \\ 0 & 2088 & 464 \\ 0 & 0 & 4408 \end{bmatrix} = 58 \cdot \begin{bmatrix} 1 & 27 & 62 \\ 0 & 36 & 8 \\ 0 & 0 & 76 \end{bmatrix}$$

Thus the three generators, say g_1, g_2, g_3, each have order divisible by 58 and $(g_1 g_2^{27} g_3^{62})^{58} = e$, and g_2^{58} and g_3^{58} satisfy the matrix row relations

$$\begin{bmatrix} 36 & 8 \\ 0 & 76 \end{bmatrix} = 4 \cdot \begin{bmatrix} 9 & 2 \\ 0 & 19 \end{bmatrix}$$

Thus we check that $(g_2^9 g_3^2)^{4 \cdot 58} = (g_2^9 g_3^2)^{232} = e$ and $(g_2^4 g_3)^{4 \cdot 9 \cdot 19 \cdot 58} = (g_2^4 g_3)^{39672} = e$. We verify that the set of elements $\{h_1 = g_1 g_2^{27} g_3^{62},\ h_2 = g_2^9 g_3^2,\ h_3 = g_2^4 g_3\}$ is a new basis of generators under the basis transformation matrix

$$U = \begin{bmatrix} 1 & 27 & 62 \\ 0 & 9 & 2 \\ 0 & 4 & 1 \end{bmatrix}$$

satisfying $h_1^{58} = e$, $h_2^{232} = e$, and $h_3^{39672} = e$, where $58|232|39672$ and $58 \cdot 232 \cdot 39672 = 533826432$. We conclude that the group structure is

$$\mathbb{Z}/58\mathbb{Z} \times \mathbb{Z}/232\mathbb{Z} \times \mathbb{Z}/39672\mathbb{Z},$$

and the abelian invariants are 58, 232, 39672. Since each of these factors has even order we find the 2-torsion subgroup to be isomorphic to $\mathbb{Z}/2\mathbb{Z}^3$, embedded as

$$29\mathbb{Z}/58\mathbb{Z} \times 116\mathbb{Z}/232\mathbb{Z} \times 19836\mathbb{Z}/39672\mathbb{Z}$$

in the larger group (i.e. with generators h_1^{29}, h_2^{116}, and h_3^{19836}).

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?

Solution The abelian invariants of a finite abelian group must have the form $n_i | n_{i+1}$, whereas the diagonal entries of the echelon form of the matrix (see above) need not be so normalized.

The determinant of the echelon form U for M must have the same determinant as M, up to a unit, since T is invertible and $\det(TM) = \det(T)\det(M) = \det(U)$. In this case the matrix T has determinant -1.

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] ];
```

Solution The output of the above `Magma` code is the sequence

$$[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]$$

consisting of the multiplicative identity 1 in $\mathbb{Z}/n\mathbb{Z}^*$, so the row vectors are in the kernel of the map to the multiplicative group of $\mathbb{Z}/n\mathbb{Z}$.

To show that M doesn't generate a subgroup of the kernel of the map $\mathbb{Z}^{19} \to \mathbb{Z}/n\mathbb{Z}^*$, we need to know the group order. Making use of the factorization of n (below), this order is

$$(233-1)\cdot(1103-1)\cdot(2089-1) = 533826432 = \det(M).$$

It follows that M is surjective on the kernel of the map to $\mathbb{Z}/n\mathbb{Z}^*$.

4. Given the factorization $n = 233\cdot1103\cdot2089$, 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 $p_1, p_2, \ldots, p_t$.

Solution The group $\mathbb{Z}/n\mathbb{Z}^*$ is isomorphic to $\mathbb{Z}/233\mathbb{Z}^*\times\mathbb{Z}/1103\mathbb{Z}^*\times\mathbb{Z}/2089\mathbb{Z}^*$, which in turn, is isomorphic to the additive abelian group $\mathbb{Z}/232\mathbb{Z}\times\mathbb{Z}/1102\mathbb{Z}\times\mathbb{Z}/2088\mathbb{Z}$. From the factorizations $232 = 2^3 29$, $1102 = 2\cdot19\cdot29$ and $2088 = 2^3\cdot3^2\cdot29$, we obtain an isomorphism with

$$\mathbb{Z}/2^3\mathbb{Z}\times\mathbb{Z}/29\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/19\mathbb{Z}\times\mathbb{Z}/29\mathbb{Z}\times\mathbb{Z}/2^3\mathbb{Z}\times\mathbb{Z}/3^2\mathbb{Z}\times\mathbb{Z}/29\mathbb{Z}.$$

Reordering the factors we find that $\mathbb{Z}/n\mathbb{Z}^*$ is isomorphic to

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^3\mathbb{Z}\times\mathbb{Z}/2^3\mathbb{Z}\times\mathbb{Z}/3^2\mathbb{Z}\times\mathbb{Z}/19\mathbb{Z}\times\mathbb{Z}/29\mathbb{Z}\times\mathbb{Z}/29\mathbb{Z}\times\mathbb{Z}/29\mathbb{Z}.$$

In this prime-power decomposition we can recombine coprime factors to find an isomorphic group

$$\mathbb{Z}/2\cdot29\mathbb{Z}\times\mathbb{Z}/2^3\cdot29\mathbb{Z}\times\mathbb{Z}/2^3\cdot3^2\cdot19\cdot29\mathbb{Z},$$

i.e. with $m_1 = 2\cdot29 = 58$, $m_2 = 2^3\cdot29 = 232$ and $m_3 = 2^3\cdot3^2\cdot19\cdot29 = 39672$.

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

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

Solution The 2-torsion subgroup of $\mathbb{Z}/n\mathbb{Z}^*$ is the image of those elements v in $A = \mathbb{Z}^{19}$ such that $2v \in B$. The nontrivial elements can be computed by interpretting M as a matrix over $\mathbb{F}_2$ and solving for its kernel.

Let $\overline{M}$ be this matrix over $\mathbb{F}_2$, and let $\bar{u}\overline{M} = 0 \in \mathbb{F}_2^{19}$. If $\bar{u}$ is any element of $\mathbb{Z}^{19}$ which reduced to $\bar{u}$, then uM is an element of $2A \cap B$, and $v = (1/2) * uM$ is an element of A such that $2v \in B$. It follows that the map

$$\bar{u} \mapsto \frac{1}{2}uM$$

defines an isomorphism $\ker(\overline{M}) \to A/B[2] = C[2]$, and the latter group is isomorphic to $\mathbb{Z}/n\mathbb{Z}^*[2]$. Solving for this space, we find the basis matrix

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

for the rank three 2-torsion subgroup. The duplicate of this matrix is produced by the three lines of `Magma` commands below.

```
M2 := MatrixAlgebra(FiniteField(2),19)!M;
N2 := BasisMatrix(Kernel(M2));
RMatrixSpace(Integers(),Nrows(N2),19)!N2*M;
```

On the other hand, given the factorization $n = 233 \cdot 1103 \cdot 2089$, the 2-torsion elements of $\mathbb{Z}/n\mathbb{Z}^*$ are those which have image in $\{\pm 1\}$ in each of $\mathbb{Z}/233\mathbb{Z}$, $\mathbb{Z}/1103\mathbb{Z}$ and $\mathbb{Z}/2089\mathbb{Z}$. A representative element in $\mathbb{Z}/n\mathbb{Z}$ can be found by the Chinese remainder theorem algorithm.

For example the `Magma` command `CRT([1,1,-1],[233,1103,2089])` finds the representative 61936760 of $(1, 1, -1)$, and the other 2-torsion elements

$$403504974, 465441733, 71429178, 133365937, 474934151$$

together with 1 and $-1 = 536870910$ are found similarly.

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]
]);
```