THE UNIVERSITY OF SYDNEY
MATH3925 PUBLIC KEY CRYPTOGRAPHY

Semester 2 | **Exercises for Week 1** | 2004

Residue Class Rings. Let n and m be integers with no common factors. We say that n and m are *coprime*. The Chinese Remainder Theorem says that $\mathbb{Z}/nm\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ are isomorphic.

Torsion Subgroups. Given an additive abelian group A, the *p-torsion subgroup* $A[p]$ of A is the subgroup $\{x \in A \,|\, px = 0\}$. For a multiplicative abelian group G, the p-torsion subgroup $G[p]$ is the subgroup $\{x \in G \,|\, x^p = 1\}$.

1. Let n and m be coprime integers.

a. Prove that there exist integers r and s such that $rn + sm = 1$. An algorithm for producing r and s is called the extended greatest common divisor, or XGCD.

b. Show that the diagonal map

$$\mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

given by $x \mapsto (x, x)$ is injective, and conclude that it is an isomorphism.

c. Define the inverse to the diagonal map of the previous part using solutions r and s to the XGCD.

d. The `Magma` syntax for creating the map $\mathbb{Z}/323\mathbb{Z} \to \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z}$ is

```
m := 17;
n := 19;
A<x> := AbelianGroup([m*n]);
B<x1,x2> := AbelianGroup([m,n]);
h := hom< A -> B | g :-> [v[1],v[1]] where v := Eltseq(g) >;
h(x); // x1 + x2
```

Use the function XGCD to construct the inverse map.

N.B. The function `Eltseq` is short for `ElementToSequence` and is used to extract the defining coordinates for many types of `Magma` elements which are defined by underlying sequences.

2. Let n be an odd integer which is the product of two primes p and q.

a. Show that $\mathbb{Z}/n\mathbb{Z}^*[2]$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

b. Given an element $g \in \mathbb{Z}/n\mathbb{Z}^*[2]$, not equal to ± 1, show how to find a factorization of n. *Hint:* consider the image of g in $\mathbb{Z}/p\mathbb{Z}^* \times \mathbb{Z}/q\mathbb{Z}^*$.