THE UNIVERSITY OF SYDNEY
MATH3925 PUBLIC KEY CRYPTOGRAPHY

Semester 2 | **Exercises and Solutions 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.

Solution

a. Consider the ideal $n\mathbb{Z}+m\mathbb{Z}$ generated by n and m, which must be of the form $a\mathbb{Z}$ for some positive integer a. Since $n, m \in a\mathbb{Z}$ both n and m must be divisible by a. By assumption we must have $a = 1$. Since a is in $n\mathbb{Z} + m\mathbb{Z}$, we have expressed $1 = nr + ms$. A more algorithmic solution is obtained using the Euclidean algorithm.

b. An element x of $\mathbb{Z}/nm\mathbb{Z}$ is in the kernel of reduction to $\mathbb{Z}/n\mathbb{Z}$ if and only if x is divisible by n. Similarly it is in the kernel of reduction to $\mathbb{Z}/m\mathbb{Z}$ if and only if it is divisible by m. Since n and m are coprime, such an element must be divisible by nm, hence is zero in $\mathbb{Z}/nm\mathbb{Z}$.

c. The inverse map is given by $(x,y) \mapsto x+nr(y-x)$, as is verified by reducing the expression modulo n and m. By symmetry the expression $(x,y) \mapsto y+ms(x-y)$ must also give the inverse map, and taking the difference we indeed find

$$\big(x + nr(y-x)\big) - \big(y + ms(x-y)\big) = x(1 - nr - ms) + y(-1 + nr + ms) = 0.$$

d. The inverse map can be constructed with the `Magma` syntax:

```
one, r, s := XGCD(17,19);
h_inv := hom< B -> A |
    x :-> [v[1]+17*r*(v[2]-v[1])] where v := Eltseq(x) >;
```

We can test that this function is indeed an inverse map on randomly selected elements:

```
> h_inv(h(A![4]));
4*x
> h(h_inv(B![4,3]));
4*x1 + 3*x2
> h(h_inv(B![4,7]));
4*x1 + 7*x2
```

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 $\mathbb{Z}/p\mathbb{Z}^* \times \mathbb{Z}/q\mathbb{Z}^*$.

Solution

a. The ring $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ by the Chinese Remainder Theorem. The group of units $\mathbb{Z}/n\mathbb{Z}^*$ is therefore isomorphic to the product of $\mathbb{Z}/p\mathbb{Z}^*$ and $\mathbb{Z}/q\mathbb{Z}^*$. The 2-torsion subgroup $\mathbb{Z}/n\mathbb{Z}^*[2]$ is then the product of the 2-torsion subgroups $\mathbb{Z}/p\mathbb{Z}^*[2] \times \mathbb{Z}/q\mathbb{Z}^*[2] = \{(\pm 1, \pm 1)\}$.

Note that the elements $\{\pm 1\}$ in $\mathbb{Z}/n\mathbb{Z}^*[2]$ are the diagonally embedded elements $\{(1,1), (-1,-1)\}$ in $\mathbb{Z}/p\mathbb{Z}^* \times \mathbb{Z}/q\mathbb{Z}^*$, but the elements $\{(1,-1), (-1,1)\}$ are not immediately recognizable in $\mathbb{Z}/n\mathbb{Z}^*$, but can be identified as indicated in the next part.

b. Suppose that $g \mapsto (-1,1)$. We note that the isomorphism of *rings* $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ preserves both addition and multiplication. The multiplication law determines the multiplicative group isomorphisms of the previous part.

We use the fact that $1 \mapsto (1,1)$, and then use addition to find $g+1 \mapsto (-1,1) + (1,1) = (0,2)$. Therefore $g+1$ is divisible by p in $\mathbb{Z}/n\mathbb{Z}$ but not by q, and so $\mathrm{GCD}(g+1, n) = p$. The other case, $g \mapsto (1,-1)$, is analogous and gives rise instead to the factor q.