HW 5 (to be tested on Mar 8)

1. Prove that the gcd can be found using the Euclidean algorithm in the ring of Gaussian integers. Also prove the Bezout identity.

2. Prove that for any integral domain, primes are irreducibles. Prove that irreducibles are primes in the ring of Gaussian integers.

3. Prove that $\phi(ab) = \phi(a)\phi(b)$ where a and b are coprime. (Take a look at the exercises in Childs' book for a hint.)

4. Prove that the inverse of a ring isomorphism is a ring homomorphism.

5. Define a vector space $(V, 0 \in V, \mathbb{F}, +, .)$ over a field F as a set V with operations $+ : V \times V \to V$ and $. : \mathbb{F} \times V \to V$ satisfying $(V, 0, +)$ is an Abelian group, and if $a, b \in \mathbb{F}, v \in V$, then $a.(b.v) = (ab).v$, $(a+b).v = a.v + b.v$, $1.v = v$, and $a.(v+w) = a.v + a.w$. Define the linear independence of vectors $v_1, \ldots, v_k$ as the non-existence of non-trivial $c_1, \ldots, c_k \in \mathbb{F}$ such that $\sum_i c_i v_i = 0$. Define a basis to be a set of linearly independent vectors such that every vector in the space is a linear combination of these. If a vector space has a finite basis, it is said to be finite-dimensional.

   (a) Prove that if V is a finite-dimensional vector space over a field F, then every basis has the same cardinality.

   (b) Prove that if $\mathbb{F}$ is a finite-field of characteristic p, then it is a vector space over $\mathbb{Z}_p$.

   (c) Conclude that any finite-field has size p^n where p is a prime.