Exercise Sheet 1

Exercise 2

Let $k \in \mathbb{Z}_{>0}$.

1. Show that $k = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ if and only if for every prime $p \equiv 3 \mod 4$, the exponent of p in the prime decomposition of k (in $\mathbb{Z}$) is even.

2. In this case, describe how to obtain all solutions $(a, b) \in \mathbb{Z}^2$.

Solution

<u>1.</u>

Let $k = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. We show that for for every prime $p \equiv 3 \mod 4$, the exponent of p in the prime decomposition of k is even.

First, let $p \in \mathbb{Z}$ be a prime number and consider p in $\mathbb{Z}[i]$. We have $N(p) = p$ and from the multiplicative property of the norm it follows that p is also irreducible in $\mathbb{Z}[i]$.

Now, we have $k = a^2 + b^2 = (a + ib)(a - ib)$ and let p be a prime in the decomposition of k. As p divides k and is a irreducible element in $\mathbb{Z}[i]$, it divides $(a + ib)$ or $(a - ib)$. But since p is real it has to divide both $(a + ib)$ and $(a - ib)$. Let p^n be the highest exponent that divides $(a + ib)$, then p^{2n} divides $(a + ib)(a - ib) = k$. We conclude that every prime in the prime decomposition of k have even exponents.