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

1.

Step 1: Let $z \in \mathbb{Z}_{>0}$ such that $z \equiv 3 \mod 4$. Then, $z = 3 + 4n$ for some $n \in \mathbb{Z}$. Consider $\alpha, \beta \in \mathbb{Z}_{>0}$ with $\alpha \equiv 1 \mod 4$ and $\beta \equiv 3 \mod 4$. For some $m_\alpha, m_\beta \in \mathbb{N}$, we have

$$z\alpha = (3 + 4n)(1 + 4m_\alpha) = 3 + 4n + 12m_\alpha + 16nm_\alpha \equiv 3 \mod 4 \tag{1}$$
$$z\beta = (3 + 4n)(3 + 4m_\alpha) = 9 + 12n + 12m_\alpha + 16nm_\alpha \equiv 1 \mod 4 \tag{2}$$
$$z2 = (3 + 4n)2 = 6 + 8n \equiv 2 \mod 4. \tag{3}$$

In short, z must be multiplied with an integer equivalent to 3 mod 4 if one wants to obtain an integer equivalent to 1 mod 4.

Step 2: Similarly as above, let $z \in \mathbb{Z}_{>0}$ such that $z \equiv 1 \mod 4$. Then, $z = 1 + 4n$ for some $n \in \mathbb{Z}$. Consider $\alpha, \beta \in \mathbb{Z}_{>0}$ with $\alpha \equiv 1 \mod 4$ and $\beta \equiv 3 \mod 4$. For some $m_\alpha, m_\beta \in \mathbb{N}$, we have

$$z\alpha = (1 + 4n)(1 + 4m_\alpha) = 1 + 4n + 4m_\alpha + 16nm_\alpha \equiv 1 \mod 4 \tag{4}$$
$$z\beta = (1 + 4n)(3 + 4m_\alpha) = 3 + 12n + 4m_\alpha + 16nm_\alpha \equiv 3 \mod 4 \tag{5}$$
$$z2 = (1 + 4n)2 = 2 + 8n \equiv 2 \mod 4. \tag{6}$$

In short, any product of integers equivalent to 1 mod 4 requires even number of integers equivalent to 3 mod 4.

Step 3: Let $k = a^2 + b^2$. According to Theorem 1.0.1. this is equivalent to $k = 2$ or $k \equiv 1 \mod 4$. If $k = 2$, then it is clear immediately. So consider the case $k \neq 2$. From step 1, we know that the prime factorization of k must contain even number of primes that are equivalent to 3 mod 4. Therefore, each exponent of such prime must also be even.

Step 2 shows that