Math 2001, Spring 2023. Katherine E. Stange.

1 Assignment

Prove the following theorem.

Theorem 1. *Let $n \in \mathbb{Z}$. If $n = x^2 + y^2$ for some integers x and y, then $n \not\equiv 3$ modulo 4.*

Hint: There are only four 'numbers' in the mod 4 world. Try squaring and adding them in all possible ways.

Proof. Let $n \in \mathbb{Z}$, and suppose $n = x^2 + y^2$ where x and y are integers. Then, $x \equiv x_0 \pmod 4$ and $y \equiv y_0 \pmod 4$, for some $x_0, y_0 \in \{0, 1, 2, 3\}$.

Working modulo 4, we have

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 0, \quad 3^2 \equiv 1.$$

Now,

$$x^2 + y^2 \equiv x_0^2 + y_0^2 \pmod 4.$$

The quantity $x_0^2 + y_0^2$ is equivalent modulo 4 to one of the following: $0 + 0 \equiv 0$, $0 + 1 \equiv 1$ or $1 + 1 \equiv 2$. Hence it is not $3 \mod p$. Therefore

$$x^2 + y^2 \not\equiv 3 \pmod 4.$$

□

The following is a shorter version of the same thing.

Proof. Working modulo 4, we have

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 0, \quad 3^2 \equiv 1.$$

Thus, any sum of squares modulo 4 is one of $0 + 0 \equiv 0$, $0 + 1 \equiv 1$ or $1 + 1 \equiv 2$. Thus a sum of squares cannot be $3 \pmod 4$. Since n can be written as a sum of squares, it is not 3 modulo 4. □