CHAPTER 2, QUESTION 11

11. Prove that if p is a prime with $p \equiv 3 \pmod 4$ then there do not exist integers x and y such that $p = x^2 + y^2$.

Solution. Let p be a prime with $p \equiv 3 \pmod 4$. Suppose that there exist integers x and y such that $p = x^2 + y^2$. Now $x^2 \equiv 0$ or $1 \pmod 4$ and $y^2 \equiv 0$ or $1 \pmod 4$ so that $p = x^2 + y^2 \equiv 0 + 0,\ 0 + 1,$ or $1 + 1 \pmod 4$, that is

$$p \equiv 0,\ 1 \text{ or } 2 \pmod 4,$$

contradicting $p \equiv 3 \pmod 4$. Hence there are no integers x and y such that $p = x^2 + y^2$ when p is a prime $\equiv 3 \pmod 4$. Note that the result is true if p is an arbitrary integer $\equiv 3 \pmod 4$. ∎

June 20, 2004