CHAPTER 2, QUESTION 12

12. Let $p$ be a prime. Use Theorem 2.5.1 and Question 11 to deduce that

$$p = x^2 + y^2 \iff p = 2 \text{ or } p \equiv 1 \pmod{4}.$$

Solution. Let $p$ be a prime. If $p = 2$ then $p = x^2 + y^2$ with $x = y = 1$. If $p \equiv 1 \pmod{4}$ there exist integers $x$ and $y$ such that $p = x^2 + y^2$ by Theorem 2.5.1. If $p \equiv 3 \pmod{4}$ there do not exist integers $x$ and $y$ such that $p = x^2 + y^2$ by Question 11. Hence,

$$p = x^2 + y^2 \iff p = 2 \text{ or } p \equiv 1 \pmod{4}. \qquad \blacksquare$$