CHAPTER 2, QUESTION 28

28. Prove that if $p$ is a prime with $p \equiv 1,\ 4 \pmod 5$ then there are integers $x$ and $y$ such that $p = x^2 + xy - y^2$. [Hint: Use Theorems 1.4.5 and 2.2.7.]

Solution. Let $p$ be a prime with $p \equiv 1$ or $4 \pmod 5$. Then, by the law of quadratic reciprocity, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{1 \text{ or } 4}{5}\right) = 1$. The domain $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{5}}{2})$ is Euclidean with respect to $\phi_5$ by Theorem 2.2.7. Then, by Theorem 2.1.2, $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{5}}{2})$ is a principal ideal domain. Now

$$T^2 + TU - U^2 = -1$$

for $T = 0$, $U = 1$. So, by Theorem 1.4.5, there exist integers $x$ and $y$ such that $p = x^2 + xy - y^2$. ∎

June 20, 2004