CHAPTER 2, QUESTION 21

21. Let p be a prime with $p \equiv 1,\ 5,\ 19,\ 23 \pmod{24}$. Deduce fromTheorem 2.5.8 that

$$p = x^2 - 6y^2, \text{ if } p \equiv 1,\ 19 \pmod{24},$$
$$p = 6y^2 - x^2, \text{ if } p \equiv 5,\ 23 \pmod{24},$$

for some integers x and y.

Solution. Let p be a prime with $p \equiv 1,\ 5,\ 19,\ 23 \pmod{24}$. By Theorem 2.5.8 there exist integers x and y such that either $p = x^2 - 6y^2$ or $p = 6y^2 - x^2$.

Suppose $p \equiv 1$ or $19 \pmod{24}$. Then $p \equiv 1 \pmod 3$. As $6y^2 - x^2 \equiv -x^2 \equiv 0$ or $2 \pmod 3$, $p \neq 6y^2 - x^2$. Hence $p = x^2 - 6y^2$.

Suppose $p \equiv 5$ or $23 \pmod{24}$. Then $p \equiv 2 \pmod 3$. As $x^2 - 6y^2 \equiv x^2 \equiv 0$ or $1 \pmod 3$, $p \neq x^2 - 6y^2$. Hence $p = 6y^2 - x^2$. ∎

June 20, 2004