CHAPTER 2, QUESTION 8

8. Prove a modification of Theorem 2.3.1 which allows one of the primes p and q to be the prime 2.

Solution. We prove

Theorem. Let m be a positive squarefree integer $\equiv 3 \pmod 4$. If there exists an odd prime q such that

$$\left(\frac{m}{p}\right) = -1,$$

and positive integers t and u such that

$$2t + qu = m,\ t \equiv \frac{m-1}{2} \pmod 4,\ q \nmid u,$$

and an integer r such that

$$r^2 \equiv 2t \pmod m,$$

then $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ is not Euclidean with respect to ϕ_m.

Proof. Suppose that $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ is Euclidean with respect to ϕ_m. Then there exist $\gamma, \delta \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ such that

$$r\sqrt{m} = m\gamma + \delta,\ \phi_m(\delta) < \phi_m(m).$$

Setting $\gamma = x + y\sqrt{m}\ \ (x, y \in \mathbb{Z})$ we obtain

$$\phi_m(r\sqrt{m} - m(x + y\sqrt{m})) < \phi_m(m),$$

that is

$$|m^2x^2 - m(r - my)^2| < m^2,$$

so that

$$|mx^2 - (r - my)^2| < m.$$

Since

$$mx^2 - (my - r)^2 \equiv -r^2 \equiv -2t \pmod m$$

and

$$0 < 2t < 2t + qu = m,$$

we must have

$$mx^2 - (my - r)^2 = -2t \text{ or } m - 2t,$$

that is

$$mX^2 - Y^2 = -2t \text{ or } qu$$

for integers $X (= x)$ and $Y (= my - r)$. Suppose that $mX^2 - Y^2 = 2t$. Taking this equation modulo 4, we obtain

$$3X^2 - Y^2 \equiv 2 \pmod 4.$$

Thus $X \equiv Y \equiv 1 \pmod 2$. Now taking the equation modulo 8, we have

$$m - 1 \equiv -2t \equiv -(m - 1) \pmod 8,$$

so that $m \equiv 1 \pmod 4$, contradicting $m \equiv 3 \pmod 4$. Now suppose that $mX^2 - Y^2 = qu$. As $\left(\frac{m}{q}\right) = -1$, we have $q \nmid m$. Also as $q \nmid u$ we have $q || qu$. Hence $q \nmid X$ and $q \nmid Y$. Thus,

$$\left(\frac{m}{q}\right) = \left(\frac{mX^2}{q}\right) = \left(\frac{Y^2}{q}\right) = 1,$$

contradicting $\left(\frac{m}{q}\right) = -1$. This proves that $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ is not Euclidean with respect to ϕ_m. ∎

It follows from this theorem that $\mathbb{Z} + \mathbb{Z}\sqrt{43}$ is not Euclidean with respect to ϕ_{43} by taking $m = 43$, $q = 11$, $t = 5$, $u = 3$, $r = 15$.

June 19, 2004