CHAPTER 3, QUESTION 14

14. Let p be a prime and m a positive nonsquare integer such that the Legendre symbol $\left(\frac{\pm p}{q}\right) = -1$ for some odd prime factor q of m. Prove that the equation $x^2 - my^2 = \pm p$ has no solution in integers x and y. Deduce that p is an irreducible element of $\mathbb{Z} + \mathbb{Z}\sqrt{m}$.

Solution. Suppose that x and y are integers such that

$$x^2 - my^2 = \pm p.$$

Taking this equation modulo q, we obtain

$$x^2 \equiv \pm p \pmod{q}$$

so that

$$\left(\frac{\pm p}{q}\right) = 0 \text{ or } 1$$

contradicting

$$\left(\frac{\pm p}{q}\right) = -1.$$

Hence the equation $x^2 - my^2 = \pm p$ has no solution in integers x and y.

Suppose that p is not an irreducible element of $\mathbb{Z} + \mathbb{Z}\sqrt{m}$. Then there exist $x, y, u, v \in \mathbb{Z}$ such that

$$p = (x + y\sqrt{m})(u + v\sqrt{m})$$

with $x + y\sqrt{m}, u + v\sqrt{m} \notin U(\mathbb{Z} + \mathbb{Z}\sqrt{n})$. Hence

$$p = (xu + yvm) + (xv + yu)\sqrt{m}.$$

As m is a positive nonsquare integers, $\sqrt{m}$ is irrational. Thus

$$p = xu + yvm, \quad xv + yu = 0.$$

Hence

$$(x - y\sqrt{m})(u - v\sqrt{m}) = (xu + yvm) - (xv + yu)\sqrt{m} = p.$$

Therefore

$$p^2 = (x^2 - my^2)(u^2 - mv^2).$$

Thus

$$x^2 - my^2 = \pm 1, \ \ \pm p, \ \ \pm p^2.$$

The possibility $x^2 - my^2 = \pm 1$ cannot occur as $x + y\sqrt{m} \notin U(\mathbb{Z} + \mathbb{Z}\sqrt{m})$. The possibility $x^2 - my^2 = \pm p$ cannot occur as the equation has no solutions in integers x and y. The possibility $x^2 - my^2 = \pm p^2$ cannot occur as $u + v\sqrt{m} \notin U(\mathbb{Z} + \mathbb{Z}\sqrt{m})$. ∎

June 20, 2004