Chapter 11, Question 14

14. Let p be a prime $\equiv 3 \pmod 8$. Let $t + u\sqrt{p}$ be the fundamental unit of $O_{\mathbb{Q}(\sqrt{p})}$, which necessarily is of norm 1. Starting from $t^2 - pu^2 = 1$, and using Dirichlet's way of proving Theorem 11.5.4, prove that the equation $x^2 - py^2 = -2$ is solvable in integers x and y.

Solution. We suppose first that t is odd so that $t^2 \equiv 1 \pmod 8$. Then, from $t^2 - pu^2 = 1$, we deduce that $u^2 \equiv 0 \pmod 8$ so that $u \equiv 0 \pmod 4$. Hence

$$t^2 = pu^2 + 1 \equiv 1 \pmod{16}$$

so that

$$\begin{aligned} &t \equiv 1 \pmod 8, \text{ if } t \equiv 1 \pmod 4 \\ &t \equiv -1 \pmod 8, \text{ if } t \equiv 3 \pmod 4. \end{aligned}$$

First we treat the case $t \equiv 1 \pmod 8$. In this case $\dfrac{t-1}{8}$ and $\dfrac{t+1}{2}$ are integers with

$$\begin{aligned} &\left(\frac{t-1}{8}\right)\left(\frac{t+1}{2}\right) = p\left(\frac{u}{4}\right)^2, \\ &\frac{t+1}{2} \equiv 1 \pmod 4 \text{ and } \gcd\left(\frac{t-1}{8}, \frac{t+1}{2}\right) = 1. \end{aligned}$$

Thus either

$$\frac{t-1}{8} = pv^2, \ \frac{t+1}{2} = w^2, \ \frac{u}{4} = vw,$$

or

$$\frac{t-1}{8} = v^2, \ \frac{t+1}{2} = pw^2, \ \frac{u}{4} = vw,$$

for coprime integers v and w with w odd. The latter case cannot occur as

$$\frac{t+1}{2} \equiv 1 \pmod 4, \ pw^2 \equiv 3 \pmod 8.$$

In the former case we have

$$w^2 - 4pv^2 = \left(\frac{t+1}{2}\right) - \left(\frac{t-1}{2}\right) = 1.$$

Thus $w+2v\sqrt{p}$ is a unit of norm 1. Clearly

$$\begin{aligned}(w+2v\sqrt{p})^2 &= (w^2+4pv^2)+4wv\sqrt{p}\\ &= \left(\frac{t+1}{2}+\frac{t-1}{2}\right)+u\sqrt{p}\\ &= t+u\sqrt{p}\end{aligned}$$

contradicting the minimality of $t+u\sqrt{p}$.

Now we treat the case $t\equiv -1 \pmod 8$. In this case $\frac{t+1}{8}$ and $\frac{t-1}{2}$ are integers with

$$\begin{aligned}&\left(\frac{t-1}{8}\right)\left(\frac{t+1}{8}\right)=p\left(\frac{u}{4}\right)^2,\\ &\frac{t-1}{2}\equiv -1 \pmod 4 \text{ and } \gcd\left(\frac{t-1}{2},\frac{t+1}{8}\right)=1.\end{aligned}$$

Thus either

$$\frac{t-1}{2}=pv^2,\ \frac{t+1}{8}=w^2,\ \frac{u}{4}=vw,$$

or

$$\frac{t-1}{2}=v^2,\ \frac{t+1}{8}=pw^2,\ \frac{u}{4}=vw,$$

for coprime integers v and w with v odd. The latter case cannot occur as

$$\frac{t-1}{2}\equiv 1 \pmod 4 \text{ and } v^2\equiv 1 \pmod 4).$$

In the former case we have

$$pv^2-4w^2=\left(\frac{t-1}{2}\right)-\left(\frac{t+1}{2}\right)=-1$$

so that $2w+v\sqrt{p}$ is a unit of norm 1. Clearly

$$(2w+v\sqrt{p})^2=(4w^2+pv^2)+4wv\sqrt{p}=t+u\sqrt{p},$$

contradicting the minimality of $t+u\sqrt{p}$. This proves that t is not odd, so t is even. Then, from $t^2-pu^2=1$, we deduce that $u\equiv 1 \pmod 2$. Hence $t\pm 1$ are odd integers such that

$$\begin{aligned}&(t-1)(t+1)=pu^2,\\ &\gcd(t-1,t+1)=1.\end{aligned}$$

Thus either

$$t - 1 = pv^2,\ t + 1 = w^2,\ u = vw,$$

or

$$t - 1 = v^2,\ t + 1 = pw^2,\ u = vw,$$

for coprime odd integers v and w. In the former case we have

$$w^2 - pv^2 = 2,$$

which is impossible as

$$w^2 - pv^2 \equiv 1 - 3 \equiv -2 \pmod 8.$$

Hence the latter possibility occurs and

$$v^2 - pw^2 = -2. \qquad \blacksquare$$

February 17, 2004