Chapter 12, Question 28

28. Let p be a prime with $p \equiv 3 \pmod 4$. It is known that $h(\mathbb{Q}(\sqrt{p}))$ is odd. Use this fact to prove that there exist integers a and b such that

$$a^2 - pb^2 = (-1)^{(p+1)/4}2.$$

[HINT: Consider the ideal $< 2, 1 + \sqrt{p} >$.]

Solution. Let p be a prime with $p \equiv 3 \pmod 4$ so that $h = h(\mathbb{Q}(\sqrt{p}))$ is odd. We consider the ideal $< 2, 1 + \sqrt{p} >$ of $O_{\mathbb{Q}(\sqrt{p})} = \mathbb{Z} + \mathbb{Z}\sqrt{p}$. On the one hand we have

$$< 2, 1 + \sqrt{p} >^2 = < 2 >$$

and on the other hand, as h is the class number of $\mathbb{Q}(\sqrt{p})$, we have

$$< 2, 1 + \sqrt{p} >^h = < \alpha >$$

for some $\alpha \in \mathbb{Z} + \mathbb{Z}\sqrt{p}$. As h is odd, $\dfrac{h-1}{2}$ is integer, and

$$\begin{aligned} < 2, 1 + \sqrt{p} > &= < 2, 1 + \sqrt{p} >^h \left(< 2, 1 + \sqrt{p} >^2\right)^{-(h-1)/2} \\ &= < \alpha >< 2 >^{-(h-1)/2} \\ &= < \frac{\alpha}{2^{(h-1)/2}} > . \end{aligned}$$

Since $< 2, 1 + \sqrt{p} >$ is an integral ideal of $\mathbb{Z} + \mathbb{Z}\sqrt{p}$, we have $\dfrac{\alpha}{2^{(h-1)/2}} \in \mathbb{Z} + \mathbb{Z}\sqrt{p}$. Thus there exist integers a and b such that

$$\frac{\alpha}{2^{(h-1)/2}} = a + b\sqrt{p}.$$

Then

$$< 2, 1 + \sqrt{p} > = < a + b\sqrt{p} > .$$

Takimg norms, we obtain

$$2 = |a^2 - pb^2|,$$

so that

$$a^2 - pb^2 = \pm 2.$$

If $b \equiv 0 \pmod 2$ then $a^2 \equiv 2 \pmod 4$, a contradiction. Hence $b \equiv 1 \pmod 2$. Thus $a \equiv 1 \pmod 2$ and

$$1 - p \equiv \pm 2 \pmod 8,$$

so that

$$\pm 1 \equiv \frac{1-p}{2} \equiv (-1)^{(p+1)/4} \pmod 4,$$

that is

$$\pm 1 = (-1)^{(p+1)/4},$$

and

$$a^2 - pb^2 = (-1)^{(p+1)/4} 2. \qquad \blacksquare$$

February 17, 2004