6(b) [Hard] Show that $1 + \sqrt{-5}$ is “prime” in the sense that if $(a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) = 1 + \sqrt{-5}$, then either $a + b\sqrt{-5} = \pm 1$ or $c + d\sqrt{-5} = \pm 1$.

**Proof.** I warned you this was difficult. It isn’t really, but we need some other concepts. In particular, we need the idea of a *norm*, which is a generalization of the idea of length. We define the norm of $a + b\sqrt{-5}$ to be

$$||a + b\sqrt{-5}|| = \sqrt{a^2 + 5b^2}.$$  

The useful property we’ll need (and we’ll prove this later) is the following multiplicative property of norms.

**Multiplicative Property of Norms.** For any integers $a$, $b$, $c$, and $d$, we have

$$||(a + b\sqrt{-5}) \cdot (c + d\sqrt{-5})|| = ||a + b\sqrt{-5}|| \cdot ||c + d\sqrt{-5}|| \tag{*}$$

or, equivalently,

$$||(a + b\sqrt{-5}) \cdot (c + d\sqrt{-5})||^2 = ||a + b\sqrt{-5}||^2 \cdot ||c + d\sqrt{-5}||^2 \tag{**}$$

We use this property as follows. We assume that $(a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) = 1 + \sqrt{-5}$, so that

$$||(a + b\sqrt{-5}) \cdot (c + d\sqrt{-5})||^2 = |1 + \sqrt{-5}|^2$$

The right-hand side is $1^2 + 5 \cdot 1^2 = 6$. We use the property to simplify the left-hand side to

$$||a + b\sqrt{-5}||^2 \cdot ||c + d\sqrt{-5}||^2 = 6,$$

or

$$(a^2 + 5b^2) \cdot (c^2 + 5d^2) = 6. \tag{†}$$

This is the key equality. Notice that everything is now an integer, and we can uniquely factor this equation. That is, $a^2 + 5b^2$ is one of 1, 2, 3 or 6. The key claim is that it can’t be 3 (and it can’t be 2 because $c^2 + 5d^2$ can’t be 3 either), so either $a^2 + 5b^2 = 1$ or $c^2 + 5d^2 = 1$. We’ll make this more explicit.

**Claim 1.** If $a$ and $b$ are integers, then $a^2 + 5b^2 \neq 3$.

**Proof.** This is simple: if $b \neq 0$, then $5b^2 > 3$. Hence we must have $b = 0$, and so the claim is simply that $a^2 \neq 3$. This is true as $a$ is an integer.

In fact more is true: $a^2 + 5b^2 \not\equiv 3 \mod 4$. We’ll prove this as well, but you may skip this without losing the thread of the proof.

We’ll show that $x^2 \equiv 0$ or $1 \mod 4$ for any $x$. Really this is just checking: if $x \equiv 0 \mod 4$, then $x^2 \equiv 0 \mod 4$. Let’s just make a small table:
Thus $a^2 + 5b^2 \equiv a^2 + 1 \cdot b^2 \not\equiv 3 \mod 4$, as I can’t add two of 0 and 1 to get 3.

**Claim 2.** If $(a^2 + 5b^2)(c^2 + 5d^2) = 6$, then either $a^2 + 5b^2 = 1$ or $c^2 + 5d^2 = 1$.

**Proof.** Since both terms on the left-hand side are integers, they must be factors of 6; that is, the only possible values for $a^2 + 5b^2$ are 1, 2, 3, or 6. We’ve already shown that $a^2 + 5b^2 \not\equiv 3$. If $a^2 + 5b^2 = 2$, then $c^2 + 5d^2 = 3$, which can’t happen by the first claim. Hence $a^2 + 5b^2$ is either 1 or 6, in which case $c^2 + 5d^2 = 1$.

Finally, we notice that if $a^2 + 5b^2 = 1$, then $a = \pm 1$. This is just as before (in the proof of Claim 1): $5b^2 > 1$ if $b \neq 0$, so we must have $b = 0$. Thus $a^2 = 1$, or $a = \pm 1$. Similarly, if $a^2 + 5b^2 = 6$, then $c^2 + 5d^2 = 1$ and $c = \pm 1$.

This completes the proof.

There is still the little matter of the proof of the multiplicative property of norms. This computation follows.

**Proof of Multiplicative Property of Norms.** We’ll prove equation (**); equation (*) is simply the square root of this.

We’ll compute each side of equation (**).

The left-hand side of equation (**) is given by

$$
| (a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) |^2 = | (ac - 5bd) + (bc + ad) \sqrt{-5} |^2 \\
= (ac - 5bd)^2 + 5(bc + ad)^2 \\
= a^2c^2 - 10abcd + 25b^2d^2 + 5b^2c^2 + 10abcd + 5a^2d^2 \\
= a^2c^2 + 25b^2d^2 + 5b^2c^2 + 5a^2d^2.
$$

On the other hand, the right-hand side of equation (**) is

$$
| a + b\sqrt{-5} |^2 \cdot | c + d\sqrt{-5} |^2 = (a^2 + 5b^2) \cdot (c^2 + 5d^2) \\
= a^2c^2 + 5b^2c^2 + 5a^2d^2 + 25c^2d^2.
$$

This two sums are equal, proving the property claimed.