Here is the end of the proof I had given in class.

Recall that our definition of "prime" – or more precisely, of "irreducible" – was the following:

Definition: We will say that an element $n \in R$ is *prime* if $|n| \neq 1$, and whenever $a, b \in R$ make $n = a \cdot b$ then $a \in \{1, -1, n, -n\}$

We gave this definition when R was the set of integers, but I started to experiment with other examples of what R might be. I asserted (but did not prove!) that nothing out-of-the-ordinary would happen if

$$R = \{a + b\,i; a, b \text{ are integers}\}$$

(this R is called the set of "Gaussian integers") but I noted that if you read the definition of *prime* with

$$R = \{a + b\sqrt{-3}; a, b \text{ are integers}\}$$

then 3 (meaning $3 + 0\sqrt{-3}$) is not a prime in R, because $3 = (\sqrt{-3})(-\sqrt{-3})$.

Even more interesting is the case of the "Goofy Integers"

$$R = \{a + b\sqrt{-5}; a, b \text{ are integers}\}$$

because in this case we have two factorizations of the goofy integer $9 + 0\sqrt{-5}$:

$$9 + 0\sqrt{-5} = (3 + 0\sqrt{-5}) \cdot (3 + 0\sqrt{-5}) = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$$

(you should check that both products really do yield 9) and each of the four factors is irreducible! In other words, the "Fundamental Theorem Of Arithmetic" is no longer true in the Goofy Integers. That should make you wonder, what is there about the *ordinary* integers that makes the FTA true for them? Hm... Guess we'll have to prove it some day!

Here is the proof that each of the four factors shown is itself irreducible. It's really the same idea for $2 \pm \sqrt{-5}$ as for 3, so let's just do that case in detail.

So suppose $a + b\sqrt{-5}$ and $c + d\sqrt{-5}$ are two goofy integers whose product is 3:

$$3 + 0\sqrt{-5} = (a + b\sqrt{-5}) \cdot (c + d\sqrt{-5})$$

When you expand this out, and compare the real and imaginary parts of both sides, you conclude that $ac - 5bd = 3$ and $ad + bc = 0$. Well, guess what: if you next expand $(a - b\sqrt{-5}) \cdot (c - d\sqrt{-5})$ you get $(ac - 5bd) - (ad + bc)\sqrt{-5} = 3 - 0\sqrt{-5} = 3$ again. So we can multiply out four factors together to get

$$(a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) \cdot (a - b\sqrt{-5}) \cdot (c - d\sqrt{-5}) = 3 \cdot 3 = 9$$

But the four factors can be multiplied in a different order to get

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

So now $a^2 + 5b^2$ and $c^2 + 5d^2$ are two ordinary integers which multiply out to be 9 (and it is clear that neither is negative). They can't both be 3, since there is no way to make $a^2 + 5b^2 = 3$ with integers a, b. So one of the two is a 1 and the other is a 9. But if (say) $a^2 + 5b^2 = 1$, then $a = \pm 1$ and $b = 0$. Thus one of our original factors is $a + b\sqrt{-5} = \pm 1 + 0\sqrt{-5} = \pm 1$.

To summarize: if we think we can write 3 as a product of two goofy integers, then at the end of the paragraph we conclude one of the factors is ± 1 (and hence the other is ± 3). From our definition of "prime", we see that 3 is indeed prime in the Goofy Integers. Similarly we can show $2 + \sqrt{-5}$ and $2 - \sqrt{-5}$ are primes. So in the Goofy Integers, 9 has two *different* decompositions as a product of two "primes"! So ... how can we be certain that this kind of event will never happen in the ordinary integers? We need proof! We will get it, later this semester.

PS – If you are interested in the TEX typesetting package, you might want to take a look at
`http://www.ma.utexas.edu/users/rusin/328K/0826.tex`
which is what I typed up and for the TEX program to get this page. If that amount of complexity seems to you like a good investment of your labor to get high-quality displays like this, then you need TEX!