EUCLID'S LEMMA, IRREDUCIBILITY AND PRIMALITY, IDEALS

Euclid's Lemma says:

Let $a, b, c \in \mathbb{Z}_{\geq 1}$. If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.

The proof is as follows. Since $\gcd(a, b) = 1$ we have $Aa + Bb = 1$ for some integers A and B. Multiply the condition by c to get $Aac + Bbc = c$. Of course $a \mid a$, and we are given that $a \mid bc$, so by the Linear Combination Lemma, $a \mid c$.

This should feel familiar. Indeed, it is virtually identical to the proof that:

Any irreducible element of $\mathbb{Z}$ is also prime.

Recall that proof, as follows. Let p be irreducible, and suppose that $p \mid ab$ where $a, b \in \mathbb{Z}_{\geq 1}$. We want to show that $p \mid a$ or $p \mid b$. If $p \mid a$ then we are done, so assume that $p \nmid a$, and now our task is to show that $p \mid b$. Since p is irreducible and $p \nmid a$, it follows that $\gcd(a, p) = 1$. Thus $Aa + Pp = 1$ for some integers A and P. Multiply the condition by b to get $Aab + Ppb = b$. We are given that $p \mid ab$, and of course $p \mid p$, so by the Linear Combination Lemma, $p \mid b$.

Thus the proof of Euclid's Lemma is essentially the proof that irreducibles are prime. In fact, en route to proving unique factorization in $\mathbb{Z}_{\geq 1}$ one can prove that irreducibles are prime by quoting Euclid's Lemma, and this is the lemma's purpose. Alternatively, once one has used the fact that irreducibles are prime to establish unique factorization in $\mathbb{Z}_{\geq 1}$ one can use unique factorization to prove Euclid's Lemma, but this deranges the ideas from their designed sequence.

Recall a second point that we have been discussing. Not only is it the case that

> *using the Linear Combination Lemma generally makes divisibility problems easier than returning to the definition of divisibility each time*,

but furthermore,

> *since ideals package linear combinations and their properties, using ideals can make the problems even easier.*

Here is an example. In the language of ideals, Euclid's Lemma says:

Let $a, b, c \in \mathbb{Z}_{\geq 1}$. If $I(bc) \subset I(a)$ and $I(a, b) = I(1)$ then $I(c) \subset I(a)$.

The proof is

$$I(c) = cI(1) = cI(a, b) = I(ac, bc) \subset I(ac, a) = I(a).$$

This proof makes no direct use of linear combination properties, but rather relies on past uses of them to establish the ideal properties being used here instead.