

## A Generic Euclid's Lemma

**Definition:** An element  $p$  of  $\mathbb{Z}$  or  $\mathbb{Q}[X]$  is called a *unit* if  $p|1$ . An element  $p$  is called *irreducible* if  $p$  is not a unit and, whenever  $a|p$ , either  $p|a$  or  $a|1$  ( $a$  is a unit).

Note that 0 is definitely not irreducible. Also, all prime integers are irreducible. In fact, the irreducible integers are exactly the primes and their negatives (since the only integers that divide 1 are  $\pm 1$ .) The units of  $\mathbb{Z}$  are just  $\pm 1$ . The units of  $\mathbb{Q}[X]$  are the non-zero constants. Generally speaking, any time  $p$  is irreducible, so is  $u \cdot p$  for any unit  $u$ .

**Euclid's Lemma:** Suppose  $p$  is irreducible and  $p|ab$ . Then either  $p|a$  or  $p|b$ .

NOTE: This version of Euclid's Lemma is for *both* integers and polynomials. The proof is valid in either case, too!

**Proof:** It is not difficult to see that the set of linear combinations of  $p$  and  $a$  is an ideal; call it  $I$ . By a previous result (Theorem 1.1.4 for integers and the analogous result for polynomials),  $I$  consists of all multiples of some  $d$ . Since  $p \neq 0$ ,  $d$  can't be 0.

Since both  $a$  and  $p$  are in  $I$ ,  $d$  divides both  $a$  and  $p$ . But  $p$  is irreducible, so either  $p|d$  or  $d|1$ .

Suppose first that  $p|d$ . Since  $d|a$ , exercise #7b from section 1.1 implies that  $p|a$ .

Now suppose that  $d|1$  and write  $1 = dc$ . Since  $d$  is in  $I$ , there are  $x$  and  $y$  such that  $d = ax + py$ .

Then

$$1 = dc = (ax + py)c$$

$$1 = axc + pyc$$

$$1b = (axc + pyc)b$$

$$b = axcb + pycb$$

$$b = abxc + pycb.$$

Recall the original hypothesis that  $p|ab$ . By #7c, this implies that  $p|ab(xc) + p(ycb)$ . Thus,  $p|b$ .