## 4. The Fundamental Theorem of Arithmetic & Euclid's Lemma

Right off the bat let's remind ourselves what the weird-looking word "lemma" means. A **lemma** is a mathematical theorem that is used to help prove other, more important theorems. Euclid's Lemma is a fantastic example of this, as it, itself, is a theorem but matematicians find it most useful in proving other results (like the Fundamental Theorem of Arithmetic).

**Lemma 6.2** (**Euclid's Lemma**). *Suppose $p$ is prime and that $p|(ab)$. Then $p|a$ or $p|b$.*

*proof. Suppose $p$ is prime and that $p|(ab)$. We proceed by setting up two cases.*

*Case 1. $p|a$ If $p|a$ then the conclusion holds, and we are done!*

*Case 2. $p \not| a$. In this case it follows that, since $p$ is prime, $\gcd(p, a) = 1$. Bezout's Identity then tells us that there are integers $x, y \in \mathbb{Z}$ so that*

$$ax + py = 1.$$

*If we multiply this equation by $b$ we find*

$$abx + bpy = b.$$

*Our hypothesis tells us that $p|(ab)$ and so it follows that $p|(abx)$. Moreover, $p$ also divides the second term, $bpy$. Since $p$ divides both terms in the sum on the left side, it follows that $p$ divides the right side. That is $p|a$.* □

It turns out that the converse to this lemma is also true, namely "If an integer $p$ has the following property then it is must be prime: whenever $p|(ab)$ it follows that $p|a \vee p|b$." One present both Euclid's Lemma and its converse altogether as an if-and-only-if statement

$$p \text{ is prime} \iff \Big(\forall\, a, b \in \mathbb{Z},\ p|(ab) \Rightarrow p|a \vee p|b\Big)$$

**Theorem 6.3** (**The Fundamental Theorem of Arithmetic**). *Every integer greater than 1 can be written as the product of primes. That is, $\forall\, a \in \mathbb{Z}$ if $a > 1$ then*

$$a = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$$

*where each $p_i$ is a prime and each $n_i \in \mathbb{N}$. Moreover, this expression is unique (up to re-ordering the primes).*

For example the integer 12 can be expressed as a product of primes, namely $12 = 2^2 \cdot 3$. Similarly

$$154746 = 2 \cdot 3^2 \cdot 8597.$$

Finding the prime factors of a given (large) number can be very, very difficult, but this theorem is amazing nonetheless. It tells us that *primes are the fundamental building blocks of natural numbers.*

There are many ways to prove the Fundamental Theorem of Arithmetic, and UH's own Dr. Min Ru has a lovely proof available by clicking this link. You'll note that (an extended version of) Euclid's Lemma is used to prove the uniqueness portion of the theorem.