TWO PROOFS OF EUCLID'S LEMMA

Lemma (Euclid). *Let p be a prime, and let a, b be integers. If $p \mid ab$ then $p \mid a$ or $p \mid b$.*

There are many ways to prove this lemma.

First Proof. Assume p is the smallest prime for which this assertion fails, and let a and b be such that $p \mid ab$ and $p \nmid a$ and $p \nmid b$. By replacing a and b with their remainders when dividing by p, we may assume that $1 \le a < p$ and $1 \le b < p$. Then $kp = ab$; clearly, $1 \le k < p$. We have $k \ne 1$ since p is a prime. Let q be a prime divisor of k. Then $q \mid ab$, and so, by the minimality assumption on p, we have $q \mid a$ or $q \mid b$. Then dividing q into k and into one of a or b, we obtain an equation $k'p = a'b'$, where $1 \le k' < k$, $1 \le a' < p$, and $1 \le b' < p$. Repeating this step as long as necessary, we arrive at an equation $k''p = a''b''$ with $k'' = 1$, $1 \le a'' < p$, and $1 \le b'' < p$. This equation contradicts the primality of p, completing the proof. $\square$

The second proof gives Euclid's Lemma is a corollary of the following.

Lemma. *Let let a and c be positive integers and let t be the smallest positive integer such that $c \mid at$. Let b be a positive integer such that $c \mid ab$. Then $t \mid b$. In particular, $t \mid c$.*

Proof. Assume $t \nmid b$; let q and r be such that $b = tq + r$ and $1 \le r < t$. Then

$$ab = atq + ar.$$

As c is a divisor of the left-hand side and of the first term on the right-hand side, it follows that c is also a divisor of the second term on the right-hand side; i.e., $c \mid ar$. This, however, contradicts the minimality of t. This contraction shows that $t \mid b$. Since we have $c \mid ac$, this assertion with $c = b$ shows that $t \mid c$ holds. $\square$

Corollary 1 (Euclid). *Let p be a prime, and let a and b be positive integers. If $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof. Let t be the smallest positive integer such that $p \mid at$. Then we have $t \mid b$ and $t \mid p$ by the Lemma. The latter implies that $t = 1$ or $t = p$. In the former case we have $p \mid a$, in the latter case we have $p \mid b$. $\square$

Corollary 2. *Let a, b, and c be positive integers such that $(b, c) = 1$. If $c \mid ab$ then $c \mid a$.*

Proof. Let t be the smallest positive integer such that $c \mid at$. Then we have $t \mid b$ and $t \mid c$ by the Lemma. As $(b, c) = 1$, we must have $t = 1$. Since $c \mid at$, this means that $c \mid a$. $\square$

[0]Notes for Course Mathematics 1311 at Brooklyn College of CUNY. Attila Máté, February 16, 2018.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX