# 1 Divisibility

Now that we have our basic building-blocks of proofs, we'll come up with some good concepts to build with them. So far the only idea we've really played with is parity. We'll followup with an idea which builds, after a fashion, on the concept of "even numbers"

**Definition 1.** An integer $a$ *divides* an integer $b$ (or, alternatively: $b$ is divisible by $a$; $b$ is a multiple of $a$), written $a \mid b$ if and only if $b = ka$ for some integer $k$.

Note that "$n$ is divisible by 2" and "$n$ is even" are the same statement: both assert that $n = 2k$ for some integer $k$.

There are several statements which are universal divisibility rules, which we can assert simply by observing that the equality they require is indeed true:

**Proposition 1.** *If $n$ is an integer, then it is the case that $n \mid n$, $n \mid 0$, and $1 \mid n$.*

*Proof.* For an integer $n$, $n = 1n$, and thus by definition, since 1 is an integer, $n \mid n$. Likewise, since $0 = 0n$, $n \mid 0$. Finally, since $n = n1$, it follows that $1 \mid n$. □

More interesting are divisibility rules which allow us to work from a known division to a new one. Here are a few such, along with their proofs:

**Proposition 2** (Transitivity of divisibility)**.** *For integers $a$, $b$, and $c$, if $a \mid b$ and $b \mid c$, then $a \mid c$.*

*Proof.* Our premise is that $a \mid b$ and $b \mid c$, so it must be the case that $b = ka$ for some integer $k$ and $c = \ell b$ for some integer $\ell$. Then

$$c = \ell b = \ell(ka) = (\ell k)a$$

so since $\ell k$ is an integer, $a \mid c$. □

**Lemma 1.** *For integers $a$, $b$, and $k$, if $a \mid b$, then $a \mid kb$.*

*Proof.* Our premise is that $a \mid b$, so it must be the case that $b = ra$ for some integer $r$. Then $kb = k(ra) = (kr)a$, so since $kr$ is an integer, $a \mid kb$. □

**Lemma 2.** *For integers $a$, $b$, and $c$, if $a \mid b$ and $a \mid c$, then $a \mid b + c$.*

*Proof.* Our premise is that $a \mid b$ and $a \mid c$, so it must be the case that $b = ka$ for some integer $k$ and $c = \ell a$ for some integer $\ell$. Then $b + c = ka + \ell a = (k + \ell)a$, so since $k + \ell$ is an integer, $a \mid (b + c)$. □

**Theorem 1.** *For integers $a$, $b$, $c$, $k$, and $\ell$, if $a \mid b$ and $a \mid c$, then $a \mid kb + \ell c$.*

*Proof.* Since $a \mid b$ and $a \mid c$, we may apply Lemma 1 to conclude taht $a \mid kb$ and $a \mid \ell c$ respectively. Then, applying Lemma 2 to these two most recently-concluded divisibility results, we see that $a \mid (kb + \ell c)$. □

The above three proofs show large-scale proof sturcture: we have auxiliary results, called *lemmas* (or *lemmata* if you want a particularly pretentious plural). Labelling them as lemmas telegraphs that they are in service of a larger result, normally called a *theorem*. With the right heavy lifting done by a lemma, a theorem, even a very broadly applicable result, may have a very simple proof.

Finally, for good measure, a proof best demonstrated by appeal to its contrapositive, and to a symmetry-reduction.

**Proposition 3.** *For integers $n$, $a$, and $b$, if $n \nmid ab$, then $n \nmid a$ and $n \nmid b$.*

*Proof.* We shall prove the contrapositive instead: we shall take as our presime that it is not the case that both $n \nmid a$ and $n \nmid b$ — in other words, at least one of $n \mid a$ or $n \mid b$ is true, and we shall strive to prove that $n \mid ab$.

Since one of the two interchangable statements $n \mid a$ or $n \mid b$ is true, we may assume without loss of generality that $n \mid a$ is true. By Lemma 1, it then follows that $n \mid ab$. □