

3 Some useful facts about divisibility

Recall: $a|b$ means a divides b , or b is divisible by a

Lemma 3.1. *Let $a, b, c \in \mathbb{Z}$. Then:*

1. *If $a|b$ and $a|c$ then $a|(b + c)$*
2. *If $a|b$ and $a|c$ then $a|(b - c)$*
3. *If $a|b$ then $a|(bc)$*
4. *If $a|b$ and $b|c$ then $a|c$*
5. *If $a|b$ and $b|a$ then $a = \pm b$*
6. *If $a|b$ and a and b are both > 0 then $a \leq b$*
7. *If $m \neq 0$ and $a|b$ then $(am)|(bm)$*

Proof. **1,2:** See Stein p.15

3,6,7: Exercises

4,5 : Class

□

Questions:

Why did we avoid division? (Or *did* we?)

What properties of arithmetic are used in the proofs?

Discuss the path from definition to assertion to proof.

What is the difference between a ‘Lemma’ and a ‘Theorem’?

Lemma 3.2. *Let $a \in \mathbb{Z}$, $a > 1$. Then a has at least one prime divisor.*

Remark: A prime divisor is sometimes called a *factor*.

Proof. Class. □

4 Euclid's theorem

This will be an example of *Proof by Contradiction* (or *reductio ad absurdum*).

Idea: To prove a statement **S**, first assume that **S** is *false*.

Next: Show that this assumption (of **S**'s falsity) leads to something which is *indisputably* false (eg, "0=1"). At this point we often say "This is a contradiction"

Conclude: That **S** must in fact be true.

Remarks:

Let P, Q, R be statements

Modus Tollens: From $P \implies Q$ and $\neg Q$ infer $\neg P$. (In this case, put $P = \neg S$ and $Q =$ the contradiction.)

Contrapositive: The statement $P \implies Q$ is logically equivalent to its contrapositive $(\neg Q) \implies (\neg P)$.

Theorem 4.1. (*Euclid*) *There are infinitely many primes.*

Proof. Suppose instead there are only *finitely* many primes: $2, 3, 5, 7, 11, \dots, p_N$

Form the number

$$M = (2 \times 3 \times 5 \times 7 \times 11 \times 13 \times \cdots \times p_N) + 1$$

M has a prime factor, p .

p must be one of the primes in the list, so

$$p | (2 \times 3 \times 5 \times \cdots \times p_N)$$

Then $p | (M - (2 \times 3 \times 5 \times \cdots \times p_N))$, i.e., $p | 1$

This is a contradiction (since the only positive divisor of 1 is itself).

□

Corollary 4.1. *Let $\{p_1, p_2, p_3, \dots, p_N\}$ be any finite set of primes. Then any prime factor of $(p_1 \times p_2 \times p_3 \times p_4 \times p_5 \cdots \times p_N) + 1$ is different from p_1, \dots, p_n*

Proof. This is the ‘middle part’ of the proof of Euclid’s Theorem. □