Divisibility

Ryan C. Daileda

Trinity University

Number Theory

Introduction

"*Mathematics is the queen of the sciences and number theory is the queen of mathematics.*" –C. F. Gauss

"*The great modern achievements of applied mathematics have been in relativity and quantum mechanics, and these subjects are, at present at any rate, almost as 'useless' as the theory of numbers.*" –G. H. Hardy

Number theory is concerned with the study of the arithmetic of $\mathbb{Z}$ and its generalizations.

It is possibly the most ancient mathematical discipline, yet there are still numerous unanswered number-theoretic questions.

Modern number theory uses tools from many other branches of mathematics: analysis, algebra, probability, topology, etc.

Preliminaries

An *integer* is any element of the set

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}.$$

The *natural numbers* are the positive integers:

$$\mathbb{N} = \mathbb{Z}^+ = \{n \in \mathbb{Z} \,|\, n > 0\} = \{1, 2, 3, 4, \ldots\}.$$

For convenience we also set

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}.$$

Fundamental Properties of $\mathbb{Z}$

The set $\mathbb{Z}$ together with ordinary addition and multiplication is a *commutative ring*:

- $\mathbb{Z}$ is closed under addition and multiplication, both of which are associative and commutative;
- $\mathbb{Z}$ has additive and multiplicative identity elements (0 and 1);
- $\mathbb{Z}$ has additive inverses, i.e. is closed under subtraction;
- Multiplication distributes over addition.

Furthermore, $\mathbb{Z}$ is a *domain*:

- For all $a, b \in \mathbb{Z}$, if $ab = 0$, then $a = 0$ or $b = 0$.

An Important Observation

Let $a, b \in \mathbb{Z}$.

We claim that If $b \neq 0$ and $|a| > 1$, then $|ab| > |b|$.

To prove this we simply observe that

$$|ab| - |b| = |a| \cdot |b| - |b| = (|a| - 1)|b| > 0$$

by our assumptions.

In particular, if $a, b \in \mathbb{N}$ and $a > 1$, then $ab > b$.

The Divisibility Relation in $\mathbb{Z}$

Definition

Let $a, b \in \mathbb{Z}$. We say that a *divides* b (denoted $a|b$) iff there is a $c \in \mathbb{Z}$ so that $b = ac$.

Examples.

1. We have $3|6$ since $6 = 3 \cdot 2$ and $2 \in \mathbb{Z}$.
2. For any $n \in \mathbb{Z}$ we have $\pm 1|n$, since $n = (\pm 1)(\pm n)$ and $\pm n \in \mathbb{Z}$.
3. Every integer n divides 0 since $0 = n \cdot 0$.
4. 0 only divides itself, since $n \cdot 0 = 0$ for all $n \in \mathbb{Z}$.

Remarks

Let $a, b \in \mathbb{Z}$.

- If a does *not* divide b, we write $a \nmid b$.
- If $a|b$ we also say that a is a *divisor* or *factor* of b, or that b is *divisible* by a.
- Suppose $a \neq 0$ and $a|b$, so that $b = ac$ for some $c \in \mathbb{Z}$. Then c is unique (HW) and clearly $c|b$ as well. We call c the divisor *complementary* to a.
- The preceding remark implies that the divisors of $b \neq 0$ always *occur in pairs*.

Properties of Divisibility

Theorem 1

For all $a, b, c, d \in \mathbb{Z}$*:*

1. $a|0$, $\pm 1|a$, $a|a$;
2. *If* $0|a$, *then* $a = 0$;
3. *If* $a|b$ *and* $b \neq 0$, *then* $|a| \leq |b|$;
4. *If* $a|1$, *then* $a = \pm 1$;
5. $a|b$ *and* $b|a$ *iff* $a = \pm b$;
6. *If* $a|b$ *and* $b|c$, *then* $a|c$;
7. *If* $a|b$ *and* $c|d$, *then* $ac|bd$;
8. *If* $a|b$ *and* $a|c$, *then* $a|xb + yc$ *for any* $x, y \in \mathbb{Z}$.

Sketch of Proof

1. We've already observed $a|0$ and $\pm 1|a$. That $a|a$ follows from $a = a \cdot 1$.

2. We've already noted zero can only divide itself.

3. If $a|b$ and $b \neq 0$, write $b = ac$ with $c \in \mathbb{Z}$. By part 2., $a \neq 0$ and $c \neq 0$. If $|c| = 1$, then

$$|b| = |ac| = |a| \cdot |c| = |a|,$$

and we're done. Otherwise, $|c| > 1$ and our earlier observation implies that $|b| = |ac| > |a|$, and again we're finished.

4. Suppose $a|1$ and write $1 = ac$ for some $c \in \mathbb{Z}$. Then a and c are both nonzero. Assume, for the sake of contradiction, that $|a| > 1$.
   By our earlier observation we would then have $1 = |ac| > |c| \geq 1$, which is impossible. Therefore $|a| = 1$ and $a = \pm 1$.

5. Suppose $a|b$ and $b|a$. Then there exist $c, d \in \mathbb{Z}$ so that $b = ac$ and $a = bd$. If either a or b is zero, then they both are, so that $a = b$. So we may assume a and b are both nonzero. Substituting the second equation into the first yields

   $$b = ac = (bd)c = b(dc) \quad \Rightarrow \quad b(1 - dc) = 0 \quad \Rightarrow \quad 1 - dc = 0,$$

   because $b \neq 0$ and $\mathbb{Z}$ is a domain. But then $1 = dc$ so that $d|1$. By part 3. we conclude that $d = \pm 1$ so that $a = bd = \pm b$. The converse is clear.

6. HW

7. HW

8. If $a|b$ and $a|c$, then we may find $r, s \in \mathbb{Z}$ so that $b = ar$ and $c = as$. Let $x, y \in \mathbb{Z}$. We then have

$$xb + yc = x(ar) + y(as) = a(xr + ys).$$

Since $xr + ys \in \mathbb{Z}$, this proves that $a|xb + yc$.

Remarks

- If $a, b \in \mathbb{N}$, then part 4. becomes

$$a|1 \quad \Rightarrow \quad a = 1,$$

and part 5. becomes

$$a|b \text{ and } b|a \quad \Rightarrow \quad a = b.$$

- In the language of relations, parts 1., 5., and 6. show that $a|b$ is a *partial ordering* of $\mathbb{N}$.
- An expression of the form $xa + yb$ is called an (integral) *linear combination* of a and b.

The Division Algorithm

Consider the "obviously" true statement $3 \nmid 7$. How might we prove it?

Because it is a negative statement, we try proof by contradiction. So we assume $3 \mid 7$.

This means there is a $c \in \mathbb{Z}$ so that $3c = 7$. But this implies $7/3 = c \in \mathbb{Z}$, which is a contradiction since $7/3 \notin \mathbb{Z}$.

Unfortunately, this "proof" is circular: to show that $7/3 \notin \mathbb{Z}$ we must show that $3 \nmid 7$, which is what we are trying to prove!

The Problem: There is no division operation defined on $\mathbb{Z}$, so we cannot solve the equation $3c = 7$ for c.

The following fundamental result tells us how to correctly "divide" in $\mathbb{Z}$.

Theorem 2 (The Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist unique $q, r \in \mathbb{Z}$ so that

1. $a = bq + r$;
2. $0 \leq r < |b|$.

Proof. See Textbook or Intro to Abstract notes. □

The quantities q and r are called the *quotient* and *remainder* (resp.) when a is divided by b.

q and r can be computed using elementary long division.

The remainder in the Division Algorithm measures the extent to which b fails to divide a.

Specifically, we have the following corollary.

Corollary 1

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Use the Division Algorithm to write $a = bq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < |b|$. Then

$$b|a \quad \Leftrightarrow \quad r = 0.$$

Proof. If $r = 0$, then we have $a = bq + r = bq$, which proves that $b|a$.

Conversely, if $b|a$, then there is a $c \in \mathbb{Z}$ so $a = bc = bc + 0$. The uniqueness statement of the Division Algorithm implies that $q = c$ and $r = 0$, as claimed. □

$3 \nmid 7$

Now we can carefully prove that $3 \nmid 7$.

Since

$$7 = 3 \cdot 2 + 1,$$

and $0 \leq 1 < 3$, uniqueness in the Division Algorithm implies that $q = 2$ and $r = 1 \neq 0$.

By the (contrapositive of the) corollary, we conclude that $3 \nmid 7$.

Example

Example 1

Prove that if $n \in \mathbb{Z}$ is odd, then $8|n^2 - 1$.

Proof. Let $n \in \mathbb{Z}$ be odd. Apply the Division Algorithm to write $n = 4q + r$ with $r \in \{0, 1, 2, 3\}$.

If $r = 0$ or $r = 2$, then $n = 4q = 2(2q)$ or $n = 4q + 2 = 2(2q + 1)$, both of which are even. So these cases are impossible.

This leaves us to consider what happens when $r = 1, 3$.

If $r = 1$, then $n - 1 = (4q + 1) - 1 = 4q$ so that $4|n - 1$. Since $n + 1$ is even, we also have $2|n + 1$. Multiplying these together gives us

$$8|(n - 1)(n + 1) = n^2 - 1.$$

Similarly, if $r = 3$, then $n + 1 = (4q + 3) + 1 = 4(q + 1)$ and $4|n + 1$. As $n - 1$ is also even, we likewise have $2|n - 1$, so that again

$$8|(n + 1)(n - 1) = n^2 - 1.$$

Having considered every possible remainder, our proof is complete. □