MATH 4150: Introduction to Number Theory

Frank Qiang
Instructor: Joshua Stucky

Georgia Institute of Technology
Fall 2025

Contents

Lecture 1

Aug. 18 — Divisibility

1.1 Basic Properties of Divisibility

Definition 1.1. Let $a, b \in \mathbb{Z}$. We say that a *divides* b, and we write $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = ac$. We also say that a is a *divisor* (or *factor*) of b. We write $a \nmid b$ if a does not divide b.

Example 1.1.1. We have the following:

1. We have $3 \mid 6$ since $6 = 3 \cdot 2$, and $3 \mid -6$ since $-6 = 3 \cdot (-2)$.
2. For any $a \in \mathbb{Z}$, we have $a \mid 0$ since $0 = a \cdot 0$.
3. Technically, we have $0 \mid 0$, but do not confuse this with the indeterminate form $0/0$.

Proposition 1.1. *Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$. In particular, divisibility is transitive.*

Proof. Since $a \mid b$ and $b \mid c$, there exist integers e, f such that $b = ae$ and $c = bf$. We can write

$$c = bf = (ae)f = a(ef),$$

so that a divides c by definition. □

Proposition 1.2. *Let $a, b, c, m, n \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid (am + bn)$. In other words, c divides any integral linear combination of a and b.*

Proof. Since $c \mid a$ and $c \mid b$, we have $a = ce$ and $b = cf$ for some $e, f \in \mathbb{Z}$. Then

$$am + bn = (ce)m + (cf)n = c(em + fn),$$

so that c divides $am + bn$ by definition. □

1.2 The Division Algorithm

Definition 1.2. Let $x \in \mathbb{R}$. The *greatest integer function* (or *floor function*) of x, denoted $[x]$ (or $\lfloor x \rfloor$), is the greatest integer less than or equal to x.

Example 1.2.1. We have the following:

1. If $a \in \mathbb{Z}$, then $[a] = a$. The converse is also true: If $[a] = a$ for $a \in \mathbb{R}$, then $a \in \mathbb{Z}$.
2. We have $[\pi] = 3$, $[e] = 2$, $[-1.5] = -2$, and $[-\pi] = -4$.

Lemma 1.1. *Let $x \in \mathbb{R}$. Then $x - 1 < [x] \leq x$.*

Proof. The upper bound is obvious. To show the lower bound, suppose to the contrary that $[x] \leq x - 1$. Then $[x] < [x] + 1 \leq x$, which contradicts the maximality of $[x]$ as $[x] + 1$ is an integer. $\square$

Example 1.2.2. We can write $5 = 3 \cdot 1 + 2$ and $26 = 6 \cdot 4 + 2$; this is the *division algorithm*.

Theorem 1.1 (Division algorithm). *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that*

$$a = bq + r, \quad 0 \leq r < b.$$

Call q the quotient *and r the* remainder *of the division.*

Proof. First we show existence. Let $q = [a/b]$ and $r = a - b[a/b]$. By construction, $a = bq + r$. To check that $0 \leq r < b$, note that by Lemma 1.1, we have $a/b - 1 < [a/b] \leq a/b$. Multiplying by $-b$ gives

$$-a \leq -b[a/b] < b - a,$$

and adding a gives the desired inequality $0 \leq a - b[a/b] = r < b$.

Now we prove uniqueness. Assume there are $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

$$a = bq_1 + r_1 = bq_2 + r_2, \quad 0 \leq r_1, r_2 < b.$$

Then $0 = (bq_1 + r_1) - (bq_2 + r_2) = b(q_1 - q_2) + (r_1 - r_2)$, so we find that

$$r_2 - r_1 = b(q_1 - q_2).$$

So $b \mid r_2 - r_1$. But $0 \leq r_1, r_2 < b$ implies $-b < r_2 - r_1 < b$, so we must have $r_2 - r_1 = 0$, i.e. $r_1 = r_2$. This then implies $0 = b(q_1 - q_2)$, which gives $q_1 - q_2 = 0$ since $b > 0$, so $q_1 = q_2$ as well. $\square$

Remark. In the division algorithm, we have $r = 0$ if and only if $b \mid a$.

Example 1.2.3. Suppose $a = -5$, $b = 3$. Then $q = [a/b] = -2$ and $r = a - b[a/b] = 1$, i.e.

$$-5 = 3 \cdot (-2) + 1.$$

Note that $-5 = 3 \cdot (-1) + (-2)$ also, but this does not contradict uniqueness since $-2 \notin [0, 3)$.

Definition 1.3. Let $n \in \mathbb{Z}$. Then n is *even* if $2 \mid n$, and *odd* otherwise.