MATH 4150: Introduction to Number Theory

Frank Qiang
Instructor: Joshua Stucky

Georgia Institute of Technology
Fall 2025

Contents

Lecture 1

Aug. 18 — Divisibility

Why is it impossible to have two docks? Because that would be a pair a' docks.

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. □

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. □

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.

Lecture 2

Aug. 20 — Prime Numbers

Two fish are in a tank. One says to the other, "Ha, how do you drive this thing?"

2.1 Prime Numbers

Definition 2.1. Let $p \in \mathbb{Z}$ with $p > 1$. Then p is *prime* if the only positive divisors of p and 1 and p. If $n \in \mathbb{Z}$, $n > 1$ and n is not prime, then n is *composite*.

Remark. The number 1 is neither prime nor composite.

Example 2.1.1. The following are prime numbers: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots$.

Lemma 2.1. *Every integer greater than* 1 *has a prime divisor.*

Proof. Assume to the contrary that there exists $n > 1$ that has no prime divisor. By the well-ordering principle,[1] we may take n to be the smallest such positive integer. Since n has no prime divisors, n cannot be prime. Thus n has a divisor a with $1 < a < n$. Since $1 < a < n$, a must have a prime divisor p by the minimality of n. But then $p \mid a$ and $a \mid n$, so $p \mid n$ by transitivity, a contradiction. □

Theorem 2.1 (Euclid)**.** *There are infinitely many prime numbers.*

Proof. Assume to the contrary that there are only finitely many primes $p_1, p_2, \ldots, p_n$. Consider

$$N = p_1 p_2 \cdots p_n + 1.$$

By Lemma 2.1, N has a prime divisor $p = p_j$ for some $1 \leq j \leq n$. Since p divides N and p divides $p_1 p_2 \cdots p_n$, p also divides $N - p_1 p_2 \cdots p_n = 1$, which is a contradiction. □

Exercise 2.1. Modify the proof and construct infinitely many problematic N.

2.2 Sieve of Eratosthenes

Proposition 2.1. *If n is composite, then n has a prime divisor that is less than or equal to $\sqrt{n}$.*

Proof. Since n is composite, $n = ab$ where $1 < a, b < n$. Without loss of generality, assume $a \leq b$. We claim $a \leq \sqrt{n}$. To see this, suppose to the contrary that $a > \sqrt{n}$. Then $n = ab \geq a^2 > n$, a contradiction. By Lemma 2.1, a has a prime divisor $p \leq a \leq \sqrt{n}$. But then $p \mid a$ and $a \mid n$, so $p \mid n$. □

[1] The *well-ordering principle* says that every nonempty subset of the positive integers contains a least element.

Remark. The proposition implies that if all the prime divisors of an integer n are greater than $\sqrt{n}$, then n is prime. So to check the primality of n, it suffices to check divisibility by primes $\leq \sqrt{n}$.

Example 2.1.2. The *sieve of Eratosthenes* proceeds as follows. To find primes ≤ 50, we can delete multiples of primes $\leq \sqrt{50} \approx 7.07$. To start, we know that 2 is prime. Then cross out all multiples of 2. The smallest number remaining is 3, which we now know must be prime. Then cross out all multiples of 3. Continue this process until we cross out all multiples of 7, and then all remaining numbers are prime.

2.3 Gaps in Primes

Proposition 2.2. *For any positive integer n, there are at least n consecutive composite positive integers.*

Proof. Consider the following list of n consecutive numbers:

$$(n+1)!+2, \quad (n+1)!+3, \quad (n+1)!+4, \quad \ldots, \quad (n+1)!+(n+1).$$

Note that for any $2 \leq m \leq n+1$, we have $m \mid m$ and $m \mid (n+1)!$, so m divides $(n+1)!+m$. Thus each number in the above list is composite, so we have at least n consecutive composite integers. □

Remark. With some modifications to this proof (namely a more "efficient" construction), one can find asymptotic lower bounds for the length of long prime gaps.

Conjecture 2.1.1. *There are infinitely many pairs of primes that differ by exactly 2.*

Remark. Zhang (2013) was able to show that there are infinitely many pairs of pairs of primes whose difference is $\leq 70,000,000$. This has been lowered to 246 by the Polymath project, which included Tao and Maynard. Assuming other strong conjectures (Elliot-Halberstam), we can get down to 6.

Remark. In addition to long and short prime gaps, we can also consider the average length of prime gaps. Gauss conjectured that as $x \to \infty$, the number of primes $\leq x$, denoted $\pi(x)$, satisfies

$$\pi(x) \sim \frac{x}{\log x},$$

i.e. $\pi(x)$ is asymptotic to $x/\log x$. Said differently, this says that the "probability" that an integer $\leq x$ is prime is $\pi(x)/x \sim 1/\log x$. This conjecture was proved independently in 1896 by de la Vallé-Poussin and Hadamard, and is now known as the *prime number theorem.*

Definition 2.2. Let $x \in \mathbb{R}$. Define $\pi(x) = |\{p : p \text{ prime}, p \leq x\}|$.

Theorem 2.2 (Prime number theorem)**.** *As $x \to \infty$, $\pi(x)$ is asymptotic to $x/\log x$, i.e.*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

2.4 Other Open Problems

Conjecture 2.2.1 (Goldbach)**.** *Every even integer ≥ 4 is a sum of two primes.*

Theorem 2.3 (Ternary Goldbach)**.** *Every odd integer ≥ 7 is a sum of three primes.*

Remark. Goldbach's conjecture implies ternary Goldbach (subtract 3), but not vice versa.

Definition 2.3. Primes of the form $p = 2^n - 1$ are called *Mersenne primes*, and primes of the form $p = 2^{2^n} + 1$ are called *Fermat primes*.

Conjecture 2.3.1. *There are infinitely many Mersenne primes but only finitely many Fermat primes.*

Lecture 3

Aug. 25 — Greatest Common Divisors

What do you call a root vegetable, fresh off the oven, and a pig that you throw off the balcony? One is a heated yam, and the other is a yeeted ham.

3.1 Greatest Common Divisors

Remark. Given $a, b \in \mathbb{Z}$, not both zero, we can consider the set

$$S = \{c \in \mathbb{Z} : c \mid a \text{ and } c \mid b\},$$

of common divisors of both a and b. Note that $\pm 1 \in S$, so S is nonempty, and S is also finite as at least one of a, b is nonzero. Thus S has a maximal element.

Definition 3.1. Let $a, b \in \mathbb{Z}$, not both zero. Then the *greatest common divisor* of a and b, denoted (a, b), is the largest integer d such that $d \mid a$ and $d \mid b$. If $(a, b) = 1$, then we say that a, b are *relatively prime* (or *coprime*).

Remark. Note that $(0, 0)$ is not defined. Also note that if $(a, b) = d$, then

$$(a, b) = (-a, b) = (a, -b) = (-a, -b) = d.$$

Example 3.1.1. We will compute $(24, 60)$. The list of positive divisors of 24 and 60 are

$$24 : 1, 2, 3, 4, 6, 8, 12, 24;$$
$$60 : 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.$$

We can then see that $(24, 60) = 12$.

Remark. In general, we have $(a, 0) = |a|$.

Proposition 3.1. *Let $(a, b) = d$. Then $(a/d, b/d) = 1$.*

Proof. Let $d' = (a/d, b/d) > 0$. Then $d' \mid (a/d)$ and $d' \mid (b/d)$, so there exist e, f such that $a/d = ed'$ and $b/d = fd'$. We can write this as $a = ed'd$ and $b = fd'd$. Thus $d'd$ is a common divisor of a and b, so we must have $d' = 1$ by the maximality of d. □

Proposition 3.2. *Let $a, b \in \mathbb{Z}$, not both zero, and let*

$$T = \{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}.$$

Then $\min T$ exists and is equal to (a, b).

Proof. Without loss of generality, we can assume $a \neq 0$. Note that $|a| \in T$, so T is nonempty. Thus by the well-ordering principle, T has a minimal element d. Then $d = m'a + n'b$ for some $m', n' \in \mathbb{Z}$. We will show that $d \mid a$, a similar argument shows that $d \mid b$. By the division algorithm, we may write

$$a = dq + r, \quad 0 \leq r < d.$$

It suffices to show that $r = 0$. We can rewrite the above as

$$r = a - dq = a - (m'a + n'b)q = a(1 - m'q) - b(n'q).$$

So r is an integral linear combination of a, b. Since d is the smallest positive integral linear combination of a, b and $0 \leq r < d$, we must have $r = 0$. So d is a common divisor of a, b.

Now suppose $c \mid a$ and $c \mid b$, then $c \mid (ma + nb)$, so c divides $d = m'a + n'b$. Thus $c \leq d$, so $d = (a, b)$. □

Remark. If $(a, b) = d$, then $d = ma + nb$ for some $m, n \in \mathbb{Z}$. If $d = 1$, then the converse also holds: If

$$1 = ma + nb,$$

and d' is a common divisor of a, b, then $d' \mid 1$, so $d' = 1$.

Remark. Along the way, we showed that any common divisor of a, b divides (a, b).

Definition 3.2. Let $a_1, \ldots, a_n \in \mathbb{Z}$, with at least one nonzero. Then the *greatest common divisor* of $a_1, \ldots, a_n$, denoted $(a_1, \ldots, a_n)$, is the largest integer d such that $d \mid a_i$ for $1 \leq i \leq n$. If $(a_1, \ldots, a_n) = 1$, then we say that $a_1, \ldots, a_n$ are *relatively prime*, and if $(a_i, a_j) = 1$ for all $1 \leq i \neq j \leq n$, then we say that $a_1, \ldots, a_n$ are *pairwise relatively prime*.

Remark. Pairwise relatively prime implies relatively prime, but the converse is not true (e.g. $\{2, 4, 3\}$).

3.2 The Euclidean Algorithm

Lemma 3.1. *If $a, b \in \mathbb{Z}$ with $0 < b \leq a$ and $a = bq + r$ with $q, r \in \mathbb{Z}$, then $(a, b) = (r, b)$.*

Proof. It suffices to show that the two sets of common divisors (of a, b and of r, b) are the same. Denote by S_1 and S_2 these two sets, respectively. First let $c \in S_1$, so $c \mid a$ and $c \mid b$. We can write

$$r = a - bq,$$

so we have $c \mid r$. Thus $c \in S_2$, so $S_1 \subseteq S_2$. Now let $c \in S_2$, so $c \mid r$ and $c \mid b$. We have

$$a = bq + r$$

by hypothesis, so $c \mid a$, i.e. $c \in S_1$. Thus $S_1 = S_2$, so $(a, b) = \max S_1 = \max S_2 = (r, b)$. □

Example 3.2.1. The above lemma allows us to compute greatest common divisors more efficiently. We will compute $(803, 154)$. We can write $803 = 5 \cdot 154 + 33$, so $(803, 154) = (154, 33)$. Continuing, we get

$$(803, 154) = (154, 33) = (33, 22) = (22, 11) = (11, 0) = 11.$$

Theorem 3.1 (Euclidean algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $0 < b \leq a$. Set $r_{-1} = a$, $r_0 = b$, and inductively write $r_{i-1} = q_i r_i + r_{i+1}$ by the division algorithm for $n \geq 1$. Then $r_n = 0$ for some $n \geq 1$ and $(a, b) = r_{n-1}$.*

Proof. Note that $r_1 > r_2 > r_3 > \cdots$. If $r_n \neq 0$ for all $n \geq 1$, then this is a strictly decreasing infinite sequence of positive integers, which is not possible. So $r_n = 0$ for some $n \geq 1$. The conclusion $(a, b) = r_{n-1}$ follows by repeatedly applying the lemma since $(a, b) = (r_i, r_{i+1}) = (r_{n-1}, 0) = r_{n-1}$. □

Example 3.2.2. By reversing this process, we can write (a, b) explicitly as an integer linear combination of a, b. Using the previous example of computing $(803, 154)$, we can see that

$$\begin{aligned}(803, 154) = 11 &= 33 - 1 \cdot 22 \\ &= 33 - 1 \cdot (154 - 4 \cdot 33) = 5 \cdot 33 - 1 \cdot 154 \\ &= 5 \cdot (803 - 5 \cdot 154) - 1 \cdot 154 = 5 \cdot 803 - 26 \cdot 154.\end{aligned}$$

Thus we have found that $(803, 154) = 5 \cdot 803 - 26 \cdot 154$. Note that this representation is not unique, e.g. we can also write $11 = 19 \cdot 803 - 99 \cdot 154$. In fact, there are infinitely many such representations.