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. $\square$

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. $\square$

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 $p \mid n$. $\square$

[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. $\square$

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

$$\begin{aligned} &24 : 1, 2, 3, 4, 6, 8, 12, 24; \\ &60 : 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60. \end{aligned}$$

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.

Lecture 4

Aug. 27 — Fundamental Theorem of Arithmetic

What's the difference between a mediocre clown and a rabbit in the gym? One's a bit funny, the other's a fit bunny.

4.1 The Fundamental Theorem of Arithmetic

Lemma 4.1 (Euclid)**.** *Let $a, b \in \mathbb{Z}$ and let p be a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. If $p \mid a$, then we are done, so assume $p \nmid a$. Then $(p, a) = 1$. Thus we can write $1 = ma + np$ for some $m, n \in \mathbb{Z}$. Since $p \mid ab$, we can write $ab = pc$ for some $c \in \mathbb{Z}$. Multiplying by b, we have

$$b = bma + bnp = m(cp) + nbp = p(mc + nb).$$

Thus we see that $p \mid b$, as desired. □

Remark. This fails if p is composite: Take $p = 6$, $a = 2$, and $b = 3$.

Exercise 4.1. Determine where the proof fails if p is composite.

Corollary 4.0.1. *Let $a_1, \ldots, a_n \in \mathbb{Z}$ and p a prime. If $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some $1 \leq i \leq n$.*

Proof. Induct on n. The base case $n = 1$ is trivial. If $n = 2$, then this is just Lemma 4.1. Now suppose $n \geq 2$, and we show the result for $n + 1$. Specifically, assume that if $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some $1 \leq i \leq n$. Suppose $p \mid a_1 \cdots a_n a_{n+1}$. Then $p \mid (a_1 \cdots a_n)a_{n+1}$. So by Lemma 4.1, we have $p \mid a_1 \cdots a_n$ or $p \mid a_{n+1}$. If $p \mid a_{n+1}$, then we are done. Otherwise, $p \mid a_1 \cdots a_n$, so $p \mid a_i$ for some $1 \leq i \leq n$ by the induction hypothesis. In particular, $p \mid a_i$ for some $1 \leq i \leq n + 1$, as desired. □

Theorem 4.1 (Fundamental theorem of arithmetic)**.** *Every integer $m > 1$ may be expressed in the form $m = p_1^{a_1} \cdots p_n^{a_n}$ where $p_1, \ldots, p_n$ are distinct primes and $a_1, \ldots, a_n$ are positive integers. This form is called the* prime factorization *of the integer m. Moreover, this factorization is essentially unique, i.e. unique up to permutations of the factors $p_i^{a_i}$.*

Proof. We first prove existence. Assume to the contrary that there exists $m > 1$ that does not have a prime factorization. Without loss of generality, we can assume m is the smallest such integer by the well-ordering principle. In particular, m cannot be prime. So $m = ab$ for some $1 < a, b < m$. Then a, b have prime factorizations. Thus so too does m, a contradiction.

Now we prove uniqueness. Assume that $m = p_1^{a_1} \cdots p_n^{a_n} = q_1^{b_1} \cdots q_r^{b_r}$. Without loss of generality, we can assume $p_1 < p_2 < \cdots < p_n$ and $q_1 < q_2 < \cdots < q_r$. We need to show that $n = r$, $p_i = q_i$ for each i, and $a_i = b_i$ for each i. Let $p_i \mid m$. Then $p_i \mid q_1^{b_1} \cdots q_r^{b_r}$, so $p_i \mid q_j$ for some $1 \le j \le r$. Thus $p_i = q_j$ since both are prime. Similarly, given q_i, we have $q_i = p_j$ for some j. Thus the primes in the two factorizations (as sets) are the same. Thus $n = r$, and by the ordering assumption, we have $p_i = q_i$ for each $1 \le i \le n$. So

$$m = p_1^{a_1} \cdots p_n^{a_n} = p_1^{b_1} \cdots p_n^{b_n}.$$

Suppose to the contrary that $a_i \neq b_i$ for some i. Without loss of generality, assume $a_i < b_i$. We have $p_i^{b_i} \mid m$, so $p_i^{b_i} \mid p_1^{a_1} \cdots p_{i-1}^{a_{i-1}} p_i^{a_i} p_{i+1}^{a_{i+1}} \cdots p_n^{a_n}$. Thus $p_i^{b_i - a_i} \mid p_1^{a_1} \cdots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \cdots p_n^{a_n}$. Since $a_i < b_i$, we have $b_i - a_i > 0$, so $p_i \mid p_1^{a_1} \cdots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \cdots p_n^{a_n}$ by the transitivity of divisibility. Then $p_i \mid p_j$ for some $j \neq i$, so $p_i = p_j$, which is a contradiction since the p_i are all distinct primes. This proves uniqueness. □

Remark. This is one reason why we do not consider 1 to be a prime, as we would lose uniqueness.

Example 4.0.1. We can write $60 = 2^2 \cdot 3 \cdot 5$ and $756 = 2^2 \cdot 3^3 \cdot 7$.

4.2 Least Common Multiples

Definition 4.1. Let $a, b \in \mathbb{Z}$ with $a, b > 0$. The *least common multiple* of a and b, denoted $[a, b]$, is the least positive integer m such that $a \mid m$ and $b \mid m$.

Remark. Since ab is a common multiple of a and b, $[a, b]$ always exists by the well-ordering principle.

Example 4.1.1. We will compute $[6, 7]$. The multiples of 6 and 7 include:

$$\begin{aligned} &6 : 6, 12, 18, 24, 30, 36, 42, 48, \ldots; \\ &7 : 7, 14, 21, 28, 35, 42, 49, \ldots. \end{aligned}$$

So we can see that $[6, 7] = 42 = 6 \cdot 7$. On the other hand, $[6, 8] = 24 \neq 6 \cdot 8$.

Remark. The fundamental theorem of arithmetic can be used to calculate both GCDs and LCMs.

Proposition 4.1. *Let $a, b \in \mathbb{Z}$ with $a, b > 1$. Write $a = p_1^{a_1} \cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdots p_n^{b_n}$, where the p_i are distinct primes, and $a_i, b_i \ge 0$. Then we have*

$$(a, b) = p_1^{\min\{a_1, b_1\}} \cdots p_n^{\min\{a_n, b_n\}} \quad \textit{and} \quad [a, b] = p_1^{\max\{a_1, b_1\}} \cdots p_n^{\max\{a_n, b_n\}}.$$

Proof. Left as an exercise. □

Example 4.1.2. Calculate $(756, 2205)$ and $[756, 2205]$. We can write

$$756 = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^1 \quad \text{and} \quad 2205 = 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^2.$$

So we have $(756, 2205) = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^1 = 63$ and $[756, 2205] = 2^2 \cdot 3^3 \cdot 5 \cdot 7^2 = 26460$.

Lemma 4.2. *Given $x, y \in \mathbb{R}$, we have* $\min\{x, y\} + \max\{x, y\} = x + y$.

Proof. The result is obvious if $x = y$. Otherwise, one is the minimum and the other is the maximum. □

Theorem 4.2. *Let $a, b \in \mathbb{Z}$ with $a, b > 1$. Then $(a, b)[a, b] = ab$.*

Proof. Write $a = p_1^{a_1} \cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdots p_n^{b_n}$ with $a_i, b_i \geq 0$ and p_i distinct. By Proposition 4.1,

$$\begin{aligned}(a,b)[a,b] &= p_1^{\min\{a_1,b_1\}} \cdots p_n^{\min\{a_n,b_n\}} p_1^{\max\{a_1,b_1\}} \cdots p_n^{\max\{a_n,b_n\}} \\ &= p_1^{\min\{a_1,b_1\}+\max\{a_1,b_1\}} \cdots p_n^{\min\{a_n,b_n\}+\max\{a_n,b_n\}} = p_1^{a_1+b_1} \cdots p_n^{a_n+b_n} = ab,\end{aligned}$$

where the third equality follows from Lemma 4.2. $\square$

Lecture 5

Sept. 3 — Congruences

No, Tony's the guy with no shins.

5.1 Dirichlet's Theorem

Theorem 5.1 (Dirichlet's theorem on primes in arithmetic progressions)**.** *Let $a, b \in \mathbb{Z}$ with $a, b > 0$ and $(a, b) = 1$. Then the arithmetic progression $a, a+b, a+2b, a+3b, \ldots$ contains infinitely many primes.*

Remark. Setting $a = b = 1$ recovers the fact that there are infinitely many primes.

Remark. The general case of Dirichlet's theorem is difficult, but we can use the fundamental theorem of arithmetic to prove some special cases, e.g. when $a = 3$ and $b = 4$.

Lemma 5.1. *Let $a, b \in \mathbb{Z}$. If a and b are expressible as $4n+1$, then so is their product ab.*

Proof. Let $a = 4m+1$ and $b = 4n+1$. Then

$$ab = (4m+1)(4n+1) = 16mn + 4m + 4n + 1 = 4(4mn + m + n) + 1,$$

which proves the desired result. □

Proposition 5.1. *There are infinitely many primes of the form $4n+3$ with $n \geq 0$.*

Proof. Assume to the contrary that there are finitely many primes of the form $4n+3$, say $3, p_1, \ldots, p_r$. Then consider the integer $N = 4p_1 \cdots p_r + 3$. The prime factorization of N must contain a prime of the form $4n+3$, since otherwise N would be a product of primes of the form $4n+1$, which must again be of the form $4n+1$. Thus we have $3 \mid N$ or $p_i \mid N$ for some $1 \leq i \leq r$.

If $3 \mid N$, then $3 \mid N - 3 = 4p_1 \ldots p_r$, which is a contradiction. Otherwise, $p_i \mid N$ for some $1 \leq i \leq r$, and we have $p_i \mid N - 4p_1 \cdots p_r = 3$, which is a contradiction as well. □

Remark. The same proof does not work for primes of the form $4n+1$, since a product of numbers of the form $4n+3$ is not necessarily again of the form $4n+3$.

5.2 Congruences

Definition 5.1. Let $a, b, m \in \mathbb{Z}$ with $m > 0$. Then we say that a is *congruent to b modulo m*, and we write $a \equiv b \pmod{m}$, if $m \mid (a - b)$. The integer m is called the *modulus* of the congruence. We write $a \not\equiv b \pmod{m}$ if a is not congruent to b modulo m.

Example 5.1.1. We have $25 \equiv 1 \pmod 4$ and $25 \equiv 4 \pmod 7$.

Proposition 5.2. *Congruence modulo m is an equivalence relation on $\mathbb{Z}$.*

Proof. Reflexivity is clear since $m \mid 0 = (a-a)$ any $a \in \mathbb{Z}$, so $a \equiv a \pmod m$. For symmetry, suppose that $a \equiv b \pmod m$. Then $m \mid a-b$. But then $m \mid (-1)(a-b) = b-a$, so $b \equiv a \pmod m$ as well.

Finally, for transitivity, suppose that $a \equiv b \pmod m$ and $b \equiv c \pmod m$. Then $m \mid a-b$ and $m \mid b-c$, so m also divides their sum $m \mid (a-b)+(b-c) = a-c$, i.e. $a \equiv c \pmod m$. □

Remark. A consequence of Proposition 5.2 is that $\mathbb{Z}$ is partitioned into its equivalence classes under congruence modulo m. For $a \in \mathbb{Z}$, we write $[a]$ to denote the equivalence class of a modulo m (not to be confused with the floor function).

Example 5.1.2. The equivalence classes of $\mathbb{Z}$ under congruence modulo 4 are

$$\begin{aligned}
[0] &= \{\dots,-8,-4,0,4,8,\dots\},\\
[1] &= \{\dots,-7,-3,1,5,9,\dots\},\\
[2] &= \{\dots,-6,-2,2,6,10,\dots\},\\
[3] &= \{\dots,-5,-1,3,7,11,\dots\}.
\end{aligned}$$

Definition 5.2. A set of m integers such that every integer is congruent modulo m to exactly one integer of the set is called a *complete residue system* modulo m.

Example 5.2.1. $\{0,1,2,3\}$ is a complete residue system modulo 4. So is $\{4,5,-6,-1\}$.

Proposition 5.3. *The set $\{0,1,\dots,m-1\}$ is a complete residue system modulo m.*

Proof. First we prove that every integer is congruent to one of $0,1,\dots,m-1$ modulo m. By the division algorithm, for any $a \in \mathbb{Z}$, there exist $q, r \in \mathbb{Z}$ with $0 \le r \le m-1$ such that $a = qm + r$. Thus we have $a - r = qm$, so $m \mid a-r$, i.e. $a \equiv r \pmod m$. This proves existence since $r \in \{0,1,\dots,m-1\}$.

Now we show uniqueness. Suppose $a \equiv r_1 \pmod m$ and $a \equiv r_2 \pmod m$ where $r_1, r_2 \in \{0,1,\dots,m-1\}$. By transitivity, we have $r_1 \equiv r_2 \pmod m$, so $m \mid r_1 - r_2$. But $0 \le r_1, r_2 \le m-1$, so

$$-(m-1) \le r_1 - r_2 \le m-1,$$

so we must have $r_1 - r_2 = 0$, i.e. $r_1 = r_2$. This proves uniqueness. □

Definition 5.3. The set $\{0,1,\dots,m-1\}$ is called the set of *least nonnegative residues* modulo m.

Proposition 5.4. *Let $a,b,c,d,m \in \mathbb{Z}$, $m > 0$ such that $a \equiv b \pmod m$ and $c \equiv d \pmod m$. Then*

1. $a + c \equiv b + d \pmod m$;
2. $ac \equiv bd \pmod m$.

Proof. Since $a \equiv b \pmod m$ and $c \equiv d \pmod m$, we have $m \mid b-a$ and $m \mid d-c$. Then m divides

$$(b-a)+(d-c) = (b+d)-(a+c),$$

so we have $a + c \equiv b + d \pmod m$. This proves (1).

To prove (2), note that since $m \mid a-b$, we also have $m \mid c(a-b)$. Likewise, $m \mid d-c$ implies $m \mid b(d-c)$. Then m divides the difference

$$c(a-b) - b(d-c) = ac - bd,$$

which shows that $ac \equiv bd \pmod{m}$. This shows (2). □

Remark. This shows that the congruence classes of $\mathbb{Z}$ modulo m form a *ring*.

Remark. Consider the complete residue system $\{0, 1, 2, 3\}$ modulo 4. Their squares modulo 4 are

$$\{0^2, 1^2, 2^2, 3^2\} \equiv \{0, 1, 0, 1\} \equiv \{0, 1\} \pmod{4}.$$