MATH 4150: Introduction to Number Theory

Frank Qiang
Instructor: Joshua Stucky

Georgia Institute of Technology
Fall 2025

Contents

Lecture 1

Aug. 18 — Divisibility

Something something pair a' docks. (I forgot to write it down oops.)

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. $\square$

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. $\square$

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 $(a, b) = (r_i, r_{i+1}) = (r_{n-1}, 0) = r_{n-1}$. $\square$

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 $1 \le i \le n$.*

Proof. Induct on n. The base case $n = 1$ is trivial. If $n = 2$, then this is just Lemma 4.1. Now suppose $n \ge 2$, 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 $1 \le i \le n$. 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 $1 \le i \le n$ by the induction hypothesis. In particular, $p \mid a_i$ for some $1 \le i \le n + 1$, 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 $1 \leq j \leq r$. 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 $1 \leq i \leq n$. 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 $a_i, b_i \geq 0$. Then we have*

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

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. □

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. $\square$

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. $\square$

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*.

Example 5.3.1. Consider the complete residue system $\{0, 1, 2, 3\}$ modulo 4. Their squares mod 4 are

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

Lecture 6

Sept. 8 — Congruences, Part 2

6.1 More on Congruences

Example 6.0.1. Compute a complete residue system modulo 5 using

- only even numbers: $\{0, 2, 4, 6, 8\}$,
- only prime numbers: $\{2, 3, 5, 11, 19\}$.

Example 6.0.2. Compute a complete residue system modulo 5 using only numbers $\equiv 1 \pmod 4$.

Remark. Recall that the set of equivalence classes of $\mathbb{Z}$ modulo m form a ring. In particular, we can construct addition and multiplication tables. For $m = 4$, this looks like:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Addition modulo 5 is similar, but the multiplication table for $m = 5$ is:

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Recall that a ring with no zero divisors (nonzero elements a, b such that $ab = 0$) is an *integral domain*, in particular we see from the multiplication table that $\mathbb{Z}/5\mathbb{Z}$ is an integral domain. Since a finite integral domain is automatically a *field*, we see that $\mathbb{Z}/5\mathbb{Z}$ is a field.

Proposition 6.1. *Let $a, b, c, m, \in \mathbb{Z}$ with $m > 0$. Then*

$$ca \equiv cb \pmod m \quad \textit{if and only if} \quad a \equiv b \pmod{m/(m, c)}.$$

In particular, if m is prime, then $ca \equiv cb \pmod m$ if and only if $a \equiv b \pmod m$ for $c \not\equiv 0 \pmod m$.

Proof. ($\Rightarrow$) We have $ca \equiv cb \pmod m$ if and only if $m \mid ca - cb = c(a - b)$. Let $d = (m, c)$. By the transitivity of divisibility, we have $(m/d) \mid (c/d)(a - b)$. But $(m/d, c/d) = 1$, so $(m/d) \mid a - b$. Then we have $a \equiv b \pmod{m/d}$ by the definition of congruence.

($\Leftarrow$) Again let $d = (m, c)$. Then $a \equiv b \pmod{m/d}$, so $(m/d) \mid a - b$. Then $m \mid d(a - b)$, and so

$$m \mid d(a - b)(c/d) = c(a - b) = ca - cb,$$

which means $ca \equiv cb \pmod{m}$ by the definition of congruence. $\square$

Remark. This shows that the congruence classes modulo m form a field if and only if m is prime.

6.2 Linear Congruences in One Variable

Definition 6.1. Let $a, b \in \mathbb{Z}$. A congruence of the form

$$ax \equiv b \pmod{m}$$

is called a *linear congruence* in the variable x.

Example 6.1.1. Consider the following linear congruences:

- $2x \equiv 3 \pmod{4}$ has no solutions;
- $2x \equiv 4 \pmod{6}$ has $x = 2, 5$ as solutions;
- $3x \equiv 9 \pmod{6}$ has $x = 1, 3, 5$ as solutions.

Theorem 6.1. *Let $ax \equiv b \pmod{m}$, and let $d = (a, m)$. If $d \nmid b$, then there are no solutions for x in $\mathbb{Z}$. If $d \mid b$, then the congruence has exactly d incongruent solutions modulo m in $\mathbb{Z}$.*

Proof. Note that $ax \equiv b \pmod{m}$ if and only if $m \mid ax - b$, if and only if $ax - b = my$ for some integer y. This is equivalent to $ax - my = b$. Thus $ax \equiv b \pmod{m}$ is solvable in x if and only if the equation $ax - my = b$ is solvable in x, y.

Let x, y be a solution of $ax - my = b$. Since $d \mid a$ and $d \mid m$, we must have $d \mid b$. Taking contrapositives, this proves the first part of the theorem.

Assume now that $d \mid b$. We prove the second part in 4 steps:

1. We will show that $ax \equiv b \pmod{m}$ has a solution x_0.
2. We will show that there are infinitely many solutions of a particular form involving x_0.
3. We will show that any solution has a particular form involving x_0. (Note that this combines with (2) to give all possible solutions.)
4. We will show that there are exactly d equivalence classes of solutions.

(1) Since $d = (a, m)$, there exist $r, s \in \mathbb{Z}$ such that $d = ra + sm$. Since $d \mid b$, we can write

$$b = \frac{b}{d} \cdot d = \frac{b}{d}(ra + sm) = \frac{br}{d} \cdot a + \frac{bs}{d} \cdot m.$$

Thus $b - a(br/d) = (bs/d)m$, so $m \mid b - a(br/d)$, so $a(br/d) \equiv b \pmod{m}$. Thus $x_0 = br/d$ is a solution.

(2) Let x_0 be any solution of $ax \equiv b \pmod{m}$. Consider $x_0 + (m/d)n$ for $n \in \mathbb{Z}$. Then

$$a(x_0 + (m/d)n) \equiv ax_0 + a(m/d)n \equiv b + (a/d)mn \equiv b \pmod{m},$$

so $x_0 + (m/d)n$ is also solution for any $n \in \mathbb{Z}$.

(3) Let x_0 be a solution of $ax \equiv b \pmod{m}$. Recall from the beginning of the proof that this is equivalent to there being $y_0 \in \mathbb{Z}$ such that $ax_0 - my_0 = b$. Let x be any other solution. Then $ax - my = b$ for some $y \in \mathbb{Z}$, so

$$0 = b - b = (ax_0 - my_0) - (ax - my) = a(x_0 - x) - m(y_0 - y),$$

which gives $a(x_0 - x) = m(y_0 - y)$. This is equivalent to $(a/d)(x_0 - x) = (m/d)(y_0 - y)$. Note that if $y_0 - y = 0$, then $x_0 - x = 0$ as well since $a/d \neq 0$. So we may assume $y_0 - y \neq 0$. Then

$$(m/d) \mid (a/d)(x_0 - x),$$

and since $(a/d, m/d) = 1$, we have $(m/d) \mid (x_0 - x)$. Thus $x \equiv x_0 \pmod{m/d}$. In particular, all solutions to $ax \equiv b \pmod{m}$ are given by $x = x_0 + (m/d)n$ for $n \in \mathbb{Z}$ and any particular solution x_0.

(4) Let $x_0 + (m/d)n_1$ and $x_0 + (m/d)n_2$ be solutions. Then we have

$$x_0 + (m/d)n_1 \equiv x_0 + (m/d)n_2 \pmod{m}$$

if and only if $(m/d)n_1 \equiv (m/d)n_2 \pmod{m}$. This happens if and only if $m \mid (m/d)(n_1 - n_2)$, if and only if $(m/d)(n_1 - n_2) = km$ for some $K \in \mathbb{Z}$, if and only if $n_1 - n_2 = kd$. In particular, this is equivalent to $n_1 \equiv n_2 \pmod{d}$. Since there are exactly d congruence classes for n, there are exactly d congruence classes of solutions as well, which completes the proof. $\square$

Lecture 7

Sept. 10 — Chinese Remainder Theorem

7.1 More on Linear Congruences

Corollary 7.0.1. *Consider the linear congruence $ax \equiv b \pmod{m}$ and let $d = (a, m)$. If $d \mid b$, then there are exactly d incongruent solutions modulo m, given by*

$$x = x_0 + \frac{m}{d} \cdot n, \quad n = 0, 1, \ldots, d - 1$$

where x_0 is any particular solution.

Example 7.0.1. We solve $16x \equiv 8 \pmod{28}$. We compute $d = (16, 28)$ by the Euclidean algorithm:

$$\begin{aligned} 28 &= 1 \cdot 16 + 12 \\ 16 &= 1 \cdot 12 + 4 \\ 12 &= 3 \cdot 4 + 0. \end{aligned}$$

So $d = 4$. Since $4 \mid 8$, the congruence has 4 incongruent solutions. Working backwards, we have

$$4 = 2 \cdot 16 + (-1) \cdot 28.$$

Multiplying by 2, we get that $8 = 4 \cdot 16 + (-2) \cdot 28$. Taking this equation modulo 28, we get

$$16 \cdot 4 \equiv 8 \pmod{28},$$

so $x_0 = 4$ is a particular solution. Thus all the incongruent solutions are given by $x = 4 + (28/4)n$ for $n = 0, 1, 2, 3$, that is $x = 4, 11, 18, 25$.

Definition 7.1. Any solution of $ax \equiv 1 \pmod{m}$ is called the *multiplicative inverse* of a modulo m. The multiplicative inverse of a is often denoted $\overline{a}$.

Corollary 7.0.2. *The congruence $ax \equiv 1 \pmod{m}$ has a solution if and only if $(a, m) = 1$. In this case, the congruence has a unique solution. In particular, the multiplicative inverse, if it exists, is unique.*

7.2 The Chinese Remainder Theorem

Example 7.1.1. Consider the following problem: Find a positive integer having remainder 2 when divided by 3, remainder 1 when divided by 4, and remainder 3 when divided by 5. The problem can be rephrased as asking for a solution to the system of congruences:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{4} \\ x \equiv 3 \pmod{5}. \end{cases}$$

Theorem 7.1 (Chinese remainder theorem)**.** *Let $m_1, \ldots, m_n$ be pairwise relatively prime positive integers, and let $b_1, \ldots, b_n \in \mathbb{Z}$. Then the system of congruences*

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv b_n \pmod{m_n} \end{cases}$$

has a unique solution modulo $M = m_1 \cdots m_n$.

Proof. Let $M = m_1 \cdots m_n$ and $M_i = M/m_i$. Then $(M_i, m_i) = 1$, so there are solutions to each system $M_i x_i \equiv 1 \pmod{m_i}$ given by $x_i = \overline{M}_i$. Consider

$$x = b_1 M_1 \overline{M}_1 + b_2 M_2 \overline{M}_2 + \cdots + b_n M_n \overline{M}_n.$$

Note that $m_i \mid M_j$ for $i \neq j$, so $x \equiv b_i M_i \overline{M}_i \equiv b_i \pmod{m_i}$, so x is a solution to the system.

For uniqueness modulo M, let x' be another solution. Then $x' \equiv b_i \pmod{m_i}$ for each $1 \leq i \leq n$. Then

$$x \equiv x' \pmod{m_i}, \quad 1 \leq i \leq n.$$

Thus $m_i \mid x - x'$, so $M \mid x - x'$ since the m_i are pairwise relatively prime, so $x \equiv x' \pmod{M}$. □

Example 7.1.2. We now solve Example 7.1.1. Using the notation in the proof, we have

$$(m_1, m_2, m_3) = (3, 4, 5), \quad (b_1, b_2, b_3) = (2, 1, 3), \quad M = 60, \quad (M_1, M_2, M_3) = (20, 15, 12).$$

We still need to compute $\overline{M}_i$. In general, this can be done via the Euclidean algorithm. In this case,

$$(\overline{M}_1, \overline{M}_2, \overline{M}_3) = (2, 3, 3).$$

Now we can calculate the solution using

$$x = b_1 M_1 \overline{M}_1 + b_2 M_2 \overline{M}_2 + b_3 M_3 \overline{M}_3 = (2 \cdot 20 \cdot 2) + (1 \cdot 15 \cdot 3) + (3 \cdot 12 \cdot 3) = 233.$$

Reducing modulo 60, we get that the unique solution is given by $x \equiv 53 \pmod{60}$.

7.3 Wilson's Theorem

Lemma 7.1. *Let p be a prime and let $a \in \mathbb{Z}$. Then a is its own inverse modulo p (i.e., $a \equiv \overline{a} \pmod{p}$) if and only if $a \equiv \pm 1 \pmod{p}$.*

Proof. ($\Rightarrow$) Suppose $a \equiv \overline{a} \pmod{p}$. Then $a^2 \equiv a\overline{a} \equiv 1 \pmod{p}$, so $p \mid a^2 - 1 = (a-1)(a+1)$. Since p is prime, we have $p \mid a - 1$ or $p \mid a + 1$, so $a \equiv \pm 1 \pmod{p}$.

($\Leftarrow$) This is obvious since $(\pm 1)^2 = 1$ in $\mathbb{Z}$, so they are also equal after reducing modulo p. □

Theorem 7.2 (Wilson's theorem)**.** *Let p be a prime. Then $(p-1)! \equiv -1 \pmod{p}$.*

Example 7.1.3. The idea behind the proof is the following: Concretely, if $p = 11$, we have

$$(11-1)! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \pmod{11}$$

By Lemma 7.1, 10 and 1 are their own inverses modulo 11. For each other integer $2 \le n \le 9$, we can pair them with their inverses: $(2,6)$, $(3,4)$, $(5,9)$, $(7,8)$. Then we can write

$$(11-1)! \equiv (9 \cdot 5) \cdot (8 \cdot 7) \cdot (6 \cdot 2) \cdot (4 \cdot 3) \cdot 10 \cdot 1 \equiv 10 \cdot 1 \equiv -1 \pmod{11}.$$

Proof of Theorem 7.2. We can easily check the theorem for $p = 2, 3$, so suppose $p > 3$ is a prime. Then each a with $1 \le a \le p-1$ has a unique inverse modulo p, and this inverse is distinct from a if $2 \le a \le p-2$. Pair each such integer with its inverse modulo p, say a and a'. The product of all of these pairs is $(p-2)!$, so $(p-2)! \equiv 1 \pmod{p}$. Thus $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$. □

Proposition 7.1 (Converse of Wilson's theorem)**.** *Let $n \in \mathbb{Z}$ with $n > 1$. If $(n-1)! \equiv -1 \pmod{n}$, then n is prime.*

Proof. Suppose $n = ab$ with $1 \le a < n$. It suffices to show that $a = 1$. Since $a < n$, we have $a \mid (n-1)!$. Also, $n \mid (n-1)! + 1$ by assumption, so $a \mid (n-1)! + 1$ also since $a \mid n$. Thus

$$a \mid ((n-1)! + 1) - (n-1)! = 1,$$

so we must have $a = 1$. □

Definition 7.2. A prime p is a *Wilson prime* if $(p-1)! \equiv -1 \pmod{p^2}$.

Example 7.2.1. The first few Wilson primes are $5, 13, 563$. In fact, these are the only known ones.

Lecture 8

Sept. 15 — Fermat's Little Theorem

What do you call it when you have your grandmother on speed dial? It's an insta gram.

8.1 Fermat's Little Theorem

Theorem 8.1 (Fermat's little theorem)**.** *Let p be a prime and $a \in \mathbb{Z}$ such that $p \nmid a$. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. Consider the $p-1$ integers $a, 2a, 3a, \dots, (p-1)a$. Note that $p \nmid a_i$ for any $1 \leq i \leq p-1$. Note also that no two of these integers are congruent modulo p: If $ai \equiv aj \pmod{p}$ for some $i \neq j$, then we can multiply by the inverse $\overline{a}$ of a (which exists since $p \nmid a$) to get $i \equiv j \pmod{p}$, which is impossible. Thus $\{a, 2a \dots, (p-1)a\}$ is a complete nonzero residue system, so

$$a(2a)(3a)\cdots((p-1)a) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}.$$

Then $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$, so $a^{p-1} \equiv 1 \pmod{p}$ since $p \nmid (p-1)!$. □

Corollary 8.1.1. *Let p be prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then a^{p-2} is the inverse of a modulo p.*

Proof. By Fermat's little theorem, $a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod{p}$. □

Corollary 8.1.2. *Let p be prime and $a \in \mathbb{Z}$. Then $a^p \equiv a \pmod{p}$.*

Proof. If $p \mid a$, then both sides are congruent to 0 modulo p. Otherwise, if $p \nmid a$, then we can write $a^p = a \cdot a^{p-1} \equiv a \cdot 1 = a \pmod{p}$ by Fermat's little theorem. □

Corollary 8.1.3. *Let p be prime. Then $2^p \equiv 2 \pmod{p}$.*

Definition 8.1. If $n \in \mathbb{Z}$ is composite and $2^n \equiv 2 \pmod{n}$, then n is called a *pseudoprime.*

Remark. It is known that there are infinitely many (even and odd) pseudoprimes.

Example 8.1.1. Consider $n = 341 = 11 \cdot 31$. To prove that $2^{341} \equiv 2 \pmod{341}$, it suffices to show that $2^{341} \equiv 2 \pmod{11}$ and $2^{341} \equiv 2 \pmod{31}$ by the Chinese remainder theorem. Note that

$$\begin{aligned} 2^{341} = (2^{10})^{34} \cdot 2 \equiv 1^{34} \cdot 2 = 2 \pmod{11} \\ 2^{341} = (2^{30})^{11} \cdot 2^{11} \equiv 1^{11} \cdot (2^5)^2 \cdot 2 \equiv 1^2 \cdot 2 = 2 \pmod{31} \end{aligned}$$

by Fermat's little theorem, so 341 is a pseudoprime.

8.2 Euler's Theorem

Definition 8.2. Let $n \in \mathbb{Z}$, $n > 0$. *Euler's phi function*, denoted $\varphi(n)$, is the number of positive integers $\leq n$ that are relatively prime to n. In other words,

$$\varphi(n) = \#\{m \in \mathbb{Z} : 1 \leq m \leq n, (m, n) = 1\}.$$

Example 8.2.1. We have $\varphi(4) = 2$, $\varphi(14) = 6$, and $\varphi(p) = p - 1$ for any prime p.

Theorem 8.2 (Euler's theorem)**.** *Let $a, m \in \mathbb{Z}$ with $m > 0$. If $(a, m) = 1$, then*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Proof. Let $r_1, r_2, \ldots, r_{\varphi(m)}$ be the distinct positive integers not exceeding m such that $(r_i, m) = 1$. Then consider the integers $ar_1, ar_2, \ldots, ar_{\varphi(m)}$. Note first that $(ar_i, m) = 1$ since $(r_i, m) = 1$ and $(a, m) = 1$ by assumption. Note also that $ar_i \not\equiv ar_j \pmod{m}$ for $i \neq j$ since $\overline{a}$ exists (since $(a, m) = 1$), and multiplying by $\overline{a}$ implies $r_i \equiv r_j \pmod{m}$, which is impossible. Thus the least nonnegative residues of $\{ar_1, \ldots, ar_{\varphi(m)}\}$ coincide with $\{r_1, \ldots, r_{\varphi(m)}\}$, so we have

$$(ar_1)(ar_2)\cdots(ar_{\varphi(m)}) = r_1 r_2 \cdots r_{\varphi(m)} \pmod{m},$$

thus $a^{\varphi(m)}(r_1 \cdots r_{\varphi(m)}) \equiv (r_1 \cdots r_{\varphi(m)}) \pmod{m}$. Since $(r_1 \cdots r_{\varphi(m)}, m) = 1$, the inverse of $r_1 \cdots r_{\varphi(m)}$ modulo m exists, and multiplying by the inverse gives $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Remark. Taking $m = p$ recovers Fermat's little theorem since $\varphi(p) = p - 1$ for prime p.

Definition 8.3. Let m be a positive integer. A set of $\varphi(m)$ integers such that each integer is relatively prime to m and no two are congruent modulo m is called a *reduced residue system* modulo m.

Example 8.3.1. $\{1, 5, 7, 11\}$ is a reduced residue system modulo 12. So is

$$\{5(1), 5(5), 5(7), 5(11)\} = \{5, 25, 35, 55\}.$$

For a prime p, the set $\{1, 2, \ldots, p - 1\}$ is always a reduced residue system modulo p.

Corollary 8.2.1. *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Then $\overline{a} \equiv a^{\varphi(m)-1} \pmod{m}$.*

8.3 Arithmetic Functions and Multiplicativity

Definition 8.4. An *arithmetic function* is a function whose domain is the set of positive integers.

Example 8.4.1. The following are examples of arithmetic functions:

1. Euler's φ function;
2. $v(n)$, the number of positive divisors of n;
3. $\sigma(n)$, the sum of the positive divisors of n;
4. $\omega(n)$, the number of distinct prime factors of n;
5. $p(n)$, the number of integer partitions of n;

6. $\Omega(n)$, the number of total prime factors (counted with multiplicity) of n.

Definition 8.5. An arithmetic function f is *multiplicative* if $f(mn) = f(m)f(n)$ whenever $(m,n) = 1$. We say that f is *completely multiplicative* if $f(mn) = f(m)f(n)$ for all m,n.

Remark. Note that if $n > 1$, then we can write $n = p_1^{a_1} \cdots p_r^{a_r}$. If f is multiplicative, then

$$f(n) = f(p_1^{a_1} \cdots p_r^{a_r}) = f(p_1^{a_1}) \cdots f(p_r^{a_r}).$$

So multiplicative functions are determined by their values at prime powers. If f is completely multiplicative, then $f(n) = f(p_1)^{a_1} \cdots f(p_r)^{a_r}$ and f is determined by its values at primes.

Example 8.5.1. The functions φ, v, σ from Example 8.4.1 are multiplicative, while ω, p, Ω are not.

Example 8.5.2. The functions $f(n) = 1$ and $f(n) = 0$ are completely multiplicative. The function f defined by $f(1) = 1$ and $f(n) > 0$ if $n > 1$ is also completely multiplicative.

Remark. If f is multiplicative and not identically zero, then $f(1) = 1$. To see this, take n such that $f(n) \neq 0$ (since f is not identically zero). Then $f(n) = f(n \cdot 1) = f(n)f(1)$, so $f(1) = 1$ since $f(n) \neq 0$.

Lecture 9

Sept. 17 — Arithmetic Functions

9.1 Properties of Multiplicative Functions

Remark. We write $\sum_{d|n} f(d)$ to denote a sum over the positive divisors of n. For instance,

$$\sum_{d|12} f(d) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12).$$

Theorem 9.1. *Let f be an arithmetic function, and for $n \in \mathbb{Z}$, $n > 0$, define*

$$F(n) = \sum_{d|n} f(d).$$

If f is multiplicative, then so is F.

Proof. Let m, n be relative prime. We need to show that $F(mn) = F(m)F(n)$. We have

$$F(mn) = \sum_{d|mn} f(d).$$

We claim that every divisor d of mn can be written uniquely as $d = d_1 d_2$, where $d_1 \mid m$ and $d_2 \mid m$. Moreover, any such product $d_1 d_2$ is a divisor of mn. To see this, write $m = p_1^{a_1} \dots p_r^{a_r}$ and $n = q_1^{b_1} \dots q_s^{b_s}$, where all the $p_1, \dots, p_r, q_1, \dots, q_s$ are distinct. Then if $d \mid mn$, then

$$d = p_1^{e_1} \dots p_r^{e_r} q_1^{f_1} \dots q_s^{f_s}, \quad 0 \le e_i \le q_i, 0 \le f_j \le b_j.$$

Then we must choose $d_1 = p_1^{e_1} \dots p_r^{e_r}$ and $d_2 = q_1^{f_1} \dots q_s^{f_s}$, which proves the claim.

Using the claim, we can split the sum into

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) = \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) = F(m)F(n),$$

where we note that $(d_1, d_2) = 1$ since $(m, n) = 1$. $\square$

Example 9.0.1. Let $m = 4$, $n = 3$. Then we can write

$$\begin{aligned} F(3 \cdot 4) = \sum_{d|12} f(d) &= f(1) + f(2) + f(3) + f(4) + f(6) + f(12) \\ &= f(1 \cdot 1) + f(1 \cdot 2) + f(3 \cdot 1) + f(1 \cdot 4) + f(3 \cdot 2) + f(3 \cdot 4) \\ &= f(1)f(1) + f(1)f(2) + f(3)f(1) + f(1)f(4) + f(3)f(2) + f(3)f(4) \\ &= (f(1) + f(3))(f(1) + f(2) + f(4)) = F(3)F(4). \end{aligned}$$

9.2 Properties of the Euler Phi Function

Theorem 9.2. *The Euler φ function is multiplicative.*

Proof. Let $m, n \in \mathbb{Z}$, $m, n > 0$ with $(m, n) = 1$. We need to show that $\varphi(mn) = \varphi(m)\varphi(n)$. Consider the array of positive integers $\leq mn$ organized as follows:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ i & m+i & 2m+i & \cdots & (n-1)m+i \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m & 2m & 3m & \cdots & nm \end{array}$$

Consider the ith row. If $(i, m) > 1$, then no element on the ith row is relatively prime to m (and hence cannot be relatively prime to mn). Thus we may restrict our attention to those i that satisfy $(i, m) = 1$. There are, by definition, $\varphi(m)$ such values of i. The entries in the ith row are

$$i, \quad m+i, \quad 2m+i, \quad \ldots, \quad (n-1)m+i.$$

We claim that this is a complete residue system modulo n. To see this, suppose that

$$km + i \equiv jm + i \pmod{n}, \quad 0 \leq k, j \leq n-1.$$

Then $km \equiv jm \pmod{n}$. Since $(m, n) = 1$, this implies $k \equiv j \pmod{n}$. Since $0 \leq k, j \leq n-1$, we must have $k = j$. The claim follows since we have n non-congruent elements (modulo n) in the list. Thus, there are $\varphi(n)$ elements in the ith row that are relatively prime to n. Also, $(km + i, m) = (i, m) = 1$ by the Euclidean algorithm, so they are relatively prime to m as well. Thus $\varphi(mn) = \varphi(m)\varphi(n)$. □

Theorem 9.3. *Let p be prime, $a \in \mathbb{Z}$, $a > 0$. Then $\varphi(p^a) = p^a - p^{a-1}$.*

Proof. The total number of integers not exceeding p^a is p^a. The only integers not relatively prime to p^a are the multiples of p: $p, 2p, 3p, \ldots, (p^{a-1})p$. There are p^{a-1} such integers, so $\varphi(p^a) = p^a - p^{a-1}$. □

Theorem 9.4. *Let $n \in \mathbb{Z}$, $n > 0$. Then*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Proof. Write $n = p_1^{a_1} \ldots p_r^{a_r}$. Then

$$\begin{aligned} \varphi(n) = \varphi(p_1^{a_1} \cdots p_r^{a_r}) &= \varphi(p_1^{a_1}) \cdots \varphi(p_r^{a_r}) = (p_1^{a_1} - p_1^{a_1-1}) \cdots (p_r^{a_r} - p_r^{a_r-1}) \\ &= p_1^{a_1} \cdots p_r^{a_r} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \end{aligned}$$

This proves the desired formula. □

Remark. One can interpret Theorem 9.4 probabilistically: It says that $\varphi(n)$ is n times the "probability" that an integer is not divisible by any of the primes dividing n.

Example 9.0.2. Consider $n = 504 = 2^3 \cdot 3^2 \cdot 7$. Then $\varphi(n)$ is given by

$$\varphi(504) = 504\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right) = 504 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 144.$$

Theorem 9.5 (Gauss)**.** *Let $n \in \mathbb{Z}$, $n > 0$. Then*

$$\sum_{d|n} \varphi(d) = n.$$

Proof. Let d be a divisor of n. Define the set

$$S_d = \{1 \leq m \leq n : (m, n) = d\}.$$

Note that $(m, n) = d$ if and only if $(m/d, n/d) = 1$. Thus $|S_d| = \varphi(n/d)$. Note also that every integer less than or equal to n belongs to exactly one of the S_d, so

$$n = \sum_{d|n} |S_d| = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d),$$

which the last equality follows since $\{d : d \mid n\} = \{n/d : d \mid n\}$. □

Example 9.0.3. Let $n = 12$. We verify that $12 = \sum_{d|12} \varphi(d)$. Write the table

d	S_d
1	$\{1, 5, 7, 11\}$
2	$\{2, 10\}$
3	$\{3, 9\}$
4	$\{4, 8\}$
6	$\{6\}$
12	$\{12\}$

Summing the $|S_d| = \varphi(12/d)$, we indeed get $12 = 4 + 2 + 2 + 2 + 1 + 1$.

Lecture 10

Sept. 22 — Exam 1 Review

Why are Saturday and Sunday the strongest days? The other are week days.

10.1 Practice Problems

Exercise 10.1. Show that φ is multiplicative but not completely multiplicative.

Proof. The idea for the first part is to draw an $m \times n$ table of the first mn integers, see the proof of Theorem 9.2 for the details. For the second part, note that $\varphi(2) = 1$, $\varphi(2)^2 = 1$, but $\varphi(4) = 2$. $\square$

Alternative proof. Let R_k denote the set of residue classes modulo k that are coprime to k. Note that $|R_k| = \varphi(k)$, so it suffices to show there is a bijection $\psi : R_{mn} \to R_m \times R_n$ for $(m, n) = 1$. Define

$$\psi(a) = (a \bmod m, a \bmod n).$$

To see that ψ is surjective, let $(b, c) \in R_m \times R_n$. Since $(m, n) = 1$, by the Chinese remainder theorem there exists $a \in \mathbb{Z}$, defined modulo mn, such that $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$. So $\psi(a) = (b, c)$. Note that $(a, mn) = 1$ since $(a, m) = (b, m) = 1$ and $(a, n) = (c, n) = 1$, so $a \in R_{mn}$. Injectivity follows since the choice of a is unique modulo mn by the Chinese remainder theorem. $\square$

Exercise 10.2. Compute $(163, 67)$ by the Euclidean algorithm.

Proof. We compute that

$$\begin{aligned}(163, 67) &= (163 - 134, 67) = (29, 67)\\ &= (29, 67 - 2 \cdot 29) = (29, 9)\\ &= (29 - 3 \cdot 9, 9) = (2, 9)\\ &= (2, 9 - 4 \cdot 2) = (2, 1),\end{aligned}$$

so we have $(163, 67) = 1$. $\square$

Exercise 10.3. State and prove Wilson's theorem.

Proof. Wilson's theorem states that $(p-1)! \equiv -1 \pmod{p}$ for prime p (the converse also holds). The idea behind the proof is to note that each residue modulo p other than ± 1 can be paired with its (distinct) additive inverse modulo p. For the details, see the proof of Theorem 7.2. $\square$

Exercise 10.4. Find the least positive solution x to the congruence $x \equiv 20^{110} \pmod{17}$.

Proof. Use Fermat's little theorem: The division algorithm gives $110 = 6 \cdot 16 + 14$, so

$$\begin{aligned} x &\equiv 20^{6\cdot 16+14} \equiv (20^{16})^6 \cdot 20^{14} \pmod{17} \\ &= 1^6 \cdot 20^{14} \equiv 20^{14} = 3^{14} \pmod{17}. \end{aligned}$$

Multiplying both sides by 3^2 gives $9x \equiv 3^2 x \equiv 3^{16} \equiv 1 \pmod{17}$, so it suffices to find the inverse of 9 modulo 17. Using the Euclidean algorithm, we have

$$(17, 9) = (17 - 9, 9) = (8, 9) = (8, 9 - 8) = (8, 1) = 1,$$

so $1 = 9 - 8 = 9 - (17 - 9) = 2 \cdot 9 - 17$. Thus $\overline{9} \equiv 2 \pmod{17}$, so we can take $x = 2$. □

Exercise 10.5. Find the least positive solution x to the congruence $x \equiv 38^{110} \pmod{21}$.

Proof. First we compute that $\varphi(21) = \varphi(7)\varphi(3) = 6 \cdot 2 = 12$. By Euler's theorem,

$$x \equiv 38^{110} \equiv 17^{110} \equiv 179 \cdot 12 + 2 \equiv (17^{12})^9 \cdot 17^2 \equiv 17^2 \pmod{21}.$$

Now we notice that $17^2 \equiv (-4)^2 \equiv 16 \pmod{21}$, so we can take $x = 16$. □

Exercise 10.6. Let $a, m \in \mathbb{Z}$ and $m > 1$. If $(a, m) = 1$, show that $a^{\varphi(m)-1}$ is the multiplicative inverse of a modulo m.

Proof. By Euler's theorem, $a \cdot a^{\varphi(m)-1} = a^{\varphi(m)} \equiv 1 \pmod{m}$, so $\overline{a} \equiv a^{\varphi(m)-1} \pmod{m}$. □

Exercise 10.7. Prove that for odd primes p, we have $2(p-3)! \equiv -1 \pmod{p}$.

Proof. By Wilson's theorem, $(p-1)! \equiv -1 \pmod{p}$. Then we have

$$(p-3)!(p-2)(p-1) \equiv -1 \pmod{p},$$

so $2(p-3)! \equiv -1 \pmod{p}$ since $(p-2)(p-1) \equiv 2 \pmod{p}$. □

Exercise 10.8. Find integers a, b such that $(a, b) = 3$ and $a + b = 66$.

Proof. It suffices to write $a = 3a_1$, $b = 3b_1$, where $(a_1, b_1) = 1$. One way to do this is $(a_1, b_1) = (1, 21)$:

$$3(a_1 + b_1) = 3(1 + 21) = 3 \cdot 22 = 66.$$

Thus we may take $a = 3$, $b = 63$. □

Remark. Recall that a *reduced* residue system modulo m is a set $\{r_1, \ldots, r_{\varphi(m)}\}$ of integers coprime to m and pairwise incongruent modulo m. Note that the r_i themselves need not be coprime, in fact they may share arbitrarily large common factors: Take any $r_\ell \neq 1$ and consider

$$\{r_\ell r_1, \ldots, r_\ell r_{\varphi(m)}\}.$$

By repeating this, we can get arbitrarily large powers of r_ℓ as a common factor.