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. □

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 $a_1, \dots, a_n \in \mathbb{Z}$, with at least one nonzero. Then the *greatest common divisor* of $a_1, \dots, a_n$, denoted $(a_1, \dots, a_n)$, is the largest integer d such that $d \mid a_i$ for $1 \leq i \leq n$. If $(a_1, \dots, a_n) = 1$, then we say that $a_1, \dots, a_n$ are *relatively prime*, and if $(a_i, a_j) = 1$ for all $1 \leq i \neq j \leq n$, then we say that $a_1, \dots, a_n$ 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 $a_1, \dots, a_n \in \mathbb{Z}$ 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 $p_1, \dots, p_n$ are distinct primes and $a_1, \dots, a_n$ 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*

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

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. □

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*.

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

$\times$	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:

$\times$	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. □

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. □

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 $m_1, \dots, m_n$ be pairwise relatively prime positive integers, and let $b_1, \dots, b_n \in \mathbb{Z}$. 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 $2 \leq n \leq 9$, 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 $1 \leq a \leq p-1$ has a unique inverse modulo p, and this inverse is distinct from a if $2 \leq a \leq p-2$. 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 $1 \leq a < n$. 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 $a, 2a, 3a, \ldots, (p-1)a$. 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 $\{a, 2a \ldots, (p-1)a\}$ 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. $\tau(n)$, 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

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

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 $(m, n) = 1$. □

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*

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

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

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

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*

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

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

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

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

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

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 $12 = \sum_{d\mid 12}\varphi(d)$. 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 $\varphi(4) = 2$. □

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. □

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 $(163, 67) = 1$. □

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. □

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.

Lecture 11

Sept. 29 — Arithmetic Functions, Part 2

11.1 The Divisor Function

Definition 11.1. Let $n \in \mathbb{Z}$. The *number of positive divisors* of n, denoted $\tau(n)$, is defined by

$$\tau(n) = \#\{d \in \mathbb{Z} : d > 0, d \mid n\}.$$

Theorem 11.1. *$\tau(n)$ is multiplicative.*

Proof. Observe that $\tau(n) = \sum_{d|n} 1$ and 1 is multiplicative, so the result follows from Theorem 9.1. □

Remark. Since $\tau(n)$ is multiplicative, it is determined by its behavior on prime powers.

Theorem 11.2. *Let p be prime and let $a \in \mathbb{Z}$, $a > 0$. Then $\tau(p^a) = a + 1$.*

Proof. The divisors of p^a are exactly the integers $1, p, p^2, \ldots, p^a$. There are $a + 1$ of these. □

Theorem 11.3. *Let $n = p_1^{a_1} \cdots p_r^{a_r}$ with $p_1, \ldots, p_r$ distinct primes and $a_1, \ldots, a_r$ positive integers. Then*

$$\tau(n) = \prod_{i=1}^{r} (a_i + 1).$$

Proof. This follows from τ being multiplicative and Theorem 11.2. □

Remark. For some interesting reading about $\tau(n)$, see *Dirichlet's divisor problem.*

Example 11.1.1. Consider $504 = 2^3 \cdot 3^2 \cdot 7$. Then $\tau(504) = (3 + 1)(2 + 1)(1 + 1) = 24$.

11.2 The Sum of Divisors Function

Definition 11.2. Let $n \in \mathbb{Z}$, $n > 0$. The *sum of divisors function*, denoted $\sigma(n)$, is defined by

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

Theorem 11.4. *$\sigma(n)$ is multiplicative.*

Proof. This follows from $f(d) = d$ being multiplicative and Theorem 9.1. □

Theorem 11.5. *Let p be a prime and $a \in \mathbb{Z}$, $a > 0$. Then $\sigma(p^a) = (p^{a+1} - 1)/(p - 1)$.*

Proof. The divisors of p^a are $1, p, p^2, \dots, p^a$, so

$$\sigma(p^a) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}$$

by the formula for a (finite) geometric series. □

Theorem 11.6. *Let $n = p_1^{a_1} \cdots p_r^{a_r}$ with $p_1, \dots, p_r$ distinct primes and $a_1, \dots, a_r$ positive integers. Then*

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Example 11.2.1. Consider $504 = 2^3 \cdot 3^2 \cdot 7$. Then

$$\sigma(504) = \frac{2^{3+1} - 1}{2 - 1} \cdot \frac{3^{2+1} - 1}{3 - 1} \cdot \frac{7^{1+1} - 1}{7 - 1} = 15 \cdot 13 \cdot 8 = 1560.$$

11.3 Perfect Numbers

Definition 11.3. Let $n \in \mathbb{Z}$, $n > 0$. Then n is a *perfect number* if $\sigma(n) = 2n$, or $\sigma(n) - n = n$.

Remark. Note that $\sigma(n) - n$ is the sum of *proper* divisors of n, so perfect numbers are those that equal the sum of their proper divisors.

Example 11.3.1. 6 and 28 are perfect numbers.

Conjecture 11.6.1. *There are infinitely many perfect numbers.*

Conjecture 11.6.2. *All perfect numbers are even.*

Theorem 11.7. *Let $n \in \mathbb{Z}$, $n > 0$. Then n is an even perfect number if and only if*

$$n = 2^{p-1}(2^p - 1)$$

for some prime p, and $2^p - 1$ is prime (i.e. $2^p - 1$ is a Mersenne prime).

Proof. ($\Rightarrow$ Euler) Assume n is an even perfect number. Then we can write $n = 2^a b$ with $a, b \in \mathbb{Z}$, $a \geq 1$, and b odd. Then we have

$$\sigma(2^a b) = \sigma(2^a)\sigma(b) = (2^{a+1} - 1)\sigma(b).$$

Also, since n is perfect, we can also write $\sigma(2^a b) = 2 \cdot 2^a b = 2^{a+1} b$, thus

$$(2^{a+1} - 1)\sigma(b) = 2^{a+1} b. \tag{1}$$

This implies that $2^{a+1} \mid (2^{a+1} - 1)\sigma(b)$, so $2^{a+1} \mid \sigma(b)$ since $(2^{a+1}, 2^{a+1} - 1) = 1$. Then $\sigma(b) = 2^{a+1} c$ (2) for some integer $c \geq 1$. Substituting this into (1), we get

$$(2^{a+1} - 1)2^{a+1} c = 2^{a+1} b,$$

so we have $(2^{a+1}-1)c = b$ (3). We now show that $c = 1$. Suppose to the contrary that $c > 1$. Then (3) implies that b has at least 3 distinct divisors, namely $1, b, c$. Then

$$\sigma(b) \geq 1 + b + c.$$

But (2) implies $\sigma(b) = 2^{a+1}c = (2^{a+1}-1+1)c = (2^{a+1}-1)c + c = b + c$ by (3), a contradiction. So $c = 1$, and by (3), $b = 2^{a+1}-1$. Also, (2) implies $\sigma(b) = b + 1$, so b must be prime. One can show that $2^{a+1}-1$ being prime implies $a+1$ is prime, so $n = 2^a(2^{a+1}-1)$ with $2^{a+1}-1$ and $a+1$ prime.

($\Leftarrow$ Euclid) Assume that $n = 2^{p-1}(2^p-1)$ with p and 2^p-1 both prime. Then

$$\sigma(2^{p-1}(2^p-1)) = \sigma(2^{p-1})\sigma(2^p-1) = (2^p-1)(2^p-1+1) = (2^p-1)2^p = 2\cdot 2^{p-1}(2^p-1),$$

which shows that $\sigma(n) = 2n$. Thus n is perfect. □

Remark. Theorem 11.7 gives a characterization of even perfect numbers and a bijection between even perfect numbers and Mersenne primes.

Example 11.3.2. The first 5 perfect numbers correspond to $p = 2, 3, 5, 7, 13$.

11.4 The Möbius Function

Definition 11.4. Let $n \in \mathbb{Z}$, $n > 0$. The *Möbius function*, denoted $\mu(n)$, is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } p^2 \mid n \text{ for some } p, \\ (-1)^r & \text{if } n = p_1, \dots, p_r \text{ with } p_i \text{ distinct primes.} \end{cases}$$

Example 11.4.1. Since $504 = 2^3\cdot 3^2\cdot 7$, we have $\mu(504) = 0$. On the other hand,

$$\mu(6) = (-1)^2 = 1 \quad \text{and} \quad \mu(30) = (-1)^3 = -1$$

Theorem 11.8. *$\mu(n)$ is multiplicative.*

Proof. Let m, n be relatively prime positive integers. We need to show that $\mu(mn) = \mu(m)\mu(n)$. This is clear if $m = 1$ or $n = 1$, so we may assume $m, n > 1$. Note that m or n is divisible by a square if and only if mn is divisible by a square, since $(m, n) = 1$. In this case, both $\mu(m)\mu(n)$ and $\mu(mn)$ are 0.

Now suppose m, n are products of distinct primes, say $m = p_1\cdots p_r$ and $n = q_1\cdots q_s$. Since $(m, n) = 1$, we have $p_i \neq q_j$ for any $1 \leq i \leq r$ and $1 \leq j \leq s$. Thus

$$\mu(mn) = \mu(p_1\cdots p_r q_1\cdots q_s) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(p_1\cdots p_r)\mu(q_1\cdots q_s) = \mu(m)\mu(n),$$

as desired. So μ is multiplicative. □

Proposition 11.1. *Let $n \in \mathbb{Z}$, $n > 0$. Then*

$$\sum_{d\mid n}\mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Proof. Since μ is multiplicative, so is $F(n) = \sum_{d|n} \mu(d)$ by Theorem 9.1. Thus it suffices to show that $F(p^a) = 0$ for prime powers p^a. We have

$$F(p^a) = \sum_{d|p^a} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^a).$$

Note that $p^2 \mid p^j$ for $j \geq 2$, so $\mu(p^j) = 0$ for $j \geq 2$. Thus

$$F(p^a) = \mu(1) + \mu(p) = 1 - 1 = 0.$$

It is clear that $F(1) = \sum_{d|1} \mu(d) = \mu(1) = 1$, so the result follows. □

Example 11.4.2. Let $n = 12$. Then we have

$$\begin{aligned}\sum_{d|12} \mu(d) &= \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12)\\ &= 1 - 1 - 1 + 0 + 1 + 0 = 0.\end{aligned}$$

Lecture 12

Oct. 1 — Quadratic Residues

What do you call a bear with no ear? A bee.

What do you call a magician who loses his magic? Ian.

12.1 Möbius Inversion

Theorem 12.1 (Möbius inversion)**.** *Let f, g be arithmetic functions. Then*

$$f(n) = \sum_{d \mid n} g(d) \quad \textit{if and only if} \quad g(n) = \sum_{d \mid n} \mu(d) f(n/d) = \sum_{d \mid n} \mu(n/d) f(d).$$

Proof. ($\Rightarrow$) Assume $f(n) = \sum_{d \mid n} g(d)$. Then we can write

$$\sum_{d \mid n} \mu(d) f(n/d) = \sum_{d \mid n} \mu(d) \sum_{a \mid (n/d)} g(a).$$

Note that $a \mid (n/d)$ if and only if $d \mid (n/a)$, so we can switch the order of summation to get

$$\sum_{d \mid n} \mu(d) f(n/d) = \sum_{a \mid n} g(a) \sum_{d \mid (n/a)} \mu(d) = \sum_{a \mid n} g(a) \begin{cases} 1 & \text{if } n = a \\ 0 & \text{otherwise} \end{cases} = g(n),$$

where the second equality is by by Proposition 11.1. This proves the forward direction.

($\Leftarrow$) Assume that $g(n) = \sum_{d \mid n} \mu(n/d) f(d)$. Then we have

$$\sum_{d \mid n} g(d) = \sum_{d \mid n} \sum_{a \mid d} \mu(d/a) f(a) = \sum_{a \mid n} f(a) \sum_{\substack{d \mid n \\ a \mid d}} \mu(d/a) = \sum_{a \mid n} f(a) \sum_{b \mid (n/a)} \mu(b)$$

where we let $d = ab$ and noted that $ab \mid n$ if and only $ab \mid n$ if and only if $b \mid (n/a)$. Then

$$\sum_{d \mid n} g(d) = \sum_{a \mid n} f(a) \begin{cases} 1 & \text{if } n = a \\ 0 & \text{otherwise} \end{cases} = f(n)$$

by Proposition 11.1, which proves the reverse direction. □

Example 12.0.1. Recall that $\sum_{d|n}\varphi(d) = n$ by Theorem 9.5. By Möbius inversion,

$$\varphi(n) = \sum_{d|n}\mu(d)\frac{n}{d} = n\sum_{d|n}\frac{\mu(d)}{d} = n\prod_{p^a|n}\sum_{d|p^a}\frac{\mu(d)}{d} = n\prod_{p|n}\left(1-\frac{1}{p}\right),$$

where $\mu(d)/d$ is multiplicative since $\mu(d)$ and $1/d$ both are. This recovers the product formula for φ.

Example 12.0.2. We have $\tau(n) = \sum_{d|n} 1$. So by Möbius inversion,

$$1 = \sum_{d|n}\tau(n/d)\mu(d).$$

Example 12.0.3. We have $\sigma(n) = \sum_{d|n} d$. So by Möbius inversion,

$$n = \sum_{d|n}\mu(d)\sigma(n/d).$$

12.2 Quadratic Residues

Remark. So far, we have only studied linear congruences, which take the form $ax \equiv b \pmod{m}$. Now we will be interested in *quadratic* congruences, i.e. congruences of the form $ax^2 + bx \equiv c \pmod{m}$. We will primarily restrict to the case $x^2 \equiv a \pmod{p}$ for p an odd prime (the question is easy for $p = 2$).

Definition 12.1. Let $a, m \in \mathbb{Z}$, $m > 0$, and $(a, m) = 1$. Then a is a *quadratic residue modulo m* if the congruence $x^2 \equiv a \pmod{m}$ has a solution. Otherwise, a is a *quadratic non-residue modulo m*.

Example 12.1.1. The quadratic residues modulo 11 are

$$\{1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2\} \equiv \{1, 4, 9, 5, 3, 3, 5, 9, 4, 1\} \equiv \{1, 3, 4, 5, 9\} \pmod{11}.$$

The quadratic non-residues are $\{2, 6, 7, 8, 10\}$. Note that the sizes of these sets are the same.

Proposition 12.1. *Let p be an odd prime and $a \in \mathbb{Z}$, $p \nmid a$. Then $x^2 \equiv a \pmod{p}$ has either 0 or 2 incongruent solutions modulo p.*

Proof. Assume $x^2 \equiv a \pmod{p}$ has a solution x_0. Then $-x_0$ is also a solution. It is also incongruent to p, since if $x_0 \equiv -x_0 \pmod{p}$, then $2x_0 \equiv 0 \pmod{p}$, which implies $p \mid 2x_0$. Since p is odd, we must have $p \mid x_0$, so $x_0 \equiv 0 \pmod{p}$. But then $a \equiv x_0^2 \equiv 0 \pmod{p}$, a contradiction. Thus $x^2 \equiv a \pmod{p}$ has at least two incongruent solutions modulo p if it has a solution at all.

We now show $x^2 \equiv a \pmod{p}$ has at most 2 incongruent solutions. Suppose x_0, x_1 are solutions. Then

$$x_0^2 \equiv x_1^2 \equiv a \pmod{p}.$$

Then $x_0^2 - x_1^2 \equiv 0 \pmod{p}$, so $p \mid x_0^2 - x_1^2 = (x_0 - x_1)(x_0 + x_1)$. Thus $p \mid x_0 - x_1$ or $p \mid x_0 + x_1$. In the first case, $x_0 \equiv x_1 \pmod{p}$, and in the second case, $x_0 \equiv -x_1 \pmod{p}$. So any solution is congruent to either x_0 or $-x_0$, which means that $x^2 \equiv a \pmod{p}$ has at most 2 incongruent solutions. □

Corollary 12.1.1. *Let p be an odd prime and $a \in \mathbb{Z}$, $p \nmid a$. If $x^2 \equiv a \pmod{p}$ is solvable with $x = x_0$, then the two solutions are given by x_0 and $p - x_0$.*

Proposition 12.2. *Let p be an odd prime. Then there are exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues modulo p.*

Proof. For each $1 \le x \le p-1$, if $x^2 \equiv a \pmod{p}$, then $(p-x)^2 \equiv a \pmod{p}$ as well, and these are the only two such residues which square to a. That is, for each pair

$$(1, p-1), \quad (2, p-2), \quad \ldots, \quad (i, p-i)$$

for $1 \le i \le (p-1)/2$, we get a unique quadratic residue, namely i^2. Since there are $(p-1)/2$ pairs of residues modulo p formed in this way, there are exactly $(p-1)/2$ quadratic residues modulo p. These are given by $1^2, 2^2, \ldots, ((p-1)/2)^2$. The remaining $(p-1)/2$ elements are quadratic non-residues. □

12.3 The Legendre Symbol

Definition 12.2. Let p be an odd prime and $a \in \mathbb{Z}$, $p \nmid a$. The *Legendre symbol* is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Example 12.2.1. Recall that $1, 3, 4, 5, 9$ are quadratic residues modulo 11, so

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1.$$

The quadratic non-residues modulo 11 were $2, 6, 7, 8, 10$, so

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1.$$

Example 12.2.2. Evaluate $\left(\frac{3}{7}\right)$. This asks whether 3 is a quadratic residue modulo 7. That is, whether there is a solution to the quadratic congruence $x^2 \equiv 3 \pmod{7}$. One can check that

$$\{1^2, 2^2, 3^2\} \equiv \{1, 4, 2\} \pmod{7},$$

and these are all of the quadratic residues by Proposition 12.2. Thus $\left(\frac{3}{7}\right) = -1$.

Lecture 13

Oct. 8 — The Legendre Symbol

13.1 More on the Legendre Symbol

Exercise 13.1. Find all the quadratic residues modulo 23.

We known that the quadratic residues modulo 23 are the squares of $1, \dots, 11$, so

$$\begin{aligned}\{1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2\} &\equiv \{1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6\} \pmod{23} \\ &= \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\} \pmod{23}\end{aligned}$$

is the set of quadratic residues modulo 23.

Theorem 13.1 (Euler's criterion)**.** *Let p be an odd prime with $a \in \mathbb{Z}$ and $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Proof. Suppose first that $\left(\frac{a}{p}\right) = 1$. Then $x^2 \equiv a \pmod{p}$ has a solution, say $x = x_0$. Then

$$a^{(p-1)/2} \equiv (x_0^2)^{(p-1)/2} \equiv x_0^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}$$

by Fermat's little theorem. Now suppose that $\left(\frac{a}{p}\right) = -1$. Since $p \nmid a$, for each $1 \leq i \leq p-1$, the linear congruence $ij \equiv a \pmod{p}$ has a unique solution j with $1 \leq j \leq p-1$. Note that $i \neq j$ since a is not a quadratic residue modulo p. Thus we can pair the residues $1, 2, \dots, p-1$ into $(p-1)/2$ pairs (i, j) such that $ij \equiv a \pmod{p}$. Multiplying these pairs together, we get

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

The left-hand side is congruent to $-1 = \left(\frac{a}{p}\right)$ by Wilson's theorem, which completes the proof. □

Example 13.0.1. We compute $\left(\frac{3}{7}\right)$. Using Euler's criterion,

$$\left(\frac{3}{7}\right) \equiv 3^{(7-1)/2} \equiv 3^3 \equiv 27 \equiv 6 \equiv -1 \pmod{7},$$

so we get that $\left(\frac{3}{7}\right) = -1$.

Proposition 13.1. *Let p be an odd prime and $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$. Then*

1. *$\left(\frac{a^2}{p}\right) = 1$;*
2. *if $b \equiv a \pmod{p}$, then $\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)$;*
3. *$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

Proof. (1) The congruence $x^2 \equiv a^2 \pmod{p}$ has a solution $x = a$.

(2) The congruence $x^2 \equiv a \pmod{p}$ is equivalent to the congruence $x^2 \equiv b \equiv a \pmod{p}$.

(3) By Euler's criterion, $\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$. Since $\left(\frac{ab}{p}\right)$, $\left(\frac{a}{p}\right)$, and $\left(\frac{b}{p}\right)$ are each ± 1, congruence modulo p is equivalent to equality (since $1 \neq -1$ for $p \geq 3$). □

Example 13.0.2. Calculate $\left(\frac{-11}{7}\right)$. Using the above properties and Euler's criterion, we have

$$\left(\frac{-11}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{11}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{4}{7}\right) = \left(\frac{-1}{7}\right) \equiv (-1)^3 \equiv -1 \pmod{7}$$

since 4 is a quadratic residue modulo 7. So $\left(\frac{-11}{7}\right) = -1$.

13.2 Particular Cases of the Legendre Symbol

Remark. If $a = \pm 2^{a_0} p_1^{a_1} \cdots p_r^{a_r}$, then we have

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{a_1}\left(\frac{p_1}{p}\right)^{a_1} \cdots \left(\frac{p_r}{p}\right)^{a_r}.$$

Thus to evaluate $\left(\frac{a}{p}\right)$, it suffices to understand $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, and $\left(\frac{q}{p}\right)$ for odd primes q.

Theorem 13.2. *Let p be an odd prime. Then*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Proof. The first equality follows from Euler's criterion. The second is a direct computation: Note that p can only be congruent to 1 or 3 modulo 4. If $p \equiv 1 \pmod{4}$, then $p = 1 + 4k$ for some $k \in \mathbb{Z}$. Then

$$(-1)^{(p-1)/2} = (-1)^{(1+4k-1)/2} = (-1)^{2k} = 1.$$

Similarly, if $p \equiv 3 \pmod{4}$, then $p = 3 + 4k$ for some $k \in \mathbb{Z}$, and

$$(-1)^{(p-1)/2} = (-1)^{(3+4k-1)/2} = (-1)^{1+2k} = -1.$$

This proves the second equality. □

Lemma 13.1 (Gauss's lemma)**.** *Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Let n be the number of least positive residues of the integers*

$$a, \quad 2a, \quad 3a, \quad \ldots, \quad \left(\frac{p-1}{2}\right)a$$

that are greater than $p/2$. Then $\left(\frac{a}{p}\right) = (-1)^n$.

Proof. Let $r_1, \ldots, r_n$ be the least positive residues among $a, 2a, \ldots, ((p-1)/2)a$ that are greater than $p/2$, and let $s_1, \ldots, s_m$ be the residues which are less than $p/2$. Note that none of the r_i, s_j are congruent to 0 modulo p since $p \nmid a$. Now consider the $(p-1)/2$ integers given by

$$p - r_1, \quad p - r_2, \quad , \ldots, \quad p - r_n, \quad s_1, \quad s_2, \quad \ldots, \quad s_m.$$

We claim that this is the set of residues $1, 2, \ldots, (p-1)/2$ in some order. All elements are ≥ 1, and are $\leq (p-1)/2$ since they are $< p/2$ and are integers. So it suffices to show that there are no duplicates.

If $p - r_i \equiv p - r_j \pmod{p}$, then $r_i \equiv r_j \pmod{p}$, so $k_i a \equiv k_j a \pmod{p}$ for some $k_i \neq k_j$. Since $(a, p) = 1$, we can multiply by its inverse $\overline{a}$ to get $k_i \equiv k_j \pmod{p}$, which is a contradiction. By a similar argument, the s_j are all distinct. It only remains to consider $p - r_i \equiv s_j \pmod{p}$. Then

$$-k_i a \equiv k_j a \pmod{p}$$

for some $1 \leq k_i, k_j \leq (p-1)/2$. The congruence then implies $-k_i \equiv k_j \pmod{p}$. But $p - k_i > p/2 \geq (p-1) \geq k_j$, so this congruence is impossible. This proves the claim.

Thus, multiplying all the numbers together gives

$$\begin{aligned} \left(\frac{p-1}{2}\right)! \equiv (p - r_1) \cdots (p - r_n) s_1 \cdots s_m &\equiv (-1)^n a \cdot 2a \cdots \left(\frac{p-1}{2}\right) a \\ &\equiv (-1)^n a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod{p}. \end{aligned}$$

Since $p \nmid ((p-1)/2)!$, we can multiply by its inverse to get $a^{(p-1)/2} \equiv (-1)^n \pmod{p}$. The result then follows since the left-hand side is congruent to $\left(\frac{a}{p}\right)$ by Euler's criterion and $\left(\frac{a}{p}\right), (-1)^n$ are ± 1. □

Example 13.0.3. We use Gauss's lemma to calculate $\left(\frac{6}{11}\right)$. We have $\left(\frac{6}{11}\right) = (-1)^n$, where n is the number of least positive residues among

$$6, \quad 2 \cdot 6, \quad 3 \cdot 6, \quad 4 \cdot 6, \quad 5 \cdot 6$$

that are larger than $11/2 = 5.5$. Reducing the above gives $\{6, 1, 7, 2, 8\}$, so $n = 3$. Thus $\left(\frac{6}{11}\right) = -1$.

Lecture 14

Oct. 13 — Quadratic Reciprocity

*W*hy did the man bring his watch to the bank? He wanted to save time.

14.1 Applications of Gauss's Lemma

Exercise 14.1. Calculate the following:

$$\left(\frac{-1}{13}\right), \quad \left(\frac{2}{17}\right), \quad \left(\frac{-14}{11}\right), \quad \left(\frac{18}{23}\right).$$

For the first, since $13 \equiv 1 \pmod 4$, we have $\left(\frac{-1}{13}\right) = 1$. For the second, we compute

$$\{2, 2(2), 3(2), 4(2), 5(2), 6(2), 7(2), 8(2)\} \equiv \{2, 4, 6, 8, 10, 12, 14, 16\} \pmod{17}.$$

Four of these residues are greater that $17/2 = 8.5$, so $\left(\frac{2}{17}\right) = (-1)^4 = 1$. For the third, write

$$\left(\frac{-14}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{14}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{3}{11}\right) = -\left(\frac{3}{11}\right)$$

since $11 \equiv 3 \pmod 4$. To compute $\left(\frac{3}{11}\right)$, we list

$$\{3, 2(3), 3(3), 4(3), 5(3)\} \equiv \{3, 6, 9, 1, 4\} \pmod{11}.$$

Two of the above are greater than $11/2 = 5.5$, so $\left(\frac{3}{11}\right) = (-1)^2 = 1$. Thus $\left(\frac{-14}{11}\right) = -1$. For the last,

$$\left(\frac{18}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{9}{23}\right) = \left(\frac{2}{23}\right),$$

which we can compute by enumerating

$$\begin{aligned}&\{2, 2(2), 3(2), 4(2), 5(2), 6(2), 7(2), 8(2), 9(2), 10(2), 11(2)\}\\ &\equiv \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\} \pmod{23}.\end{aligned}$$

Six of the above are greater than $23/2 = 11.5$, so $\left(\frac{18}{23}\right) = \left(\frac{2}{23}\right) = (-1)^6 = 1$.

Theorem 14.1. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8, \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

Proof. By Gauss's lemma, we have $\left(\frac{2}{p}\right) = (-1)^n$, where n is the number of least positive residues of

$$2, \quad 2(2), \quad 3(2), \quad 4(2), \quad \ldots, \quad \left(\frac{p-1}{2}\right)2.$$

Let $k \in \mathbb{Z}$ with $1 \le k \le (p-1)/2$. Note that $2k < p/2$ if and only if $k < p/4$ (we always have $2k < p$), so there are $\lfloor p/4 \rfloor$ values of k for which $2k < p/2$. Thus, there are $(p-1)/2 - \lfloor p/4 \rfloor$ values of k for which $2k > p/2$ (recall that p is odd), so $n = (p-1)/2 - \lfloor p/4 \rfloor$. To show that $(p^2-1)/8$ and $(p-1)/2 - \lfloor p/4 \rfloor$ always have the same parity, we can just check the four cases:

- $p \equiv 1 \pmod 8$. Then $p = 8m+1$ for some $m \in \mathbb{Z}$. Then

  $$n = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{8m+1-1}{2} - \left\lfloor \frac{8m+1}{4} \right\rfloor = 4m - 2m = 2m.$$

  Note that this is even. On the other hand, we can check that

  $$\frac{p^2-1}{8} = \frac{(8m+1)^2-1}{8} = 8m^2 + 2m.$$

  This is also even, so the parity matches in this case.

- Check the cases $p \equiv 3, 5, 7 \pmod 8$ similarly as an exercise.

Since $(p^2-1)/8$ and n agree modulo 2, we have $(-1)^{(p^2-1)/8} = (-1)^n = \left(\frac{2}{p}\right)$. □

Example 14.0.1. We have $\left(\frac{2}{23}\right) = 1$ since $23 \equiv 7 \pmod 8$.

14.2 Quadratic Reciprocity

Remark. We will now try to understand $\left(\frac{q}{p}\right)$ for distinct odd primes p, q.

Theorem 14.2 (Law of quadratic reciprocity)**.** *Let p, q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } q \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Remark. Quadratic reciprocity allows us to simplify the calculation for $\left(\frac{p}{q}\right)$. For example, consider

> Which primes are quadratic residues modulo 17, i.e. evaluate $\left(\frac{p}{17}\right)$?

This is a finite problem: We may just compute all squares modulo 17. Now consider

> For which primes p is 17 a quadratic residue, i.e. evaluate $\left(\frac{17}{p}\right)$?

This is a priori an infinite problem, but we can convert it to the previous one by quadratic reciprocity.

Example 14.0.2. Compute $\left(\frac{7}{53}\right)$. We use quadratic reciprocity: $7 \equiv 3 \pmod 4$ and $53 \equiv 1 \pmod 4$, so

$$\left(\frac{7}{53}\right) = \left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = 1$$

since 4 is always a square modulo any prime.

Example 14.0.3. Calculate $\left(\frac{-158}{101}\right)$. We can first write

$$\left(\frac{-158}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{158}{101}\right) = \left(\frac{158}{101}\right) = \left(\frac{57}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{19}{101}\right)$$

since $101 \equiv 1 \pmod 4$, $158 \equiv 57 \pmod{101}$, and $57 = 3 \cdot 19$. We can now apply quadratic reciprocity (note that we could not have done this earlier, since $158, 57$ are not prime):

$$\left(\frac{-158}{101}\right) = \left(\frac{101}{3}\right)\left(\frac{101}{19}\right) = \left(\frac{2}{3}\right)\left(\frac{6}{19}\right) = \left(\frac{2}{3}\right)\left(\frac{25}{19}\right) = -1 \cdot 1 = 1.$$

Lemma 14.1. *Let p be an odd prime number and let $a \in \mathbb{Z}$, $p \nmid a$, a odd. Let*

$$N = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor .$$

Then $\left(\frac{a}{p}\right) = (-1)^N$.

Proof. Let $r_1, r_2, \ldots, r_n$ be the least non-negative residues among $a, 2a, \ldots, ((p-1)/2)a$ that are $> p/2$. Likewise, let $s_1, \ldots, s_m$ be the remaining residues that are $< p/2$. Note that

$$r_1, \ldots, r_n, s_1, \ldots, s_m$$

are all distinct modulo p (they come from $a, 2a, 3a, \ldots, ((p-1)/2)a$, which are distinct since $p \nmid a$). This means that the fractions r_i/p, s_j/p are also all distinct. Then

$$ja = p \cdot \frac{ja}{p} = p\left(\left\lfloor \frac{ja}{p} \right\rfloor + \frac{\text{remainder}}{p}\right) = p\left\lfloor \frac{ja}{p} \right\rfloor + \text{remainder depending on } j,$$

where the remainders are exactly the numbers $r_1, \ldots, r_n, s_1, \ldots, s_m$. Then

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p\left\lfloor \frac{ja}{p} \right\rfloor + \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j. \tag{1}$$

Note also that

$$\sum_{j=1}^{(p-1)/2} j = \sum_{i=1}^{n}(p - r_i) + \sum_{j=1}^{m} s_j = pn - \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j. \tag{2}$$

Subtracting (2) from (1) gives the equation

$$\sum_{j=1}^{(p-1)/2} j(a-1) = \sum_{j=1}^{(p-1)/2} p\left\lfloor \frac{ja}{p} \right\rfloor - pn + 2\sum_{i=1}^{n} r_i.$$

Taking the above equation modulo 2, since a is odd, we get

$$\sum_{j=1}^{(p-1)/2} p\left\lfloor \frac{ja}{p} \right\rfloor - pn \equiv 0 \pmod 2,$$

so $pN \equiv pn \pmod 2$, so $N \equiv n \pmod 2$ since $2 \nmid p$. So $(-1)^N = (-1)^n = \left(\frac{a}{p}\right)$ by Gauss's lemma. □

Example 14.0.4. We compute $\left(\frac{7}{11}\right)$ using Lemma 14.1. We calculate

$$N = \sum_{j=1}^{5} \left\lfloor \frac{7j}{11} \right\rfloor = \left\lfloor \frac{7}{11} \right\rfloor + \left\lfloor \frac{14}{11} \right\rfloor + \left\lfloor \frac{21}{11} \right\rfloor + \left\lfloor \frac{28}{11} \right\rfloor + \left\lfloor \frac{35}{11} \right\rfloor = 0 + 1 + 1 + 2 + 3 = 7,$$

so $\left(\frac{7}{11}\right) = (-1)^7 = -1$ by Lemma 14.1.

Lecture 15

Oct. 15 — Quadratic Reciprocity, Part 2

What do you call a place in America that receives shipments of pollinators? A U.S. bee port.

15.1 Proof of Quadratic Reciprocity

Proof of Theorem 14.2. Without loss of generality, assume $p > q$. Consider a $q \times p$ grid on $\mathbb{R}^2$. Let L be the line from $(0,0)$ to $N = (q,p)$. Let $A = ((p-1)/2, 0)$, $B = (0, (q-1)/2)$. Let M be the intersection of L with the line $x = (p-1)/2$ and D be the intersection of L with the line $y = (q-1)/2$. Also let $C = ((p-1)/2, (q-1)/2)$. We count the number of lattice points in the rectangle $OABC$, not including the axes. This number is clearly $(p-1)(q-1)/4$. Now observe that:

1. The line ON has slope q/p. In particular, ON contains no lattice points.
2. The y-coordinate of M is $((p-1)/2)(q/p) = q/2 - q/2p$. This lies between the consecutive integers $(q-1)/2$ and $(q+1)/2$:
$$\frac{q-1}{2} = \frac{q}{2} - \frac{1}{2} < \frac{q}{2} - \frac{q}{2p} < \frac{q}{2} < \frac{q+1}{2}.$$

So the number of lattice points in $OABC$ excluding the axes, and below the line ON is

$$N_1 = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor.$$

Likewise, the number of lattice points above the line ON is

$$N_2 = \sum_{j=1}^{(q-1)/2} \left\lfloor \frac{jp}{q} \right\rfloor.$$

Thus the total number of lattice points in question is $N_1 + N_2 = (p-1)(q-1)/4$. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{N_2}(-1)^{N_1} = (-1)^{N_1+N_2} = (-1)^{(p-1)(q-1)/4}$$

by Lemma 14.1, which proves the claim. □

15.2 Applications of Quadratic Reciprocity

Remark. Note that we have characterized the primes for which -1 and 2 are quadratic residues.

Example 15.0.1. For what primes p is 3 a quadratic residue? It suffices to compute when $\left(\frac{3}{p}\right) = 1$. By quadratic reciprocity, we have

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & p \equiv 1 \pmod{4}, \\ -\left(\frac{p}{3}\right) & p \equiv 3 \pmod{4}. \end{cases}$$

Note that the only (non-zero) quadratic residue modulo 3 is 1. If $p \equiv 1 \pmod{4}$, then $\left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \pmod{3}$. If $p \equiv 3 \pmod{4}$, then $\left(\frac{p}{3}\right) = -1$ if and only if $p \equiv 2 \pmod{3}$. By the Chinese remainder theorem, we can rewrite the first condition as $p \equiv 1 \pmod{12}$ and the second condition as $p \equiv -1 \pmod{12}$. Thus we see that $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$.

Example 15.0.2. Characterize the primes p for which both 2 and 3 are quadratic residues modulo p. We want p such that $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$. We already know that $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{8}$ and $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$. So by the Chinese remainder theorem, we have $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{24}$.

Example 15.0.3. Characterize the primes p for which 13 is a quadratic residue modulo p. By quadratic reciprocity, we have $\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right)$. The non-zero quadratic residues modulo 13 are

$$\{1, 3, 4, 9, 10, 12\},$$

So $\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) = 1$ if and only if $p \equiv 1, 3, 4, 9, 10, 12 \equiv \pm 1, \pm 3, \pm 4 \pmod{13}$.

Example 15.0.4. Characterize the primes p for which 11 is a quadratic residue modulo p. By quadratic reciprocity, we have that

$$\left(\frac{11}{p}\right) = \begin{cases} \left(\frac{p}{11}\right) & p \equiv 1 \pmod{4}, \\ -\left(\frac{p}{11}\right) & p \equiv 3 \pmod{4}. \end{cases}$$

The quadratic residues modulo 11 are $1, 3, 4, 5, 9$, and the quadratic non-residues are $2, 6, 7, 8, 10$. If $p \equiv 1 \pmod{4}$, then $\left(\frac{p}{11}\right) = 1$ if and only if $p \equiv 1, 3, 4, 5, 9 \pmod{11}$, and if $p \equiv 3 \pmod{4}$, then $\left(\frac{p}{11}\right) = -1$ if and only if $p \equiv 2, 6, 7, 8, 10 \pmod{11}$. One can check each of these cases by the Chinese remainder theorem, and one gets $\left(\frac{11}{p}\right) = 1$ if and only if $p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 \pmod{44}$, or

$$p \equiv \pm 1, \pm 5, \pm 7, \pm 9, \pm 19 \pmod{44}.$$

Example 15.0.5. Characterize the primes p for which -1 and 2 are both quadratic residues modulo p. Recall that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{4}$ and $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{8}$, so we see that $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{8}$.

Example 15.0.6. Characterize the primes p for which both -1 and 3 are quadratic residues modulo p. Recall that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{4}$ and $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$. So we have $\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{12}$.

Exercise 15.1. Characterize the primes p for which 3 and 5 are quadratic residues modulo p.

Lecture 16

Oct. 20 — Primitive Roots

What happens when you step on a grape? Nothing, it lets out a little whine.

16.1 Orders

Remark. Let m be a positive integer and $(a, m) = 1$. By Euler's theorem, we know that

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

However, it may happen that $a^g \equiv 1 \pmod{m}$ for some smaller g.

Definition 16.1. Let $a, m \in \mathbb{Z}$ with $m > 0$, $(a, m) = 1$. Then the *order of a modulo m*, denoted $\operatorname{ord}_m a$, is the least positive integer n such that $a^n \equiv 1 \pmod{m}$.

Example 16.1.1. We compute $\operatorname{ord}_7 2$. We can compute that

$$\begin{aligned}
2^1 &\equiv 2 \pmod{7},\\
2^2 &\equiv 4 \pmod{7},\\
2^3 &\equiv 1 \pmod{7},
\end{aligned}$$

so we see that $\operatorname{ord}_7 2 = 3$. Note that Euler's theorem only guarantees $\operatorname{ord}_7 2 \leq \phi(7) = 6$.

Example 16.1.2. We compute $\operatorname{ord}_7 3$. We can compute that

$$\begin{aligned}
3^1 &\equiv 3 \pmod{7},\\
3^2 &\equiv 2 \pmod{7},\\
3^3 &\equiv 6 \pmod{7},\\
3^4 &\equiv 4 \pmod{7},\\
3^5 &\equiv 5 \pmod{7},\\
3^6 &\equiv 1 \pmod{7},
\end{aligned}$$

so we see that $\operatorname{ord}_7 3 = 6$.

Proposition 16.1. *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Then $a^n \equiv 1 \pmod{m}$ for some positive integer n if and only if $\operatorname{ord}_m a \mid n$. In particular, $\operatorname{ord}_m a \mid \varphi(m)$.*

Proof. $(\Rightarrow)$ Suppose that $a^n \equiv 1 \pmod{m}$. By the division algorithm, there exists $q, r \in \mathbb{Z}$ such that

$$n = q(\operatorname{ord}_m a) + r, \quad 0 \leq r < \operatorname{ord}_m a.$$

Then $1 = a^n \equiv a^{q(\operatorname{ord}_m a)+r} \equiv (a^{\operatorname{ord}_m a})^q a^r \equiv a^r \pmod{m}$, which can only happen if $r = 0$ by the definition of $\operatorname{ord}_m a$ and $0 \leq r < \operatorname{ord}_m a$. Therefore, $\operatorname{ord}_m a \mid n$.

($\Leftarrow$) Suppose that $\operatorname{ord}_m a \mid n$. Then $n = q(\operatorname{ord}_m a)$, so $a^n = a^{q(\operatorname{ord}_m a)} \equiv (a^{\operatorname{ord}_m a})^q \equiv 1 \pmod{m}$. □

Example 16.1.3. We compute $\operatorname{ord}_{13} 2$. By Proposition 16.1, it suffices to check divisors of $\varphi(13) = 12$:

$$\begin{aligned}
2^1 &\equiv 2 \pmod{13},\\
2^2 &\equiv 4 \pmod{13},\\
2^3 &\equiv 8 \pmod{13},\\
2^4 &\equiv 3 \pmod{13},\\
2^6 &\equiv 12 \pmod{13},\\
2^{12} &\equiv 1 \pmod{13},
\end{aligned}$$

thus $\operatorname{ord}_{13} 2 = 12$. Note that we did not need to compute 2^7, 2^8, etc. to verify this.

Proposition 16.2. *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If i, j are non-negative integers, then $a^i \equiv a^j \pmod{m}$ if and only if $i \equiv j \pmod{\operatorname{ord}_m a}$.*

Proof. Without loss of generality, suppose $i \geq j$.

($\Rightarrow$) Assume $a^i \equiv a^j \pmod{m}$. Then we can write

$$a^j \equiv a^i \equiv a^j a^{i-j} \pmod{m}.$$

Since $(a, m) = 1$, we can cancel a^j to get $1 \equiv a^{i-j} \pmod{m}$. Then by Proposition 16.1, $\operatorname{ord}_m a \mid i - j$.

($\Leftarrow$) Assume $i \equiv j \pmod{\operatorname{ord}_m a}$. Then $\operatorname{ord}_m a \mid i - j$, so there exists $n \in \mathbb{Z}$ such that $i - j = n(\operatorname{ord}_m a)$. Thus $i = j + n(\operatorname{ord}_m a)$, and we have $a^i \equiv a^{j+n(\operatorname{ord}_m a)} \equiv a^j (a^{\operatorname{ord}_m a})^n \equiv a^j \pmod{m}$. □

Example 16.1.4. We have seen previously that $\operatorname{ord}_7 2 = 3$. So if i, j are non-negative integers, then $2^i \equiv 2^j \pmod{7}$ if and only if $i \equiv j \pmod{3}$ by Proposition 16.2. Note that

$$2000 \equiv 2 \pmod{3},$$

so we can calculate $2^{2000} \equiv 2^2 \equiv 4 \pmod{7}$.

16.2 Primitive Roots

Definition 16.2. Let $r, m \in \mathbb{Z}$ with $m > 0$ and $(r, m) = 1$. Then r is called a *primitive root modulo m* if $\operatorname{ord}_m r = \varphi(m)$.

Remark. See *primitive root diffusers* for an interesting application (also *quadratic residue diffusers*).

Example 16.2.1. We have seen that 3 is a primitive root modulo 7 and 2 is a primitive root modulo 13. On the other hand, 2 is not a primitive root modulo 7.

Example 16.2.2. We prove that there are no primitive roots modulo 8. The reduced residues modulo 8 are $1, 3, 5, 7$, and $\varphi(8) = 4$. But $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1$, so none of these are primitive roots modulo 8.

In particular, not all integers m possess a primitive root. The *primitive root theorem* (later) tells us that m has a primitive root if and only if $m = 1, 2, 4, p^k, 2p^k$, where p is an odd prime.

Proposition 16.3. *Let r be a primitive root modulo m. Then $\{r, r^2, r^3, \dots, r^{\varphi(m)}\}$ is a complete set of reduced residues modulo m.*

Proof. Since r is a primitive root modulo m, we have $(r, m) = 1$, and so $(r^n, m) = 1$ for any $n \geq 1$. Also, there are $\varphi(m)$ elements in the list, so it remains to show that they are distinct modulo m.

To do this, suppose that $r^i \equiv r^j \pmod{m}$ for some $1 \leq i, j \leq \varphi(m)$. Then Proposition 16.2 implies that $i \equiv j \pmod{\varphi(m)}$, so $i = j$. Thus the r^i are distinct modulo m. □

Remark. Proposition 16.3 says that a primitive root (when it exists) generates the reduced residues modulo m.

Example 16.2.3. Recall that 3 is a primitive root modulo 7. We saw in Example 16.1.2 that

$$\{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\} \equiv \{3, 2, 6, 4, 5, 1\} \pmod{7},$$

in particular this is a complete set of reduced residues modulo 7.

Example 16.2.4. Recall that 2 is a primitive root modulo 13. We can compute

$$\{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\} \equiv \{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\} \pmod{13},$$

which is a complete set of reduced residues modulo 13.

Remark. If a primitive root exists, it is in general not unique. We will determine how many there are next lecture (we will see that there are $\varphi(\varphi(m))$ of them).

Exercise 16.1. Show there are no primitive roots modulo 12.

To do this, write $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, then we have

$$(\mathbb{Z}/12\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/4\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

which is not cyclic. Alternatively, one can just compute directly for $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$ that

$$1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12},$$

so none of these can be primitive roots modulo 12.

Lecture 17

Oct. 22 — Primitive Roots, Part 2

17.1 More on Primitive Roots

Proposition 17.1. *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If i is a positive integer, then*

$$\operatorname{ord}_m(a^i) = \frac{\operatorname{ord}_m a}{(\operatorname{ord}_m a, i)}.$$

Proof. Let $d = (\operatorname{ord}_m a, 1)$. Then there exist $b, c \in \mathbb{Z}$ such that $\operatorname{ord}_m a = db$, $i = dc$ and $(b, c) = 1$. Note

$$(a^i)^b = (a^{dc})^{(\operatorname{ord}_m a)/d} = (a^c)^{\operatorname{ord}_m a} = (a^{\operatorname{ord}_m a})^c = 1 \pmod{m}.$$

By Proposition 16.1, this implies $\operatorname{ord}_m(a^i) \mid b$. Also,

$$1 \equiv (a^i)^{\operatorname{ord}_m(a^i)} \equiv a^{i \operatorname{ord}_m(a^i)} \pmod{m},$$

so by Proposition 16.1, $\operatorname{ord}_m a \mid i \operatorname{ord}_m(a^i)$. Thus $db \mid dc \operatorname{ord}_m(a^i)$, so $b \mid c \operatorname{ord}_m(a^i)$. Since $(b, c) = 1$, we must have $b \mid \operatorname{ord}_m(a^i)$. Thus we see that $\operatorname{ord}_m(a^i) = b = (\operatorname{ord}_m a)/d = (\operatorname{ord}_m a)/(\operatorname{ord}_m a, i)$. □

Corollary 17.0.1. *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If i is a positive integer, then*

$$\operatorname{ord}_m(a^i) = \operatorname{ord}_m a$$

if and only if $(\operatorname{ord}_m a, i) = 1$.

Corollary 17.0.2. *If a primitive root modulo m exists, then there are exactly $\varphi(\varphi(m))$ incongruent primitive roots modulo m.*

Proof. Let r be a primitive root. Then the $\operatorname{ord}_m r = \varphi(m)$. By Proposition 16.3, the set

$$\{r^1, r^2, \ldots, r^{\varphi(m)}\}$$

is a reduced residue system modulo m. If $1 \le i \le \varphi(m)$, then by Corollary 17.0.1, $\operatorname{ord}_m(r^i) = \operatorname{ord}_m r = \varphi(m)$ if and only if $(i, \varphi(m)) = 1$. There are $\varphi(\varphi(m))$ such i, and each gives a distinct primitive root. □

Example 17.0.1. We showed previously that 3 is a primitive root modulo 7. There are exactly

$$\varphi(\varphi(7)) = \varphi(6) = 2$$

primitive roots modulo 7. In particular, we must have $\operatorname{ord}_m(3^i) = \varphi(7)$ if and only if $(i, \varphi(7)) = (1, 6) = 1$. Thus $i = 1, 5$, so $3^1 = 3$ and $3^5 \equiv 5 \pmod{7}$ are the two primitive roots modulo 7.

Example 17.0.2. Recall that 2 is a primitive root modulo 13. Thus there are $\varphi(\varphi(13)) = \varphi(2) = 4$ primitive roots. Find the other three primitive roots as an exercise.

Remark. Note that $\varphi(\varphi(8)) = \varphi(4) = 2$, but this does not imply that 8 has 2 primitive roots. We need to know that a primitive root exists first for Corollary 17.0.2 to apply.

17.2 Primitive Roots for Primes

Theorem 17.1 (Lagrange)**.** *Let p be a prime and let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

be a polynomial with degree n and integer coefficients $a_0, a_1, \ldots, a_n$, such that $p \nmid a_n$. Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n incongruent solutions.

Proof. We proceed by induction on n. Suppose $n = 1$. Then $f(x) = a_1 x + a_0$ where $p \nmid a_1$. Then

$$a_1 x + a_0 \equiv 0 \pmod{p},$$

which is equivalent to $a_1 x = -a_0 \pmod{p}$. Now since $p \nmid a_1$, we can multiply both sides by $\overline{a}_1$ to get $x = -a_0\overline{a}_1$. This proves the base case.

Suppose $k \geq 1$ and that the theorem holds for polynomials of degree k. Let $n = k+1$, then we can write

$$f(x) = a_{k+1}x^{k+1} + \cdots + a_1 x + a_0$$

where $p \nmid a_{k+1}$. If $f(x) \equiv 0 \pmod{p}$ has no solutions, then we are done. Now suppose x_0 is a solution. By polynomial long division, there exists a polynomial $q(x)$ with integer coefficients such that

$$f(x) = (x - x_0)q(x) + r$$

for some integer r, where $q(x)$ has degree k. Note that

$$0 \equiv f(x_0) \equiv (x_0 - x_0)q(x_0) + r \equiv r \pmod{p},$$

so $r \equiv 0 \pmod{p}$, and we have $f(x) \equiv (x - x_0)q(x) \pmod{p}$. If

$$0 \equiv f(x_1) \equiv (x_1 - x_0)q(x) \pmod{p},$$

then $x_1 - x_0 \equiv 0 \pmod{p}$ or $q(x_1) \equiv 0 \pmod{p}$. If $x_1 \not\equiv x_0 \pmod{p}$, then $q(x_1) \equiv 0 \pmod{p}$, and $q(x)$ has at most k roots by the induction hypothesis. Thus $f(x)$ has at most $k+1$ roots. □

Proposition 17.2. *Let p be a prime and $d \in \mathbb{Z}$ with $d > 0$ and $d \mid p - 1$. Then the congruence*

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d incongruent solutions modulo p.

Proof. Since $d \mid p-1$, there exists $e \in \mathbb{Z}$ such that $p-1 = de$. Note that if $p \nmid x$, then

$$0 \equiv x^{p-1} - 1 \equiv x^{de-1} \equiv (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1) \pmod{p}.$$

Thus $x^d - 1 \equiv 0 \pmod{p}$ (call this (1)) or $x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1 \equiv 0 \pmod{p}$ (call this (2)). By Theorem 17.1, (2) has at most $d(e-1) = p-1-d$ solutions. Also (1) has at most d solutions. By Fermat's little theorem, $x^{p-1} - 1 \equiv \pmod{p}$ has exactly $p-1$ solutions, so $x^d - 1 \equiv 0 \pmod{p}$ has least d solutions. Therefore, it has exactly d solutions. □

Remark. Proposition 17.2 is a generalization of the fact that $x^2 \equiv 1 \pmod{p}$ has exactly 2 solutions for odd primes p.

Example 17.0.3. Prove that 3 is a primitive root modulo 43, and then use this to calculate all elements of order 14. To show that 3 is a primitive root, we need to check 3^i for $i \mid \varphi(43) = 42$, so for

$$i = 1, 2, 3, 6, 7, 14, 21, 42.$$

We can compute that

$$\begin{aligned}
3^1 &\equiv 3 \pmod{43},\\
3^2 &\equiv 9 \pmod{43},\\
3^3 &\equiv 27 \pmod{43},\\
3^6 &\equiv 3^4 \cdot 3^2 \equiv (-5) \cdot 9 \equiv -2 \pmod{43},\\
3^7 &\equiv -6 \pmod{43},\\
3^{14} &\equiv 36 \equiv -7 \pmod{43},\\
3^{21} &\equiv 42 \equiv -1 \pmod{43},\\
3^{42} &\equiv 1 \pmod{43}.
\end{aligned}$$

This confirms that 3 is a primitive root modulo 43. To find elements of order 14, we want i such that

$$14 = \operatorname{ord}_{43}(3^i) = \frac{\operatorname{ord}_{43}(3)}{(\operatorname{ord}_{43}(3), i)} = \frac{42}{(42, i)},$$

so we want $(42, i) = 42/14 = 3$. This works for $i = 3, 9, 15, 27, 33, 39$. Thus the elements of order 14 are represented by $3^3, 3^9, 3^{15}, 3^{27}, 3^{33}, 3^{39}$ modulo 43.

Lecture 18

Oct. 27 — Primitive Roots, Part 3

18.1 Primitive Roots for Primes, Continued

Theorem 18.1 (Legendre). *Let p be a prime and let $d \in \mathbb{Z}$ with $d > 0$ and $d \mid p-1$. Then there are exactly $\varphi(d)$ incongruent integers having order d modulo p.*

Proof. Given $d \mid p-1$, let $f(d)$ be the number of integers among $1, 2, \ldots, p-1$ that have order d modulo p. We wish to show that $f(d) = \varphi(d)$. We will first show that if $f(d) \neq 0$, then $f(d) = \varphi(d)$. Then we will show that $f(d) \neq 0$ for all $d \mid p-1$.

Suppose first that $f(d) > 0$. Then there exists an integer a with order d. Note that the integers $a^1, a^2, \ldots, a^d$ are incongruent modulo p. To see this, suppose otherwise that $a^i \equiv a^j \pmod{p}$ for some $i > j$. Then $a^{i-j} \equiv 1 \pmod{p}$ with $i - j < d$, contradicting $\operatorname{ord}_p a = d$. Note also that

$$(a^k)^d \equiv (a^d)^k \equiv 1 \pmod{p},$$

so each is a solution to $x^d - 1 \equiv 0 \pmod{p}$. Since this congruence has exactly d solutions, $a^1, \ldots, a^d$ must be all of them. So any integer of order d modulo p must be congruent to one of these. In particular, any element of order d must be a power of a. Recall that

$$\operatorname{ord}_p(a^i) = \frac{\operatorname{ord}_p a}{(\operatorname{ord}_p a, i)},$$

so $\operatorname{ord}_p(a^i) = d$ if and only if $\operatorname{ord}_p(a)/(\operatorname{ord}_p a, i) = d$, which holds only when $(d, i) = 1$ since $\operatorname{ord}_p(a) = d$. Thus there are exactly $\varphi(d)$ values of i, so $f(d) = \varphi(d)$.

We now show that $f(d)$ cannot be 0. Note that any integer b with $1 \leq b \leq p-1$ must have order dividing $p-1$, so any such b is counted by exactly one $f(d)$. Thus

$$\sum_{d \mid p-1} f(d) = p - 1,$$

so we have $\sum_{d \mid p-1} f(d) = p - 1 = \sum_{d \mid p-1} \varphi(d)$. Rearranging, we get

$$\sum_{d \mid p-1} (\varphi(d) - f(d)) = 0.$$

If $f(d) \neq 0$, then $f(d) = \varphi(d)$, so the corresponding summand is 0. Then

$$0 = \sum_{\substack{d \mid p-1 \\ f(d)=0}} (\varphi(d) - f(d)) = \sum_{\substack{d \mid p-1 \\ f(d)=0}} \varphi(d),$$

which is a sum of positive integers, so this can only happen if $f(d) \neq 0$ for all $d \mid p-1$. □

Corollary 18.1.1. *Let p be a prime. Then there are exactly $\varphi(p-1)$ primitive roots modulo p.*

Remark. Note that Theorem 18.1 gives no way to construct a primitive root.

Example 18.0.1. Let $p = 7$. Theorem 18.1 implies that there exist residues of orders $1, 2, 3, 6$ since $\varphi(7) = 6$. Further, we can compute the following table:

order	# residues	residues
1	$\varphi(1) = 1$	1
2	$\varphi(2) = 1$	6
3	$\varphi(3) = 2$	$2, 4$
6	$\varphi(6) = 2$	$3, 5$

Exercise 18.1. Construct the analogous table for $p = 13$. The solution is:

order	# residues	residues
1	$\varphi(1) = 1$	1
2	$\varphi(2) = 1$	12
3	$\varphi(3) = 2$	$3, 9$
4	$\varphi(4) = 2$	$8, 5$
6	$\varphi(6) = 2$	$4, 10$
12	$\varphi(12) = 4$	$2, 6, 11, 7$

Example 18.0.2. Find all incongruent integers having orders 6 and 7 modulo 19. Immediately we know that there are 0 integers of order 7 modulo 19 since $7 \nmid \varphi(19) = 18$. To find the elements of order 6, we would like to have a primitive root. We check that 2 is a primitive root:

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^6 = 7, \quad 2^9 = -1, \quad 2^{18} = 1.$$

Now to find the integers of order 6, we solve the equation

$$6 = \operatorname{ord}_{19}(2^a) = \frac{\operatorname{ord}_{19} 2}{(\operatorname{ord}_{19} 2, a)} = \frac{18}{(18, a)},$$

so $(18, a) = 18/6 = 3$. Thus $a = 3, 15$, which corresponds to $2^3 = 8$ and $2^{15} = (2^7)^2 \cdot 2 = 3$ modulo 19.

Remark. The frequency with which 2 appears as a primitive root motivates the following conjecture:

> **Conjecture 18.1.1.** *There are infinitely many primes p for which 2 is a primitive root modulo p.*

This conjecture is still open. A generalization of the above is the following:

> **Conjecture 18.1.2** (Artin). *If r is any non-square integer other than -1, then there are infinitely many primes p for which r is a primitive root modulo p.*

In this direction, Heath-Brown proved in 1986 that there are at most two integers r for which the conjecture is false.

18.2 The Primitive Root Theorem

Remark. We will prove this over the course of the next few lectures. The following two propositions limit the cases we need to consider.

Proposition 18.1. *There are no primitive roots modulo 2^n where $n \in \mathbb{Z}$, $n \geq 3$.*

Proof. Note that any primitive root modulo 2^n must be odd and have order

$$\varphi(2^n) = 2^n - 2^{n-1} = 2^{n-1}.$$

Let a be an odd integer. To prove that there are no primitive roots, it suffices to show that

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}.$$

We prove this by induction on n. When $n = 3$, one can check that $1^2 = 3^2 = 5^2 = 7^2 \equiv 1 \pmod 8$, so the desired condition is satisfied. Now suppose $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ for some $n \geq 3$. Then

$$a^{2^{n-2}} = b2^n + 1, \quad b \in \mathbb{Z}.$$

Note that $(x^{2^{n-2}})^2 = x^{2^{n-1}}$, so squaring both sides yields

$$a^{2^{n-1}} = (a^{2^{n-2}})^2 = (b2^n + 1)^2 = b^2 2^{2n} + 2^{n+1} b + 1 \equiv 1 \pmod{2^{n+1}},$$

which proves thee inductive step. So there are no primitive roots modulo 2^n for $n \geq 3$. □

Lecture 19

Nov. 29 — Primitive Roots, Part 4

Lecture 20

Nov. 10 — Index Arithmetic

20.1 Index Arithmetic

Remark. Recall that if r is a primitive root modulo m, then the set

$$\{r, r^2, r^3, \dots, r^{\varphi(m)}\}$$

is a reduced residue system modulo m.

Definition 20.1. Let r be a primitive root modulo m. If $(a, m) = 1$, then the *index of a relative to r*, denoted $\operatorname{ind}_r a$, is the least positive integer n for which $r^n \equiv a \pmod{m}$.

Remark. The index $\operatorname{ind}_r a$ always exists and satisfies $1 \leq \operatorname{ind}_r a \leq \varphi(m)$.

Example 20.1.1. Recall that 3 is a primitive root modulo 7. We can compute that

$$\begin{aligned}
3^1 &\equiv 3 \pmod{7},\\
3^2 &\equiv 2 \pmod{7},\\
3^3 &\equiv 6 \pmod{7},\\
3^4 &\equiv 4 \pmod{7},\\
3^5 &\equiv 5 \pmod{7},\\
3^6 &\equiv 1 \pmod{7}.
\end{aligned}$$

Thus we see that the indices are

$$\begin{aligned}
\operatorname{ind}_3 3 &= 1,\\
\operatorname{ind}_3 2 &= 2,\\
\operatorname{ind}_3 6 &= 3,\\
\operatorname{ind}_3 4 &= 4,\\
\operatorname{ind}_3 5 &= 5,\\
\operatorname{ind}_3 1 &= 6.
\end{aligned}$$

Remark. If a, b are coprime with m and $a \equiv b \pmod{m}$, then $\operatorname{ind}_r a = \operatorname{ind}_r b$.

Remark. Indices enjoy similar properties as logarithms.

Proposition 20.1. *Let r be a primitive root modulo m and $a, b \in \mathbb{Z}$ coprime to m. Then*

1. $\operatorname{ind}_r 1 \equiv 0 \pmod{\varphi(m)}$,

2. $\operatorname{ind}_r r \equiv 1 \pmod{\varphi(m)}$,

3. $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \pmod{\varphi(m)}$,

4. $\operatorname{ind}_r(a^n) \equiv n \operatorname{ind}_r a \pmod{\varphi(m)}$ *if* $n > 0$ *is an integer.*

Proof. (1)-(2) These are clear.

(3) By definition, we have $r^{\operatorname{ind}_r a} \equiv a \pmod m$ and $r^{\operatorname{ind}_r b} \equiv b \pmod m$. Thus

$$r^{\operatorname{ind}_r a + \operatorname{ind}_r b} \equiv ab \equiv r^{\operatorname{ind}_r(ab)} \pmod m.$$

By Proposition 16.2, we have $\operatorname{ind}_r a + \operatorname{ind}_r b \equiv \operatorname{ind}_r(ab) \pmod{\varphi(m)}$, since $\operatorname{ord}_m r = \varphi(m)$.

(4) We argue similarly as in (3): By definition, $r^{\operatorname{ind}_r a^n} \equiv a^n \pmod m$. Also,

$$r^{n \operatorname{ind}_r a} \equiv (r^{\operatorname{ind}_r a})^n \equiv a^n \pmod m,$$

so again by Proposition 16.2, $n \operatorname{ind}_r a \equiv \operatorname{ind}_r(a^n) \pmod{\varphi(m)}$. □

Example 20.1.2. We work modulo 7 with primitive root 3. Then $\operatorname{ind}_3 2 = 2$ and $\operatorname{ind}_3 3 = 1$, so

$$\operatorname{ind}_3 6 \equiv \operatorname{ind}_3(2 \cdot 3) \equiv \operatorname{ind}_3 2 + \operatorname{ind}_3 3 \equiv 3 \pmod 6.$$

So $\operatorname{ind}_3 6 = 3$, which agrees with our previous calculations.

Remark. Suppose r is a primitive root modulo m and $(a, m) = (b, m) = 1$. Consider for $n > 0$

$$ax^n \equiv b \pmod m.$$

This congruence is equivalent to $\operatorname{ind}_r(b) \equiv \operatorname{ind}_r(ax^n) \equiv \operatorname{ind}_r(a) + n \operatorname{ind}_r(x) \pmod{\varphi(m)}$, so

$$n \operatorname{ind}_r(x) \equiv \operatorname{ind}_r(b) - \operatorname{ind}_r(a) \pmod{\varphi(m)}.$$

This is now a linear congruence which is equivalent to the original one.

Example 20.1.3. Use indices to find all incongruent solutions to

$$6x^4 \equiv 3 \pmod 7.$$

Since 3 is a primitive root, we can compute that

$$4 \operatorname{ind}_3(x) \equiv \operatorname{ind}_3(3) - \operatorname{ind}_3(6) \equiv 1 - 3 \equiv 4 \pmod 6.$$

Note $(4, 6) = 2$ and $2 \mid 4$, so this congruence has 2 solutions by Theorem 6.1. Dividing by 2, we get

$$2 \operatorname{ind}_3(x) \equiv 2 \pmod 3,$$

so $\operatorname{ind}_3(x) \equiv 1 \pmod 3$. Thus $\operatorname{ind}_3(x) \equiv 1, 4 \pmod 6$. This corresponds to $x \equiv 3^1, 3^4 \equiv 3, 4 \pmod 7$.

20.2 Power Residues

Definition 20.2. Let $a, m, n \in \mathbb{Z}$ with $m, n > 0$ and $(a, m) = 1$. Then a is an *nth power residue modulo* m if the congruence $x^n \equiv a \pmod m$ has a solution.

Example 20.2.1. We have the following:

1. 6 is a 3rd power residue modulo 7 (we have calculated $\operatorname{ind}_3 6 = 3$).
2. 3 is a 4th power residue modulo 13 (one has $2^4 \equiv 16 \equiv 3 \pmod{13}$).
3. 3 is not a 4th power residue modulo 7 (exercise).

Theorem 20.1. *Let $a, m, n \in \mathbb{Z}$ with $m, n > 0$ and $(a, m) = 1$. If m has a primitive root, then a is an nth power residue modulo m if and only if*

$$a^{\varphi(m)/d} \equiv 1 \pmod{m},$$

where $d = (n, \varphi(m))$. Furthermore, in this case, the congruence $x^n \equiv a \pmod{m}$ has exactly d incongruent solutions modulo m.

Proof. Let r be a primitive root modulo m. Then the congruence $x^n \equiv a \pmod{m}$ is equivalent to

$$n \operatorname{ind}_r(x) \equiv \operatorname{ind}_r(a) \pmod{\varphi(m)}.$$

This congruence is solvable if and only if $d = (n, \varphi(m))$ divides $\operatorname{ind}_r a$ by Theorem 6.1. In this case, there are d incongruent solutions. The condition $d \mid \operatorname{ind}_r a$ is equivalent to

$$\frac{\varphi(m)}{d} \operatorname{ind}_r a \equiv 0 \pmod{\varphi(m)}.$$

The forward implication is clear, and the congruence implies $(\varphi(m)/d) \operatorname{ind}_r a = k\varphi(m)$ for some $k \in \mathbb{Z}$, so $\operatorname{ind}_r a = dk$, so $d \mid \operatorname{ind}_r a$. The congruence is equivalent to $a^{\varphi(m)/d} \equiv 1 \pmod{m}$. □

Corollary 20.1.1 (Euler's criterion). *Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then a is a quadratic residue modulo p if and only if*

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Moreover, if this is the case, there are exactly 2 incongruent solutions to $x^2 \equiv a \pmod{p}$.

Proof. Take $m = p$ and $n = 2$ in Theorem 20.1. □

Example 20.2.2. Let $a = 6$, $m = 7$, $n = 3$. A primitive root modulo 7 is 3. The congruence

$$x^3 \equiv 6 \pmod{7}$$

has $d = (3, \varphi(7)) = (3, 6) = 3$ solutions, so 6 is a 3rd power residue modulo 7.

Example 20.2.3. Find all 15th power residues modulo 9. Since 9 has a primitive root by the primitive root theorem, the congruence $x^{15} \equiv a \pmod{9}$ has has solutions if and only if

$$a^{\varphi(9)/d} \equiv 1 \pmod{9},$$

where $d = (15, \varphi(9)) = (15, 6) = 3$. Thus we must have $1 \equiv a^{6/3} \equiv a^2 \pmod{9}$, so $a \equiv \pm 1 \pmod{9}$ are the only solutions. So the only 15th power residues modulo 9 are ± 1.

Lecture 21

Nov. 12 — Diophantine Equations

21.1 Linear Diophantine Equations

Definition 21.1. Any equation with one or more variables to be solved in the integers is called a *Diophantine equation.*

Example 21.1.1. We can consider $5x^2 - 2x + 1 = 0$ as a Diophantine equation.

Definition 21.2. Let $a_1, \dots, a_n, b \in \mathbb{Z}$ with $a_1, \dots, a_n \neq 0$. A Diophantine equation of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

is called a *linear Diophantine equation.*

Theorem 21.1. *Let $ax = b$ be a linear Diophantine equation in the variable x. If $a \mid b$, then there is a unique solution $x = b/a$. If $a \nmid b$, then there is no solution.*

Theorem 21.2. *Let $ax + by = c$ be a linear Diophantine equation in the variables x, y. Let $d = (a, b)$. If $d \nmid c$, then there are no solutions. If $d \mid c$, there are infinitely many solutions, given by*

$$x = x_0 + (b/d)n \quad \textit{and} \quad y = y_0 - (a/d)n, \quad n \in \mathbb{Z}$$

for a particular solution $x_0, y_0 \in \mathbb{Z}$.

Proof. If there were a solution $x, y \in \mathbb{Z}$, then $d \mid a$ and $d \mid b$, so then $d \mid ax + by = c$. Taking the contrapositive implies that if $d \nmid c$, then there cannot be any solutions.

Now assume that $d \mid c$. Using the Euclidean algorithm we can find $r, s \in \mathbb{Z}$ such that

$$d = (a, b) = ra + sb.$$

Further, if $d \mid c$, then $c = dq$ for some $q \in \mathbb{Z}$, so we may write

$$c = (ra + sb)q = a(rq) + b(sq).$$

Thus $x = rq$ and $y = sq$ is a particular solution.

Now, let x_0, y_0 be any particular solution and $x = x_0 + (b/d)n$, $y = y_0 - (a/d)n$ for some $n \in \mathbb{Z}$. Then

$$\begin{aligned} ax + by &= a(x_0 + (b/d)n) + b(y_0 - (a/d)n) \\ &= ax_0 + by_0 + nab/d - nab/d = ax_0 + by_0 = c, \end{aligned}$$

so x, y is a solution for any integer n.

Finally, we check that every solution is of this form. Let x, y be any solution. Note that

$$0 = (ax + by) - (ax_0 + by_0) = a(x - x_0) + b(y - y_0),$$

so $a(x - x_0) = b(y_0 - y)$. Dividing both sides by d, we get

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

Since $d = (a, b)$, we have $(a/d, b/d) = 1$, so $a/d \mid y_0 - y$. Thus $y_0 - y = (a/d)n$ for some $n \in \mathbb{Z}$, so we have $y = y_0 - (a/d)n$. Substituting this above, we get $x = x_0 + (b/d)n$. □

Example 21.2.1. Determine if $803x + 154y = 11$ has solutions. If so, calculate all of them.

Using the Euclidean algorithm, we can compute that

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

where we used that

$$\begin{aligned} 803 &= 5 \cdot 154 + 33 \\ 154 &= 4 \cdot 33 + 22 \\ 33 &= 1 \cdot 22 + 11. \end{aligned}$$

Thus we can write

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

Thus $22 = 803 \cdot 10 + 154 \cdot (-52)$, so $(10, -52)$ is a particular solution. The other solutions are given by

$$x = 10 + \frac{154}{11}n = 10 + 14n \quad \text{and} \quad y = -52 - \frac{803}{11}n = -52 - 73n, \quad n \in \mathbb{Z}.$$

21.2 Nonlinear Diophantine Equations

Definition 21.3. A Diophantine equation is *nonlinear* if it is not linear.

Example 21.3.1. The Diophantine equations $ax^2 + bx = c$ and $5x^3 - 2 = 7x^{420}$ are nonlinear.

Remark. We can now use a method that shows some equations are *not* solvable. The idea is the following: if a Diophantine equation has solutions, then the equation will also have a solution when viewed as a congruence modulo any modulus. Taking the contrapositive, if a particular congruence modulo some modulus modulus is not solvable, then neither is the original equation.

Example 21.3.2. Prove that $3x^2 + 2 = y^2$ is not solvable.

Assume by way of contradiction that there is a solution. Consider the equation modulo 3:

$$y^2 \equiv 3x^2 + 2 \equiv 2 \pmod{3}.$$

This says that 2 is a quadratic residue modulo 3, which is false. Therefore, there are no solutions.

Example 21.3.3. Prove that $7x^3 + 2 = y^3$ has no solutions.

Consider the equation modulo 7:

$$y^3 \equiv 7x^3 + 2 \equiv 2 \pmod{7}.$$

This is solvable if and only if 2 is a cubic residue modulo 7, but we can compute that

$$\{0^3, 1^3, 2^3, 3^3, 4^3, 5^3, 6^3\} \equiv \{0, 1, 1, 6, 1, 6, 6\} \pmod{7},$$

so the only nonzero cubic residues are $1, 6$. Thus the congruence modulo 4 has no solutions, hence the original equation also has no solutions.

Example 21.3.4. Prove that $x^2 + y^2 + 1 = 4z$ has no solutions.

Take this equation modulo 4, we get the following congruence:

$$x^2 + y^2 \equiv 3 \pmod{4}.$$

The only quadratic residues modulo 4 are $\{0, 1\}$, and none of $0 + 0$, $0 + 1$, or $1 + 1$ is equal to 3, so there are no solutions to this congruence.

Exercise 21.1. Prove that $x^2 + 2y^2 + 3 = 8z$ has no solutions.

Take this equation modulo 8:

$$x^2 + 2y^2 \equiv 5 \pmod{8}.$$

Note that the only quadratic residues modulo 8 are $0, 1, 4$. Taking the above equation modulo 2 we see that x^2 must be odd, so $x^2 \equiv 1 \pmod{8}$. Then we get

$$2y^2 \equiv 4 \pmod{8},$$

so after dividing by 2 we get $y^2 \equiv 2 \pmod{4}$, which is not possible.

Lecture 22

Nov. 17 — Pythagorean Triples

22.1 Classification of Pythagorean Triples

Definition 22.1. A triple x, y, z of positive integers satisfying the Diophantine $x^2 + y^2 = z^2$ is said to be a *Pythagorean triple.*

Example 22.1.1. The following are Pythagorean triples: $3, 4, 5$ and $5, 12, 13$.

Remark. The triples $-3, 4, 5$ and $0, 1, 1$ are solutions to $x^2 + y^2 = z^2$, but they are not Pythagorean triples (as they are not positive integers).

Remark. We take the following conventions:

- We only describe solutions with $x, y, z > 0$.
- If x, y, z is a Pythagorean triple and $(x, y, z) = d$, then $x/d, y/d, z/d$ is also a Pythagorean triple, and $(x/d, y/d, z/d) = 1$. Thus we will only describe Pythagorean triples x, y, z with $(x, y, z) = 1$. Such triples are called *primitive.*
- Under the assumption that x, y, z is a primitive Pythagorean triple, we show that exactly one of x, y is even. We can see this as follows:

  First assume that x and y are both even. Then $2 \mid x$ and $2 \mid y$, and since $z^2 = x^2 + y^2$, we have $2 \mid z^2$, and so $2 \mid z$. This contradicts $(x, y, z) = 1$.

  Now assume that x and y are both odd. Then z is even, so $z^2 \equiv 0 \pmod 4$, and $x^2 \equiv y^2 \equiv 1 \pmod 4$. Since $x^2 + y^2 = z^2$, we have that $1 + 1 \equiv 0 \pmod 4$, a contradiction.

  Thus exactly one of x or y is even, so without loss of generality we will only describe Pythagorean triples where y is even.

Theorem 22.1 (Euclid)**.** *There are infinitely many primitive Pythagorean triples x, y, z with y even. They are given by $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$, where $m, n \in \mathbb{Z}$, $m > n > 0$, $(m, n) = 1$, and exactly one of m or n is even.*

Example 22.1.2. The case $m = 2$, $n = 1$ yields $3, 4, 5$, and the case $m = 3$, $n = 2$ yields $5, 12, 13$.

Proof of Theorem 22.1. We first show that given a primitive Pythagorean triple with y even, there exist $m, n \in \mathbb{Z}$ with the properties described in the theorem. Since y is even, x and z are both odd (see the argument from before). A similar argument shows that $(x, y) = (y, z) = (x, z) = 1$. Now

$$y^2 = z^2 - x^2 = (z + x)(z - x)$$

Since $y, z+x, z-x$ are all even, dividing by 2 everywhere gives

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right). \tag{1}$$

Now we claim $((z+x)/2, (z-x)/2) = 1$. To see this, let $d = ((z+x)/2, (z-x)/2)$. Then $d \mid (z+x)/2$ and $d \mid (z-x)/2$, so taking linear combinations gives

$$d \mid \frac{z+x}{2} + \frac{z-x}{2} = z,$$
$$d \mid \frac{z+x}{2} - \frac{z-x}{2} = x$$

so $d = 1$ since $(x, z) = 1$. Thus (1) implies that $(z+x)/2$ and $(z-x)/2$ are both perfect squares by the fundamental theorem of arithmetic. Let $m, n \in \mathbb{Z}$ positive such that

$$\frac{z+x}{2} = m^2 \quad \text{and} \quad \frac{z-x}{2} = n^2.$$

Then $m > n > 0$, $(m, n) = 1$ since their squares are coprime, and

$$m^2 - n^2 = x, \quad 2mn = y, \quad m^2 + n^2 = z.$$

Also, $(m, n) = 1$ implies that not both m and n are even. If m and n are both odd, then we have that

$$z = m^2 + n^2 \quad \text{and} \quad x = m^2 - n^2$$

are both even, contradicting the fact that $(x, z) = 1$. This completes the first part.

The second part of the proof is to show that given m and n as described and

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2,$$

then x, y, z is a primitive Pythagorean triple with y even. We check that

$$x^2 + y^2 = (m^4 - 2m^2n^2 + n^4) + 4m^2n^2 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = z^2,$$

so x, y, z is indeed a Pythagorean triple. Clearly y is even. It remains to prove that $(x, y, z) = 1$. To see this, let $(x, y, z) = d$. Since exactly one of m or n is even, we have that x and z are both odd. Then d is odd, and so $d = 1$ or $p \mid d$ for some odd prime p. Assume that $p \mid d$. Then $p \mid x$ and $p \mid z$, and so $p \mid z + x$ and $p \mid z - x$. Thus $p \mid m^2 + n^2 + m^2 - n^2 = 2m^2$ and $p \mid m^2 + n^2 - (m^2 - n^2) = 2n^2$. Since p is odd, we have $p \mid m^2$ and $p \mid n^2$, from which $p \mid m$ and $p \mid n$. Then $(m, n) \neq 1$, a contradiction. Thus the triple x, y, z is primitive, which completes the proof. □

Remark. Given Pythagorean triples, it is natural to consider the equation $x^n + y^n = z^n$ for $n \geq 3$.

Theorem 22.2 (Wiles-Taylor, 1994)**.** *The Diophantine equation $x^n + y^n = z^n$ has no solutions in the non-zero integers x, y, z for any integer $n \geq 3$.*

Remark. The proof for the general case is extremely difficult, but special cases are much easier. For example, the case $n = 4$ can be shown via *Fermat descent.*

Exercise 22.1. Find all solutions in positive integers to $x^2 + 2y^2 = z^2$.

Lecture 23

Nov. 19 — Fermat Descent

23.1 Fermat's Last Theorem for $n = 4$

Remark. The idea is the following: One shows that a given Diohpantine equation has no solutions in positive solutions by assuming the existence of such a solution and then constructing another solution in positive integers having one component strictly smaller than that same component of the original solution. This process cannot be continued ad infinitum, since it is not possible to construct an infinite strictly decreasing sequence of positive integers. Thus we obtain a contradiction.

Theorem 23.1. *The Diophantine equation $x^4 + y^4 = z^2$ has no solutions in non-zero integers x, y, z.*

Proof. Assume by way of contradiction that that $x^4 + y^4 = z^2$ has a solution x_1, y_1, z_1 in non-zero integers. Without loss of generality, we may assume that $x_1, y_1, z_1 > 0$ and $(x_1, y_1) = 1$. We will show that there is another solution x_2, y_2, z_2 in positive integers such that $(x_2, y_2) = 1$ and $0 < z_2 < z_1$. Now x_1^2, y_1^2, z_1 is a Pythagorean triple with $(x_1^2, y_1^2, z_1) = 1$, and without loss of generality we may assume y_1^2 is even (thus y_1 is even). Thus by Theorem 22.1, there exist $m, n \in \mathbb{Z}$ such that $m > n > 0$, $(m, n) = 1$, exactly one of m, n is even, and

$$x_1^2 = m^2 - n^2, \quad y_1^2 = 2mn, \quad z_1 = m^2 + n^2.$$

Now $x_1^2 = m^2 - n^2$ implies that $x_1^2 + n^2 = m^2$, so x_1, n, m is also a Pythagorean triple $(x_1, n, m) = 1$ and n even. So m is odd, and by Theorem 22.1, there exist $a, b \in \mathbb{Z}$ such that $a > b > 0$, $(a, b) = 1$, exactly one of a, b is even, and

$$x_1 = a^2 - b^2, \quad n = 2ab, \quad m = a^2 + b^2.$$

We wish to prove that m, a, b are perfect squares. Since $y_1^2 = 2mn = m(2n)$, and $(m, 2n) = 1$, we have that m and $2n$ must be perfect squares. Since $2n$ is a perfect square, there exists an integer $c \in \mathbb{Z}$ such that $2n = 4c^2$, or equivalently, $n = 2c^2$. Now $n = 2ab$ implies $c^2 = ab$. Since $(a, b) = 1$, we have that a and b must be perfect squares. Thus m, a, b are all perfect squares, and there exist $x_2, y_2, z_2 \in \mathbb{Z}_{>0}$ such that $m = z_2^2$, $a = x_2^2$, and $b = y_2^2$. Then $m = a^2 + b^2$ implies that $z_2^2 = x_2^4 + y_2^4$. Also $(x_2, y_2) = 1$ since $(a, b) = 1$, and we have

$$0 < z_2 \leq z_2^2 = m \leq m^2 < m^2 + n^2 = z_1.$$

This argument can be iterated arbitrarily many times, which gives a contradiction. □

Remark. Any non-zero solution to $x^4 + y^4 = z^4$ gives a nonzero solution to $x^4 + y^4 = z^2$ by taking $z' = z^2$, so this also shows that $x^4 + y^4 = z^4$ has no solutions.

Lecture 24

Nov. 24 — RSA Cryptosystem

24.1 Basics of Cryptography

Remark. The objective of *cryptography* is to render communication unintelligible to all persons except the sender and the intended recipients. Today we will discuss *public-key cryptography.*

Definition 24.1. The information to be encoded is called *plaintext*, and the encoded message is called *ciphertext.* The processes of going to ciphertext from plaintext is called *encryption*, and the reverse is called *decryption.*

Remark. We will convert all plaintext to numeric values first, e.g.

$$\text{A} \to 01, \quad \text{B} \to 02, \quad \dots, \quad \text{Z} \to 26, \quad \text{␣} \to 27$$

Remark. The idea of *public-key cryptography* is as follows: Any member of a network can send an encrypted message to any other member. This is done by associating a key to each individual that can be looked up and used: If these members are labeled $1, \dots, n$, then we have

1. A directory of public keys $e_1, \dots, e_n$.
2. If a member of the network wants to encode and send a message to member j, then the key e_j is used to encode the message.
3. Each member has a decryption key d_j known only to them, which is used to decrypt the messages sent to them back to plaintext.
4. In principle, d_j can be calculated from e_j, but it is sufficient if this cannot be done in a reasonable amount of time.

The idea that underlies the dichotomy between e_j and d_j is that there is some mathematical operation which is "cheap" to perform in one direction but extremely "expensive" in the reverse direction. In RSA, this operation is the multiplication of two large primes (factoring is difficult).

24.2 RSA Cryptosystem

Remark. The *RSA encryption algorithm* is a public-key cryptosystem introduced in 1977 by Ronald Rivest, Adi Shamir, and Len Adleman.

Definition 24.2 (RSA encryption scheme)**.** The *RSA encryption scheme* involves the following:

1. *Public encryption keys:* Let p, q be large primes (typically $\sim$1000 digits each). Let $m = pq$, and e a positive integer such that $(e, \varphi(m)) = 1$. Then the encryption key is the pair (e, m).

   Note that $p, q, \varphi(m)$ are *not* made public.

2. *Formatting:* Translate each symbol into numeric values and arrange the resulting numerical string into blocks of length less than m. If a block is incomplete, pad it with "dummy" symbols.

3. *Encryption:* Given a block P (think of P as just a number $< m$), we encrypt via

   $$P^e \equiv C \pmod{m},$$

   where C is viewed as a number $0 \le C < m$.

Example 24.2.1. Consider the message "I␣LIKE␣MATH", which corresponds to the plaintext

$$09 \quad 27 \quad 12 \quad 09 \quad 11 \quad 05 \quad 27 \quad 13 \quad 01 \quad 20 \quad 08.$$

Grouping this into blocks of length 4, we get:

$$0927 \quad 1209 \quad 1105 \quad 2713 \quad 0120 \quad 0899.$$

Taking $p = 53$, $q = 59$, $m = pq = 3127$, $\varphi(m) = 3016$, $e = 11$, we have

$$\begin{aligned} 0927^{11} &\equiv 2982 \pmod{3127} \\ 1209^{11} &\equiv 1069 \pmod{3127} \\ 1105^{11} &\equiv 2619 \pmod{3127} \\ 2713^{11} &\equiv 2005 \pmod{3127} \\ 0120^{11} &\equiv 2579 \pmod{3127} \\ 0899^{11} &\equiv 0231 \pmod{3127}. \end{aligned}$$

Thus the ciphertext is

$$2982 \quad 1069 \quad 2619 \quad 2005 \quad 2579 \quad 0231.$$

Definition 24.3 (RSA decryption scheme)**.** The *RSA decryption scheme* involves the following:

1. *Private decryption key*: The decryption key is (d, m), where d is the inverse of e modulo $\varphi(m)$.

   Note that calculating a modular inverse is *not* an expensive operation (Euclidean algorithm), but this requires knowing $\varphi(m)$, which is not public.

2. *Decryption:* We decrypt a ciphertext block C via

   $$C^d \equiv P \pmod{m}.$$

   Then concatenate the results and de-format in the obvious way.

Example 24.3.1. Consider the encrypted message 2982 1069 2619 2005 2579 0231 from Example 24.2.1. One can compute that $d = 1371$, so the decryption key is $(1371, 3127)$. The calculations are then

$$\begin{aligned} 0927 &\equiv 2982^{1371} \pmod{3127} \\ 1209 &\equiv 1069^{1371} \pmod{3127} \\ 1105 &\equiv 2619^{1371} \pmod{3127} \\ 2713 &\equiv 2005^{1371} \pmod{3127} \\ 0120 &\equiv 2579^{1371} \pmod{3127} \\ 0899 &\equiv 0231^{1371} \pmod{3127}, \end{aligned}$$

which recovers the original message after de-formatting.

Remark. Why does this work? Suppose $0 \leq P < m$ is some block to be encoded via $P^e \equiv C \pmod{m}$. We have $ed \equiv 1 \pmod{\varphi(m)}$. Thus $ed = 1 + k\varphi(m)$ for some integer $k > 0$. Then if $(P, m) = 1$,

$$C^d \equiv (P^e)^d \equiv P^{1+k\varphi(m)} \equiv P(P^{\varphi(m)})^k \equiv P \pmod{m},$$

where the last step is by Euler's theorem.

Exercise 24.1. Let $m, P > 1$, $(e, \varphi(m)) = 1$, and $ed \equiv 1 \pmod{\varphi(m)}$. If m is squarefree (but m, P not necessarily coprime), show that

$$P^{ed} \equiv P \pmod{m}.$$

In particular, the RSA decryption step still works for P and $m = pq$ with $(P, m) \neq 1$.