Elementary Discrete Mathematics

These notes are largely a selection of passages
that were more or less directly copied from:

- Kenneth Rosen's
  Elementary Number Theory and its Applications,
- Jerry Shurman's writeups,
- and Paolo Aluffi's *Algebra: Notes from the Underground*.

Of course, MathSE and Wikipedia were also consulted.

There being no clean digital copy of Rosen's book, I wrote these notes.

Contents

CHAPTER 1

Integers

The word *integer* comes from the Latin for "intact" or "whole."

The integers are a collection of numbers – a collection so special that entire subfields of mathematics are devoted to understanding them.

The integers include the positive integers,

$$1, \quad 2, \quad 3, \quad 4, \quad 5, \quad \ldots$$

as well as the negative integers,

$$-1, \quad -2, \quad -3, \quad -4, \quad -5, \quad \ldots$$

There is also an integer called 0 that is neither positive nor negative, thought of as a neutral element of the collection.

All together, the postive integers, negative integers, and zero form the collection of integers, which we will denote $\mathbf{Z}$.

We will also denote the collection of positive integers by $\mathbf{Z}^+$.

1.1. Well-Ordering and Induction

A fundamental fact about the integers is:

> *The Well-Ordering Principle.* Every nonempty subset $X \subseteq \mathbf{Z}^+$ has a least element.

It is logically equivalent to the following:

> *The Principle of Induction.* If a subset $X \subseteq \mathbf{Z}^+$ satisfies $1 \in X$ and ($n \in X \implies n + 1 \in X$), then $X = \mathbf{Z}^+$.

PROOF. Let X be a subset of $\mathbf{Z}^+$ satisfying $1 \in X$ and

$$n \in X \implies n+1 \in X.$$

We proceed by contradiction: suppose $X \neq \mathbf{Z}^+$. Then there is a positive integer not in X, i.e. $\mathbf{Z}^+ \setminus X$ is nonempty. Then $\mathbf{Z}^+ \setminus X$ has a least element n. Note that $n \neq 1$, since $1 \in X$. Thus $n > 1$, and since n is the least element not in X, $n-1$ must be in X. But by assumption, $(n-1)+1 = n \in X$, contradicting our assumption that $n \notin X$. This proves that the well-ordering principle implies the principle of induction.

Conversely, consider a nonempty subset $Y \subseteq \mathbf{Z}^+$. If Y has just one element, then that element is the least element of Y. Now suppose the well ordering principle is true for all subsets of $\mathbf{Z}^+$ with n elements, and suppose Y has $n+1$ elements. Take $y \in Y$ and let z be the least element of $Y \setminus y$. Then $\min(\{y, z\})$ is the least element of Y. This proves that the principle of induction implies the well-ordering principle. □

Also relevant is the following variation on the principle of induction:

Strong Induction. If a subset $X \subseteq \mathbf{Z}^+$ satisfies $1 \in X$ and

$$1, \ldots, n \in X \implies n+1 \in X,$$

then $X = \mathbf{Z}^+$.

Despite looking like a stricter requirement, strong induction is actually implied by the principle of induction.

PROOF. Let $Y \subseteq \mathbf{Z}^+$ satisfy $1 \in Y$ and

$$1, \ldots, n \in Y \implies n+1 \in Y.$$

Let $X \subseteq \mathbf{Z}^+$ be the set of all positive integers n such that all positive integers less than or equal to n are in Y. Then $1 \in X$. Furthermore, if $n \in X$, then $n+1 \in X$. So then by the principle of induction, $X = \mathbf{Z}^+$, which implies $Y = \mathbf{Z}^+$. □

A function is said to be *defined recursively* if it is defined at 1 and if there exists a rule for finding $f(n)$ in terms of $f(1)$ through $f(n-1)$. By strong induction, such functions are defined on all of $\mathbf{Z}^+$.

The archetypal example of a recursively defined function is the *factorial function*, given by

$$n! = \begin{cases} 1 & \text{if } n = 0 \\ n \cdot (n-1)! & \text{otherwise} \end{cases}$$

For example, $6! = 720$.

Defined in terms of the factorial function are the *binomial coefficients*,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

A quick computation shows that

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Also note that $\binom{n}{0} = \binom{n}{n} = 1$.

By these observations, binomial coefficients are always integers.

THEOREM 1.1.1 (Binomial theorem). *Let* a *and* b *be integers and* n *a nonnegative integer. Then*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

PROOF. By induction. To see that the claim is true for $n = 0$, note that

$$(a+b)^0 = 1 = \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k}.$$

Now assume the claim is true for all integers $n \leq m$. Then

$$
\begin{aligned}
(a+b)^{m+1} &= (a+b)^m(a+b) \\
&= \left(\sum_{k=0}^{m}\binom{m}{k}a^k b^{m-k}\right)(a+b) \qquad \text{by the inductive step} \\
&= \left(\sum_{k=0}^{m}\binom{m}{k}a^{k+1} b^{m-k}\right) + \left(\sum_{k=0}^{m}\binom{m}{k}a^k b^{m-k+1}\right) \\
&= \left(\sum_{k=0}^{m-1}\binom{m}{k}a^{k+1} b^{m-k}\right) + a^{m+1} + \left(\sum_{k=1}^{m}\binom{m}{k}a^k b^{m-k+1}\right) + b^{m+1} \\
&= \left(\sum_{k=1}^{m}\binom{m}{k-1}a^{k} b^{m-k+1}\right) + a^{m+1} + \left(\sum_{k=1}^{m}\binom{m}{k}a^k b^{m-k+1}\right) + b^{m+1} \\
&= a^{m+1} + \left(\sum_{k=1}^{m}\left(\binom{m}{k-1}+\binom{m}{k}\right)a^k b^{m-k+1}\right) + b^{m+1} \\
&= a^{m+1} + \left(\sum_{k=1}^{m}\binom{m+1}{k}a^k b^{m-k+1}\right) + b^{m+1} \\
&= \sum_{k=0}^{m+1}\binom{m+1}{k}a^k b^{m+1-k}.
\end{aligned}
$$

By induction, the claim is true for all nonnegative integers n. □

Two consequences of this formula are that

$$2^n = \sum_{k=0}^{n}\binom{n}{k} \quad \text{and} \quad 0 = \sum_{k=0}^{n}(-1)^k\binom{n}{k}.$$

1.2. Divisibility

The integers are closed under addition, subtraction, and multiplication. However, not every integer quotient forms another integer.

DEFINITION 1.2.1. Let $a, b \in \mathbf{Z}$. We say a *divides* b (or that b *is divisible by* a, or that b *is a multiple of* a, or that a *is a factor of* b) and write $a \mid b$ if there is some $c \in \mathbf{Z}$ such that $b = ac$.

PROPOSITION 1.2.2. *If* $x \mid n$ *and* $x \mid m$*, then for any integers* a *and* b*,*

$$x \mid (an + bm).$$

PROOF. We have $cx = n$ and $dx = m$ for some integers c and d. So

$$an + bm = acx + bdx = (ac + bd)x,$$

which implies $x \mid (an + bm)$. □

THEOREM 1.2.3 (Division with remainder). *If* a *and* b *are integers such that* $b > 0$*, then there exist unique integers* q *and* r *such that*

$$a = bq + r \quad \textit{and} \quad 0 \leq r < b.$$

PROOF. Define the *floor* of x (denoted $\lfloor x \rfloor$) to be the largest integer less than or equal to x. Noting that

$$x - 1 < \lfloor x \rfloor \leq x,$$

we set $q = \lfloor a/b \rfloor$, $r = a - b\lfloor a/b \rfloor$. Now observe that

$$a/b - 1 < \lfloor a/b \rfloor \leq a/b.$$

Multiplying through by b yields

$$a - b < b\lfloor a/b \rfloor \leq a.$$

Invert the inequality to obtain

$$-a \leq -b\lfloor a/b \rfloor < b - a,$$

and then add a:

$$0 \leq a - b\lfloor a/b \rfloor < b.$$

To show q and r are unique, suppose we have q' and r' such that $a = bq' + r'$. Then $0 = b(q - q') + (r - r')$, i.e. b divides $r - r'$. But since r and r' are both between 0 and b, their difference is between $\pm b$, so b can divide $r - r'$ only if $r - r' = 0$, so we must have $r = r'$, and $q = q'$ immediately after. □

1.3. Prime Numbers

The positive integer 1 has just one positive divisor. Every other positive integer has at least two positive divisors, being divisible by itself and 1.

DEFINITION 1.3.1. A *prime number* is a positive integer with exactly two positive divisors. A positive integer with more than two positive divisors is *composite*.

PROPOSITION 1.3.2. *Every integer greater than 1 has a prime divisor.*

PROOF. By contradiction. Assume there is a positive integer n greater than 1 with no prime divisors. By the well-ordering principle we may take n to be the smallest such number. If an integer is prime, it has a prime divisor (namely, itself). Taking the contrapositive, an integer with no prime divisors must not be prime. Hence, n is not prime, so we may write $n = ab$ with $1 < a < n$ and $1 < b < n$. Because $a < n$, a must have a prime divisor. But any prime divisor of a must also be a prime divisor of n, contradicting our assumption that n had no prime divisors. □

THEOREM 1.3.3. *There are infinitely many prime numbers.*[1]

PROOF. Consider

$$Q_n = n! + 1.$$

We know Q_n has a prime divisor, which we will call q_n. Observe that $q_n > n$: otherwise, we would have $q_n \leq n$, hence $q_n \mid n!$, hence $q_n \mid (Q_n - n!) = 1$, which is impossible. We have thus found a prime larger than n for any n, so there must be infinitely many primes. □

The gap between primes can be of any length. Indeed, consider

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

These n consecutive integers are all composite.

[1] Consequently, 0 has infinitely many divisors, and is also the unique integer satisfying this condition.

CHAPTER 2

Coprimality and Factorization

2.1. Greatest Common Divisors

DEFINITION 2.1.1. We say an integer d is a *common divisor* of a and b if both $d \mid a$ and $d \mid b$, and that a common divisor is *greatest* if any common divisor c of a and b also divides d. We denote by (a, b) the greatest common divisor of a and b.

THEOREM 2.1.2 (Bezout's identity). *If a and b are integers not both 0, then (a, b) is the smallest positive linear combination of a and b, e.g. there are integers m and n such that*

$$am + bn = (a, b).$$

PROOF. Consider all integer linear combinations of a and b.

Some of these linear combinations are positive, such as $a^2 + b^2$, so the set of all positive linear combinations of a and b is nonempty. By the well-ordering principle this set has a least element, which we will call d. Let m and n be such that $d = am + bn$.

Use division with remainder to obtain $a = dq + r$. Note that

$$r = a - dq = a - (am + bn)q = a(1 - mq) - b(nq),$$

i.e. r is a linear combination of a and b. If r were positive then d wouldn't be the smallest positive linear combination of a and b, so $r = 0$, i.e. $d \mid a$. A nearly identical argument shows that $d \mid b$.

Suppose c is a common divisor of a and b. Then there exist integers u and v such that $a = uc$ and $b = vc$. But then

$$d = am + bn = ucm + vcn = (um + vn)c,$$

i.e. $c \mid d$. So $d = (a, b)$, and the proof is complete. □

DEFINITION 2.1.3. We say two integers a and b are *coprime* if $(a, b) = 1$.

2.2. The Euclidean Algorithm

Here is a way to compute greatest common divisors.

Euclidean Algorithm. Let $r_0 = a$ and $r_1 = b$ be nonnegative integers with $b \neq 0$. Divide repeatedly to obtain

$$r_j = r_{j+1}q_{j+1} + r_{j+2}, \qquad 0 < r_{j+2} < r_{j+1}$$

for $j \in \{0, \dots, n-2\}$. If $r_n = 0$, then $r_{n-1} = (a, b)$.

We begin by showing that whenever $a = bq + r$, we have $(a, b) = (b, r)$.

PROOF. If both $c \mid a$ and $c \mid b$ then $c \mid a - bq = r$. Also, if both $c \mid b$ and $c \mid r$ then $c \mid bq + r = a$. Since the common divisors of a and b are the same as the common divisors of b and r, we have $(a, b) = (b, r)$. □

Now we show the Euclidean algorithm works.

PROOF. In the situation described above, note that

$$(a, b) = (b, r_2) = (r_2, r_3) = \cdots = (r_{n-1}, 0) = r_{n-1}.$$

We hit 0 eventually because the sequence of remainders cannot contain more than $|a|$ terms. □

2.3. The Fundamental Theorem of Arithmetic

THEOREM 2.3.1. *Any positive integer can be uniquely factored into primes.*

First we prove existence by contradiction.

PROOF. Let $n \in \mathbf{Z}^+$. Suppose n were the least positive integer such that n cannot be factored into primes. Then n cannot itself be prime, so $n = ab$ with $1 < a < n$ and $1 < b < n$. Thus, a and b admit factorizations into primes. Combining these yields a prime factorization of n, which contradicts our assumption that n had no such prime factorization. □

Before proving uniqueness, we need an auxillary fact.

PROPOSITION 2.3.2 (Euclid's lemma). *If* a, b, c *are positive integers with* $(a, b) = 1$ *and* $a \mid bc$, *then* $a \mid c$.

PROOF. Since $(a, b) = 1$, we may write $1 = am + bn$. Multiply by c to obtain $c = amc + bnc$. But $a \mid amc$ and $a \mid bnc$, so $a \mid c$. □

Next, we need to show that primes do not decompose as factors.

PROPOSITION 2.3.3. *If* $a_1, \ldots, a_n$ *are integers and* p *prime,*

$$p \mid a_1 \cdots a_n \implies p \mid a_i \quad \textit{for some } i.$$

PROOF. By induction. If $n = 1$, then $p = a_1$, hence $p \mid a_1$. Now suppose the claim holds for $n = m$, and consider $p = a_1 \cdots a_{m+1}$. Then by what was just shown, either $p \mid a_1 \cdots a_m$ or $p \mid a_{m+1}$. But if $p \mid a_1 \cdots a_m$ then $p \mid a_i$ for some i by the inductive hypothesis. □

We are now ready to prove uniqueness of prime factorization.

PROOF. Suppose n is the smallest positive integer with

$$n = p_1 \cdots p_s = q_1 \cdots q_t$$

where the p_i and q_j are prime. Consider p_1. It must divide one of the q_i, let's say q_1 without loss of generality. But q_1 is prime, and since $p_1 \neq 1$, we must have $p_1 = q_1$. Divide through by p_1 to obtain

$$n/p_1 = p_2 \cdots p_s = q_2 \ldots q_t,$$

contradicting our assumption that n was the smallest positive integer with at least two prime factorizations. □

CHAPTER 3

Congruences

The language of congruences was developed by Gauss.

3.1. Basic Properties

DEFINITION 3.1.1. Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{Z}^+$. We say a is *congruent to* b *modulo* m and write $a = b \pmod{m}$ if $m \mid (a - b)$.

PROPOSITION 3.1.2. *Being congruent modulo* m *is an equivalence relation: it is reflexive, symmetric, and transitive.*

PROOF. Since every number divides 0, we have $m \mid (a - a)$, thus $a = a \pmod{m}$. Suppose $a = b \pmod{m}$. Then $m \mid (a - b)$, hence $m \mid (b - a)$, hence $b = a \pmod{m}$. Finally, suppose $a = b \pmod{m}$ and $b = c \pmod{m}$. Then $m \mid (a - b)$ and $m \mid (b - c)$, hence

$$m \mid ((a - b) + (b - c)) = (a - c),$$

hence $a = c \pmod{m}$. □

One can do arithmetic with congruences.

PROPOSITION 3.1.3. *Let* $a, b, c, d \in \mathbf{Z}$ *and* $m \in \mathbf{Z}^+$. *If* $a = b \pmod{m}$ *and* $c = d \pmod{m}$, *then*

(1) $a + c = b + d \pmod{m}$,
(2) $a - c = b - d \pmod{m}$, *and*
(3) $ac = bd \pmod{m}$.

PROOF. We have $m \mid (a - b)$ and $m \mid (c - d)$. Observe that

$$m \mid ((a - b) + (c - d)) = ((a + c) - (b + d)),$$

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

and

$$m \mid (a - b)c + b(c - d) = ac - bc + bc - bd = ac - bd,$$

from which the result follows. □

3.2. Sun's Remainder Theorem

THEOREM 3.2.1. *Given integers* $a_1, \dots, a_k$ *and pairwise coprime integers* $n_1, \dots, n_k$*, the system of congruences*

$$x = a_i \pmod{n_i}$$

has a solution unique modulo $N = \prod_{i=1}^{k} n_i$.

PROOF. Let $N_i = N/n_i$. By pairwise coprimality of the n_i, we have $(N_i, n_i) = 1$. Hence, we can find inverses y_i such that $N_i y_i = 1 \pmod{n_i}$. Consider

$$x = a_1 N_1 y_1 + \cdots + a_k N_k y_k.$$

Since $N_1 y_1 = 1 \pmod{n_1}$, we have $a_1 N_1 y_1 = a_1 \pmod{n_1}$. Since $n_1 \mid N_j$ for $j \neq 1$, all the other terms vanish, so $x = a_1 \pmod{n_1}$. Similarly, $x = a_i \pmod{n_i}$ for all $i \in \{1, \dots, k\}$.

To see that the solution is unique modulo N, suppose x and $\widetilde{x}$ are both solutions. Then $x - \widetilde{x} = 0 \pmod{n_i}$. Multiplying these congrunces together, we have $x - \widetilde{x} = 0 \pmod{N}$. □

3.3. Wilson's Theorem

THEOREM 3.3.1. *If* p *is prime, then* $(p-1)! = -1 \pmod{p}$.

PROOF. Note that the only solutions to $x^2 = 1 \pmod{p}$ are 1 and -1, i.e. 1 and $p-1$ are the only equivalence classes that are their own inverses modulo p. Thus every element from 2 to $p-2$ has an inverse that isn't itself. Multiplying the $(p-3)/2$ classes together gives the result. □

3.4. Binomials Modulo p

Note that the binomial coefficients are divisible modulo p, for if $N = \frac{p!}{(p-r)!r!}$ then $p \mid p!$ but $p \nmid (p-r)!$ and $p \nmid r!$, thus implying $p \mid N$. Thus,

$$(a+b)^p = a^p + b^p \pmod{p}.$$

CHAPTER 4

Arithmetic Functions

An *arithmetic function* is a function from $\mathbf{Z}^+$ to $\mathbf{Z}$.

One example of an arithmetic function is (n, k) for fixed k.

PROPOSITION 4.0.1. *For coprime* m *and* n,

$$(m, k)(n, k) = (mn, k).$$

PROOF. We will show $(mn, k) \mid (m, k)(n, k)$ and $(m, k)(n, k) \mid (mn, k)$. Note that $(m, k)(n, k)$ certainly divides both mn and k, and thus also divides (mn, k). Since we have $(m, k) = am + bk$ and $(n, k) = cn + dk$ by Bezout's identity,

$$(m, k)(n, k) = mn \cdot ac + (b(cm + dk) + amd)k$$

i.e. $(mn, k) \mid (m, k)(n, k)$. This completes the proof. □

Several other such functions also exist.

4.1. The Möbius Function

DEFINITION 4.1.1. The *Möbius function* is

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^s & \text{if } n \text{ is squarefree with } s \text{ prime factors} \\ 0 & \text{otherwise} \end{cases}$$

PROPOSITION 4.1.2. *For coprime* m *and* n,

$$\mu(mn) = \mu(m)\mu(n)$$

i.e. μ *is multiplicative.*

PROOF. By cases. Suppose (without loss of generality) that $m = 1$. Then $mn = n$, and in particular

$$\mu(mn) = \mu(n) = 1 \cdot \mu(n) = \mu(1)\mu(n) = \mu(m)\mu(n).$$

Now suppose m and n are coprime integers both not equal to 1. If (without loss of generality) m is not squarefree, then mn will also be not squarefree, wherein

$$\mu(mn) = 0 = 0 \cdot \mu(n) = \mu(m)\mu(n).$$

If m and n are both squarefree, then mn will also be squarefree. Since m and n are coprime, m having s divisors and n having t divisors implies mn has $s + t$ divisors. □

THEOREM 4.1.3 (Möbius Inversion Formula). *If* f *and* g *are such that*

$$f(n) = \sum_{d|n} g(d), \quad n \in \mathbf{Z}^+$$

then equivalently

$$g(n) = \sum_{d|n} \mu(d) f(n/d), \quad n \in \mathbf{Z}^+.$$

PROOF. Define the *convolution* of any two arithmetic functions f, g as

$$(f * g)(n) = \sum_{d|n} f(d) g(n/d).$$

Rewriting the sum as

$$(f * g)(n) = \sum_{ab=n} f(a) g(b)$$

makes it clear that convolution is both commutative and associative.

Now we will show that

$$\mu * \mathbf{1} = \delta$$

where

$$\delta(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

and $\mathbf{1}(n) = 1$ for all n.

If $n = 1$, then $\sum_{d|1} \mu(n) = \mu(1) = 1$. So suppose $n \neq 1$ with k prime factors. All the non-squarefree factors of n vanish in the sum, so

$$\sum_{d|n} \mu(d) = \sum_{\ell=0}^{k} \binom{k}{\ell} \mu(p_1 \cdots p_\ell) = (1-1)^k = 0.$$

Now we prove the formula. Observe that

$$g = \delta * g = (\mu * \mathbf{1}) * g = \mu * (\mathbf{1} * g) = \mu * f$$

and also

$$f = f * \delta = f * (\mu * \mathbf{1}) = (f * \mu) * \mathbf{1} = g * \mathbf{1}$$

which is what we wanted to show. □

PROPOSITION 4.1.4.

$$\prod_{p|n}(1 - p^{-1}) = \sum_{d|n} \frac{\mu(d)}{d}.$$

PROOF. All the non-squarefree factors of n vanish in the sum on the right, and multiplying out the product on the left yields the remaining sum. □

4.2. The Euler Totient

DEFINITION 4.2.1. The *Euler totient function* is

$$\phi(n) = n \prod_{p|n}(1 - p^{-1})$$

where the product is over all primes dividing n.

PROPOSITION 4.2.2. *The ϕ function counts the integers coprime to n:*

$$\phi(n) = |\{k : (n, k) = 1, 1 \leq k < n\}|.$$

PROOF. When $p \mid n$, the number of positive integers up to n divisible by p is n/p. Thus, each $(1 - p^{-1})$ term in the product filters out the integers divisible by p. For example, if $n = \prod_{j=1}^{k} p_j^{a_j}$, then there are

$$n(1 - p_1^{-1}) = n - n/p_1$$

integers between 1 and n not divisible by p_1. Having a $(1 - p_i^{-1})$ term for each p_i results in the product counting the positive integers up to n coprime to n. □

PROPOSITION 4.2.3. *For coprime m and n,*

$$\phi(mn) = \phi(m)\phi(n),$$

i.e. ϕ is multiplicative.

PROOF. Consider the system of congruences

$$x = a \pmod{m}, \qquad x = b \pmod{n}.$$

Since m and n are coprime, this system has a unique solution modulo mn by Sun's remainder theorem. We claim x is coprime to mn if and only if a is coprime to m and b is coprime to n.

$(\implies)$: Suppose x is coprime to mn. Then x is coprime to both m and n. Write $x = km + a$ and $x = \ell n + b$. Were a not coprime to m, x would be not coprime to m (since m is not coprime to m), so a must be coprime to m. Similarly, b must be coprime to n.

$(\impliedby)$: Now suppose a is coprime to m and b is coprime to n. Again consider $x = km + a$ and $x = \ell n + b$. Were x not coprime to m, then a would not be coprime to m, so x must be coprime to m. Similarly, x is coprime to n. Since m and n are coprime, x is coprime to mn.

Since there are $\phi(m)$ numbers coprime to m and $\phi(n)$ numbers coprime to n, and since each pair (a, b) produces a unique number x coprime to mn, it follows that there are $\phi(m)\phi(n)$ numbers between 1 and mn coprime to mn. □

PROPOSITION 4.2.4.

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

PROOF. We want to show $\mathrm{id} = \mathbf{1} * \phi$, so by Möbius inversion it suffices to show $\phi = \mu * \mathrm{id}$. From the definition of ϕ and a previous proposition,

$$\phi(n) = n \prod_{p|n} (1 - p^{-1}) = \sum_{d|n} \mu(d) \frac{n}{d} = (\mu * \mathrm{id})(n).$$

This proves the result. □

PROPOSITION 4.2.5.

$$\sum_{\ell=1}^{n} \left\lfloor \frac{n}{\ell} \right\rfloor \phi(\ell) = \binom{n}{2}.$$

PROOF. Since

$$n = \sum_{d|n} \phi(d),$$

we have

$$\binom{n}{2} = \sum_{k=1}^{n} k = \sum_{k=1}^{n} \sum_{d|k} \phi(d) = \sum_{k=1}^{n} \sum_{\ell=1}^{n} \phi(\ell)[\ell \mid k],$$

where

$$[\ell \mid k] = \begin{cases} 1 & \text{if } \ell \mid k \\ 0 & \text{otherwise} \end{cases}$$

noting that for $\ell > k$ we have $[\ell \mid k] = 0$.

Swapping the order of summation,

$$\sum_{k=1}^{n} \sum_{\ell=1}^{n} \phi(\ell)[\ell \mid k] = \sum_{\ell=1}^{n} \phi(\ell) \sum_{k=1}^{n} [\ell \mid k] = \sum_{\ell=1}^{n} \phi(\ell) \left\lfloor \frac{n}{\ell} \right\rfloor,$$

which completes the proof. □

4.3. Euler's Theorem

THEOREM 4.3.1. *If a and n are coprime positive integers, then*

$$a^{\phi(n)} = 1 \pmod{n}.$$

PROOF. For any two integers a and b both coprime to n, their product is also coprime to n. Said another way,

$$\prod_{(b,n)=1} b = \prod_{(b,n)=1} ab = a^{\phi(n)} \prod_{(b,n)=1} b \pmod{n},$$

from which the result follows. □

We note that the case $\phi(p) = p - 1$ is known as Fermat's Little Theorem.

4.4. The Sum of Divisors

DEFINITION 4.4.1. The *sum of divisors function* is

$$\sigma_k(n) = \sum_{d|n} d^k.$$

THEOREM 4.4.2. *For coprime m and n,*

$$\sigma_k(mn) = \sigma_k(m)\sigma_k(n).$$

PROOF. We'll show that if f and g are multiplicative, then so is $f * g$.

$$\begin{aligned}
(f * g)(mn) &= \sum_{ab=mn} f(a)g(b) \\
&= \sum_{a_m b_m = m} \sum_{a_n b_n = n} f(a_m a_n) g(b_m b_n) \\
&= \sum_{a_m b_m = m} \sum_{a_n b_n = n} f(a_m) f(a_n) g(b_m) g(b_n) \\
&= \left(\sum_{a_m b_m = m} f(a_m) g(b_m) \right) \left(\sum_{a_n b_n = n} f(a_n) g(b_n) \right) \\
&= (f * g)(m) \cdot (f * g)(n)
\end{aligned}$$

With this established, note that $\sigma_k = \mathrm{id}^k * \mathbf{1}$. This proves the result. □

CHAPTER 5

Primitive Roots

5.1. The Order of an Integer

By Euler's theorem, the set of positive integers x satsifying

$$a^x = 1 \pmod{n}$$

is nonempty.

DEFINITION 5.1.1. The smallest positive integer x satisfying the above congruence is denoted $\text{ord}_n(a)$ and is called the *order* of a modulo n.

PROPOSITION 5.1.2. *If a and n are coprime with $n > 0$, then the positive integer x is a solution to $a^x = 1 \pmod{n}$ if and only if*

$$\mathit{ord}_n(a) \mid x.$$

PROOF. Suppose $\text{ord}_n(a) \mid x$. Then $x = \text{ord}_n(a) \cdot k$ for some k, hence

$$a^x = a^{\text{ord}_n(a)\cdot k} = (a^{\text{ord}_n(a)})^k = 1^k = 1 \pmod{n}.$$

Conversely, if $a^x = 1 \pmod{n}$, divide to obtain

$$x = q \cdot \text{ord}_n(a) + r, \qquad 0 \leq r < \text{ord}_n(a).$$

Thus $a^x = a^r \pmod{n}$. But we must have $r = 0$, since $y = \text{ord}_n(a)$ is the smallest positive integer such that $a^y = 1 \pmod{n}$. Hence $\text{ord}_n(a) \mid x$, as desired. □

So, in particular, $\text{ord}_n(a) \mid \phi(n)$.

PROPOSITION 5.1.3. *Let a, b, and n be integers with ord(a) and ord(b) coprime and $n > 0$. Then*

$$\mathit{ord}_n(a)\mathit{ord}_n(b) = \mathit{ord}_n(ab).$$

PROOF. Let $\text{ord}_n(a) = x$, $\text{ord}_n(b) = y$, and $\text{ord}_n(ab) = z$. Note that $z \mid xy$, since

$$(ab)^{xy} = a^{xy}b^{xy} = (a^x)^y(b^y)^x = 1 \pmod{n}.$$

Since x and y are coprime,

$$(ab)^z = 1 \implies 1 = ((ab)^z)^x = (a^x)^z b^{xz} = b^{xz} \implies y \mid xz \implies y \mid z$$

where the third implication follows via Euclid's lemma. Similarly, $x \mid z$. By coprimality of x and y again, we have $xy \mid z$. We may thus conclude that $xy = z$. □

5.2. Existence of Primitive Roots

DEFINITION 5.2.1. If r and n are coprime with $n > 0$ and if

$$\text{ord}_n(r) = \phi(n),$$

then r is called a *primitive root* modulo n.

THEOREM 5.2.2. *Primitive roots exist modulo a prime.*

PROOF. By Fermat's Little Theorem, the equation

$$X^{p-1} - 1 = 0$$

has $p-1$ solutions modulo p. For any divisor d of $p-1$ consider the factorization

$$X^{p-1} - 1 = (X^d - 1)(1 + X^d + \cdots + X^{p-1-d}).$$

The polynomial $X^d - 1$ has at most d roots and the other one has at most $p-1-d$ roots and $X^{p-1}-1$ has exactly $p-1$ roots. Hence, $X^d - 1$ has exactly d roots.

Factor $p-1$ into

$$p - 1 = \prod q^{e_q}$$

For each factor q^e of $p-1$, $x^{q^e} - 1$ has q^e roots and $x^{q^{e-1}} - 1$ has q^{e-1} roots; hence, there are $q^e - q^{e-1} = \phi(q^e)$ elements x_q for which $\text{ord}_p(x_q) = q^e$. By the proposition about $\text{ord}_n(a)$ respecting multiplication with coprime factors, any product $\prod_q x_q$ has order $p-1$, and thus is a primitive root. □

THEOREM 5.2.3. *Primitive roots exist modulo an odd prime power.*

PROOF. Let g be a primitive root modulo p. By the binomial theorem,

$$(g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p \pmod{p^2},$$

thus $(g+p)^{p-1} \neq g^{p-1} \pmod{p^2}$, and in particular either $g^{p-1} \neq 1 \pmod{p^2}$ or $(g+p)^{p-1} \neq 1 \pmod{p^2}$. Replace g with $g+p$ if necessary to ensure that $g^{p-1} \neq 1 \pmod{p^2}$, i.e.

$$g^{p-1} = 1 + k_1 p, \quad p \nmid k_1.$$

Again by the binomial theorem,

$$g^{p(p-1)} = (1+k_1 p)^p = 1 + k_2 p^2, \quad p \nmid k_2.$$

So g is now a primitive root modulo p^2. Let $e > 2$ be an integer. Again by the binomial theorem,

$$g^{p^{e-2}(p-1)} = 1 + k_{e-1} p^{e-1}, \quad p \nmid k_{e-1}.$$

We have that $\mathrm{ord}_{p^e}(g) \mid \phi(p^e) = p^{e-1}(p-1)$. Note that $\mathrm{ord}_{p^e}(g)$ can't be of the form $p^{\varepsilon} d$ where $\varepsilon \leq e-1$ and d a proper divisor of $p-1$ because then

$$g^{p^{\varepsilon} d} = 1 \pmod{p^e}$$

reduces mod p to $g^d = 1 \pmod{p}$, contradicting the fact that g is a primitive root modulo p. So we must have

$$\mathrm{ord}_{p^e}(g) = p^{\varepsilon}(p-1)$$

where $\varepsilon \leq e-1$, and the calcluation above shows $\varepsilon = e-1$, completing the proof. □

CHAPTER 6

Quadratic Residues

DEFINITION 6.0.1. If m is a positive integer, we say a is a *quadratic residue* of m if $(a, m) = 1$ and

$$x^2 \equiv a \pmod{m}$$

has a solution. If the congruence above has no solution, then a is a *quadratic nonresidue* of m.

PROPOSITION 6.0.2. *Let p be an odd prime and a an integer not divisible by p. Then*

$$x^2 \equiv a \pmod{p}$$

either has no solutions or exactly two distinct (i.e. incongruent) solutions modulo p.

PROOF. If $x^2 \equiv a \pmod{p}$ has a solution x_0, then $-x_0$ is also a solution. If $x_0 \equiv -x_0 \pmod{p}$ then $2x_0 \equiv 0 \pmod{p}$, and we may divide through by 2 since p is odd, showing that $p \mid x_0$, contradiction. So there are at least two distinct solutions.

To see that there are exactly two distinct solutions, suppose x_0 and x_1 both solve $x^2 \equiv a \pmod{p}$. Then $x_0^2 \equiv x_1^2 \pmod{p}$, hence

$$(x_0 - x_1)(x_0 + x_1) \equiv 0 \pmod{p},$$

implying that $x_0 \equiv \pm x_1$. □

PROPOSITION 6.0.3. *If p is an odd prime, there are exactly $\frac{p-1}{2}$ residues and $\frac{p-1}{2}$ nonresidues of p among the integers*

$$1, \quad \ldots, \quad p-1.$$

PROOF. Since each square from 1^2 to $(p-1)^2$ has exactly two distinct solutions among 1 through $p-1$, the conclusion follows. □

6.1. The Legendre Symbol

DEFINITION 6.1.1. Let p be an odd prime and a an integer. We define

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p \\ 0 & \text{if } a \mid p \end{cases}$$

PROPOSITION 6.1.2 (Euler's criterion). *Let p be an odd prime and a an integer not divisible by p. then*

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

PROOF. First assume that $\left(\frac{a}{p}\right) = 1$. Then $x^2 = a$ has a solution, say x_0. By Fermat's Little Theorem,

$$a^{\frac{p-1}{2}} = (x_0^2)^{\frac{p-1}{2}} = x_0^{p-1} = 1 \pmod{p}.$$

Now assume that $\left(\frac{a}{p}\right) = -1$. Then $x^2 = a$ has no solutions, Note that for each i in 1 through $p-1$ there exists a unique j in 1 through $p-1$ for which $ij = a$, and since $x^2 = a \pmod{p}$ has no solutions, we know $i \neq j$. So then

$$(p-1)! = a^{\frac{p-1}{2}},$$

and applying Wilson's theorem completes the proof. □

THEOREM 6.1.3. *Let p be an odd prime and a, b integers not divisible by p. Then*

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

PROOF. (1) If $a = b \pmod{p}$, then $x^2 = a \pmod{p}$ has solutions if and only if $x^2 = b \pmod{p}$ has solutions, so $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
(2) By Euler's criterion,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} = \left(\frac{ab}{p}\right) \pmod{p},$$

and since the Legendre symbol takes the values ± 1, we may conclude that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(3) This follows from the previous part.

□

PROPOSITION 6.1.4. *If* p *is an odd prime, then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p = 1 \pmod 4 \\ -1 & \text{if } p = -1 \pmod 4 \end{cases}$$

PROOF. Apply Euler's criterion. If $p = 1 \pmod 4$, then

$$(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1.$$

If $p = -1 \pmod 4$, then

$$(-1)^{\frac{p-1}{2}} = (-1)^{2k-1} = -1.$$

□

6.2. Gauss' Lemma

THEOREM 6.2.1. *Let* p *be an odd prime and* a *an integer coprime to* p. *If* s *is the least number of positive residues modulo* p *of the integers*

$$a, \quad 2a, \quad \ldots, \quad \frac{p-1}{2}a$$

that are greater than $p/2$, *then*

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

PROOF. Let $u_1, \ldots, u_s$ represent the residues of the integers

$$a, \quad 2a, \quad \ldots, \quad \frac{p-1}{2}a$$

greater than $p/2$, and let $v_1, \ldots, v_t$ represent the residues of these integers less than $p/2$. We will show

$$\{p - u_1, \ldots, p - u_s, v_1, \ldots, v_t\} = \{1, \ldots, p-1\}.$$

It suffices to show that no two of these numbers are congruent modulo p. Were $u_i = u_j$, then since a does not divide p,

$$ma = na \pmod p \implies m = n \pmod p,$$

contradiction. So $u_i \neq u_j$, and similarly $v_i \neq v_j$. In addition, we cannot have $p - u_i = v_j$, for if so, then

$$ma = p - na \pmod p \implies m = -n \pmod p,$$

which contradicts the fact that m and n are both in 1 through $\frac{p-1}{2}$.

Now we multiply things together. We know

$$\begin{aligned}(p-u_1)\cdots(p-u_s)v_1\cdots v_t &= (-1)^s u_1\cdots u_s v_1\cdots v_t\\ &= (-1)^s\left(\frac{p-1}{2}\right)! \pmod p\end{aligned}$$

Yet at the same time,

$$u_1\cdots u_s v_1\cdots v_t = a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \pmod p$$

By Euler's criterion,

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = (-1)^s,$$

which completes the proof. □

PROPOSITION 6.2.2. *If* p *is an odd prime, then*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

PROOF. First, we compute the number of residues in

$$1\cdot 2,\quad 2\cdot 2,\quad \cdots,\quad \frac{p-1}{2}\cdot 2$$

greater than $p/2$. This is a direct count since all of the above residues are less than p. When $1 \le j \le \frac{p-1}{2}$, $2j < p/2$ when $j \le p/4$, so there are $\lfloor \frac{p}{4} \rfloor$ integers less than $p/2$, and thus

$$s = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$$

greater than $p/2$. By Gauss' lemma, it remains to show that

$$\frac{p^2-1}{8} = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \pmod 2.$$

We first consider $\frac{p^2-1}{8}$. If $p = \pm 1 \pmod 8$, then

$$\frac{p^2-1}{8} = \frac{64k^2 \pm 16k}{8} = 0 \pmod 2.$$

If $p = \pm 3 \pmod 8$, then

$$\frac{p^2-1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 1 \pmod 2.$$

Now we consider $x = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$.

$$p = 8k+1 \implies x = 4k - \left\lfloor 2k + \frac{1}{4} \right\rfloor = 0 \pmod 2$$

$$p = 8k+3 \implies x = 4k+1 - \left\lfloor 2k + \frac{3}{4} \right\rfloor = 1 \pmod 2$$

$$p = 8k+5 \implies x = 4k+2 - \left\lfloor 2k + \frac{5}{4} \right\rfloor = 1 \pmod 2$$

$$p = 8k+7 \implies x = 4k+3 - \left\lfloor 2k + \frac{7}{4} \right\rfloor = 0 \pmod 2$$

Since $\frac{p^2-1}{8} = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor \pmod 2$ in all cases, the proof is complete. □

6.3. The Law of Quadratic Reciprocity

PROPOSITION 6.3.1. *If* p *is an odd prime and* a *an integer not divisible by* p*, then*

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$$

where

$$T(a,p) = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{aj}{p} \right\rfloor$$

PROOF. As in the proof of Gauss' lemma, let $u_1, \dots, u_s$ represent the residues of

$$a, \quad 2a, \quad \dots, \quad \frac{p-1}{2}a$$

that are greater than $p/2$, and $v_1, \dots, v_t$ the residues of the above numbers that are less than $p/2$. Dividing,

$$ja = p\left\lfloor \frac{aj}{p} \right\rfloor + r$$

where $r = u_i$ or $r = v_j$. Adding $\frac{p-1}{2}$ of these together yields

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{aj}{p} \right\rfloor + \sum_{i=1}^{s} u_i + \sum_{j=1}^{t} v_j$$

We also showed, though, that $p - u_1, \ldots p - u_s, v_1, \ldots, v_t$ are all the integers from 1 through $\frac{p-1}{2}$, so

$$\sum_{j=1}^{\frac{p-1}{2}} j = ps - \sum_{i=1}^{s} u_i + \sum_{j=1}^{t} v_j.$$

Subtracting these equations, we find

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = pT(a,p) - ps + 2\sum_{i=1}^{s} u_i$$

and since a and p are odd, this reduces mod 2 to

$$T(a,p) = s \pmod 2,$$

and applying Gauss' lemma completes the proof. □

THEOREM 6.3.2 (Quadratic Reciprocity). *Let p and q be odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

PROOF. We consider pairs of integers (x, y) where $1 \le x \le \frac{p-1}{2}$ and $1 \le y \le \frac{q-1}{2}$. There are $\frac{p-1}{2}\frac{q-1}{2}$ such pairs. We divide these pairs into two groups based on relative sizes of qx and py.

First we note that for all such pairs (x, y) we have $qx \ne py$, for if $qx = py$, then $q \mid py$, implying either $q \mid p$ or $q \mid y$. But $q \mid p$ cannot happen since q and p are distinct primes, and $q \mid y$ cannot happen since $1 \le y \le \frac{q-1}{2}$.

To count the pairs for which $qx > py$, note that these are the pairs for which $1 \le x \le \frac{p-1}{2}$ and $1 \le y \le \frac{qx}{p}$, hence their number is $T(q, p)$.

To count the pairs for which $qx < py$, note that these are the pairs for which $1 \le y \le \frac{q-1}{2}$ and $1 \le x \le \frac{py}{q}$, hence their number is $T(p, q)$.

So

$$T(q,p) + T(p,q) = \frac{p-1}{2}\frac{q-1}{2},$$

hence

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{T(q,p)+T(p,q)} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

as desired. □