MAT 541 Intro to Number Theory
Lecture Notes

George Z. Miao

2023
Spring

Chapter 1

Preliminary

1.1 Math Induction

Definition 1.1.1 (Set of integers)**.** $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

Definition 1.1.2 (Set of whole numbers)**.** $\mathbb{O} = \{0, 1, 2, \dots\}$

Definition 1.1.3 (Set of natural numbers)**.** $\mathbb{N} = \{1, 2, 3, \dots\}$

1.1.1 Language of sets

- Universal set (S)
- Subset ($\subseteq$, $\subset$)
- Intersections
$$A \cap B = \{x \in S \mid x \in A \wedge x \in B\}$$
- Union
$$A \cup B = \{x \in S \mid x \in A \vee x \in B\}$$

Definition 1.1.4 (Well ordering principle)**.** *Every nonempty subset of $\mathbb{O}$ contains a least (smallest) element.*

Theorem 1.1.1 (Archimedean Principle)**.** *If $a, b \in \mathbb{N}$ then $\exists c \in \mathbb{N}.\ ac > b$*

Proof. Suppose false. Then $\forall u \in \mathbb{N}.\ au < b$. Now $S = \{b - au \mid u \in \mathbb{N}\} \in \mathbb{O}$. By W.O. Principle, there exists a least element in S.

$$b - aM_0 \in S$$
$$b - a(M_0 + 1) = (a - an_0) - a < b - an_0 \in S$$

□

Theorem 1.1.2 (1st principle of Fin. Induction)**.** *Let $S \subseteq \mathbb{N}$ s.t.*

1. $1 \in S$
2. *If $k \in S$ then $k + 1 \in S$*

Then $S = \mathbb{N}$.

Proof. Let $T = \{M \in \mathbb{N} \mid m \notin S\}$. Suppose $T \neq \varnothing$, then T has a least element m. $m \neq 1$ since $1 \in S$ so $m - 1 \in \mathbb{N}$. Now let $k = m - 1 \in S$, meaning $k + 1 = (m - 1) + 1 = m \in S$. Contradiction. Suppose $T = \varnothing$, then $S = \mathbb{N}$. □

Chapter 2

Divisibility Theorem

2.3 Greatest Common Devisor

Definition 2.3.1 (Cancellation)**.** *Let $a, b, c \in \mathbb{Z}, c \neq 0$ and $ac = bc$. Then $a = b$.*

Proof.

$$\begin{aligned} ac &= bc \\ ac - bc &= 0 \\ (a-b)c &= 0 \end{aligned}$$

Since $c \neq 0$

$$\begin{aligned} a - b &= 0 \\ a &= b \end{aligned}$$

$\square$

Theorem 2.3.1. *Assume $a, b \in \mathbb{Z}$ that not both 0 and $d = \gcd(ab)$. Then $\exists s, t \in \mathbb{Z}.\ as + bt = d$*

Corollary 2.3.1. *If $c \mid a$ and $c \mid d$ then $c \mid d = \gcd(a, b)$*

Corollary 2.3.2. *Let $a, b \in \mathbb{Z}$, not both 0 and let $T = \{ax + by \mid x, y \in Z\} = \mathbb{Z}_a + \mathbb{Z}_b$, then $T = \mathbb{Z}_d$*

Proof. (a) To prove that $T \subseteq \mathbb{Z}_d$. Let $x, y \in \mathbb{Z}$

$$ax + by = (a_0 d)x + (b_0 d)y$$

for some $a_0, b_0 \in \mathbb{Z}$

$$= d(a_0 x + b_0 y) \in \mathbb{Z}_d$$

gives that $T \subseteq \mathbb{Z}_d$

(b) To prove that $\mathbb{Z}_d \subseteq T$. We can find $s, t \in \mathbb{Z}$ s.t. $as + bt = d$. Let $m \in \mathbb{Z}$

$$\begin{aligned} ud &= u(as + bt) \\ &= a(us) + b(ut) \in T \\ \Rightarrow \mathbb{Z}_d &\subseteq T \end{aligned}$$

$\therefore \mathbb{Z}_d = T$

$\square$

Corollary 2.3.3. *Let $a, b \in \mathbb{Z}$ not both 0 with $d = \gcd(a, b)$. Then $\gcd(\frac{a}{b}, \frac{b}{d}) = 1$.*

Proof. $d \mid a$ as $a = a_0 d$ as $a_0 = \frac{a}{d}$. $\exists s, t \in \mathbb{Z}.\ as + bt = d$, gives that

$$\begin{aligned} b_0 &= \frac{b}{d} \\ a_0 ds + b_0 dt &= d \\ d(a_0 s + b_0 t) &= d \\ a_0 s + b_0 t &= 1 \end{aligned}$$

□

Corollary 2.3.4. *If $a \mid c$ and $b \mid c$ with $\gcd(a, b) = 1$ then $ab \mid c$.*

Proof. $a \mid c$, $b \mid c$ means $c = ac_0 = bd_0$ for some $c_0, b_0 \in \mathbb{Z}$. Now $1 = as + bt$ for some $s, t \in \mathbb{Z}$. So

$$\begin{aligned} c &= c1 \\ &= c(as + bt) \\ &= cas + cbt \\ &= bd_0 as + ac_0 bt \\ &= ab(d_0 s + c_0 t) \\ ab &\mid c \end{aligned}$$

□

Lemma 2.3.1. *Let $a, b \in \mathbb{Z}$, $b \neq 0$. If $a = qb + r$, $q, r \in \mathbb{Z}$ then $\gcd(a, b) = \gcd(b, r)$*

Theorem 2.3.2. *Assume $a, b \in \mathbb{Z}$, not both 0. $k \in \mathbb{N}$. Then*

$$\gcd(ka, kb) = k \gcd(a, b)$$

Proof. We know that $\gcd(ka, kb) = e$ where $e > 0$

$$\begin{aligned} \mathbb{Z}e &= \{kax + kby \mid x, y \in \mathbb{Z}\} \\ &= \{k(ax + by) \mid x, y \in \mathbb{Z}\} \\ &= k\{ax + by \mid x, y \in \mathbb{Z}\} \end{aligned}$$

Let $d = \gcd(a, b)$

$$\begin{aligned} &= k(\mathbb{Z}d) = \mathbb{Z}(kd) \\ &= \mathbb{Z}(kd) \end{aligned}$$

□

Corollary 2.3.5. *If $a, b \in \mathbb{Z}$ not both 0 and $a \neq b \in \mathbb{Z}$ then*

$$\gcd(ka, kb) = |k| \gcd(a, b)$$

Definition 2.3.2 (Common multiple)**.** *$a, b \in \mathbb{Z}$ are nonzero. $c \in \mathbb{Z}$ is a **common multiple** if $a \mid c$ and $b \mid c$, or $c = as = bt$, for some $s, t \in \mathbb{Z}$.*

Definition 2.3.3 (Least common multiple)**.** *If $a, b \in Z$ are nonzero, their **least common multiple** is an integer $m \in \mathbb{N}$ s.t.*

(a) $a \mid m$ and $b \mid m$

(b) m is smallest positive multiple of a and b

Notation: $\operatorname{lcm}(a, b)$

Theorem 2.3.3. *If $a, b \in \mathbb{Z}$ and nonzero, an LCM exists and is unique.*

Theorem 2.3.4. *Let $a, b \in \mathbb{Z}$ be nonzero, then*

$$ab = \operatorname{lcm}(a, b) \cdot \gcd(a, b)$$

Proof. Let $d = \gcd(a, b)$, then $a = dr$, $b = ds$ for some $r, s \in \mathbb{Z}$. Let $m = \frac{ab}{d}$. $d = ax + by$ for some $x, y \in \mathbb{Z}$. Let c be any common multiple of a and b.

$$\begin{aligned}
\frac{c}{m} &= \frac{c}{\frac{ab}{d}} \\
&= \frac{cd}{ab} \\
&= \frac{c(ax+by)}{ab} \\
&= \frac{cax}{ab} + \frac{cby}{ab} \\
&= \frac{c}{b}x + \frac{c}{a}y
\end{aligned}$$

Since $b \mid c$ and $a \mid c$

$$\begin{aligned}
&\in \mathbb{Z} \\
&\Rightarrow m \mid c \\
&\Rightarrow m \leq |c|
\end{aligned}$$

Then $m = \operatorname{lcm}(a, b)$ □

Corollary 2.3.6. *If $a, b \in \mathbb{Z}$ are nonzero and $m = \operatorname{lcm}(a, b)$ then m devides all common multiple of a and b.*

Theorem 2.3.5. *If $a, b \in \mathbb{N}$ then $\operatorname{lcm}(a, b) = ab$ iff $\gcd(a, b) = 1$*

2.5 Diophantine Equations

Goal. Study solution to $ax + by = c$, $a, b, c \in \mathbb{Z}$

Theorem 2.5.6. *Let $ax + by = c$ be given with a, b, c be fixed. Then there exists a solution for x and y precisely iff $\gcd(a, b) \mid c$. When a solution $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ exists then all relations are given by*

$$(x, y) = \left(x_0 + \left(\frac{b}{a}\right) t, y_0 - \left(\frac{a}{d}\right) t\right), t \in \mathbb{Z}$$

Proof. Recall $\{ax + by \mid x, y \in \mathbb{Z}\} = \mathbb{Z}d$ where $d = \gcd(a, b)$. So a solution $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ exists iff $d \mid c$. Assume the solution exists and (x, y) is any other solution.

$$\begin{aligned}
ax + by &= c \\
ax_0 + by_0 &= c \\
a(x - x_0) + b(y - y_0) &= 0 \\
a(x - x_0) &= -b(y - y_0) \\
\frac{a}{d}(x - x_0) &= -\frac{b}{d}(y - y_0) \\
\gcd\left(\frac{a}{d}, \frac{b}{d}\right) &= 1 \\
\frac{b}{a} &\mid \left(\frac{a}{d}(x - x_0)\right) \\
\Rightarrow \frac{b}{a} &\mid x - x_0
\end{aligned}$$

We get $x - x_0 = t\left(\frac{b}{a}\right)$, $t \in \mathbb{Z}$, $x = x_0 + t\left(\frac{b}{a}\right)$, $t \in \mathbb{Z}$. □

Theorem 2.5.7. *For $ax + by = c$, where a, b, c are fixed, not all 0, then a solution exists iff $d = \gcd(a, b) \mid c$. If (x_0, y_0) is a solution for (x, y), then all solution are*

$$(x, y) = \left(x_0 + \frac{bt}{d},\ y_0 + \frac{at}{d}\right)$$

Proof. When $d \mid c$. Assume (x_0, y_0) is one solution and (x, y) are other.

$$\begin{aligned} ax_0 + by_0 &= c \\ ax + by &= c \\ a(x - x_0) + b(y - y_0) &= 0 \\ a(x_0 - x) &= b(y - y_0) \\ \frac{a}{d}(x_0 - x) &= \frac{b}{d}(y - y_0) \end{aligned}$$

Since $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, given

$$\begin{aligned} \frac{b}{a} &\mid \left(\frac{a}{d}\right)(x - x_0) \\ \frac{b}{a} &\mid (x - x_0) \\ x - x_0 &= t \cdot \frac{b}{a} && (t \in \mathbb{Z}) \\ x &= x_0 + t \cdot \frac{b}{a} \\ \frac{a}{d}\left(t \cdot \frac{b}{a}\right) &= \frac{b}{a}(y_0 - y) \\ \frac{at}{d} &= y_0 - y \\ y &= y_0 - \frac{at}{d} \end{aligned}$$

Follows that

$$\begin{aligned} a(x_0 + \frac{bt}{d}) + b(y_0 - \frac{at}{d}) &= c \\ ax_0 + by_0 + \frac{abt}{d} - \frac{bat}{d} &= c \\ ax_0 + by_0 &= c \end{aligned}$$

□

Chapter 3

Primes

3.1 Fundamental Theorem of Arithmetic

Definition 3.1.1. *$P \in \mathbb{N}$ is prime if*

1. $P > 1$
2. *If $d \in \mathbb{N}$ with $d \mid P$ then $d = 1, P$*

Definition 3.1.2. *If $P \in \mathbb{N}$ is prime, $a, b \in \mathbb{Z}$ with $P \mid ab$ then $P \mid a$ or $P \mid b$.*

Theorem 3.1.1. *If $m \in \mathbb{N}$, $m \geq 2$ then m is a product of primes.*

$$m = P_1 P_2 \dots P_t$$

And this is unique up to order of factors.

Lemma 3.1.1. *If $P \in \mathbb{N}$ is prime, $a_1, \dots, a_m \in \mathbb{N}$ with $P \mid a_1, \dots, a_m$ when $P \mid a_i$ for some i.*

Proof. Induct on m

Base case. $m = 2$. True from definition.

Inductive step. Let result be true for $m = k$. Suppose

$$P \mid a_1, a_2, \dots, a_{k+1}$$

, then

$$P \mid (a_1, a_2, \dots, a_k)a_{k+1}$$
$$P \mid a_1, a_2, \dots, a_k \vee P \mid a_{k+1}$$
$$\exists i.\ 1 \leq i \leq k \rightarrow P \mid a_i \vee P \mid a_{k+1}$$

□

Theorem 3.1.2. *Let $m \in \mathbb{N}$, $m \geq 2$. Then $m = P_1 P_2 \dots P_t$ where each P_i is prime, and this is unique up to the order of factors.*

Proof. Let $T = \{n \in \mathbb{N} \mid n \geq 2$ and n is not a product of prime$\}$. To show that T is empty. Suppose not. Select the $a \in T$ smallest element. Then a cannot be prime or $a = P_1$, $P_1 = a$. Then $a = bc$, $b, c > 1$.

$$b > 1 \rightarrow c < a$$
$$c > 1 \rightarrow b < a$$
$$\Rightarrow b, c \notin T$$
$$b = P_1 P_2 \dots P_t,\ c = Q_1 Q_2 \dots Q_s \text{ where } P_i, Q_j \text{ are prime}$$
$$\Rightarrow a \notin T$$
$$\perp$$

Uniqueness Suppose

$$m = P_1P_2 \dots P_t = Q_1Q_2 \dots Q_s$$

where P_i, Q_j are all prime.

Base case. Result is true for $m = 2$

Inductive step. Assume it's true for all integers less than m, then

$$\begin{aligned} P_1 \mid m &\Rightarrow P_1 \mid Q_1 \dots Q_s = m \\ &\Rightarrow \exists j.\ P_1 \mid Q_j \end{aligned}$$

since Q_j is prime

$$\begin{aligned} &\Rightarrow P_1 = Q_j \\ m &= P_1P_2 \dots P_t = P_1Q_1 \dots Q_s \\ &\Rightarrow P_2 \dots P_t = Q_2 \dots Q_s < m \end{aligned}$$

By induction $t - 1 = s - 1$ and $P_i = Q_i$ for $2 \leq i \leq t$ after relabeling

□

Corollary 3.1.1. *If $m \in \mathbb{N}$, $m > 1$, then $m = P_1^{k_1} \dots P_t^{k_t}$ where $P_1, \dots, P_t$ are distinct primes, $k_j \geq 1$.*

Ex 3.1.1. $96 = 2 \cdot 48 = 2^2 \cdot 24 = 2^3 \cdot 12 = 2^4 \cdot 6 = 2^5 \cdot 3$

Theorem 3.1.3 (Pythagorean's)**.** $\sqrt{2} \notin \mathbb{Q}$

Proof. Suppose $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$. We can assume $\gcd(a, b) = 1$. Then

$$\begin{gathered} b\sqrt{2} = a \\ 2b^2 = a^2 \\ 2 \mid a^2 \Rightarrow 2 \mid a \cdot a \Rightarrow 2 \mid a \\ \exists c \in \mathbb{Z}.\ a = 2c \\ 2b^2 = 4c^2 \\ b^2 = 2c^2 \\ 2 \mid b^2 \Rightarrow 2 \mid b \\ \Rightarrow \gcd(a, b) \neq 1 \\ \perp \end{gathered}$$

□

Theorem 3.1.4. *Let $a, b \in \mathbb{N}$ with $\gcd(a, b) = 1$ then the sequence $\{a, a + b, a + 2b, \dots\}$ contains infinitely many primes.*

Definition 3.1.3 (Greatest Integer Function)**.** *If $x \in \mathbb{R}$, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x.*

Theorem 3.1.5 (Mill's Constant)**.** $\exists A > 0.$ *s.t.* $\lfloor x^{n^3} \rfloor$ *is a prime for all n*

Proof. There is u_a

$$f = a_u x^u + a_{u-1} x^{u-1} + \dots + a_0 \text{ where } u \geq 1$$

and $a_i \in \mathbb{Z}$ s.t. $f(k)$ is a prime for all $k \in \mathbb{N}$ □

Chapter 4

The Theory of Congruences

4.2 Congruences

Definition 4.2.1 (Congruence)**.** *$a, b \in \mathbb{Z}$ are congrent modulo n for $m \in \mathbb{N}$ if $n \mid b - a$. Written as*

$$a \equiv b \pmod{n}$$

By divisibility,

$$\begin{aligned} a = qn + r \quad 0 \leq r < u &\iff a \equiv r \pmod{n} \\ a \equiv r \pmod{n} &\iff r \in \{0, 1, \ldots, n-1\} \end{aligned}$$

Definition 4.2.2 (Complete Set of Residues)**.** *$a_1, a_2, \ldots, a_n$ is a complete set of residues modulo n if they are congruent to $0, 1, 2, \ldots, n-1$ in some order.*

Theorem 4.2.1. *Let $n > 1, a, b, c, d \in \mathbb{Z}$. Then*

(a) $a \equiv a \pmod{n}$

(b) $a \equiv b \pmod{n}$ *implies*

$$b \equiv a \pmod{n}$$

(c) $a \equiv b \pmod{n}$ *and* $b \equiv a \pmod{n}$ *implies*

$$a \equiv c \pmod{n}$$

(d) $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$ *implies*

$$ac \equiv bd \pmod{n} \textit{ and } a + b \equiv c + d \pmod{n}$$

(e) $b \equiv c \pmod{n}$ *implies*

$$ab \equiv ac \pmod{n}$$

(f) $a \equiv b \pmod{n}$ *and* $k \geq 1$ *implies*

$$a^k \equiv b^k \pmod{n}$$

Theorem 4.2.2. *$a, b, c \in \mathbb{Z}$, $n \in \mathbb{N}$. If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$*

Proof.

$$\begin{aligned} & ca \equiv cb \pmod{n} \\ \Rightarrow \quad & n \mid cb - ca \\ \Rightarrow \quad & n \mid c(b - a) \\ \Rightarrow \quad & n \mid b - a \\ \Rightarrow \quad & a \equiv b \pmod{n} \end{aligned}$$

□

Corollary 4.2.1. *If P is prime and $P \nmid n$, $n \in \mathbb{N}$, then $pa \equiv pb \pmod{n} \Rightarrow a \equiv b \pmod{n}$.*

Theorem 4.2.3. *Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $ca \equiv cb \pmod{n}$ then $a \equiv b \left(\operatorname{mod} \frac{n}{d}\right)$ where $d = \gcd c, n$*

Proof.

$$\begin{aligned} & ca \equiv cb \pmod{n} \\ \Rightarrow \quad & n \mid c(b - a) \\ & n = \left(\frac{n}{d}\right) d, \quad c = \left(\frac{c}{d}\right) d \\ \Rightarrow \quad & \frac{n}{d} \mid \frac{c}{d}(b - a) \\ \Rightarrow \quad & \left(\frac{c}{d}\right) a \equiv \left(\frac{c}{d}\right) b \left(\operatorname{mod} \left(\frac{n}{d}\right)\right) \end{aligned}$$

But $\gcd\left(\frac{c}{d}, \frac{n}{d}\right) = 1$

$$\Rightarrow \quad a \equiv b \left(\operatorname{mod} \frac{n}{d}\right)$$

□

4.3 Binary and Decimal Representations of $\mathbb{N}$

Theorem 4.3.1. *Let $b > 1$, $N \in \mathbb{N}$, then we can write*

$$N = a_m b^m + \cdots + a_1 b + a_0$$

where $0 \leq a_i < b$ and $a_m \neq 0$. Also, this representation is unique.

4.4 Linear congruences

Theorem 4.4.1 (Chinese Remainder Theorem)**.** *If $m_1, \ldots, m_r \in \mathbb{N}$ with $\gcd(m_i, m_j) = 1$ if $i \neq j$. Then the system*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a unique solution modulo $N = n_1 n_2 \ldots n_r$

Proof. Let $N_i = \frac{N}{m_i} = \frac{n_1 n_2 \dots n_r}{n_i}$. The equation $N_i x \equiv 1 \pmod{n_i}$ has a solution, x_i. Now

$$N_i x_i \equiv 1 \pmod{n_i}$$
$$N_i x_i \equiv 0 \pmod{n_j} \qquad \text{(if j} \neq \text{i since } n_j \mid N_i\text{)}$$

Let $\mathbb{X} = a_1 N_1 x_1 + \cdots + a_r N_r x_r$. then

$$\mathbb{X} \equiv a_1 1 + a_2 0 + \dots a_r 0 \pmod{n_1}$$
$$\mathbb{X} \equiv a_1 \pmod{n_1}$$

Similarly, $\mathbb{X} \equiv a_2 \pmod{n_2}$

$$\mathbb{X} \equiv a_i \pmod{n_i},\ i = 1, 2, \dots, r$$

we have a solution to system, $\mathbb{X}$. Let $\mathbb{Y}$ be any other solution,

$$\mathbb{Y} \equiv \mathbb{X} \equiv a_i \pmod{n_i}$$
$$n_1 \mid \mathbb{Y} - \mathbb{X}$$

But $\gcd(n_i, n_j) = 1$ if $i \neq j$

$$N \mid \mathbb{Y} - \mathbb{Z}$$

If $Z \equiv \mathbb{X} \pmod{N}$

$$Z \equiv \mathbb{X} \pmod{n_i}$$
$$Z \equiv \mathbb{X} \equiv a_i \pmod{n_i}$$

Note that for all solutions,

$$x = \mathbb{X} + kN, \quad k \in \mathbb{Z}$$

$\square$

Chapter 5

Fermats's Theorem

5.2 Fermat's Little Theorem and Pseudoprimes

Theorem 5.2.1 (Fermat's Theorem)**.** *Let p be a prime and $a \in \mathbb{Z}$. Then $a^{p-1} \equiv 1 \pmod p$.*

Corollary 5.2.1. *If p is a prime, then $a^p \equiv a \pmod p$ for any integer a.*

Theorem 5.2.2. *If n is an odd pseudoprime, then $M_n = 2^n - 1$ is a larger one.*

5.3 Wilson's Theorem

Theorem 5.3.1. *Let p be an odd prime. The equation $x^2 \equiv -1 \pmod p$ has a solution iff $p \equiv 1 \pmod 4$.*

Proof. Assume $p = 4k+1$, $k \geq 1$.

$$\begin{aligned}
(p-1)! &\equiv -1 \pmod p \\
(p-1)! &= [1,2,3,\dots,2k][(2k+1)\dots(p-1)] \\
p-2k &= (4k+1)-2k \\
&= 2k+1 \\
(p-1)! &= [1,2,3,\dots,2k][(p-2k)\dots(p-1)] \\
&\equiv (2k)![(p-2k)\dots(p-1)] && \text{(mod } p\text{)} \\
&\equiv (2k)!(-1)^{2k}(2k)! && \text{(mod } p\text{)} \\
&\equiv [(2k)!]^2 && \text{(mod } p\text{)}
\end{aligned}$$

Conversely, assume $x^2 \equiv -1$ has a solution. Assume $a^2 \equiv -1 \pmod p$, $a \in \mathbb{Z}$ and $p \nmid a$. By F.L.T,

$$\begin{aligned}
a^{p-1} &\equiv 1 \pmod p \\
a^{p-1} &= (a^2)^{\frac{p-1}{2}} \\
&\equiv (-1)^{\frac{p-1}{2}} && \text{(mod } p\text{)} \\
&\equiv 1 && \text{(mod } p\text{, by F.L.T.)} \\
(-1)^{\frac{p-1}{2}} &= \pm 1 \\
-1 &\Rightarrow p \mid 2, \quad \perp \\
(-1)^{\frac{p-1}{2}} &= 1 \\
\frac{p-1}{2} &= 2k \\
p &= 4k+1
\end{aligned}$$

□

Chapter 6

Number Theoretic Functions

Definition 6.0.1 (Convolution). *Let $f, g : \mathbb{N} \to \mathbb{Z}$, The convolution of f and g is*

$$\begin{aligned} f * g &: \mathbb{N} \longrightarrow \mathbb{Z} \\ f * g &= a \longmapsto \sum_{d|a} f(d) g\left(\frac{a}{d}\right) \end{aligned}$$

Definition 6.0.2.

$$\begin{aligned} f &: \mathbb{N} \longrightarrow \mathbb{R} \\ I(u) &= u \\ \lambda(u) &= 1 \\ \epsilon(u) &= \begin{cases} 1 & u = 1 \\ 0 & u > 1 \end{cases} \\ \tau(u) &= \text{\# of divisors of } u \\ \sigma(u) &= \sum_{d|u} d \\ \mu(u) &: \mathbb{N} \longrightarrow \mathbb{R} \\ &= \begin{cases} (-1)^r & u = P_1 P_2 \dots P_r \text{ where } P_1, \dots, P_r \text{ are distinct primes} \\ 0 & otherwise \end{cases} \end{aligned}$$

Definition 6.0.3. *$f : \mathbb{N} \to \mathbb{R}$ is multiplicative if $f(ab) = f(a)f(b)$ where $\gcd(a, b) = 1$.*

Lemma 6.0.1. *If $f : \mathbb{N} \to \mathbb{R}$ then $f * \epsilon = f = \epsilon * f$*

Lemma 6.0.2. *If $f, g : \mathbb{N} \to \mathbb{R}$ then $f * g = f = g * f$*

Lemma 6.0.3. *μ is multiplicative.*

Theorem 6.0.1. *Let $f, g, h : \mathbb{N} \to \mathbb{R}$, then*

- $f * g = g * g$
- $\epsilon * f = f * \epsilon = f$
- $f * (g + h) = f * g + g * h$
- $(f * g) * h = f * (g * h)$
- $(f * \sigma)(u) = \sum_{d|u} f(d) = F(u)$

Theorem 6.0.2. *Let $f, g : \mathbb{N} \to \mathbb{R}$ be multiplicative. Then $f * g$ is multiplicative.*

Ex 6.0.1. *Show that $\mu * \tau = \lambda$*

Proof. Because μ, τ are multiplicative, we have $\mu * \tau$ is multiplicative. And multiplicative function is determinied by value at p^k where p is prime and $k \geq 0$.

$$\begin{aligned}
\lambda(p^k) &= 1 \\
(\mu * \tau)(p^k) &= \sum_{i=0}^{k} \mu(p^i)\tau(p^{k-i}) \\
&= \mu(1)\tau(p^k) + \mu(p)\tau(p^{k-1}) + 0 + \cdots + 0 \\
&= 1(k+1) + (-1)k \\
&= 1
\end{aligned}$$

□

Chapter 7

Euler's Generalization of Fermat's Theorem

7.4 Properties of Phi Function

Theorem 7.4.1. *If* $m \in \mathbb{N}$ *then* $n = \sum_{d|n} \phi(d)$

Proof. (1) Let $S_d = \{a \mid 1 \leq a \leq n, \gcd(a,n) = d\}$, then $\{1, 2, \ldots, n\} = \bigcup_{d|u} S_d$, which is a disjoint union.

$$
\begin{aligned}
|n| &= \sum_{d|u} |S_d| \\
a \in S_d &\Longrightarrow d \mid a,\ a = dl \\
\gcd(a,n) = d &\iff \gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1 \\
&\iff \gcd\left(l, \frac{n}{d}\right) = 1 \\
|S_d| &= \phi\left(\frac{n}{d}\right) \\
n &= \sum_{d|n} |S_d| \\
&= \sum_{d|n} \phi\left(\frac{n}{d}\right) \\
&= \sum_{d|n} \phi(d)
\end{aligned}
$$

□

Proof. (2)

$$\sum_{d|u} \phi(d) = \sum_{d|u} \phi(d)\lambda\left(\frac{u}{d}\right)$$
$$= (\phi * \lambda)(u)$$

Both are multiplicative. Suppose to show that $(\phi * \lambda)(p^k) = p^k$, where p is prime and $k \geq 0$.

- $k = 0 \quad (\phi * \lambda)(1) = \phi(1)\lambda(1) = 1$
- $k \geq 1$

$$\begin{aligned}(\phi * \lambda)(p^k) &= \sum_{i=0}^{k} \phi(p^i)\lambda(p^{k-i}) \\ &= 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) \\ &= p^k\end{aligned}$$

□

Theorem 7.4.2.

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

where $\Phi_d(x)$ is a monic polynomial with coefficients in $\mathbb{Z}$ that does not factor over $\mathbb{Q}$ and $\deg \Phi_d(x) = \phi(d)$.

Chapter 8

Primitive Roots and Indices

8.1 The Order of an integer mod n

Definition 8.1.1 (Order). *If* $\gcd(a, n) = 1$ *order of* $\mod n$ *is the smallest* $k \geq 1$ *s.t.* $a^k \equiv 1 \pmod{n}$

Theorem 8.1.1. *Order of a devisor of* $\phi(n)$*.*

Theorem 8.1.2. *If* $d \mid \phi(p) = p - 1$ *and* $x^d - 1 \equiv 0 \pmod{p}$*, there's exactly* d *incongruent.*

Theorem 8.1.3 (Lagrange). *Let* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *be a polynomial with* $a_n \not\equiv 0 \pmod{p}$ *where* p *is a prime,* $a_i \in \mathbb{Z}$*. Then the congruence equation* $f(x) \equiv 0 \pmod{p}$ *has at most* n *incongruent solutions.*

Proof. If $n = 1$ we have $a_1 x + a_0 \equiv 0 \pmod{p}$, then $g(a, p) = 1$, implies there is a unique solution mod p. Now assume the result is true for $n - 1$ and $a \in \mathbb{Z}$ is one solution of $f(x) \equiv 0 \pmod{p}$. Divide $f(x)$ by $x - a$

$$\begin{aligned} f(x) &= (x - a)q(x) + r, r \in \mathbb{Z} \\ f(a) &\equiv 0 \pmod{p} \\ r &\equiv 0 \pmod{p} \end{aligned}$$

If c is any solution with $c \not\equiv a \pmod{p}$

$$\begin{aligned} 0 &\equiv f(c) \pmod{p} \\ &\equiv (c - a)q(c) + r \pmod{p} \\ &\equiv (c - a)q(c) \pmod{p} \end{aligned}$$

Since $gcd(p, c - a) = 1$

$$\begin{aligned} q(c) &\equiv 0 \pmod{p} \\ q(x) &= a_n x^{n-1} + \text{ lower degree} \end{aligned}$$

By induction

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

has at most $n - 1$ incongruent solutions mod p, then the equation has at most n incongruent solutions mod p.

□

Lemma 8.1.1. *Let $f(x), g(x)$ be polynomials with integers coefficients. If a is a solution to $f(x)g(x) \equiv 0 \pmod p$, then either $f(a) \equiv 0 \pmod p$ or $g(a) \equiv 0 \pmod p$.*

Proof.

$$\begin{aligned} & f(a)g(a) \equiv 0 \pmod p \\ \Rightarrow\ & p \mid f(a)g(a) \\ \Rightarrow\ & p \mid f(a) \vee p \mid g(a) \\ \Rightarrow\ & f(a) \equiv 0 \pmod p \vee g(a) \equiv 0 \pmod p \end{aligned}$$

□

Corollary 8.1.1. *Assume p is prime and $d \mid \phi(p) = p - 1$, then $x^\alpha - 1$ has mostly d incongruent solutions mod p.*

Theorem 8.1.4. *Assume p is a prime and $d \mid p - 1 = \phi(p)$, then there are precisely $\phi(d)$ incongruent modulo p integers of order d modulo p.*

Proof. Let $\alpha(d)$ be the number of noncongruent integers of order d mod p. Every integer $1, 2, \ldots, p - 1$ has an order mod p, entails that

$$p - 1 = \sum_{d \mid p-1}^{\alpha(d)}$$

By Lagrange's,

$$p - 1 = \sum_{d \mid p-1}^{\phi(d)}$$

If we have $\forall d \mid p - 1.\ \alpha(d) \leq \phi(d)$ we must have $\forall d \mid p - 1.\ \alpha(d) = \phi(d)$. □

Theorem 8.1.5. *If p is a prime, then $2p$ has a prime root.*

Proof. If p is an odd prime, $\phi(2p) = \phi(2)\phi(p) = p - 1$. We can find an odd primitive root of p. If a is prime root of p then $a + p$ is a prime root of p. Either a or $a + p$ is odd. We can assume a is odd, then $\gcd(a, 2p) = 1$. If a has order h mod $2p$, then

$$\begin{aligned} 2p &\mid a^h - 1 \\ p &\mid a^h - 1 \\ h &\geq p - 1 = \phi(2p) \end{aligned}$$

a is a prime root of $2p$

□

Lemma 8.1.2. *If p is an prime, $p \nmid a$, a odd, then*

$$({}^{a}/_{p}) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]}$$

Theorem 8.1.6. *If $p \neq q$ are odd primes, then*

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

Proof. Look at

$$S = \left\{(x, y) \in \mathbb{R} \mid 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}\right\}$$

with interger coordinates, $|S| = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$.

Claim. None of the points in S are on the line $y = \frac{q}{p}x$.

Proof. Suppose it does

$$\begin{aligned} m &= \frac{p}{q}u \\ pm &= qu \\ p \mid qu &\Rightarrow p \mid u \\ \text{But} \quad 1 \leq &u \leq \frac{p-1}{2} \\ &\perp \end{aligned}$$

□

Now let $S = T_1 \cup T_2$ where T_1 are points in S lower than the line $y = \frac{q}{p}x$ and T_2 are points in S above. Then

$$|T_1| = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right]$$

and

$$\begin{aligned} (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} &= (-1)^{|S|} \\ &= (-1)^{|T_1|+|T_2|} \\ &= (-1)^{|T_1|}(-1)^{|T_2|} \\ &= (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]}(-1)^{\sum_{l=1}^{\frac{q-1}{2}}\left[\frac{lp}{q}\right]} \\ &= ({}^{q}/{}_{p})({}^{p}/{}_{q}) \end{aligned}$$

□

Corollary 8.1.2. *Assume $p \neq q$ are odd primes. Then*

$$({}^{p}/{}_{q}) = ({}^{q}/{}_{p}) \textit{ if } \begin{cases} p \equiv 1 \pmod 4 \\ q \equiv 1 \pmod 4 \end{cases}$$

$$({}^{p}/{}_{q}) = -({}^{q}/{}_{p}) \textit{ if } p \equiv q \equiv 3 \pmod 4$$

Ex 8.1.1. *For what primes $P > 3$ is $({}^{3}/{}_{p}) = 1$?*

Answer. Suppose $P \equiv 1 \pmod 4$

$$({}^{3}/{}_{p}) = ({}^{p}/{}_{3}) = 1 \text{ if } p \equiv 1 \pmod 3$$

by C.R.T, need $P \equiv 1 \pmod 1$ 2. If $P \equiv 3 \pmod 4$, we have $({}^{3}/{}_{p}) = -({}^{p}/{}_{3})$, means $p \equiv 2 \pmod 3$. By C.R.T, $P \equiv 11 \equiv -1 \pmod{12}$, gives that

$$({}^{3}/{}_{p}) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{otherwise} \end{cases}$$

Ex 8.1.2. *Compute* $({}^{61}/{}_{79})$

Answer.

$$\begin{aligned} ({}^{61}/{}_{79}) &= ({}^{79}/{}_{61}) \\ &= ({}^{18}/{}_{61}) \\ &= ({}^{3^2 \cdot 2}/{}_{61}) \\ &= ({}^{3^2}/{}_{61})({}^{2}/{}_{61}) \\ &= -1 \end{aligned}$$