MAT315 Introduction to Number Theory

1 Division and Primes

1.1 Division

Definition: 1.1: Divisors

Let $n, d \in \mathbb{Z}$. We say d divides n if $\exists e \in \mathbb{Z}$ s.t. $n = de$.
Notation: $d|n$.

Theorem: 1.1: Division Algorithm

Let $a \in \mathbb{Z}$, $b \in \mathbb{N}$. There exists unique $q, r \in \mathbb{Z}$, where $a = qb + r$, $0 \leq r < b$.

Proof. Let $S = \{a - bq \geq 0 : q \in \mathbb{Z}\}$.
Note that if we let $q = -|a|$, $a - qb = a + |a|b \geq 0$, so $-|a| \in S$, $S \neq \emptyset$.
By well-ordering property, there exists a least element $r = a - bq$, s.t. $a = bq + r$, $r \geq 0$.
If $r \geq b$, then $0 \leq r - b = a - b(q + 1)$, r is not the least element in S, contradiction, thus $r < b$.

Uniqueness: Suppose $bq_1 + r_1 = bq_2 + r_2 = a$, then $r_1 - r_2 = b(q_2 - q_1)$.
Since $0 \leq r < b$, then $-b < r_1 - r_2 < b$. But it is a multiple of b, then $r_1 - r_2 = 0$, $r_1 = r_2$ and $q_1 = q_2$. □

Theorem: 1.2: Properties of Divisors

1. If $a|b$ and $b|c$, then $a|c$
2. If $a|b$ and $c|d$, then $ac|bd$
3. For all $x, y \in \mathbb{Z}$, if $d|a$ and $d|b$, then $d|ax + by$

Proof.
1. If $a|b$ and $b|c$, then by Definition 1.1, $\exists n, m \in \mathbb{Z}$ s.t. $b = na$ and $c = mb$, then $c = m(na) = (mn)a$, thus $a|c$.
2. If $a|b$ and $c|d$, then $\exists n, m \in \mathbb{Z}$ s.t. $b = na$ and $d = mc$, then $bd = (na)(mc) = (mn)(ac)$, thus $ac|bd$.
3. If $d|a$ and $d|b$, then $\exists n, m \in \mathbb{Z}$ s.t. $a = nd$ and $b = md$, then $ax + by = (nd)x + (md)y = d(nx + my)$, thus $d|(ax + by)$.

□

Definition: 1.2: Greatest Common Divisors

For $a, b \in \mathbb{Z}$, their greatest common divisor (GCD) is the natural number $\gcd(a, b)$ which is the largest common divisor of a, b. If $a = b = 0$, then $\gcd(a, b) = 1$.

Lemma: 1.1: Bezout's Lemma

Let $a, b \in \mathbb{N}$. The equation $ax + by = \gcd(a, b)$ has a solution.

Proof. Let $S = \{c \in \mathbb{N} : ax + by = c \text{ has a solution.}\}$. Obviously $a \in S$, $S \neq \emptyset$.
By well-ordering property, it has the least element s. We want to show that $s = \gcd(a, b)$.

1. Firstly, $s \geq \gcd(a, b)$, since $\gcd(a, b)|s$ by Theorem 1.2 (3).
2. Now we show that $s \leq \gcd(a, b)$
   Apply Theorem 1.1 to s, a. $a = qs + r$ with $0 \leq r < s$.
   $a = q(ax + by) + r$, which gives $a(1 - qx) + b(-y) = r$, is solvable by definition of s. Thus $r = 0$. $s|a$ and similarly $s|b$. Therefore $s \leq \gcd(a, b)$

Thus $s = \gcd(a, b)$. □

Theorem: 1.3:

Let $a, b, d \in \mathbb{N}$. If $d|a$ and $d|b$, then $d|\gcd(a, b)$.

Proof. Apply Lemma 1.1, $ax + by = \gcd(a, b)$ has a solution.
Then by Property 3 of Theorem 1.2, $d|\gcd(a, b)$. □

Definition: 1.3: Coprime

$a, b \in \mathbb{Z} \setminus \{0\}$ are coprime, if $\gcd(a, b) = 1$. *i.e.* $ax + by = 1$ has solutions.

Theorem: 1.4:

$ax + by = c$ is solvable if and only if $\gcd(a, b)|c$.

Proof. ($\Leftarrow$) If $c = k\gcd(a, b)$. By Lemma 1.1, $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = \gcd(a, b)$. Multiplying both sides by k, $a(kx) + b(ky) = k\text{gcd(a,b)} = c$

($\Rightarrow$) Solvable by property 3 of Theorem 1.2. □

Note: If we let $d = \gcd(a, b)$, $ax + by = dk$, $\frac{a}{d}x + \frac{b}{d}y = k$. $\frac{a}{d}$ and $\frac{b}{d}$ are coprime. Therefore, we can always assume that a, b are coprime.

Lemma: 1.2:

Let $a, b \in \mathbb{N}$ be coprime, $c \in \mathbb{N}$. If $a|bc$, then $a|c$.

Proof. If $a, b \in \mathbb{N}$ are coprime, by Lemma 1.1, $ax + by = 1$ has solutions.
Multiply both sides by c, $a(cx) + (bc)y = c$, has solutions. $a|a$ and $a|bc$, so $a|c$ by Theorem 1.4. □

Suppose a, b are coprime, and $(x_0, y_0), (x_1, y_1)$ are two pairs of solutions to $ax + by = c$.
$ax_0 + by_0 = c = ax_1 + by_1 \Rightarrow a(x_0 - x_1) = b(y_1 - y_0)$
Since a, b are coprime, $a|y_1 - y_0$, $b|x_0 - x_1$.
Let $t, s \in \mathbb{Z}$, $y_1 - y_0 = at$, $x_0 - x_1 = bs$.
Plug back into the equation, $abs = bat$, thus $s = t$. $x_1 = x_0 - bt$, $y_1 = y_0 + at$.
Given $ax_0 + bx_0 = c$, $ax_0 - abt + abt + by_0 = c$, and $a(x_0 - bt) + b(y_0 + at) = c$.

Theorem: 1.5: Linear Diophantine Equation Theorem

Let $a, b, c \in \mathbb{N}$, $d = \gcd(a, b)$, $x_0, y_0 \in \mathbb{Z}$ be solutions s.t. $ax_0 + by_0 = c$. Then all solutions to $ax + by = c$ are of the form $x = x_0 - \frac{b}{d}t$, $y = y_0 + \frac{a}{d}t$, $t \in \mathbb{Z}$.

Theorem: 1.6: Euclidean Algorithm

Let $a, b \in \mathbb{N}$. Apply division algorithm, $a = qb + r$, $0 \leq r < b$. Then $\gcd(a, b) = \gcd(b, r)$.

Proof. If $d = \gcd(a, b)$, $d|a$ and $d|b$, then $d|a - bq = r$
If $d = \gcd(b, r)$, $d|b$ and $d|r$, then $d|qb + r = a$. □

Example: $a = 450$, $b = 100$, $a = 4b + 50$. Let $a_1 = 100$, $b_1 = 50$, $a_1 = 2b_1 + 0$. Thus $\gcd(450, 100) = \gcd(100, 50) = \gcd(50, 0) = 50$

Example: $a = 315$, $b = 17$, $a = 18b + 9$.
Let $a_1 = 17$, $b_1 = 9$, $a_1 = 1b_1 + 8$.
Let $a_2 = 9$, $b_2 = 8$, $a_2 = 1b_2 + 1$.
Let $a_3 = 8$, $b_3 = 1$, $a_3 = 8b_3 + 0$.
Thus $\gcd(315, 17) = \gcd(17, 9) = \gcd(9, 8) = \gcd(8, 1) = 1$.

We can now iterate backwards to construct a solvable diophantine equation.

$$\begin{aligned}
1 &= 9 - 1 \cdot 8 \\
&= 9 - 1(17 - 9) = 2 \cdot 9 - 17 \\
&= 2 \cdot (315 - 18 \cdot 17) - 17 \\
&= 2 \cdot 315 + (-37)(17)
\end{aligned}$$

Thus $x = 2$, $y = -37$ is a solution to $ax + by = c$, where $a = 315$, $b = 17$, $c = \gcd(a, b) = 1$.

Theorem: 1.7: Euclidean Algorithm (Formally)

Let $a, b \in \mathbb{N}$, $a \geq b$. Define a sequence by repeated divisions

$$\begin{aligned}
a &= q_1 b + r_1, 0 \leq r_1 < b \\
b &= q_2 r_1 + r_1, \\
r_{n-3} &= q_{n-2} r_{n-2} + r_{n-1} \\
r_{n-2} &= q_{n-2} r_{n-1} + r_n \\
r_{n-1} &= q_n r_n + 0
\end{aligned}$$

Then $\gcd(a, b) = r_n$ and we can solve for x, y in $ax + by = r_n$ by $r_n = r_{n-2} - q_{n-1} r_{n-1} = r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2} r_{n-2})$.
This terminates in $\log_2(a, b)$.

1.2 Primes

Definition: 1.4: Prime Numbers

A number $p \in \mathbb{N}$, $p > 1$ is prime if its only divisors are 1 and itself.

Theorem: 1.8:

For a prime number p and any number a, $\gcd(a,p) = 1$ or p and $\gcd(a,p) = p \Leftrightarrow p|a$.

Corollary 1. *If $a, b \in \mathbb{Z}$ and $p|ab$, then $p|a$ or $p|b$.*

Proof. By Theorem 1.8, either $p|a$ or $\gcd(a,p) = 1$ and $p|b$. □

Corollary 2. *If $a_1, ..., a_n \in \mathbb{N}$, and $p|a_1 \cdots a_n$, then $p|a_i$ for some i.*

Proof. By induction on i and previous corollary. □

Theorem: 1.9: Fundamental Theorem of Arithmetics

For any $n \in \mathbb{Z}$, $n \neq 0$, there exists a factorization $n = \pm p_1^{k_1} \cdots p_r^{k_r}$ where p_j are distinct primes, $k_j \in \mathbb{N}$ and this is unique up to reordering of p_j.

Proof. Existence: (By strong induction)
Base: 1=1 and 2=2 work
Inductive step: Suppose the statment holds for 1...n, consider $n+1$
If $n+1$ is prime, then we are done. Otherwise, $\exists 1 < d < n+1$ s.t. $d|n+1$, then $n+1 = de$ for $1 < d, e \leq n$. By Induction, d, e factors, so $n+1$ factors.

Uniqueness: Observe that if p, q are prime and $p|q$, then $p = q$
Write $n = p_1^{k_1} \cdots p_r^{k_r} = q_1^{t_1} \cdots q_s^{t_s}$. By Corollary 2, since $q_1|n$, then $q_1|p_i$ for some i, and thus $q_1 = p_i$. By reordering, we can assume $p_1 = q_1$, and cancel out to get $p_1^{k_1-1} p_2^{k_2} \cdots p_r^{k_r} = q_1^{t_1-1} \cdots q_s^{t_s}$. Keep cancelling q_1, we will eventually have $p_1^{k_1-t_1} p_2^{k_2} \cdots p_r^{k_r} = q_2^{t_2} \cdots q_s^{t_s}$.
If $k_1 \neq t_1$, then $p_1|q_i$ for some other $2 \leq i \leq s$. Then q_i is not distinct from q_1, contradiction. Thus $k_1 = t_1$ and $p_2^{k_2} \cdots p_r^{k_r} = q_2^{t_2} \cdots q_s^{t_s}$.
Iterating this procedure, we get $r = s$, $k_i = t_i$, $p_i = q_i$. □

Theorem: 1.10: Properties of Prime Factorization

If $a = p_1^{k_1} \cdots p_r^{k_r}$ and $b = p_1^{t_1} \cdots p_r^{t_r}$. Then

1. $ab = p_1^{k_1+t_1} \cdots p_r^{k_r+t_r}$
2. $\frac{b}{a} = p_1^{k_1-t_1} \cdots p_r^{k_r-t_r}$ and $a|b$ if $k_i - t_i \geq 0$ for all i. The divisors of b are $d = p_1^{z_1} \cdots p_r^{z_r}$ for $0 \leq z_j \leq t_j$
3. $\gcd(a,b) = p_1^{\min(k_1,t_1)} \cdots p_r^{\min(k_r,t_r)}$

Note: $p_1^{a_1} \cdots p_r^{a_r} \in \mathbb{Z}$ if $a_j \geq 0$. Suppose $a_j < 0$ for some j, then $p_j^{a_j} \notin \mathbb{Z}$.

1.3 Counting Primes

Theorem: 1.11: Euclid

There are infinitely many primes

Proof. Let $p_1, ..., p_r$ be primes. Consider $N = p_1 \cdots p_r + 1 > 1$. It has a prime factor q.
If $p_j|N$, then $p_j|N - p_1 \cdots p_r = 1$. Contradiction. Thus $q \neq p_j$ for any j
Then $p_1, ..., p_r, p_{r+1} = q$ is a larger set of primes. □

Theorem: 1.12: Number of Primes

Let $\pi(x)$ be the number of primes $\leq x$. Then $\pi(x) \approx \frac{x}{\log x}$.

How do we estimate $\pi(x)$ and what is the distribution of primes? We can say that $p, p+1$ are not both prime if $p \geq 2$. And Bertrand postulate states that p_k and p_{k+1} can be far from each other, but for any natural number $n \in \mathbb{N}$, there is always a prime p s.t. $n \leq p \leq 2n$.

Lemma: 1.3: Upper Bound for $\pi(x)$

Let p_n denote the nth prime number, then $p_n \leq 2^{2^{n-1}}$.

Proof. Base: $p_1 = 2 \leq 2^{2^0} = 2$
Induction Step: Suppose $p_j \leq 2^{2^{j-1}}$ for $j \leq n$.
We know that there is a new prime q dividing $M = p_1 \cdot p_n + 1$ from Theorem 1.11. Then

$$\begin{aligned} p_{n+1} &\leq q \leq p_1 \cdots p_n + 1 \\ &\leq 2^{2^{1-1}} 2^{2^{2-1}} \cdots 2^{2^{n-1}} + 1 \\ &= 2^{\sum_{i=0}^{n-1} 2^i} + 1 \\ &= 2^{2^n - 1} + 1 \leq 2^{2^n} \end{aligned}$$

□

Definition: 1.5: Integer and Fraction Parts

For $x \in \mathbb{R}$, $\lfloor x \rfloor = n \in \mathbb{Z}$ when $n \leq x < n+1$ and $\{x\} = n - \lfloor x \rfloor$ is the fraction part.

Corollary 3. $\pi(x) \geq \lfloor \log_2 \log_2 x \rfloor + 1$

Proof. $\pi(x) = \#\text{primes} \leq x$. We want to (at least) count the primes with $2^{2^{n-1}} \leq x$ as from Lemma 1.3. Therefore, $n \leq \lfloor \log_2 \log_2 x \rfloor + 1$. □

Fact: If n is a composite number, it has non-trivial divisor $d \leq \sqrt{n}$. *i.e.* one of d, $\frac{n}{d} \leq \sqrt{n}$ for all $d|n$.

Principal of Inclusion-Exclusion: For A_1, A_2, A_3 finite sets, $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$.

Using the fact and principal of inclusion-exclusion, we can define a sum form of the number of primes $\leq x$:

$$\begin{aligned} \pi(x) &= \#n \leq x - \#n \leq x, 2|n - \#n \leq x, 3|n - \cdots - \#n \leq x, p|n \text{and} p \leq \sqrt{x} + \$n \leq x, b|n + \cdots \\ &= \lfloor x \rfloor - \sum_{p \leq \sqrt{x}} \left\lfloor \frac{x}{p} \right\rfloor + \sum_{p_1 < p_2 \leq \sqrt{x}} \left\lfloor \frac{x}{p_1 p_2} \right\rfloor - \cdots \end{aligned}$$

Then $\pi(x) - \pi(\sqrt{x}) + 1 = \sum_{d|P_{\leq \sqrt{x}}} N(d) \left\lfloor \frac{x}{d} \right\rfloor = x \sum_{d|P_{\leq \sqrt{x}}} \frac{N(d)}{d} - \sum_{d|P_{\leq \sqrt{x}}} \mu(d) \left\{ \frac{x}{d} \right\}$, where $P_{\leq \sqrt{x}}$ is the product of all primes $\leq \sqrt{x}$.

2 Congruence and Chinese Remainder Theorem

Consider $x^8 + 1 = 3y^3$. Can it be solved with $x, y \in \mathbb{Z}$?
We check if $x^8 + 1$ is divisible by 3. We consider $x^4 = 3k + r$. If $r = 0$, then $3 \not| x^8 + 1$. Similar for $r = 1$ or 2. $x^8 + 1 = 3m + 2$.
We want to find an efficient way of writing the modulo relation.

Definition: 2.1: Equivalence Relation

Given a set X, an equivalence relation on X is a relation $\sim$ s.t.

1. Reflexive: $x \sim x, \forall x \in X$
2. Symmetric: if $x \sim y$, then $y \sim x$
3. Transitive: if $x \sim y$ and $y \sim z$, then $x \sim z$

Definition: 2.2: Congruence

For $n \in \mathbb{N}$, we define an equivalence relation on $\mathbb{Z}$ by $a \sim b$ iff $n|(a - b)$. When $a \sim b$, we write $a \equiv b \mod n$

Proof. Reflexive: $n|0 = a - a$, so $a \sim a$
Symmtric: $n|a - b \Rightarrow n|b - a$, so $a \sim b \Rightarrow b \sim a$
Transitive: If $n|a - b$ and $n|b - c$, then $n|(a - b) + (b - c) = a - c$ □

Theorem: 2.1: Properties of Congruence

1. Addition is preserved: if $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then $a + b \equiv a' + b' \mod n$
2. Multiplication is preserved: if $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then $ab \equiv a'b' \mod n$

Proof. Addition: if $n|(a - a')$ and $n|(b - b')$, then $n|(a - a') + (b - b') = (a + b) - (a' + b')$, thus $a + b \equiv a' + b' \mod n$.
Multiplication: Note that $ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + b'(a - a')$, if $n|(a - a')$ and $n|(b - b')$, then $n|ab - a'b'$, so $ab \equiv a'b' \mod n$ □

Corollary 4. *If $f(x) \in \mathbb{Z}[x]$ (polynomial ring with integer coefficients) and $a, b \in \mathbb{Z}$, then $f(a) \equiv f(b) \mod n$*

Definition: 2.3: Equivalence Classes

The equivalence class of a point $x \in X$ is $[x] = \{y \in X : x \sim y\}$

Note: $[x] \cap [y] \neq \emptyset$ iff $x \sim y$ and $[x] = [y]$. We can write $X/\sim = \{[x_1], ..., [x_n], ...\}$
For congruence, there are n equivalence classes $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], ..., [n-1]\}$. Often, we drop the $[\cdot]$ bracket.

Example: $\mathbb{Z}/12\mathbb{Z} = \{0, 1, ..., 11\}$.
$3 + 9 \equiv 0 \mod 12$, $2(8) + 4 \equiv 8 \mod 12$, $3(7) \equiv 9 \mod 12$
$3(9) \equiv 3(-3) \equiv -9 \equiv 3 \mod 12$
However, we cannot divide, $\nexists x_0$ s.t. $6x_0 \equiv 1 \mod 12$.

Remark 1. For $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], ..., [n-1]\}$, define $[a] + [b] = [a + b]$, $[a][b] = [ab]$. The operations are well-defined as by Theorem 2.1.

Remark 2. So by induction, if $p(x) \in \mathbb{Z}[x]$, then $p([a]) = [p(a)]$ is well-defined. *i.e.* if we are studying polynomial equations $p(x) = 0$, the solutions in $\mathbb{Z}$ ($p(a) = 0$) give solutions modulo n ($[a]$).

Note: Similarly, we can define $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}/\sim$ as equivalence classes, where $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \cdots$. However, $f : \mathbb{Q} \to \mathbb{Z}$ s.t. $f\left(\frac{a}{b}\right) = a - b$ is not well defines, since $\frac{1}{2} = \frac{2}{4}$, but $f\left(\frac{1}{2}\right) = -1 \neq -2 = f\left(\frac{2}{4}\right)$.

We know that $[a] = [b]$ if and only if $a \equiv b \mod n$, but we don't know how to divide or if we can even divide.

Definition: 2.4: Division in Congruence Form

We can divide by $a \mod n$ if the equation $ax \equiv 1 \mod n$ has a solution. We call the solution a^{-1} or the multiplicative inverse of a modulo n. It has a solution if and only if $\gcd(a, n) = 1$.

Theorem: 2.2:

The equation $ax \equiv b \mod n$ has a solution if and only if $d = \gcd(a, n)|b$. If x_0 is a solution, then the distinct solutions modulo n are $x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, ..., x_0 + \frac{(d-1)n}{d}$.

Remark 3. $\gcd(a, n)|d$ is fine because $\gcd(m, qm + r) = \gcd(m, r)$ by Theorem 1.7, and $d|n$. So if $n|b - b'$, then $d|b \Leftrightarrow d|b'$, since $b = b' + nk$.

Proof. ($\Rightarrow$) Suppose $ax_0 \equiv b \mod n$ for some x_0. Then $n|ax_0 - b$, so there exists $y_0 \in \mathbb{Z}$ s.t. $ax_0 - b = ny_0$. Then $ax_0 + n(-y_0) = b$, $\gcd(a, n)|b$.

($\Leftarrow$) If $\gcd(a, n)|b$, then $\exists x_0, y_0 \in \mathbb{Z}$ s.t. $ax_0 + ny_0 = b$ by Lemma 1.1, so $n|ax_0 - b$, or equivalently, $ax_0 \equiv b \mod n$.

Now, we show that the solutions modulo n to $ax \equiv b \mod n$ are exactly the congruence of the x s.t. $ax + ny = b$. By Theorem 1.5, the solutions are of the form $x_0 + \frac{nd}{t}$ for $t \in \mathbb{Z}$.

Then we show that $x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, ..., x_0 + \frac{(d-1)n}{d}$ are distinct and a complete list of solutions.
Distinct: suppose $x_0 + j\frac{n}{d} \equiv x_0 + \frac{in}{d} \mod n$, then $n|\frac{(i-j)n}{d}$, but $0 \leq i - j \leq d - 1$, $\frac{(i-j)d}{n} < n$, so $i - j = 0$
Complete, for any $x = x_0 + \frac{n}{d}t$, apply Division algorithm for t and d, we get $x = x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r) = x_0 + \frac{nr}{d} + qn$ for $0 \leq r < d$. □

Corollary 5. *If* $\gcd(a, n)|b$, *then* $ax \equiv b \mod n$ *has* $d = \gcd(a, n)$ *distinct solutions modulo* n. *If* $d = 1$, *then there's a unique solution.*

Example: $10x \equiv 11 \mod 9 \equiv 2 \mod 9$, so $x \equiv 2 \mod 9$.

Example: Solve for x s.t. $7x \equiv 13 \mod 15$

Proof. since $a = 7, n = 15, b = 13$ are coprime, there is a unique solution.
We consider $7x + 15y = 13$. We can firstly solve $7x + 15y = 1$ using Theorem 1.7.
$15 = 2 \cdot 7 + 1$, and thus $x = -2, y = 1$. Multiply both sides by 13, and we get $x = -26, y = 13$ is a solution to $7x + 15y = 13$
So the solution to $7x \equiv 13 \mod 15$ is $x \equiv -26 \equiv 4 \mod 15$. □

Example: Solve for x s.t. $10x \equiv 6 \mod 16$

Proof. Apply Theorem 1.7,

$$\begin{aligned} &10x + 16y = 6 \\ &\qquad 16 = 1 \cdot 10 + 6 \\ &\qquad 10 = 1 \cdot 6 + 4 \\ &\qquad 6 = 1 \cdot 4 + 2 \\ &\qquad 4 = 2 \cdot 2 + 0 \end{aligned}$$

Then back substitute, $2 = 6 - 1(4) = 6 - 1(10 - 1(6)) = 6(2) + 10(-1) = 2(16 - 1(10)) + 10(-1) = 10(-3) + 16(2)$
Thus $x = -3$, $y = 2$ is a solution to $10x + 16y = 2$
Multiply both sides by 3, we get $x = -9$, $y = 6$ is a solution to $10x + 16y = 6$
Thus the solutions are $7 \equiv -9 \mod 16$ and $15 \equiv -9 + \frac{16}{2} \mod 16$. ☐

Theorem: 2.3: Independence Condition

If $n = p_1^{k_1} \cdots p_r^{k_r}$, then for $a \in \mathbb{Z}$, $a \equiv 0 \mod n$ if and only if $a \equiv 0 \mod p_j^{k_j}$ for all $1 \leq j \leq r$.

Proof. ($\Rightarrow$) $n = p_j^{k_j}(p_1^{k_1} \cdots p_{j-1}^{k_{j-1}} p_{j+1}^{k_{j+1}} \cdots p_r^{k_r}) | a$. Thus $p_j^{k_j} | a$.
($\Leftarrow$) by applying the corollary of Theorem 1.8. p_j^ks are coprime. ☐

Theorem: 2.4: Chinese Remainder Theorem

Let $m, n \geq 1$ be coprime integers. Then the map

$$\varphi : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \text{ s.t. } \varphi(a \mod (nm)) = (a \mod n, b \mod m)$$

is a bijection. Moreover, $\varphi(x + y) = \varphi(x) + \varphi(xy)$, $\varphi(1) = 1$, $\varphi(xy) = \varphi(x)\varphi(y)$.

Remark 4. If $p(x) \in \mathbb{Z}[x]$, then $\varphi(p(x) \mod mn) = (p(x) \mod n, p(x) \mod m)$.

Remark 5. For $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} = \{([a]_n, [b]_m) : a = 0, ..., n-1, b = 0, ..., m-1\}$,
$([a]_n, [b]_m) + ([c]_n, [d]_m) = ([a + c]_n, [b + d]_m)$, where $(0, 0)$ is the additive identity.
$([a]_n, [b]_m) \cdot ([c]_n, [d]_m) = ([ac]_n, [bd]_m)$, where $(1, 1)$ is the multiplicative identity.

Proof. Well defined: if $a \equiv a' \mod nm$, then $nm | a - a'$,since nm coprime, by Theorem 1.8, $n | a - a'$, $a \equiv a' \mod n$ and $m | a - a'$, $a \equiv a' \mod m$.

Injective: If $a \equiv b \mod n$ and $a \equiv b \mod m$, *i.e.* $\varphi(a) = \varphi(b)$, since n, m are coprime, $n | a - b$ and $m | a - b$ $\Rightarrow nm | a - b$, thus $a \equiv b \mod nm$.

Surjective: For any $b \mod n$, $c \mod m$, we want to find $a \mod nm$ s.t. $a \equiv b \mod n$ and $a \equiv c \mod m$.
By Lemma 1.1, there are $x_0, y_0 \in \mathbb{Z}$ s.t. $nx_0 + my_0 = 1$
Construct $a = b(my_0) + c(nx_0)$, then $a \equiv b(my_0) \mod n$ and $a \equiv c(nx_0) \mod m = c \mod m$.

$$\begin{aligned} \varphi(x + y) &= ((x + y) \mod n, (x + y) \mod m) = (x \mod n + y \mod n, x \mod m + y \mod m) \\ &= (x \mod n, x \mod m) + (y \mod n, y \mod m) = \varphi(x) + \varphi(y) \end{aligned}$$

$$\begin{aligned}\varphi(xy) &= (xy \mod n, xy \mod m) = (x \mod ny \mod n, x \mod my \mod m)\\ &= (x \mod n, x \mod m)\,(y \mod n, y \mod m) = \varphi(x)\varphi(y)\end{aligned}$$

$\varphi(1) = (1 \mod n, 1 \mod m) = (1, 1)$ □

Example: Solve for $x^2 \equiv 2 \mod 14$.

Proof. By Theorem 2.4, it is enough to solve for $x^2 \equiv 2 \mod 2$ and $x^2 \equiv 2 \mod 7$,
and then we can construct solutions $\mod 14$.
The first one gives $x \equiv 0 \mod 2$. The second one gives $x^2 \equiv 2 \equiv 9 \mod 7$, $x \equiv \pm 3 \mod 7$.
So we have the left side of the correspondance, $\{(0, 3), (0, -3)\}$.
This means we need to solve $\begin{cases} x \equiv 0 \mod 2 \\ x \equiv 3 \mod 7 \end{cases}$, and $\begin{cases} y \equiv 0 \mod 2 \\ y \equiv -3 \mod 7 \end{cases}$
We want $z \mod nm$ that maps to $(a \mod n, b \mod m)$.
Apply a similar idea in proving the surjection. We use $z = a(my) + b(nx)$ s.t. $nx + my = 1$, then use the Euclidean algorithm.
To solve the first one, take $z = 0(7y) + 3(2x)$, where $7y + 2x = 1$. Then $x = -3, y = 1$, $z = -18 \equiv 10 \mod 14$.
For the second one, $z = 0(7y) - 3(2x)$ where $7y + (-2)x = 1$, $x = 3, y = 1$, $z = 18 \equiv 4 \mod 14$. □

Example: Solve for $6x \equiv 15 \mod 385$.

Proof. Note $385 = 5 \cdot 7 \cdot 11$.
So we solve for $6x \equiv 15 \equiv 0 \mod 5$, $6x \equiv 15 \equiv 1 \mod 7$ and $6x \equiv 15 \equiv 4 \mod 11$.

Consider the first 2 congruence equations:
We solve for $5x + 7y = 1$ and get $x = 3$, $y = -2$, so we have $a = 0(7y) + 1(5x) \equiv 15 \mod 35$.
Then combine this with $6x \equiv 4 \mod 11$,
We solve for $11x + 35y = 1$: $35 = 3 \cdot 11 + 2$, $11 = 5 \cdot 2 + 1$, so $1 = 11 - 5(2) = 11 - 5(35 - 3(11)) = (-5)(35) + 16(11)$. *i.e.* $x = 16$, $y = -5$. Then we have $b = 4(35y) + 15(11x) = 1940 \equiv 15 \mod 385$.
Thus $6x \equiv 1940 \mod 385$, $x \equiv 195 \mod 385$. □

Example: (General Problem) You are the general of an army with less than 1000 troops. After the abttle, you have n troops left.
When you ask them to get into groups of 7, there are 5 leftover.
When you ask them to get into groups of 11, there are 9 leftover.
When you ask them to get into groups of 13, there are 2 leftover.
What is n?

Proof. We have three congruence equations:

1. $n \equiv 5 \mod 7$
2. $n \equiv 9 \mod 11$
3. $n \equiv 2 \mod 13$

Note that $1001 = 7 \cdot 11 \cdot 13$. And $n \equiv a \mod 1001$ has a unique value.
Use the first 2 equations. We solve for $7x + 11y = 1$, and get an $a = 5(11y) + 9(7x)$.
Apply Theorem 1.7, $x = -3$, $y = 2$. $a = -79 \equiv -2 \mod 77$
Use $a \equiv -2 \mod 77$ and $n \equiv 2 \mod 13$. We solve for $13x + 77y = 1$, and get $n = 2(77y) - 2(13x)$.
$x = 6$, $y = -1$. So $n = 2(77)(-1) - 2(13)(6) = -310 \equiv 691 \mod 1001$.
Thus $n = 691$. □

***Theorem:* 2.5: General Strategies**

The general strategies for solving $f(x) \equiv 0 \mod n$

1. Factor $n = p_1^{k_1} \cdots p_r^{k_r}$
2. Solve the system $f(x) \equiv 0 \mod p_1^{k_1}, \cdots, f(x) \equiv 0 \mod p_r^{k_r}$
3. Use Theorem 2.4 to combine the solutions.

Since for a number a, $\gcd(a, p^n) = 1$ if and only if $p \nmid a$. We claim that to solve $f(x) \equiv 0 \mod p^k$, we can solve in steps of solving $\mod p$, then lift to $\mod p^2$, $\mod p^3$,...

Example: $x^4 \equiv 7 \mod 81$.

Proof. Since $81 = 3^4$, we can work with $\mod 3$ first.
$x^4 \equiv 7 \equiv 1 \mod 3$, thus $x = \pm 1 \mod 3$.
And we can lift up to $x \equiv 1, 2, 4, 5, 7, 8 \mod 9$. □

3 Rationals

Previously, we consider the equation $x^2+y^2=z^2$ in the integer domain. We want to know if it has rational solutions and how to find them.

Theorem: 3.1: Property of Rationals

If $a, b \in \mathbb{Q} \setminus \{0\}$, then $\frac{a}{b} \in \mathbb{Q}$.

Then we can divide by z on both sides, $\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$ or equivalently, $u^2+v^2=1$ for $u, v \in \mathbb{Q}$.

Geometrically, the solutions lie on the unit circle. And we know that $(1,0)$ is a solution. If (u,v) is another rational solution to $u^2+v^2=1$, then the slope of the line connecting (u,v) and $(1,0)$ must be rational.

Conversely, if we have a line through $(1,0)$ with rational slope $v=t(u-1)$ for $t \in \mathbb{Q}$. Then the system $\begin{cases} v = t(u-1) \\ u^2+v^2=1 \end{cases}$ gives the other rational solution.
By substitution,

$$\begin{aligned} u^2 + t^2(u-1)^2 &= 1 \\ (1+t^2)u^2 - 2t^2u + t^2 - 1 &= 0 \end{aligned}$$

Using quadratic formula, we get $u = \frac{2t^2 \pm \sqrt{4t^2 - 4(1+t^2)(t^2-1)}}{2(t^2+1)} = \frac{2t^2 \pm 2}{2(t^2+1)}$. $u=1$ or $\frac{t^2-1}{t^2+1}$.
If t is rational, u is rational, and $v = t\,(u-1) = t\frac{t^2-1-t^2-1}{t^2+1} = \frac{-2t}{t^2+1}$ is rational.

If we write in lowest terms $t = \frac{m}{n}$, $m, n \in \mathbb{Z}$. $\frac{t^2-1}{t^2+1} = \frac{m^2-n^2}{m^2+n^2}$. $\frac{-2t}{t^2+1} = -\frac{2mn}{m^2+n^2}$.
Then clearing our denominators, we get integer solutions to $x^2+y^2=z^2$, $\left(m^2-n^2, -2mn, m^2+n^2\right)$.

Theorem: 3.2:

If $\frac{m}{n} = \frac{a}{b}$ for $a, b \in \mathbb{Z}$, then $a = \lambda m$, $b = \lambda n$, for $\lambda \in \mathbb{Z}$.

However, the same strategy will fail for degree > 2.

4 Polynomials

In previous sections, we often work with modulo a prime number. The modulo world also works nicely for polynomial long divisions.

Example: Suppose we want to divide $x^4 + 3x^3 + x + 1$, with divisor $5x^2 + 3$.
The first step is removing the highest degree term, $x^4 + 3x^3 + x + 1 - \frac{1}{5}x^2(5x^2 + 2) = 3x^4 - \frac{3}{5}x^2 + x + 1$.
Continue until the degree of polynomial drops below the degree of the divisor.
And we will get $x^4 + 3x^3 + x + 1 = q(x)(5x^2 + 3) + r(x)$, with $r(x) = 0$ or $\deg(r(x)) < 2$.

We can do exactly the same thing $\mod p$. When p is a prime, we have a division algorithm for polynomials. Suppose $f(x)$ is a polynomial with $f(a) \equiv 0 \mod p$, then $f(x) = (x - a)g(x)$.

Notation: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_p[x] = \{a_n x^n + \cdots a_1 x + a_0 : a_n, ..., a_0 \in \mathbb{F}_p\}$.

***Theorem:* 4.1: Division Algorithm for Polynomials**

Let $f(x), g(x) \in \mathbb{F}_p[x]$, $g(x)$ non constant. There exists $q(x), r(x) \in \mathbb{F}_p[x]$ s.t. $f(x) = q(x)g(x) + r(x)$ and $r(x) = 0$ or $\deg(r) < \deg(g)$.

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_i \neq 0$, $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$, $b_i \neq 0$.
If $m > n$, then $q(x) = 0$, $r(x) = f(x)$ suffices.
If $m \leq n$, then $f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots c_1 x_1 + c_0$.
Continue the iteration until it terminates. What is left is $r(x)$ and $q(x) =$ sum of all terms we multiply $g(x)$ by. □

Remark 6. The fact we have a division algorithm means we have unique factorization in $\mathbb{F}_p[x]$. More relevantly, the division algorithm lets us connect roots of polynomials with linear factors.

Suppose $f(x) \in \mathbb{F}_p[x]$ and $x - a | f(x)$, *i.e.* $\exists g(x) \in \mathbb{F}_p[x]$ with $f(x) = (x - a)g(x)$. Then $f(a) \equiv (a - a)g(a) \equiv 0 \mod p$.

***Theorem:* 4.2:**

Let $f(x) \in \mathbb{F}_p[x]$, $a \in \mathbb{F}_p$. If $f(a) \equiv 0 \mod p$, then $x - a | f(x)$.

Proof. Apply Division algorithm to get $f(x) = q(x)(x - a) + r(x)$. We know $r(x) = 0$ or $\deg(r) < \deg(x - a) = 1$, so $r(x) = b_0$ constant.
But $f(a) \equiv (a - a)q(a) + b_0 \mod p$, $0 \equiv b_0 \mod p$. □

Note: If we write $f(x) = (x - a_1)(x - a_2) \cdots (x - a_k)g(x)$, then $\deg(f) \geq k$.

***Theorem:* 4.3:**

Let $f(x) \in \mathbb{F}_p[x]$ be nonzero. Then the number of roots of $f(x) \leq \deg(f)$ counted with multiplicity.

Proof. We prove by induction on degree.
Base case: $\deg = 0$ and $\deg = 1$ are clear.
Suppose this is true if $\deg = n$. Consider $f(x)$ with degree $n + 1$.
If f has no roots, then we are done.
If f has a root, then $f(x) = (x - a)g(x)$ and $\deg(f) = 1 + \deg(g)$
So $\deg(g) = n$ and by induction, the number of roots of g with multiplicity $\leq \deg(g)$.

Therefore, the number of roots of f with multiplicity $\leq 1+$ number of roots of g with multiplicity $\leq 1+\deg(g) = 1+n = \deg(f)$. $\square$

Theorem: 4.4:

For any p, we can construct $f(x) \in \mathbb{F}_p[x]$ with no roots.

Example: $x^2+1 \equiv 0 \mod 3$ has no roots.

What are the roots of $x^p - x \equiv 0 \mod p$?
As long as p is a prime, $x^p - x \equiv 0$ has p roots. For $a \neq 0$, $a^{p-1} \equiv 1 \mod p$.

Definition: 4.1: Group of Units Modulo n

For n >1, define the group of units modulo n by $(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1\}$ = invertible elements modulo n with the following properties

1. If $x, y \in (\mathbb{Z}/n\mathbb{Z})^*$, then $xy \in (\mathbb{Z}/n\mathbb{Z})^*$. Also the product is associative and commutative.
2. $\forall x \in (\mathbb{Z}/n\mathbb{Z})^*$, $1x \equiv x \mod n$
3. $\forall x \in (\mathbb{Z}/n\mathbb{Z})^*$, $\exists y \in (\mathbb{Z}/n\mathbb{Z})^*$ s.t. $xy \equiv 1 \mod n$ (inverse exists) and the inverse is unique

Definition: 4.2: Euler ϕ-function

Define the function on the positive integers by $\phi(1) = 1$, $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ for $n > 1$.

Example: for p prime, $\phi(p) = p-1$, $\phi(p^k) = p^k - p^{k-1}$

Example: For $a \in (\mathbb{Z}/n\mathbb{Z})^*$, define $m_a : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ s.t. $m_a = ax$. m_a is a bijection.
Since the inverse a^{-1} exists, $m_a \circ m_{a^{-1}} = m_{a^{-1}} \circ m_a = \text{id}$.

Theorem: 4.5: Euler's Theorem

For $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $a^{\phi(n)} \equiv 1 \mod n$

Proof. Write $(\mathbb{Z}/n\mathbb{Z})^* = \{x_1, ..., x_{\phi(n)}\} = \{ax_1, ..., ax_{\phi(n)}\}$.
Multiply everything together, $x_1 \cdots x_{\phi(n)} = ax_1 \cdots ax_{\phi(n)} = a^{\phi(n)} x_1 \cdots x_{\phi(n)}$ by associativity.
Since inverse of $x_1 \cdots x_{\phi(n)}$ exists, we get $1 \equiv a^{\phi(n)} \mod n$. $\square$

Theorem: 4.6: Fermat's Little Theorem

For p prime, $a \not\equiv 0 \mod p$, $a^{p-1} \equiv 1 \mod p$.

Theorem: 4.7:

If n, m are coprime, then $\phi(nm) = \phi(n)\phi(m)$.

Proof. Theorem 2.4 gives us $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
And we can reduce to $(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ $\square$

Now given an arbitrary $n = p_1^{k_1} \cdots p_r^{k_r}$ with $p_i^{k_i}, p_j^{k_j}$ coprime. Then $\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r})$.
If we want $1 \leq a \leq p^k$ s.t. $\gcd(a, p^k) = 1$, there are $p^k - \left\lfloor \frac{p^k}{p} \right\rfloor = p^k - p^{k-1}$ such numbers. ($\left\lfloor \frac{p^k}{p} \right\rfloor$ is the number of elements dividing p^k in $\mathbb{Z}/p^k\mathbb{Z} = \{[0], [1], ..., [p^k - 1]\} = \{[1], [2], ..., [p^k - 1], [p^k]\}$)

Theorem: 4.8: Properties of Euler ϕ-function

1. $\phi(p^k) = p^k - p^{k-1} = p^{k-1})p - 1$ for p prime and $k \geq 1$
2. if $n = p_1^{k_1} \cdots p_r^{k_r}$, then $\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) = p_1^{k_1-1}(p_1 - 1) \cdots p_r^{k_r-1}(p_r - 1)$

Some times, we write $p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$, then $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

Example: $n = 13^4 3^5 19^7$, then $\phi(n) = \phi(13^4)\phi(3^5)\phi(19^7) = 13^3(13-1)3^4(3-1)19^6(19-1)$

Example: Compute $3^{1492} \mod 100$ (*i.e.* the last two digits)

Proof. We know $3^{\phi(100)} \equiv 1 \mod 100$.
If we apply division algorithm $1492 = q\phi(100) + r$ for $0 \leq r < \phi(100)$, then $3^{1492} \equiv (3^{\phi(100)})^q 3^r \mod 100 \equiv 3^r \mod 100$.
Since $100 = 2^2 5^2$, $\phi(100) = \phi(2^2)\phi(5^2) = 2(2-1)5(5-1) = 40$
$1492 = 37 \cdot 40 + 12$, $1492 \equiv 12 \mod \phi(100)$, then $3^{1492} \equiv 3^{12} \mod 100$

Successive squaring: every number has a binary expansion $m = c_n 2^n + \cdots c_1 2 + c_0$ where $c_j = 0$ or 1. Then $x^m = x^{c_n 2^n + c \ldots c_0} = (x^{2^n})^{c_n} \cdots (x^2)^{c_1} x^{c_0}$.

$12 = 2^3 + 2^2$, $3^2 \equiv 9 \mod 100$, $3^4 \equiv 81 \mod 100$, $3^8 \equiv (81)^2 \equiv (-19)^2 \equiv 61 \mod 100$.
$3^{12} \equiv 3^8 3^4 \equiv 61 \cdot 81 \mod 100 \equiv 41 \mod 100$. □

Suppose we want to solve $x^d \equiv 1 \mod n$. We consider $a^d \equiv 1 \mod n$, then $a^{-1} \equiv a^{d-1} \mod n$.

***Definition:* 4.3: Order**

For $a \in (\mathbb{Z}/n\mathbb{Z})^*$, the order of a is the smallest positive integer d s.t. $a^d \equiv 1 \mod n$. We write $\text{ord}(a)$ for the order.

***Theorem:* 4.9:**

For $a \in (\mathbb{Z}/n\mathbb{Z})^*$. If $a^m \equiv 1 \mod n$, then $\text{ord}(a)|m$.

Proof. Apply division algorithm, $m = q\text{ord}(a) + r$, where $0 \leq r < \text{ord}(a)$
$1 \equiv a^m \equiv a^{q\text{ord}(a)} a^r \equiv a^r \mod n$, then $r = 0$, $\text{ord}|\phi(n)$. □

Corollary 6. *For every $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $ord(a)|\phi(n)$.*

In part, we know $x^d \equiv 1 \mod n$ is only solvable with order d element when $d|\phi(n)$.
Suppose $g^{\phi(n)} \equiv 1 \mod n$ and $\phi(n) = \text{ord}(g)$, then $g^{\frac{\phi(n)}{k}}$ has order k.

Claim: We can always find an order d element for $d|\phi(n)$ if and only if we can find an order $\phi(n)$ element.

Aside (Cryptography): You have a large (hard to factor) N and some exponent e. If someone wants to send a message A in terms of $(\mathbb{Z}/n\mathbb{Z})^*$ elements. They send you $A^e \mod N$ where $\gcd(e, \phi(N)) = 1$.

Lemma 1.1 tells us that $ef + \phi(N)h = 1$ for some f, h, then $A^1 \equiv A^{ef+\phi(N)h} \equiv A^{ef}(A^{\phi(N)})^h \equiv (A^e)^f \mod N$.

If g is an element of order $\phi(N)$ (a generator), then $(\mathbb{Z}/n\mathbb{Z})^* = \left\{1, g, g^2, ..., g^{\phi(N)-1}\right\}$. The existence of a generator gives us a discrete logarithm to each $a \in (\mathbb{Z}/n\mathbb{Z})^*$. There is some unique $0 \leq k \leq \phi(N) - 1$ s.t. $g^k \equiv a \mod N$, so $k = \log_g a$ and $\log(A^e) = e \log A$.

***Definition:* 4.4: Primitive Root**

$g \in (\mathbb{Z}/n\mathbb{Z})^*$ is a primitive root if $\text{ord}(g) = \phi(N)$.

***Theorem:* 4.10:**

For $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $\text{ord}(a) = \left|\left\{a^k : k \geq 0\right\}\right|$

Proof. Define a map $\{1, ..., \text{ord}(a)\} \to \left\{a^k : k \geq 0\right\}$ by $k \mapsto a^k$
The map is surjective from division algorithm
The map is injective: if $a^i \equiv a^j \mod N$ for $i \geq j$, then $a^{i-j} \equiv 1 \mod N$, $0 \leq i - j < \text{ord}(N)$, then $i = j$. □

Consider the polynomial $x^d - 1$. If $a \in (\mathbb{Z}/p\mathbb{Z})^*$ of order d, then a is a root. In fact, $1 = a^0, a^1, ..., a^{d-1}$ are roots of the polynomial, with no repeats. Since $x^d - 1$ should have $\leq d$ roots. The set $a^0, a^1, ..., a^{d-1}$ is exactly the set of roots. The set of elements of order d is some subset of lists, consisting a^k where $\gcd(d, k) = 1$.

***Theorem:* 4.11:**

Let $a \in (\mathbb{Z}/n\mathbb{Z})^*$. If $\text{ord}(a) = d$, then $\text{ord}(a^k) = \frac{d}{\gcd(d,k)}$, $k \geq 1$.

Proof. $(a^k)^{\frac{d}{\gcd(d,k)}} \equiv (a^{\frac{k}{\gcd(d,k)}})^d \equiv 1 \mod n$.
Assume $a^{kj} \equiv (a^k)^j \equiv 1 \mod n$, then $d | kj$.
Divide both side by the gcd, $\frac{d}{\gcd(d,k)} | \frac{k}{\gcd(d,k)} j$
But now $\frac{d}{\gcd(d,k)}$ and $\frac{k}{\gcd(d,k)}$ are coprime, then by Lemma 1.2, $\frac{d}{\gcd(d,k)} | j$, so as long as $j > 0$, $j \geq \frac{d}{\gcd(d,k)}$. □

Corollary 7. *$ord(a^k) = ord(a)$ if $gcd(ord(a), k) = 1$.*

***Theorem:* 4.12:**

In $(\mathbb{Z}/p\mathbb{Z})^*$, there are either 0 elements of order d or there are $\phi(d)$ of such elements.

Let $\eta(d) =\#$ elements of order d in $(\mathbb{Z}/p\mathbb{Z})^*$. $\sum_{d|p-1} \eta(d) = \phi(p) = p - 1$. We want to show that all $\eta(d) \neq 0$.

***Theorem:* 4.13: Gauss Theorem**

For any $m \geq 1$, $\sum_{d|m} \phi(d) = m$.

Proof. Consider $\mathbb{Z}/m\mathbb{Z}$ and for each $d|m$, let

$$S_d = \{x \in \mathbb{Z}/m : dx \equiv 0 \mod m \text{ and } lx \not\equiv 0 \mod m \text{ for any } l < d\}$$

Firstly, $S_{d_1} \cap S_{d_2} =$ if $d_1 \neq d_2$.
Consider $d_1 x \equiv 0 \equiv d_2 x \mod m$ for any $x \in S_{d_1} \cap S_{d_2}$, but by definition, $d_1 \leq d_2$ and $d_2 \leq d_1$, thus $d_1 = d_2$.

Also, $\forall x \in \mathbb{Z}/m\mathbb{Z}$, $x \in S_d$ for some $d|m$, therefore, $\mathbb{Z}/m\mathbb{Z} = \bigcup_{d|m} S_d$ as disjoint union. Therefore, $m = \sum_{d|m} |S_d|$.

Suppose $x \in S_d$, $dx \equiv 0 \mod m$, equivalently, $m|dx$. Since $d|m$, we have $\frac{m}{d}|x$, so $x = \frac{m}{d}t$, $t \in \mathbb{Z}$.

We claim that $\gcd(t, d) = 1$.
Since $x = \frac{m}{d}t = \frac{m}{d/\gcd(d,t)} \frac{t}{\gcd(d,t)}$, then $\frac{d}{\gcd(d,t)} x \equiv 0 \mod m$.
But since $x \in S_d$, $d \leq \frac{d}{\gcd(d,t)} \leq d$. Therefore $d = \frac{d}{\gcd(d,t)}$, $\gcd(d, t) = 1$.
Therefore, $S_d = \left\{\frac{m}{d}t : 0 \leq t \leq d-1, \gcd(d,t) = 1\right\}$ and $|S_d| = \phi(d)$ by definition. □

Theorem: 4.14:

Primitive roots exist mod p (prime).

Proof. We have $\sum_{d|p-1} \eta(d) = p - 1 = \sum_{d|p-1} \phi(d)$ and $\eta(d) \leq \phi(d)$, so $\eta(d) = \phi(d)$.
In particular, $\eta(p-1) = \phi(p-1) > 0$. □

Example: $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$, $1^2 \equiv 1$, $3^2 \equiv 9 \equiv 1$, $5^2 \equiv 25 \equiv 1$, $7^2 \equiv 49 \equiv 1$. There are no primitive roots.

Example: Let p be an odd prime, $(\mathbb{Z}/4p\mathbb{Z})^*$ has no primitive roots.

Proof. By Theorem 2.4, $(\mathbb{Z}/4p\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$. Then $a^{p-1} \equiv 1 \mod 4p$ for all a.
But $\phi(4p) = 2(p-1)$, so there is no primitive roots. ($\phi(4p) \neq p - 1$) □

Example: Let p, q be distinct odd primes, $(\mathbb{Z}/pq\mathbb{Z})^*$ has no primitive roots.

Proof. By Theorem 2.4, $(\mathbb{Z}/pq\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$.
Consider $a^{\frac{(p-1)(q-1)}{2}}$.
Since p, q are distinct odds, $p-1, q-1$ are even. $\frac{p-1}{2}, \frac{q-1}{2} \in \mathbb{Z}$.
Then $a^{\frac{(p-1)(q-1)}{2}} \mapsto \left((a^{p-1})^{\frac{q-1}{2}} \mod p, (a^{q-1})^{\frac{p-1}{2}} \mod q\right) \equiv (1 \mod p, 1 \mod q)$ for all a, since $a^{p-1} \equiv 1 \mod p$ for p primes.
Thus, $a^{\frac{(p-1)(q-1)}{2}} \equiv 1 \mod pq$.
But $\phi(pq) = (p-1)(q-1)$, so there is no primitive roots. □

Lemma: 4.1: Reduction

For $n|m$, the reduction map $\pi : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ s.t. $\pi([x]_m) = [x]_n$ is surjective.

Proof. Let $1 \le x \le n$, $\gcd(x,n) = 1$, *i.e.* $x \in (\mathbb{Z}/n\mathbb{Z})^*$.
If $y \in (\mathbb{Z}/m\mathbb{Z})^*$ with $y \equiv x \mod n$, then for any $y' \in \mathbb{Z}/m\mathbb{Z}$, $y' \equiv x \mod n$, $y' \equiv y + nt$, so the elements in $\mathbb{Z}/n\mathbb{Z}$ above x are $x + nt$.
If $\gcd(x,m) = 1$, then we are good, there's only one element.
Otherwise there are primes $p|m$ with $p|x$. Note $m = \frac{m}{n}n$.
Since $\gcd(x,n) = 1$, $p|\frac{m}{n}$, otherwise $o|n$ and $\gcd(x,n) = p$.
Take t_0 be the product of p s.t. $p|\frac{m}{n}$.
Claim: $\gcd(x + nt_0, m) = 1$
Take a prime p s.t. $p|\frac{m}{n}$
If $p|x$, then $p|x + nt_0$ implies that $p|nt_0$, so $p|t_0$ contradiction.
If $p \not|$, then by construction $p|t_0$. So $p|x + nt_0$ implies $p|x$, contradiction.
Thus $\gcd(x + nt_0, m) = 1$. □

Theorem: 4.15:

Let $n|m$. If $(\mathbb{Z}/m\mathbb{Z})^*$ has a primitive root, then so does $(\mathbb{Z}/n\mathbb{Z})^*$.

Proof. Let $\pi : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ be a reduction map.
Suppose g is a primitive root $\mod m$.
Tkae $h = \pi(g) \mod n$, then for any $x \in (\mathbb{Z}/n\mathbb{Z})^*$, there exists $y \in (\mathbb{Z}/m\mathbb{Z})^*$ with $\pi(y) \equiv x \mod n$.
But $y = g^k \mod m$ by definition of primitive roots, $k \ge 0$.
Since π preserves multiplication, $h^k \equiv \pi(g)^k \equiv \pi(g^k) \equiv \pi(y) \equiv x \mod n$. Thus h is a primitive root $\mod n$. □

Theorem: 4.16: Obstruction Theorem

If $8|n$ or $4p|n$ for p prime or if $pq|n$ for distinct odd primes, then $(\mathbb{Z}/n\mathbb{Z})^*$ has no primitive root.

Theorem: 4.17:

$(\mathbb{Z}/p^k\mathbb{Z})^*$ has a primitive root for p odd prime, $k \ge 1$.

Proof. We have shown the theorem for $k = 1$ in Theorem 4.14.

Consider $k = 2$. Given g a primitive root $\mod p$. Claim that g or $g + p \mod p^2$ is a primitive root.
If g is a primitive root $\mod p^2$, then done.
Otherwise, let d be the order of g in $\mod p^2$. $g^d \equiv 1 \mod p^2$, then $g^d \equiv 1 \mod p$, so by order argument (Theorem 4.9), $p - 1|d$.
Also if d is the order of g in $\mod p^2$, we know that $d|\phi(p^2) = p(p-1)$. Therefore, $p - 1|d|p(p-1)$.
This implies that $d = p - 1$ or $d = p(p-1)$. Since we assume g is not a primitive root $\mod p^2$, we have $d = p - 1$.
Then $(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 + (p-1)g^{p-2}p \mod p^2$ (the higher order terms vanish)
If $(g+p)^{p-1} \equiv 1 \mod p^2$, then $0 \equiv (p-1)g^{p-2}p \mod p^2$. *i.e.* $p^2|(p-1)g^{p-2}p$, so $p|(p-1)g^{p-2}$, but this cannot hold, since p does not dive $p - 1$ or g.
Therefore $(g+p)$ has order $p(p-1)$ in $\mod p^2$, it is a primitive root.

Now we proceed by induction.
Claim: if h is a primitive root p^k, $k \ge 2$, then it is a primitive root $\mod p^{k+1}$.
Let d =order of h in $\mod p^{k+1}$, then $h^d \equiv 1 \mod p^{k+1}$ so $h^d \equiv 1 \mod p^k$.
By order argument, $\phi(p^k)|d$ and $d|\phi(p^{k+1})$. Then $d = \phi(p^k) = p^{k-1}(p-1)$ or $\phi(p^{k+1}) = p^k(p-1)$.
Observe that $\phi(p^k) = p\phi(p^{k-1})$.

$h^{\phi(p^{k-1})} \equiv 1 \mod p^{k-1}$ tells us that $h^{\phi(p^{k-1})} = 1 + p^{k-1}t$
$h^{\phi(p^k)} \not\equiv 1 \mod p^k$ tells us that $p \not| t$.
Then $h^{\phi(p^k)} \equiv h^{p\phi(p^{k-1})} \equiv \left(h^{\phi(p^{k-1})}\right)^p \equiv (1+p^{k-1}t)^p \equiv 1 + p^k t + \binom{p}{2} p^{2(k-1)} t^2 \mod p^{k+1}$.
The remaining terms vanish $\mod p^{k+1}$.
$2(k-1)$ is not always $\geq k+1$, but $p|\binom{p}{2}$, so the third term is divisible by $2(k-1)+1$ and it is $\geq k+1$, so it vanishes as well.
$h^{\phi(p^k)} \equiv 1 \mod p^{k+1} \Leftrightarrow p^k t \equiv 0 \Leftrightarrow p|t$. Contradiction.
Thus h is a primitive root $\mod p^{k+1}$ and $h6\phi(p^{k+1}) \equiv 1 \mod p^{k+1}$. □

Remark 7. If g is a primitive root $\mod p^2$, then g is a primitive root $\mod p^k$ for $k \geq 1$.

***Theorem:* 4.18:**

Note that for $\phi(2p^k) = \phi(p^k)$, $(\mathbb{Z}/2p^k\mathbb{Z})^*$ has a primitive root for p odd prime and $k \geq 0$.

Proof. $k = 0$, $(\mathbb{Z}/2\mathbb{Z})^*$ has one element only, and it is the primitive root.

When $k \geq 1$, let g be a primitive root $\mod p^k$. Suppose it is odd. let d =order of g in $\mod 2p^k$.
Then $d|\phi(2p^k) = \phi(p^k)$. and $g^d \equiv 1 \mod 2p^k$, then $g^d \equiv 1 \mod p^k$, so $\phi(p^k)|d$.
Then since $d|\phi(p^k)$, $d = \phi(p^k)$.
Hence g has a primitive root $\mod 2p^k$
If g is even, take $g + p^k$ instead. □

***Theorem:* 4.19:**

$(\mathbb{Z}/n\mathbb{Z})^*$ has a primitive root if and only if $n = 1, 2, 4, p^k, 2p^k$ for p an odd prime and $k \geq 1$.

Example: Find primitive roots $(\mathbb{Z}/9\mathbb{Z})^* = \{1, 2, 4, 5, 7, 8\}$

Proof. We know that 2 is a primitive root for $(\mathbb{Z}/3\mathbb{Z})$. We look for its powers in $(\mathbb{Z}/9\mathbb{Z})^*$ which are 2,5,8
Enumerate all powers of 2 in $(\mathbb{Z}/9\mathbb{Z})^*$: $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^6 \equiv 1$.
2 is a primitive root. Actually 2 is a primitive root for all $(\mathbb{Z}/3^k\mathbb{Z})^*$. □

Example: What are the solutions to $x^7 \equiv 8 \mod 81$?

Proof. We can always write $x \equiv 2^y \mod 81$ (by previous example). Then $2^{7y} \equiv 8 \equiv 2^3 \mod 81$
Then we only need to solve for $7y \equiv 3 \mod \phi(81)$ by Theorem 4.8. □

Notation: if p is a prime, n is an integer, $k \geq 0$, then $p^k || n$ means $p^k | n$ and $p^{k+1} \not| n$.

***Lemma:* 4.2:**

For $n \geq 0$, $2^{n+2} || 5^{2^n} - 1$

Proof. For $n = 0$, $5^{2^0} - 1 = 4$, $2^{0+2} = 4$, so $2^{0+2} || 5^{2^0} - 1$
Suppose this holds for $n \geq 0$. Now consider $5^{2^{n+1}} - 1$.
Note $5^{2^{n+1}} = 5^{2 \cdot 2^n} = \left(5^{2^n}\right)^2$, so $5^{2^{n+1}} - 1 = \left(5^{2^n} - 1\right)\left(5^{2^n} + 1\right)$.
We know by induction $2^{n+2} || 5^{2^n} - 1$.
$5^{2^n} + 1 \equiv 1 + 1 \equiv 2 \mod 4$, so only, $2 || 62^n + 1$, then $2^{n+3} || 5^{2^{n+1}} - 1$. □

Theorem: 4.20:

For $n \geq 3$,

1. 5 has order 2^{n-2} in $(\mathbb{Z}/2^n\mathbb{Z})^*$
2. Every element of $(\mathbb{Z}/2^n\mathbb{Z})^*$ can be written uniquely as $(-1)^i 5^j$, $0 \leq i \leq 1$, $0 \leq j \leq 2^{n-2} - 1$

Proof.

1. Because $\phi(2^n) = 2^{n-1}$, then $d = \text{ord}(5) = 2^k$ for some $k \geq 0$ by Theorem 4.11.
   Moreover, $5^{2^k} - 1 \equiv 0 \mod 2^n$, so $2^n | 5^{2^k} - 1$. By Lemma 4.2, $2^{k+2} || 5^{2^k} - 1$, so $n \leq k + 2$.
   We know $(\mathbb{Z}/2^n\mathbb{Z})^*$ has no primitive root, so $k < n - 1$. Therefore $n - 2 \leq k < n - 1 \Rightarrow k = n - 2$.
2. We know that each of $5^0, 5^1, ..., 5^{2^{n-2}-1}$, $-5^0, -5^1, ..., -5^{2^{n-2}-1}$ has no overlap. So in total there are $2 \cdot 2^{n-2} = 2^{n-1}$ elements and $|(\mathbb{Z}/2^n\mathbb{Z})^*| = 2^{n-1}$
   No-overlap: suppose $5^i \equiv -5^j \mod 2^{n-1}$, then $1 \equiv -1 \mod 4$ Contradiction.

□

Example: Solve $x^7 \equiv 9 \mod 280$

Proof. $280 = 2^3 \cdot 5 \cdot 7$. By Theorem 2.4, we can split it up.

1. $x^7 \equiv 9 \equiv 2 \mod 7$. By Theorem 4.5, $x^6 \equiv 1 \mod 7$, $x^7 \equiv x \mod 7$. $x \equiv 2 \mod 7$ is the only solution
2. $x^7 \equiv 9 \equiv 4 \mod 5$. By Theorem 4.5, $x^4 \equiv 1 \mod 5$, so $x^3 \equiv 4 \mod 5$, $x \equiv 4 \mod 5$ is the only solution
3. $x^7 \equiv 9 \equiv 1 \mod 8$. By Theorem 4.5, $\phi(8) = 2^2(2-1) = 4$, $x^4 \equiv 1 \mod 8$, thus $x^3 \equiv 1 \mod 8$.
   By Theorem 4.20, all elements $\mod 8$ has the form $\pm 5^0, \pm 5^1$ $(n = 3)$. $(\pm 5^i)^3 \equiv \pm 5^{3i}$, $5^4 \equiv 125 \equiv 5 \mod 8$.
   $(\pm 5^i)^3 \equiv \pm 5^{3i} \equiv \pm 5^i \equiv 1 \mod 8$. Thus $x \equiv 1 \mod 8$.

We can then combine the solutions using Theorem 2.4. □

For any general quadratic equations $x^2 + bx + c \mod p$, we can follow the quadratic formula $x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$, and the square root can be found by $y^2 \equiv r \mod p$, which has 0, 1, 2 solutions, and if s is a solution, then $-s$ is a solution.

Lemma: 4.3: Hensel's Lemma

Let $f(x)$ be a polynomial with integer coefficients. Let k be a positive integer, and r an integer such that $f(r) \equiv 0 \mod p^k$. Suppose $m \leq k$ is a positive integer. Then if $f'(r) \not\equiv 0 \mod p$, there is an integer s such that $f(s) \equiv 0 \mod p^{k+m}$ and $s \equiv r \mod p^k$. So s is a lifting of r to a root mod p^{k+m}. Moreover s is unique mod p^{k+m}.

5 Midterm

Q1. Solve $\begin{cases} x \equiv 13 \mod 514 \\ x \equiv 33 \mod 144 \end{cases}$.

Proof. $514 = 2 \cdot 257$, $144 = 12^2 = 2^4 \cdot 3^2$.

The system is the same as $\begin{cases} x \equiv 13 \equiv 1 \mod 2 \\ x \equiv 13 \mod 257 \\ x \equiv 33 \mod 144 \end{cases}$. But the first equation is implied by the third, so we can solve $\begin{cases} x \equiv 13 \mod 257 \\ x \equiv 33 \mod 144 \end{cases}$ instead. This can be done by CRT (Theorem 2.4) □

Q2.

(a) Show that if $p | n^6 + n^3 + 1$, then $p = 3$ or $p \equiv 1 \mod 9$

(b) Show that there are infinitely many primes p s.t. $p \equiv 1 \mod 9$

Proof. (a) Consider $x^3 - 1 = (x-1)(x^2+x+1)$. Let $x = n^3$, we get $n^9 - 1 = (n-1)(n^6+n^3+1)$. Since $p|(n^6+n^3+1)$, we have $p|n^9-1$.
Equivalently, $\text{ord}(n)|9 \Rightarrow \text{ord}(n) = 1, 3, 9$.
If $\text{ord}(n) = 9$, then by Theorem 4.6 and Theorem 4.9, $9|p-1$, so $p \equiv 1 \mod 9$
If $\text{ord}(n) = 1, 3$, then $n^3 \equiv 1 \mod p$, then $0 \equiv n^6 + n^3 + 1 \equiv 3 \mod p$, $p = 3$

(b) Suppose there are finitely many $p_1, ..., p_n$ s.t. $p \equiv 1 \mod 9$. Consider the prime divisors of m^6+m^3+1, $m = 3p_1, ..., p_n$. It must be distinct from any of them.

□

Q3. Find the smallest n with $n/10$ a 7th power and $n/7$ a 5th power.

Proof. $2^a 5^b 7^c p_1^{k_1} \cdots p_r^{k_r} = n = 10m^7 = 2 \cdot 5(2^d 5^e 7^f p_1^{j_1} \cdots p_r^{j_r})^7$
$2^a 5^b 7^c p_1^{k_1} \cdots p_r^{k_r} = n = 7m^5 = 7(2^g 5^h 7^i p_1^{l_1} \cdots p_r^{k_r})^7$

This gives that $\begin{cases} a = 7d + 1 = 5g \\ b = 7e + 1 = 5h \\ c = 7f = 1 + 5i \end{cases}$, and $7|k_j, 5|k_j$. We can set k_j to 0 to get the smallest number.

We just need to solve: $\begin{cases} a \equiv 1 \mod 7 \\ a \equiv 0 \mod 5 \end{cases}$, $\begin{cases} b \equiv 1 \mod 7 \\ b \equiv 0 \mod 5 \end{cases}$, $\begin{cases} c \equiv 1 \mod 5 \\ c \equiv 0 \mod 7 \end{cases}$. The solutions are $a = b = 15, c = 21$ □

Q4. Solve $ax + by = c$

Proof. Use Euclidean's algorithm (Theorem 1.7) to find $d = \gcd(a, b)$. If $d|c$, then we can find solutions to $ax_0 + by_0 = d$ □

Q6. Solve $x^3 + x^2 - 5 \equiv 0 \mod 7^4$

Proof. Use Lemma 4.3, start with $x^3 + x^2 - 5 \equiv 0 \mod 7$, $x \equiv 2 \mod 7$.
$f(x) = x^3 + x^2 - 5$, $f'(x) = 3x^2 + 2x$, $f'(2) = 3 \cdot 4 + 2^2 = 16 \not\equiv 0 \mod 7$, thus Hensel's lemma is valid.
Iteratively, we compute $a_1 = 2$, $a_2 = 2 - \frac{f(a_1)}{f'(a_1)}$ to get solution mod 7^4. □

Q7. Let p be an odd prime. Show that $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$.

Theorem: 5.1: Wilson's Thereom

$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) = 1(-1) \mod p = -1 \mod p$

Proof. For Q7, we have $\left(\left(\frac{p-1}{2}\right)!\right)^2 = \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)\left(1 \cdot 2 \cdots \frac{p-1}{2}\right)$
$\equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)(1-p)(2-p)\cdots\left(\frac{p-1}{2} - p\right)$
$\equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)(-1)^{\frac{p-1}{2}}(p-1)(p-2)\cdots\left(\frac{p-1}{2}+1\right) \equiv (-1)^{\frac{p-1}{2}}(p-1)! \equiv (-1)^{\frac{p+1}{2}} \mod p$ ◻

6 Quadratic Reciprocal

In this section, we always consider p as an odd prime.

Definition: 6.1: Quadratic Residue

$a \in \mathbb{Z}$, $a \not\equiv 0 \mod p$ is a quadratic residue (QR) if the equation $x^2 \equiv a \mod p$ has a solution. If there are no solutions, it is a non-residue (NR).

Theorem: 6.1:

There are $\frac{p-1}{2}$ QRs mod p and $\frac{p-1}{2}$ NRs.

Proof. Consider the list $1^2, 2^2, \cdots, (p-1)^2$. This contains all quadratic residues.
Since $(-x)^2 = x^2$, the list $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$ contains all quadratic residues. For $\frac{p-1}{2} < n \leq p-1$, $1 \leq p-n \leq \frac{p-1}{2}$.
There are no duplicates in the list, because if $1 \leq a, b \leq \frac{p-1}{2}$ with $a^2 \equiv b^2 \mod p$, then $(a-b)(a+b) \equiv 0 \mod p$.
$p|(a-b)(a+b) \Rightarrow p|a-b$ or $p|a+b$.
Because $2 \leq a+b \leq p-1$, $p \not| a+b$, then $p|a-b$. We know that $-p < a-b < p$, then $a = b$. □

Notation (Legendre symbol): For $a \not\equiv 0 \mod p$, $\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ is a QR mod } p \\ -1, & a \text{ is a NR mod } p \end{cases}$

Theorem: 6.2: QR Multiplicative Rule

Let $a, b \in \mathbb{Z}$, $a, b \not\equiv 0 \mod p$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. That is QR×QR=QR, QR×NR=NR, NR×NR=QR

Proof. 1) QR×QR=QR:
Suppose $a \equiv s_1^2 \mod p$, $b \equiv s_2^2 \mod p$, then $ab \equiv (s_1 s_2)^2 \mod p$
2) QR×NR=NR:
Suppose $a \equiv s_1^2 \mod p$ and b is a NR. Assume $ab \equiv t^2 \mod p$. Then $s^2 b \equiv t^2 \mod p$, $b = \left(\frac{t}{s}\right)^2 \mod p$. Contradiction.
3) NR×NR=QR:
Suppose a is NR. Let QRs be $q_1, ..., q_{\frac{p-1}{2}}$, NRs be $n_1, ..., n_{\frac{p-1}{2}}$
The list $aq_1, ..., aq_{\frac{p-1}{2}}$ consists of NRs and there are $\frac{p-1}{2}$ distinct ones, so they are all of the NRs.
The list $an_1, ..., an_{\frac{p-1}{2}}$ has $\frac{p-1}{2}$ elements and is disjoint from above. Therefore, the list is all QRs. For a NR b, ab is in the list, hence it is a QR. □

Example: Does $x^2 \equiv 3^4 5^7 11^3 \mod 13$ have a solution?

Proof. $\left(\frac{3^4 5^7 11^3}{13}\right) = \left(\frac{3}{13}\right)^4 \left(\frac{5}{13}\right)^7 \left(\frac{11}{13}\right)^3 = \left(\frac{5}{13}\right)\left(\frac{11}{13}\right)$
The list of QRs for 13 contains $1^2, 2^2, 3^2, 4^2, 5^2, 6^2 = 1, 4, 9, 3, 12, 10$, so 5 and 11 are NRs.
Thus $\left(\frac{5}{13}\right)\left(\frac{11}{13}\right) = 1$, $x^2 \equiv 3^4 5^7 11^3 \mod 13$ has a solution. □

Observation: For $n \in \mathbb{Z}$, $(-1)^k = (-1)^{k \mod 2}$. Given $n = \pm q_1^{k_1} \cdots q_r^{k_r}$ with q_j disjoint from p. Then $\left(\frac{n}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{q_1}{p}\right)^{k_1} \cdots \left(\frac{q_r}{p}\right)^{k_r} = \left(\frac{\pm 1}{p}\right)\left(\frac{q_1}{p}\right)^{k_1 \mod 2} \cdots \left(\frac{q_r}{p}\right)^{k_r \mod 2}$.
Note: $\left(\frac{1}{p}\right) = 1$. We want to understand $\left(\frac{-1}{p}\right)$, $\left(\frac{q}{p}\right)$ for prime $q \neq p$.

Theorem: 6.3: Euler's Criterion

For $a \in \mathbb{Z}$, $a \not\equiv 0 \mod p$, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

Proof. By Theorem 4.6, the polynomial $x^{p-1} - 1$ has exactly $p-1$ roots mod p.
Since p is odd, $\frac{p-1}{2} \in \mathbb{Z}$. We get $x^{p-1} - 1 = \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right)$. Therefore, $x^{\frac{p-1}{2}} - 1$ and $x^{\frac{p-1}{2}} + 1$ each have exactly $\frac{p-1}{2}$ roots.
Consider $s \not\equiv 0 \mod p$, $(s^2)^{\frac{p-1}{2}} - 1 \equiv s^{p-1} - 1 \equiv 0 \mod p$.
So $\left\{\text{roots of } x^{\frac{p-1}{2}} - 1\right\}$ = set of QRs. $\left\{\text{roots of } x^{\frac{p-1}{2}} + 1\right\}$ = set of NRs.
i.e., a is QR $\Leftrightarrow a^{\frac{p-1}{2}} - 1 \equiv 0 \mod p$, so for a QR, $a^{\frac{p-1}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right) \mod p$
a is NR $\Leftrightarrow a^{\frac{p-1}{2}} + 1 \equiv 0 \mod p$, so for a NR, $a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \mod p$ ☐

Corollary 8. $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv \begin{cases} 1, & \text{if } p \equiv 1 \mod 4 \\ -1, & \text{if } p \equiv 3 \mod 4 \end{cases}$

Using Theorem 6.3, we can prove Theorem 6.2. $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p$.
To upgrade this to an equality, observe that if p is an odd prime and $\epsilon, \delta \in \{\pm 1\}$ with $\epsilon \equiv \delta \mod p$, then $\epsilon = \delta$. This is because $\epsilon \equiv \delta \mod p \Rightarrow p | \epsilon - \delta$, but $\epsilon - \delta \in \{-2, 0, 2\}$, and only 0 can be divided by an odd prime p. Thus $\epsilon - \delta = 0, \epsilon = \delta$, so $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Example: Compute $\left(\frac{7}{11}\right)$.

Proof. By Theorem 6.3, we can compute $7^{\frac{11-1}{2}} \equiv 7^5 \mod 11$, which can be done using successive squares, which is faster ($\mathcal{O}(\log p)$) than exploring all squares mod 11 ($\mathcal{O}(p)$). ☐

To make Euler's Criterion more useful, we want to investigate $a^{\frac{p-1}{2}} \mod p$. To do this, recall the proof of Theorem 4.6 by listing all equivalence classes.
Consider the list $1, 2, ..., \frac{p-1}{2}$, adding a negative sign gives all numbers $1 \leq n \leq p-1$. Consider also the related list $a, 2a, ..., \frac{p-1}{2}a$.

Example: $p = 13, a = 7$, 1st list: $1, 2, 3, 4, 5, 6$, 2nd list: $7, 14 \equiv 1, 8, 2, 9, 3$
Reduce the second list mod 13, we get $-6, 1, -5, 2, -4, 3$.
The number of negative signs = the number of $1 \leq k \leq \frac{p-1}{2}$ so that $ka \mod p > \frac{p-1}{2}$. Call this number μ
Observe that $(-1)^\mu 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 7^6 (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)$, so $7^6 \equiv (-1)^\mu \mod 13$.

Theorem: 6.4: Gauss' Criteria

Let $a \not\equiv 0 \mod p$, μ =number of $1 \leq k \leq \frac{p-1}{2}$ s.t. $ka \mod p > \frac{p-1}{2}$. Then $a^{\frac{p-1}{2}} \equiv (-1)^\mu \mod p$, and as a result $\left(\frac{a}{p}\right) = (-1)^\mu$.

Proof. Start with the list $1, 2, 3, ..., \frac{p-1}{2}$, and consider the related list $a, 2a, ..., \frac{p-1}{2}a$. We knoe for each $1 \leq k \leq \frac{p-1}{2}$, we can work with $ka \equiv \epsilon_k y_k \mod p$ for $1 \leq y_k \leq \frac{p-1}{2}$, $\epsilon_k = \pm 1$.
As a result, the product of elements in the second list is $a(2a) \cdots \left(\frac{p-1}{2}a\right) \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \mod p$.
On the other hand,

$$a(2a) \cdots \left(\frac{p-1}{2}a\right) \equiv (\epsilon_1, y_1) \cdots \left(\epsilon_{\frac{p-1}{2}} y_{\frac{p-1}{2}}\right) \equiv \left(\epsilon_1 \cdots \epsilon_{\frac{p-1}{2}}\right) \left(y_1 \cdots y_{\frac{p-1}{2}}\right) \equiv (-1)^{\mu} \left(y_1 \cdots y_{\frac{p-1}{2}}\right) \mod p.$$

We need $y_1 \cdots y_{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)! \mod p$. One way to guarantee this is for $\left\{y_1, ..., y_{\frac{p-1}{2}}\right\} = \left\{1, 2, ..., \frac{p-1}{2}\right\}$
It suffices to show that y_k's are all distinct.
Suppose $y_i = y_j$, then $ia \equiv \epsilon_i y_i \equiv \epsilon_j y_j \equiv \pm ja \mod p$. Then $a(i \pm j) \equiv 0 \mod p$.
Since $a \not\equiv 0 \mod p$, $p | i \pm j$. Since $1 \leq i, j \leq \frac{p-1}{2}$, we require $i \pm j = 0$, so $i = \pm j$, $i = j$.
Thus $y_1 \cdot y_{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)!$, so $a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\mu} y_1 \cdots y_{\frac{p-1}{2}} \equiv (-1)^{\mu} \left(\frac{p-1}{2}\right)! \mod p$.
Thus $a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \mod p$. □

***Theorem:* 6.5:**

Let p be an odd prime, then $\left(\frac{2}{p}\right) = \begin{cases} 1, \text{ if } p \equiv 1 \mod 8 \text{ or } p \equiv 7 \mod 8 \\ -1, \text{ if } p \equiv 3 \mod 8 \text{ or } p \equiv 5 \mod 8 \end{cases}$

Proof. We want to use Theorem 6.4, so we compute $\mu(2, p)$.
We know that for $1 \leq k \leq \frac{p-1}{2}$, $2 \leq 2k \leq p - 1$, so $2k \mod p = 2k$
Case 1: $p \equiv 1 \mod 4$, $\frac{p-1}{4} \in \mathbb{Z}$, $\mu(2, p) = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}$
Case 2: $p \equiv 3 \mod 4$, $\frac{p-1}{4} = \frac{p-3}{4} + \frac{1}{2}$, so $\frac{p-1}{4} < k \Leftrightarrow \frac{p-3}{4} + 1 \leq k$. Hence, $\mu(2, p) = \frac{p-1}{2} - \frac{p-3}{4} - 1 + 1 = \frac{p+1}{4}$

Now, we compute $(-1)^{\mu(2,p)}$. All that matters is if $\mu(2, p)$ is even. This is a condition on $p \mod 8$ and there are 4 cases to consider.
Case 1: $p \equiv 1 \mod 8$. This gives $p \equiv 1 \mod 4$, $\mu(2, p) = \frac{p-1}{4} \equiv 0$ is even.
Case 2: $p \equiv 5 \mod 8$. This gives $p \equiv 1 \mod 4$, $\mu(2, p) = \frac{p-1}{4} \equiv 1$ is odd.
Case 3: $p \equiv 3 \mod 8$. This gives $p \equiv 3 \mod 4$, $\mu(2, p) = \frac{p+1}{4} \equiv 1$ is odd.
Case 4: $p \equiv 7 \mod 8$. This gives $p \equiv 3 \mod 4$, $\mu(2, p) = \frac{p+1}{4} \equiv 0$ is even. □

Because we know how to compute $\left(\frac{2}{p}\right)$ and $\left(\frac{bc}{p}\right) = \left(\frac{b}{p}\right)\left(\frac{c}{p}\right)$. We just need to know how to compute $\left(\frac{a}{p}\right)$ when a is odd.
Recall that there are unique $q_k, r_k \in \mathbb{Z}$ s.t. $ka = q_k p + r_k$, where $-\frac{p-1}{2} \leq r_k \leq \frac{p-1}{2}$.
Then $\frac{ka}{p} = q_k + \frac{r_k}{p}$, $-\frac{1}{2} < \frac{r_k}{p} < \frac{1}{2}$. Therefore $\left\lfloor \frac{ka}{p} \right\rfloor = \begin{cases} q_k, \text{ if } r_k > 0 \\ q_k - 1, \text{ if } r_k < 0 \end{cases}$.
$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^{\frac{p-1}{2}} q_k - \mu(a, p)$, where $\mu(a, p)$ =number of $1 \leq k \leq \frac{p-1}{2}$ s.t. $ka \mod p > \frac{p-1}{2}$ (negative value).

***Theorem:* 6.6:**

Let p be an odd prime, a be odd s.t. $a \not\equiv 0 \mod p$. Then $\mu(a, p) = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \mod 2$

Proof. From before, $\mu(a,p) \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} q_k \mod 2$. (plus and minus are interchangeable when mod 2)

Since a, p are odd, $ka \equiv q_k p + r_k \mod 2$, $k \equiv q_k + r_k \mod 2$.

So $\sum_{k=1}^{\frac{p-1}{2}} q_k \equiv \sum_{k=1}^{\frac{p-1}{2}} k + \sum_{k=1}^{\frac{p-1}{2}} r_k \mod 2$.

The list of r_k is exactly $\epsilon_1 1, \epsilon_2 2, ..., \epsilon_{\frac{p-1}{2}} \frac{p-1}{2}$ where $\epsilon_j = \pm 1$.

But $-1 \equiv 1 \mod 2$, so the list of $r_k \mod 2$ is $1, 2, ..., \frac{p-1}{2}$

So $\sum_{k=1}^{\frac{p-1}{2}} r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} k \mod 2$ and $\sum_{k=1}^{\frac{p-1}{2}} q_k \equiv 2 \sum_{k=1}^{\frac{p-1}{2}} k \equiv 0 \mod 2$ □

Example: $a = 7, p = 11$, find $\mu(7, 11)$

$\frac{p-1}{2} = 5$, $\left\lfloor \frac{1 \cdot 7}{11} \right\rfloor = 0$, $\left\lfloor \frac{2 \cdot 7}{11} \right\rfloor = 1$, $\left\lfloor \frac{3 \cdot 7}{11} \right\rfloor = 1$, $\left\lfloor \frac{4 \cdot 7}{11} \right\rfloor = 2$, $\left\lfloor \frac{5 \cdot 7}{11} \right\rfloor = 3$.

$\mu(7, 11) \equiv (0 + 1 + 1 + 2 + 3) \equiv 1 \mod 2$

Also, consider the list $7, 14 \equiv 3, 10, 6, 2$, $\mu(7, 11) = 3$.

Geometric perspective:

Firstly notice that $\left\lfloor \frac{ka}{p} \right\rfloor$ count the integers $1 \leq m < \frac{ka}{p} = \frac{a}{p}k$.

$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor$ =number of lattice points (integer coordinate points) inside the triangle with vertices $(0, 0)$, $\left(\frac{p}{2}, \frac{a}{2}\right)$, $\left(\frac{p}{2}, 0\right)$. Write as $T(a, p)$.

***Theorem:* 6.7: Quadratic Reciprocity**

Let p, q be distinct odd primes. Then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Equivalently, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Specifically, if $p \equiv 1 \mod 4$ or $q \equiv 1 \mod 4$, then $x^2 \equiv p \mod q$ has a solution $\Leftrightarrow x^2 \equiv q \mod p$ has a solution; if $p \equiv q \equiv 3 \mod 4$, then $x^2 \equiv p \mod q$ has a solution $\Leftrightarrow x^2 \equiv q \mod p$ does not have a solution.

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

Now, we use symmetry from triangle argument.

$T(p, q)$ =number of interior points with $y = \frac{p}{q}x$. $T(q, p)$ =number of integer points with $y = \frac{q}{p}x$.

The two triangles form a rectangle. Also, there is no lattice point on the diagonal, otherwise, p, q are not coprime.

Thus $T(p, q) + T(q, p)$ =number of interior points in the rectangle $(0, 0), \left(\frac{p}{2}, \frac{q}{2}\right) = \frac{p-1}{2}\frac{q-1}{2}$. □

Example: Let p be an odd prime, $p \neq 5$, when is $x^2 \equiv 5 \mod p$ solvable?

Proof. We want to find $\left(\frac{5}{p}\right)$, we know by Theorem 6.7 that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)(-1)^{\frac{p-1}{2}\frac{5-1}{2}} = \left(\frac{p}{5}\right)$.

$x = 1, 2$, $x^2 = 1, 4 \equiv -1$. $\left(\frac{p}{5}\right) = \begin{cases} -1, & \text{if } p \equiv 2, 3 \mod 5 \\ 1, & \text{if } p \equiv 1, 4 \mod 5 \end{cases}$. □

Example: $p \neq 7$, find $\left(\frac{7}{p}\right)$

Proof. $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)(-1)^{\frac{p-1}{2}\frac{7-1}{2}} = \left(\frac{p}{7}\right)(-1)^{\frac{p-1}{2}}$.
$x = 1, 2, 3$, $x^2 = 1, 4, 9 \equiv 2$. $\left(\frac{p}{7}\right) = \begin{cases} -1, & \text{if } p \equiv 3, 5, 6 \mod 7 \\ 1, & \text{if } p \equiv 1, 2, 4 \mod 7 \end{cases}$. Also, $(-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \mod 4 \\ -1, & \text{if } p \equiv 3 \mod 4 \end{cases}$
And we can combine the results using Thereom 2.4 □

6.1 Sum of Two Squares

Which primes can be written as a sum of two squares? *i.e.* $p = x^2 + y^2, x, y \in \mathbb{Z}$.
e.g. if $p = 2$, $p = 1^2 + 1^2$.

Theorem: 6.8:

If p is an odd prime and $p = x^2 + y^2$, then $p \equiv 1 \mod 4$

Proof. Check squares mod 4, $x \equiv 0, 1, 2, 3$, $x^2 \equiv 0, 1, 0, 1$
so $x^2 + y^2 \equiv 0, 1, 2 \mod 4$. But p is odd, so $p \equiv 1 \mod 4$. □

Theorem: 6.9:

If $p \equiv 1 \mod 4$, then p is a sum of two squares.

Recall that $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \mod 4 \\ -1, & \text{if } p \equiv 3 \mod 4 \end{cases}$, so if $p \equiv 1 \mod 4$, then there is some a with $a^2 \equiv -1 \mod p$ or equivalently, $p | a^2 + 1$, which we can write as $a^2 + 1^2 = pk$, $k \in \mathbb{Z}$.
The argument is $x^2 + y^2 + pk, k > 2$, then we can find x, y, t s.t. $x^2 + y^2 = pt, 1 \leq t < k$.
This follows from the following two facts: 1) $(x^2+y^2)(u^2+v^2) = (xu-vy)^2+(yu+vx)^2$; 2) if $x^2+y^2 = zw^2$, then z should be a sum of two squares $\left(\frac{x}{w}\right)^2 + \left(\frac{y}{w}\right)^2 = z$. The second is not literally true, because we don't always have $w|x$ and $w|y$.

Theorem: 6.10: Descent Procedure

Input: write $A^2 + B^2 = pk$, $1 \leq k < p$

1. If $k = 1$, then $A^2 + B^2 = p$, done
2. Find $-\frac{k}{2} \leq u, v \leq \frac{k}{2}$, with $u \equiv A \mod k$, $v \equiv B \mod k$
3. Notice $u^2 + v^2 \equiv A^2 + B^2 \equiv 0 \mod k$, so $u^2 + v^2 = kt$, where $1 \leq t < k$
4. Multiply $k^2 pt = (kt)(pt) = (u^2 + v^2)(A^2 + B^2) = (vA - uB)^2 + (uA + vB)^2$
5. Notice $k | vA - uB$ and $k | uA + vB$, so $pt = \left(\frac{vA-uB}{k}\right)^2 + \left(\frac{uA+vB}{k}\right)^2$

Proof. 1. is fine

2. We can do this because of Division Algo (Theorem 1.1)
3. $u^2 + v^2 \equiv A^2 + B^2 \equiv 0 \mod k$ is clear, so we can write $u^2 + v^2 = kt$.
   $kt = u^2 + v^2 \leq \frac{k^2}{4} + \frac{k^2}{4} = \frac{k^2}{2}$, so $t \leq \frac{k}{2} < k$
   Now we show that $t \leq 1$. Since $u^2 + v^2 > 0$, obviously, $t \geq 0$.
   If $t = 0$, then $u = v = 0$, $k|A$ and $k|B$. Since $A^2 + B^2 = pk$, also we have $A = ka$ and $B = kb$. Then $k^2(a^2 + b^2) = A^2 + B^2 = pk$, then $k|p$, $k = 1$ contradiction. Thus $t \geq 1$.
4. algebraic manipulation

5. $vA - uB \equiv BA - AB \equiv 0 \mod k$, $uA + vB \equiv A^2 + B^2 \equiv 0 \mod k$

□

Proof. (Theorem 6.9) We can write $a^1 + 1^2 = pk$ for some $a, k \in \mathbb{Z}$, $1 \leq k < o$, apply Descent proceudure (Theorem 6.10) until it terminates with $p = x^2 + y^2$. It takes $\mathcal{O}(\log k)$ steps. □

7 Arithmetic Functions

Definition: 7.1: Arithmetic Functions

An arithmetic function is a function $f : \mathbb{N} \to \mathbb{C}$.

Example: $\tau(n) = \#$ positive divisors, $\tau(3) = 2, \tau(12) = 6, \tau(33) = 4$
For $n > 1$, $\tau(n) = 2 \Leftrightarrow n$ is prime.

Example: $\phi(n) = |\{\mathbb{Z}/n\mathbb{Z}\}^n|$ (Euler's totient function), $\phi(3) = 2, \phi(12) = 4, \phi(33) = 30$

Example: $\sigma(n) =$sum of all positive divisors of n,
$\sigma(3) = 1 + 3 = 4$, $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$, $\sigma(33) = 1 + 3 + 11 + 33 = 48$

Example: $w(n) = \#$ prime divisors of n, $w(3) = 1, w(12) = w(33) = 2$

1. $w(n)$ is roughly $\log \log n$
2. $w(n)$ behaves like a normally distributed random variable.

Definition: 7.2: Multiplicative Arithmetic Functions

An arithmetic function f is multiplicative if
1. $f(1) = 1$
2. For all $n, m \in \mathbb{N}$, $\gcd(n, m) = 1$, $f(nm) = f(n)f(m)$

Theorem: 7.1:

Let f be multiplicative. For any $n > 1$, $n = p_1^{k_1} \cdots p_r^{k_r}$, $f(n) = f(p_1^{k_1}) \cdots f(p_r^{k_r})$.

Proof. By induction that if $m_1, ..., m_t$ are s.t. $\gcd(m_i, m_j) = 1$, $i \neq j$,
then $f(m_1 \cdots m_t) = f(m_1) \cdots f(m_t)$. □

Note: $f(p^2) \neq f(p)^2$.

Definition: 7.3: Totally Multiplicative

An arithmetic function is totally multiplicative if
1. $f(1) = 1$
2. For all $n, m \in \mathbb{N}$, $f(nm) = f(n)f(m)$

Theorem: 7.2:

Let f be totally multiplicative. For any $n > 1$, $n = p_1^{k_1} \cdots p_r^{k_r}$, $f(n) = f(p_1)^{k_1} \cdots f(p_r)^{k_r}$.

Lemma: 7.1:

Let $n, m \in \mathbb{Z}$, $\gcd(n, m) = 1$. Then $\forall d | nm, d > 0$, there exists unique divisors $d_1 | n$, $d_2 | m$ s.t. $d = d_1 d_2$.

Proof. Take $d_1 = \gcd(d, n)$, $d_1 | n$. Let $d_2 = \frac{d}{d_1}$. Then $d_1 d_2 = d$. Also $\gcd\left(\frac{d}{d_1}, \frac{n}{d_1}\right) = 1$. So $d_1 d_2 | nm \Rightarrow d_2 | \frac{n}{d_1} m \Rightarrow d_2 | m$.

Suppose $e_1|n, e_2|m$, with $d = e_1e_2$, then $d_1d_2 = d = e_1e_2$.
Since $\gcd(n, m) = 1$, $\gcd(e_1, d_2) = 1$, so $e_1|d_1$. By a similar argument, $d_1|e_1$. So $d_1 = \pm e_1$, but $e_1 \geq d_1 > 0$. So $d_1 = e_1$.
Similarly, $d_2 = e_2$. □

Note: there is a bijection ϕ : {positive divisors of n}×{positive divisors of m} → {positive divisors of nm} s.t. $\phi(d_1, d_2) = d_1d_2$.
So if n, m are coprime, then $\sum_{d|nm} \cdot = \sum_{d_1|n, d_2|m} \cdot = \sum_{d_1|n} \cdot \sum_{d_2|m} \cdot$.

Theorem: 7.3:

$\tau(n) = \sum_{d|n} 1$ and $\sigma(n) = \sum_{d|n} d$ are multiplicative.

Proof. $\tau(1) = \sigma(1) = 1$.
Let $n, m \in \mathbb{N}$, $\gcd(n, m) = 1$, $\tau(nm) = \sum_{d|nm} 1 = \sum_{d_1|n} \sum_{d_2|m} 1 = \sum_{d_1|n} 1 \sum_{d_2|m} 1 = \tau(n)\tau(m)$

Similarly, $\sigma(nm) = \sum_{d|nm} d = \left(\sum_{d_1|n} d_1\right) \left(\sum_{d_2|m} d_2\right) = \sigma(n)\sigma(m)$. □

7.1 Dirichlet Series

Definition: 7.4: Generating Series

A generating series is $\left(\sum_{n\geq1} a_n z^n\right) \left(\sum_{m\geq1} b_m z^m\right) = \sum_{k\geq1} \left(\sum_{i+j=k} a_j b_i\right) z^k$.

Definition: 7.5: Riemann Zeta Function

The Riemann zeta function is $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^\zeta}$.

Consider $D(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^\zeta}, E(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^\zeta}$, $D(s)E(s) = \sum_{n=1}^{\infty} \left(\sum_{ab=n} f(a)g(b)\right) \frac{1}{n^s}$.
We can rewrite the first term as $\sum_{d|n} f(d)g\left(\frac{n}{d}\right)$.

Definition: 7.6: Dirichlet Convolution

If f, g are arithmetic functions, the Dirichlet convolution is an arithmetic function $f*g$ s.t. $(f*g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$.

Example: Let $\mathbb{1}$ be s.t. $\mathbb{1}(n) = 1, \forall n$.
Then $(\mathbb{1} * \mathbb{1})(n) = \sum_{d|n} \mathbb{1}(d)\mathbb{1}\left(\frac{n}{d}\right) = \sum_{d|n} 1 \cdot 1 = \sum_{d|n} 1 = \tau(n)$.

Example: Let $I(n) = n$.
Then $(I * \mathbb{1})(n) = \sum_{d|n} I(d)\mathbb{1}\left(\frac{n}{d}\right) = \sum_{d|n} d = \sigma(n)$.

***Theorem:* 7.4:**

Let f, g be multiplicative, then $f * g$ is multiplicative.

Proof. $(f * g)(1) = \sum_{d|1} f(d)g\left(\frac{1}{d}\right) = f(1)g(1) = 1$
Let $n, m \in \mathbb{N}$, $\gcd(n, m) = 1$. Then

$$\begin{aligned}(f * g)(nm) &= \sum_{d|nm} f(d)g\left(\frac{nm}{d}\right) = \sum_{d_1|n}\sum_{d_2|m} f(d_1d_2)g\left(\frac{n}{d_1}\frac{m}{d_2}\right) \\ &= \sum_{d_1|n}\sum_{d_2|m} f(d_1)f(d_2)g\left(\frac{n}{d_1}\right)g\left(\frac{m}{d_2}\right) \\ &= \sum_{d_1|n} f(d_1)g\left(\frac{n}{d_1}\right)\sum_{d_2|m} f(d_2)g\left(\frac{m}{d_2}\right) \\ &= (f * g)(n)(f * g)(m)\end{aligned}$$

□

***Definition:* 7.7: Identity**

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

Claim 1. *If f is an arithmetic function, then $f * i = f$*

Proof. $(f * i)(n) = \sum_{d|n} f(d)i\left(\frac{n}{d}\right) = f(n)$ □

There is a special class of arithmetic functions f for which there is an arithmetic function g s.t. $f * g = i$.

Example: Let $f = \mathbb{1}$, $f(n) = 1$. For g to be an inverse of f, we need $f * g = i$ or $(f * g)(n) = i(n)$. *i.e.*
$\sum_{d|n} g(d) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{otherwise} \end{cases}$
$n = 1$, $g(1) = 1$; $n = 2$, $g(2) + g(1) = 0$ gives $g(2) = -1$; similarly, $n = 3$, $g(3) + g(1) = 0$ gives $g(3) = -1$
$n = 4$, $g(4) + g(2) + g(1) = 0$ gives $g(4) = 0$
Note $g(n) = \sum_{d|n, d<n} g(d) = 0$.

Definition: 7.8: Mobius Function

$$\mu(n) = \begin{cases} 1, & \text{if } n \text{ is square free and has even number of prime factors} \\ 1, & \text{if } n \text{ is square free and has odd number of prime factors} \\ 0, & \text{otherwise} \end{cases},$$

Square free means no square divisors. i.e. p^t with $t \geq 2$ are not divisors.

Theorem: 7.5:

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

Proof. RHS is multipicative. $\mu(n)$ is multiplicative and thus LHS is multiplicative.
Then it suffices to check if this equality holds for $n = p^k$, p prime, $k \geq 1$.

$$\sum_{d|p^k} \mu(d) = \sum_{j=0}^{k} \mu(p^j) = \mu(p^0) + \mu(p^1) = \mu(1) + \mu(p) = 1 + (-1) = 0$$

Note that anything larger will have a square divisor and $\mu(p^j) = 0$. □

Theorem: 7.6: Mobius Inversion Formula

Let f, g be arithmetic functions, then

$$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)$$

Proof. $(\Rightarrow)$ Suppose $f(n) = \sum_{d|n} g(d)$

$$\sum_{d|n} f(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n}\left(\sum_{e|d} g(e)\right)\mu\left(\frac{n}{d}\right)$$
$$= \sum_{d|n}\sum_{e|d} g(e)\mu\left(\frac{n}{d}\right) \qquad = \sum_{e|d} g(e) \sum_{d|n, e|d} \mu\left(\frac{n}{d}\right) \text{ (switching sums)}$$

Note $d|n, e|d \Leftrightarrow d = ed'$ and $ed'|n$ or $d'|\frac{n}{e}$.
Continuing the transformation, we get

$$= \sum_{e|n} g(e) \sum_{d'|\frac{n}{e}} \mu\left(\frac{n/e}{e'}\right)$$
$$= \sum_{e|n} g(e) i\left(\frac{n}{e}\right) = g(n)$$

i.e. $f = g * 1 \Leftrightarrow f * \mu = g * 1 * \mu = g * i = g$. □

Example: $\phi(n) = n \prod_{p|n}\left(1 - \frac{1}{p}\right) = \sum_{d|n} \mu(d)\frac{n}{d} \Leftrightarrow n = \sum_{d|n} \phi(d)$.

8 Extra Topics

8.1 Probability in Number Theory (Analytic Number Theory)

Q1: If I pick two positive integers n, m at random, how likely is it that they are coprime?
Q: If I pick two positive integers n, m at random from $\{1, 2, ..., N\}$, how likely is it that they are coprime?
If we call this probability p_N, then the limit $\lim\limits_{N\to\infty} p_N$, if exists, is a descent answer to Q1.

Total number of outcomes = total number of pairs (n, m) s.t. $1 \le n, m \le N = N^2$
Total number of pairs (n, m) s.t. $1 \le n, m \le N, \gcd(n, m) = 1 = \sum\limits_{1\le n,m\le N, \gcd(n,m)=1} 1$

Substitute $M = \gcd(n, m)$ into the Mobius function (Definition 7.8), we get $\sum\limits_{n|M} \mu(d) = \begin{cases} 1, & \text{if } M = 1 \\ 0, & \text{otherwise} \end{cases}$,

we get $\sum\limits_{n|\gcd(n,m)=1} \mu(d) = \begin{cases} 1, & \text{if } \gcd(n, m) = 1 \\ 0, & \text{otherwise} \end{cases}$. Then,

$$\begin{aligned}
\sum_{1\le n,m\le N, \gcd(n,m)=1} 1 &= \sum_{n,m\le N} \sum_{d|\gcd(n,m)} \mu(d) \\
&= \sum_{d\le N} \mu(d) \#\text{pairs } (n, m) \text{ s.t. } d|n, d|m, 1 \le n, m \le N \\
&= \sum_{d\le N} \mu(d) \left\lfloor \frac{N}{d} \right\rfloor^2
\end{aligned}$$

Note that $\frac{N}{d} - \left\{\frac{N}{d}\right\} = \left\lfloor \frac{N}{d} \right\rfloor$.
Square both sides $\left(\frac{N}{d} - \left\{\frac{N}{d}\right\}\right)^2 = \left\lfloor \frac{N}{d} \right\rfloor^2$, we get $\frac{N^2}{d^2} - 2\frac{N}{d}\left\{\frac{N}{d}\right\} + \left\{\frac{N}{d}\right\}^2 = \left\lfloor \frac{N}{d} \right\rfloor^2$
Since $0 \le \left\{\frac{N}{d}\right\} < 1$, by triangle inequality,

$$\left| -2\frac{N}{d}\left\{\frac{N}{d}\right\} + \left\{\frac{n}{D}\right\}^2 \right| \le \left| 2\frac{N}{d}\left\{\frac{N}{d}\right\} \right| + \left| \left\{\frac{n}{D}\right\}^2 \right| \le 2\frac{N}{d} + 1 \le 3\frac{N}{d}$$

Then $\left\lfloor \frac{N}{d} \right\rfloor^2 = \frac{N^2}{d^2} + \mathcal{O}\left\{\frac{N}{d}\right\}$.

$$\begin{aligned}
\sum_{1\le n,m\le N, \gcd(n,m)=1} 1 &= \sum_{d\le N} \mu(d) \left\lfloor \frac{N}{d} \right\rfloor^2 \\
&= \sum_{d\le N} \mu(d) \frac{N^2}{d^2} + \mathcal{O}\left(\sum_{d\le N} \frac{N}{d} \right) \\
&= N^2 \sum_{d\le N} \frac{\mu(d)}{d^2} + \mathcal{O}\left(N \sum_{d\le N} \frac{1}{d} \right) \\
&= N^2 \sum_{d\le N} \frac{\mu(d)}{d^2} + \mathcal{O}\left(N \log N\right)
\end{aligned}$$

$$\begin{aligned}
p_N &= \frac{1}{N^2} \sum_{1 \le n,m \le N, \gcd(n,m)=1} 1 \\
&= \frac{1}{N^2} \sum_{d \le N} \left(N^2 \frac{\mu(d)}{d^2} + \mathcal{O}\left(N \log N\right) \right) \\
&= \sum_{d \le N} \frac{\mu(d)}{d^2} + \mathcal{O}\left(\frac{\log N}{N} \right)
\end{aligned}$$

Therefore, $p = \lim_{N \to \infty} p_N = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}$.
i.e. If we pick two positive integers n, m at random, they are coprime with probability $\frac{6}{\pi^2}$

We know that $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, how is that related to $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}$?
Consider the Dirichlet convolution (Definition 7.6), $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{(\mu * \mathbb{1})(n)}{n^s} = 1$,
so $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$.

Euler's Product: Consider

$$\begin{aligned}
\prod_p \left(\frac{1}{1 - 1/p} \right) &= \prod_p \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right) = \left(1 + \frac{1}{2} + \frac{1}{4} + \cdots \right) \left(1 + \frac{1}{3} + \frac{1}{9} + \cdots \right) \\
&= \sum_{n=1}^{\infty} \frac{1}{n}
\end{aligned}$$

This is due to the unique prime factorization of integers.
This also shows that there must be infinitely many primes, because RHS is infinite.

If f is multiplicative,

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots \right).$$

If f is totally multiplicative,

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \left(\frac{f(p)}{p^s} \right)^2 + \cdots \right) = \prod_p \frac{1}{1 - f(p)/p^s}$$

For Mobius function,

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p \left(1 + \frac{\mu(p)}{p^s} + \frac{\mu(p^2)}{p^{2s}} \cdots \right) = \prod_p \left(1 - \frac{1}{p^s} \right) = \frac{1}{\zeta(s)}$$

Then,

$$\frac{6}{\pi^2} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \prod_p \left(1 - \frac{1}{p^2} \right) = \text{probability } n, m \text{ are not both divisible by } p$$

Q: If I pick two positive integers n, m at random, how likely is it that $m|n$?
Start with finite N, $q_N = \frac{\#(n,m) \text{ s.t. } n,m \leq N, m|n}{N^2}$

$$\sum_{n,m \leq N, m|n} 1 = \sum_{n \leq N} \sum_{m|n} 1 = \sum_{n \leq N} \tau(N)$$

Note that $\frac{1}{N} \sum_{n \leq N} \tau(N) \approx \log N$, so $q_N \approx \frac{\log N}{N} \to 0$ as $N \to \infty$.

Why the same technique won't work for the first problem?
Fix n, how many $m \leq N$ are there with $\gcd(n, m) = 1$?
Example: $N = 15$, $n = 4$, $\phi(n) = 2$. There are 8 such n with $\gcd(n, m) = 1$
In each modular partition, there are exactly $\phi(n)$ occurrence. But there are either $\left\lfloor \frac{N}{n} \right\rfloor$ or $\left\lfloor \frac{N}{n} \right\rfloor + 1$ different partitions. The error term cannot be ignored.

8.2 Fermat's Last Theorem (Algebraic Number Theory)

Find solutions to $x^2 - y^2 = z^2$ for $\gcd(x, y, z) = 1$, *i.e.* $\gcd(x, y) = \gcd(y, z) = \gcd(x, z) = 1$.
This means that exactly two of x, y, z are odd. WLOG, assume x, z are odd, y is even.
By difference of square $(x - y)(x + y) = z^2$.
Since $x + y = x - y + 2y$, $\gcd(x - y, x + y) = \gcd(x - y, 2y) = \gcd(x - y, y) = \gcd(x, y) = 1$.
Write $z = p_1^{k_1} \cdots p_r^{k_r}$, $z^2 = p_1^{2k_1} \cdots p_r^{2k_r}$, so $(x - y)(x + y) = p_1^{2k_1} \cdots p_r^{2k_r}$.

As a result, there are coprime s and t s.t. $\begin{cases} x - y = s^2 \\ x + y = t^2 \\ z = st \end{cases}$.

This gives $\begin{cases} x = \frac{s^2+t^2}{2} \\ y = \frac{t^2-s^2}{2} \\ z = st \end{cases}$. So we find all possible integer solutions to $x^2 = y^2 + z^2$.

However, this idea can fail for $x^3 + y^3 = z^3$, $\gcd(x, y, z) = 1$
$x^3 = z^3 - y^3 = (z - y)(z^2 + zy + y^2)$, which cannot be factored anymore in integers.

For $x^2 + y^2 = z^2$, we can also consider $x^2 - (iy)^2 = z^2$ where $i^2 = -1$. Then $(x - iy)(x + iy) = z^2$.
Now, we are wroking with Gaussian integer $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ has unique prime factorization, this still works.

With a similar idea, we consider $\omega = e^{\frac{2\pi i}{3}}$, $\omega^3 = 1$ with $\omega \neq 1$.
$x^3 - 1 = (x - 1)(x^2 + x + 1) = (x - 1)(x - \omega)(x - \omega^2)$.
Then $z^3 = x^3 + y^3 = (x + y)(x + \omega y)(x + \omega^2 y)$.
Now, we we work with the Eisenstein integers $\mathbb{Z}[\omega]$.

More geneerally, for an odd prime p, there is $\zeta_p = e^{\frac{2\pi i}{p}}$ with $\zeta_p^p = 1$ and $\zeta_p, \zeta_p^2, ..., \zeta_p^{p-1} \neq 1$.
$z^p = x^p + y^p = (x + y)(x + \zeta_p y) \cdots (x + \zeta_p^{p-1} y)$
Now, we are in $\mathbb{Z}[\zeta_p]$. As long as we can show that $\zeta_p, \zeta_p^2, ..., \zeta_p^{p-1}$ are coprime and there is unique prime factorization in $\mathbb{Z}[\zeta_p]$, we are done.
However, it fails. Consider $\mathbb{Z}[\sqrt{5}i]$, $6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i) = 2 \cdot 3$ has multiple factorizations. $x^2 + 5y^2 = (x + \sqrt{5}iy)(x - \sqrt{5}iy) = z^2$ won't work the same way.

This is the issue in Lame's proof of Fermat's Last Theorem.

Theorem: 8.1: Fermat's Last Theorem

For $n \geq 3$, there are no positive integer solutions to $x^n + y^n = z^n$.