MAT315

Jenci Wei

Winter 2024

Contents

1 Division

In this course we consider $\mathbb{N} = \{1, 2, \ldots\}$.

Overarching Question: How can I solve $ax + by = c$ where $a, b, c \in \mathbb{N}$ for solutions $x, y \in \mathbb{N}$?

Def. Let $n, d \in \mathbb{Z}$. We say d **divides** n if there is $e \in \mathbb{Z}$ with $n = de$. We write $d \mid n$.

Proof Techniques

1. Induction
2. Strong induction
3. Well-ordering property

Theorem 1.1 (Division Algorithm)**.** *Let $a \in \mathbb{Z}, b \in \mathbb{N}$. There exists $q, r \in \mathbb{Z}$ with*

$$a = qb + r, \quad 0 \leq r < b$$

and q, r are unique.

Proof. Let

$$S = \{a - bq \geq 0 : q \in \mathbb{Z}\}$$

Suppose $q = -|a|$ so that

$$a - qb = a + |a|b \geq 0$$

so $S \neq \varnothing$. By the well-ordering property, S has a least element $r = a - bq$. Then the following hold:

1. $a = bq + r$
2. $r \geq 0$
3. If $r > b$, then $0 \leq r - b = a - b(q + 1)$, contradicting minimality of r.

Uniqueness: Suppose

$$bq_1 + r_1 = a = bq_2 + r_2$$

Then

$$r_1 - r_2 = b(q_2 - q_1)$$

Notice that $-b < r_1 - r_2 < b$ since $0 \leq r_1, r_2 < b$. Then we have $r_1 = r_2$ because $r_1 - r_2$ is a multiple of b that is strictly between $-b$ and b. Then $q_1 = q_2$ follows.

□

Lemma 1.2. *Let $a, b, c, d \in \mathbb{N}$.*

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

Proof.

1. $b = an, c = bm, c = a(nm)$
2. $b = an, d = cm, bd = ac(nm)$
3. $a = dn, b = dm, ax + by = d(nx + my)$

$\square$

Def. 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 and b

- Except if $a = b = 0$, then $\gcd(a, b) = 1$.

Lemma 1.3 (Bézout's)**.** *Let $a, b \in \mathbb{N}$. The equation*

$$ax + by = \gcd(a, b)$$

has a solution.

Proof. Let

$$S = \{c \in \mathbb{N} : ax + by = c \text{ has a solution}\}$$

This is nonempty because we can take $c = a$ and set $x = 1, y = 0$. By the well-ordering property, there is a least element s. We claim that $s = \gcd(a, b)$.

First note that $s \geq \gcd(a, b)$ because $\gcd(a, b) \mid s$ (Property 3 of Lemma 1.2). To show that $s \leq \gcd(a, b)$, we will show that $s \mid a$ and $s \mid b$. Applying division algorithm to s, a:

$$a = qs + r, \quad 0 \leq r < s$$

Then

$$a = q(ax + by) + r \implies a(1 - qx) + b(-y) = r$$

Which implies that $r = 0$ because r cannot be in S, and so $s \mid a$. By symmetry $s \mid b$, so $s \leq \gcd(a, b)$. $\square$

Theorem 1.4. *Let $a, b, d \in \mathbb{N}$. If $d \mid a$ and $d \mid b$, then $d \mid \gcd(a, b)$.*

Proof. Using Bézout's lemma:

$$ax + by = \gcd(a, b)$$

Then $d \mid ax + by$ by Property 3 of Lemma 1.2, so $d \mid \gcd(a, b)$. $\square$

Theorem 1.5. *$ax + by = c$ is solvable iff $\gcd(a, b) \mid c$.*

Proof.
"$\Longleftarrow$" Say $c = \gcd(a, b)k$. By Bézout, there are $x, y \in \mathbb{Z}$ with

$$ax + by = \gcd(a, b)$$

Then

$$a(kx) + b(ky) = \gcd(a, b)k = c$$

"$\Longrightarrow$" Say $ax + by = c$. Then $\gcd(a, b) \mid c$ by the previous lemma.

$\square$

Def. We say $a, b \in \mathbb{Z} \setminus \{0\}$ are **coprime** if $\gcd(a, b) = 1$.

Lemma 1.6. *Let $a, b \in \mathbb{N}$ be coprime and $c \in \mathbb{N}$. If $a \mid bc$ then $a \mid c$.*

Proof. By Bézout $ax + by = 1$. Then

$$acx + bcy = c$$

Since $a \mid a$ and $a \mid bc$, we have that $a \mid c$ by Property 3 of Lemma 1.2.

$\square$

Back to the overarching question: denote $d = \gcd(a, b)$. Then

$$ax + by = c = dk \implies \frac{a}{d}x + \frac{b}{d}y = k$$

Assume a and b are coprime and that

$$\begin{align} ax_0 + by_0 &= c \tag{1} \\ ax_1 + by_1 &= c \tag{2} \end{align}$$

Then

$$\begin{aligned}
(1) - (2) \qquad & a(x_0 - x_1) + b(y_0 - y_1) = 0 \\
& a(x_0 - x_1) = b(y_1 - y_0) \\
& a \mid y_1 - y_0 \\
& b \mid x_0 - x_1 \\
& y_1 - y_0 = at \qquad \text{where } t = (x_0 - x_1)/b \\
& x_0 - x_1 = bs \qquad \text{where } s = (y_1 - y_0)/a \\
& abs = bat \\
& s = t
\end{aligned}$$

Therefore

$$\begin{aligned} x_1 &= x_0 - bt \\ y_1 &= y_0 + at \end{aligned}$$

Theorem 1.7 (Linear Diophantine Equations)**.** *Let $a, b, c \in \mathbb{N}$. Let $x_0, y_0 \in \mathbb{Z}$ be a solution to $ax + by = c$. Then all solutions are of the form (x, y) where*

$$\begin{aligned} x &= x_0 - \frac{b}{d}t \\ y &= y_0 + \frac{a}{d}t \end{aligned}$$

where $d = \gcd(a, b)$ and $t \in \mathbb{Z}$.

Proof. By the above observation. □

To find gcd, consider a pair of natural numbers (a, b). Divide

$$a = qb + r, \quad 0 \leq r < b$$

Then $\gcd(a, b) = \gcd(b, r)$ because say $d \mid a$ and $d \mid b$, then $d \mid a - qb = r$. Conversely, if $d \mid b$ and $d \mid r$, then $d \mid qb + r = a$.

Example: find the gcd of 315 and 17.

$$\begin{aligned} 315 &= 18 \cdot 17 + 9 \\ 17 &= 1 \cdot 9 + 8 \\ 9 &= 1 \cdot 8 + 1 \\ 8 &= 8 \cdot 1 \\ \gcd(8, 1) &= 1 \end{aligned}$$

So $\gcd(315, 17) = 1$. Try back substitution to find x, y such that $315x + 17y = 1$:

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

Theorem 1.8 (Euclidean Algorithm)**.** *Let $a, b \in \mathbb{N}$ where $a > b$. Define a sequence by repeated divisions*

$$\begin{aligned}
a &= q_1 b + r_1, \quad 0 \le r_1 < b \\
b &= q_2 r_1 + r_2 \\
&\cdots \\
r_{n-3} &= q_{n-2} r_{n-2} + r_{n-1} \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n \\
r_{n-1} &= q_n r_n
\end{aligned}$$

Then $\gcd(a, b) = r_n$. Moreover, we can solve for x, y in $ax + by = r_n$ by back substitution.

2 Prime Numbers

Def. A natural number $p > 1$ is **prime** if its only divisors are 1 and p.

Lemma 2.1. $\gcd(a, p) = 1$ *or* p. *Moreover,* $\gcd(a, p) = p$ *iff* $p \mid a$.

Corollary 2.1.1. *If a prime number p divides ab, then $p \mid a$ or $p \mid b$.*

Proof. Either $p \mid a$, or $\gcd(a, p) = 1$ and $p \mid b$. □

Corollary 2.1.2. *If $a_1, \ldots, a_m \in \mathbb{N}$ and $p \mid a_1 \cdots a_m$, then $p \mid a_i$ for some i.*

Theorem 2.2 (Fundamental Theorem of Arithmetic)**.** *For every $n \in \mathbb{Z} \setminus \{0\}$, there exists a factorization*

$$n = \pm p_1^{k_1} \cdots p_r^{k_r}$$

where p_js are distinct primes, $k_j \in \mathbb{N}$, and this is unique up to reordering of the p_j.

Proof.
Existence: By strong induction on n.

Base case: $1 = 1$, $2 = 2$.

Inductive step: suppose this holds for $1, \ldots, n$ and consider $n + 1$. If $n + 1$ is prime, then we're done. Otherwise, there is a divisor of $n + 1$ that is in $(1, n + 1)$. Can then write $n + 1 = de$ with $1 < d, e \leq n$. By induction, d, e factors, so $n + 1$ factors.

Uniqueness: First observe that if p, q are prime and $p \mid q$, then $p = q$. Write two factorizations

$$n = p_1^{k_1} \cdots p_r^{k_r} = q_1^{t_1} \cdots q_s^{t_s}$$

By the corollary, since $q_1 \mid n$, then $q_1 \mid p_i$ for some i. This means that $q_1 = p_i$ for some i. By reordering we can assume $q_1 = p_1$. Using the same technique, we can cancel off a q_1 and p_1 from both sides, which gives

$$p_1^{k_1 - 1} p_2^{k_2} \cdots p_r^{k_r} = q_1^{k_1 - 1} q_2^{t_2} \cdots q_s^{t_s}$$

Keep cancelling q_1s as long as they are on the RHS. We eventually get

$$p_1^{k_1 - t_1} p_2^{k_2} \cdots p_r^{k_r} = q_2^{t_2} \cdots q_s^{t_s}$$

Since the ps and qs are unique, if we have another p_1, it must divide one of $q_2, \ldots, q_s$, which cannot happen. Therefore $k_1 - t_1 = 0$, and so we get

$$p_2^{k_2} \cdots p_r^{k_r} = q_2^{t_2} \cdots q_s^{t_s}$$

Iterating this procedure (i.e. induction on length), we get $r = s, k_i = t_i, p_i = q_i$ for all i. □

Lemma 2.3. *Consider*

$$a = p_1^{k_1} \cdots p_r^{k_r}$$
$$b = p_1^{t_1} \cdots p_r^{t_r}$$

with $t_j, k_j \geq 0$. Then

1. $ab = p_1^{k_1 + t_1} \cdots p_r^{k_r + t_r}$
2. $b/a = p_1^{t_1 - k_1} \cdots p_r^{t_r - k_r}$, *moreover,* $a \mid b \iff t_j \geq k_j$ *for all* j
3. $\gcd(a, b) = p_1^{\min(k_1, t_1)} \cdots p_r^{\min(k_r, t_r)}$

Theorem 2.4 (Euclid)**.** *There are infinitely many primes.*

Proof. Let $p_1, \ldots, p_n$ be prime and consider $N = p_1 \cdot p_r + 1$. It has a prime factor q. If $p_j \mid N$, then $p_j \mid n - p_1 \cdots p_r = 1$, which is impossible. So $p_1, \ldots, p_r, q = p_{r+1}$ is a larger set of primes.

$\square$

Lemma 2.5. $\pi(x) =$ *number of primes* $\leq x \approx \frac{x}{\log x}$.

Questions regarding primes:

1. How did we estimate $\pi(x)$?
   - Will return to this later
2. Do they bunch together
   - Know that n and $n+1$ are not both prime if $n > 2$
   - For n and $n+2$, we don't know (twin primes conjecture)
3. Are they far apart?
   - p_k could be arbitrarily distant to p_{k+1} (requires very large p_k)
   - Bertrand's postulate: for every $n \in \mathbb{N}$, there is a prime p with $n < p < 2n$

Lemma 2.6. *Let p_n denote the nth prime number. Then*

$$p_n \leq 2^{2^{n-1}}$$

Proof. By induction.

Base case: $p_1 = 2$, $2^{2^{1-1}} = 2$.

Inductive step: assume $p_j \leq 2^{2^{j-1}}$ for all $j \leq n$. We know that there is a new prime q dividing $M = p_1 \cdots p_n + 1$. So

$$\begin{aligned}
p_{n+1} &\leq q \\
&= p_1 \cdots p_n + 1 \\
&\leq 2^{2^{1-1}} \cdots 2^{2^{n-1}} + 1 \\
&= 2^{\sum\limits_{j=1}^{n} 2^{j-1}} + 1 \\
&= 2^{\frac{2^n - 1}{2-1}} + 1 \\
&= 2^{2^n - 1} + 1 \\
&\leq 2^{2^n} \\
&= 2^{2^{(n+1)-1}}
\end{aligned}$$

$\square$

Def. For $x \in \mathbb{R}$, $\lfloor x \rfloor = n \in \mathbb{Z}$ where $\leq x < n+1$. The **fractional part** defined as

$$\{x\} = x - \lfloor x \rfloor$$

Corollary 2.6.1. $\pi(x) \geq \lfloor \log_2 \log_2 x \rfloor + 1$.

Proof. $\pi(x)$ = number of primes $\leq x$. Want to count the p_n with $2^{2^{n-1}} \leq x$. Taking a log gives

$$2^{n-1}\log_2 2 \leq 2^{n-1} \leq \log_2 x$$

Taking another log gives

$$(n-1)\log_2 2 + \log_2 2 \leq \log_2 \log_2 x$$

So

$$\begin{aligned} n \log_2 2 &\leq \log_2 \log_2 x \\ n &\leq \log_2 \log_2 x \\ &\leq \lfloor \log_2 \log_2 x \rfloor + 1 \end{aligned}$$

$\square$

Lemma 2.7. *A composite n has a nontrivial divisor $d \leq \sqrt{n}$.*

Proof. By contradiction, if all divisors are $> \sqrt{n}$, then multiplying them exceed n.

$\square$

Theorem 2.8 (Principle of Inclusion-Exclusion)**.** *For sets A_1, A_2, A_3,*

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

3 Modular Equivalence

Def. Let X be a set, then an **equivalence relation** on X is the some relation $\sim$ on $\{x \sim y \text{ pairs}\}$ such that

1. Reflective: $x \sim x$ for all $x \in X$
2. Symmetric: $x \sim y \implies y \sim x$
3. Transitive: $x \sim y, y \sim z \implies x \sim z$

For $n \in \mathbb{N}$, define an equivalence relation on $\mathbb{Z}$ by $a \sim b$ iff $n \mid a - b$

1. $n \mid 0 = a - a$, so $a \sim a$
2. $n \mid a - b \implies n \mid b - a$, so $a \sim b \implies b \sim a$
3. $n \mid a - b, n \mid b - c \implies n \mid a - c$

When $a \sim b$, we write $a \equiv b \pmod{n}$.

Lemma 3.1.

1. *Addition is preserved by modular equivalence, i.e. if* $a \equiv a' \pmod{n}$, $b \equiv b' \pmod{n}$, *then* $a+b \equiv a'+b' \pmod{n}$.
2. *Multiplication is preserved by modular equivalence, i.e. if* $a \equiv a' \pmod{n}$, $b \equiv b' \pmod{n}$, *then* $ab \equiv a'b' \pmod{n}$.

Proof.

1. $n \mid a - a'$, $n \mid b - b'$, so $n \mid a - a' + b - b' = (a + b) - (a' + b')$, so $a + b \equiv a' + b' \pmod{n}$.
2. If $n \mid a - a'$, $n \mid b - b'$, notice that

$$\begin{aligned} ab - a'b' &= ab - ab' + ab' - a'b' \\ &= a(b - b') + b'(a - a') \end{aligned}$$

So $n \mid ab - a'b'$, therefore $ab \equiv a'b' \pmod{n}$.

□

Def. The **equivalence class** of a point $x \in X$ is the set

$$[x] = \{y \in X : x \sim y\}$$

- The set of equivalence class is
$$X/\sim = \{[x] : x \in X\}$$
- In the case of modular equivalence, there are n equivalence classes
$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$$
- Take $n = 12$, then
$$\mathbb{Z}/12\mathbb{Z} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]\}$$
Then
$$\begin{aligned} 3 + 9 &\equiv 0 \pmod{12} \\ 2 \cdot 8 + 4 &\equiv 8 \pmod{12} \\ 3 \cdot 7 &\equiv 9 \pmod{12} \end{aligned}$$

For larger numbers, can use the following trick:

$$\begin{aligned} 3 \cdot 9 &\equiv 3 \cdot (-3) \pmod{12} \\ &\equiv -9 \pmod{12} \\ &\equiv 3 \pmod{12} \end{aligned}$$

Consider the case where we want to divide by 6, i.e. find x_0 such that

$$6x_0 \equiv 1 \pmod{12}$$

which is impossible, since the RHS can only be 0 or 6

- We can divide by $a \pmod{n}$ iff the equation $ax \equiv 1 \pmod{n}$ has a solution, which we call a^{-1}, the **multiplicative inverse** of $a \pmod{n}$
- Consider $ax \equiv 1 \pmod{n}$.

$$\begin{aligned} ax \equiv 1 \pmod{n} &\iff ax = 1 + ny \qquad \text{for some } y \in \mathbb{Z} \\ &\iff ax + n(-y) = 1 \end{aligned}$$

which is solvable iff a, n are coprime.

- The following are well-defined, i.e. does not depend on any choice:

$$\begin{aligned} [a] + [b] &:= [a + b] \\ [a] \cdot [b] &:= [ab] \end{aligned}$$

- $[a] = [b] \iff a \equiv b \pmod{n}$

Corollary 3.1.1. *If $p(x) \in \mathbb{Z}[x]$ (integer-coefficient polynomials), and $a \equiv b \pmod{n}$, then $p(a) \equiv p(b) \pmod{n}$.*

Proof. By induction, if $p(x) \in \mathbb{Z}[x]$, then $p([x]) = [p(x)]$ is well-defined. □

Theorem 3.2. *The equation*

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

has a solution iff $d = \gcd(a, n) \mid b$. If x_0 is a solution, then the distinct solutions modulo n are

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \cdots, x_0 + \frac{(d-1)n}{d}$$

- a is a congruence class
- $\gcd(a, n)$ is well-defined because by Euclid's algorithm $\gcd(m, qm + r) = \gcd(m, r)$

Proof.
"$\implies$": Say x_0 such that $ax_0 \equiv b \pmod{n}$, then $n \mid ax_0 - b$. So there is a $y_0 \in \mathbb{Z}$ with

$$\begin{aligned} &ny_0 = ax_0 - b \\ &b = ax_0 + n(-y_0) \\ &\gcd(a, n) \mid b \end{aligned}$$

"$\impliedby$": If $\gcd(a, n) \mid b$, then there are $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + ny_0 = b$, so $n \mid ax_0 - b$, or equivalently $ax_0 \equiv b \pmod{n}$.

By the LDET the solutions are of the form $x_0 + \frac{n}{d}t, t \in \mathbb{Z}$. Want to show that these are distinct and complete.

1. Distinct: Suppose $x_0 + jn/d \equiv x_0 + in/d \pmod{n}$. Then $n \mid (i-j)n/d$, where $0 \le i-j \le d-1$. Since $|(i-j)n/d| < n$, and that n divides this number, this number must be 0, so $i = j$.

2. Complete: For any x, know that

$$x = x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r) = x_0 + \frac{rn}{d} + qn, \quad 0 \le r < d$$

   therefore the list is complete.

$\square$

Example: simplify the following equations

- $10x \equiv 11 \pmod{9} \implies x \equiv 2 \pmod{9}$
- $7x \equiv 13 \pmod{15} \implies$ convert to $7x + 15y = 13$
  - First solve $7x + 15y = 1$, apply Euclid gives $15 = 2 \cdot 7 + 1$, $7 = 7 \cdot 1 + 0$, so $x = -2, y = 1$
  - Multiplying by 13 gives $x = -26, y = 13$
  - So the solution to $7x = 13 \pmod{15}$ is $x \equiv -26 \equiv 4 \pmod{15}$

Lemma 3.3 (Independence Condition)**.** *Let $n = p_1^{k_1} \cdots p_r^{k^r}$. Then $a \in \mathbb{Z}, a \equiv 0 \pmod{n}$ iff $a \equiv 0 \pmod{p_j^{k_j}}$ for all $1 \le j \le r$.*

Consider addition $+$ and multiplication $\cdot$ on $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$:

$$\begin{gathered}
\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} = \{([a]_n, [b]_m) : a = 0, \dots, n-1; b = 0, \cdots, m-1\} \\
([a]_n, [b]_m) \cdot ([c]_n, [d]_m) := ([ac]_n, [bd]_m) \\
([a]_n, [b]_m) + ([c]_n, [d]_m) := ([a+c]_n, [b+d]_m)
\end{gathered}$$

- $(0, 0)$ is the additive identity
- $(1, 1)$ is the multiplicative identity
- Consider $x^2 \equiv 2 \pmod{14}$, we can split into

$$\begin{aligned}
x^2 &\equiv 2 \pmod{2} \\
x^2 &\equiv 0 \pmod{2} \\
x &\equiv 0 \pmod{2}
\end{aligned}$$

  and

$$\begin{aligned}
x^2 &\equiv 2 \pmod{7} \\
x &\equiv \pm 3 \pmod{7}
\end{aligned}$$

Theorem 3.4 (Chinese Remainder Theorem)**.** *Let $m, n \ge 1$ be coprime integers. Then the map*

$$\begin{gathered}
\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\
a \pmod{nm} \mapsto (a \pmod{m}, a \pmod{n})
\end{gathered}$$

is a bijection. Moreover:

1. *It preserves addition: $\varphi(x + y) = \varphi(x) + \varphi(y)$*
2. *It preserves multiplication: $\varphi(xy) = \varphi(x)\varphi(y)$*

Proof. To show that φ is injective, want to show that $\varphi(a) = \varphi(b) \implies a = b$, which is equivalent to $a \equiv b \pmod{n} \wedge a \equiv b \pmod{m} \implies a \equiv b \pmod{nm}$. Because n, m coprime, have $n \mid a - b \wedge m \mid a - b$, which implies that $nm \mid a - b$.

To show that φ is surjective, for any $b \pmod{n}, c \pmod{m}$, we want $a \pmod{nm}$ such that $a \equiv b \pmod{n} \wedge a \equiv c \pmod{m}$. By Bezout's Lemma, there are $x_0, y_0 \in \mathbb{Z}$ such that $nx_0 + my_0 = 1$. Take

$$a = b(my_0) + c(nx_0)$$

Then when we work in modulo n, then

$$a \equiv b(my_0) + c(nx_0) \equiv b(my_0) \equiv b(1) \pmod{n} \qquad \text{Since } my_0 \equiv 1 \pmod{n} \text{ by Bezout's}$$

Similarly, $a \equiv c \pmod{m}$.

To show that φ preserves addition:

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

To show that φ preserves multiplication:

$$\begin{aligned}
\varphi(xy) &= ((xy) \pmod{n}, (xy) \pmod{m}) \\
&= (x \pmod{n} \cdot y \pmod{n}, x \pmod{m} \cdot y \pmod{m}) \\
&= (x \pmod{n}, x \pmod{m}) \cdot (y \pmod{n}, y \pmod{m}) \\
&= \varphi(x)\varphi(y)
\end{aligned}$$

□

Consider the polynomial

$$p(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0$$

Then

$$\begin{aligned}
\varphi(p(x)) &= \varphi(a_d x^d) + \cdots + \varphi(a_1 x) + \varphi(a_0) \\
&= \varphi(a_d)\varphi(x^d) + \cdots + \varphi(a_1)\varphi(x) + \varphi(a_0) \\
&= \varphi(a_n)\varphi(x)^d + \cdots + \varphi(a_1)\varphi(x) + \varphi(a_0) \\
&= a_n \varphi(x)^d + \cdots + a_1 \varphi(x) + a_0 \\
&= p(\varphi(x))
\end{aligned}$$

This means that $\varphi(p(x)) = (p(x) \pmod{n}, p(x) \pmod{m})$, and $\varphi(y) = 0 \iff y \equiv 0 \pmod{nm}$. φ gives a correspondance

$$\{(a, b) \mid p(a) \equiv 0 \pmod{n}, p(b) \equiv 0 \pmod{m}\} \longleftrightarrow \{c \mid p(c) \equiv 0 \pmod{nm}\}$$

Ex. Solve the following equations

- $6x \equiv 15 \pmod{385}$
- $x^2 \equiv 2 \pmod{14}$
  - CRT says it's enough to solve

$$x^2 \equiv 2 \pmod{2}, \qquad x^2 \equiv 2 \pmod{7}$$

  - The first one gives $x^2 \equiv 0 \pmod 2$, so $x \equiv 0 \pmod 2$
  - The second one gives $x^2 \equiv 9 \pmod 7$, so $x \equiv \pm 3 \pmod 7$, these are the only solutions (prove later)
  - On the LHS of the correspondance we have $\{(0,3),(0,-3)\}$
  - This means we need to solve simultaneous sytems

$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 3 \pmod 7 \\ y &\equiv 0 \pmod 2 \\ y &\equiv -3 \pmod 7 \end{aligned}$$

  - (First two) Use Euclidean algorithm with backsubstitution to get $7(1) + 2(-3) = 1$
  - Want $z \pmod{nm}$ that maps to $(a \pmod n, b \pmod m)$
  - $z = a(my) + b(nx) = 3(2)(-3) + 0(7)(1) = -18$, so $z \equiv 10 \pmod{14}$
  - (Second two) $z = (-3)(2)(-3) + (0)(7)(1) = 18$, so $z \equiv 4 \pmod{14}$

Strategy for solving $f(x) \equiv 0 \pmod n$:

1. Factor $n = p_1^{k_1} \cdots p_r^{k_r}$
2. Solve the system

$$\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{k_1}} \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_r^{k_r}} \end{aligned}$$

3. Use CRT to finish

- Example: $x^4 \equiv 7 \pmod{81}$
- $81 = 3^4$, so we work mod 3
$$x^4 \equiv 7 \equiv 1 \pmod 3$$
- $x \equiv 1, -1 \pmod 3$ (because the only choices are $0, 1, 2$)
- Working in mod 9, $1, -1$ correspond to $1, 4, 7, 2, 5, 8$, so we only need to check those
- If $n \equiv a \pmod{p^k}$, then there are p possible congruence classes for $n \pmod{p^{k+1}}$

4 Rational Numbers

Consider the equation $x^2 + y^2 = z^2$. Does this have rational solutions? Can we find them?

- If $a, b \in \mathbb{Q} \setminus 0$, then $a/b \in \mathbb{Q}$
- Divide by z:

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

  and so we can work with $u^2 + v^2 = 1$

- $(0, 1)$ is a rational solution. Assume that there is another rational solution (a, b), we could draw a secant line through $(0, 1)$ and (a, b), the line is defined by $v = t(u - 1)$

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

$$\begin{aligned} u &= \frac{2t \pm \sqrt{4t^4 - 4(1+t^2)(t^2-1)}}{2(1+t^2)} \\ &= \frac{2t^2 \pm \sqrt{4t^4 - 4(t^4-1)}}{2(1+t^2)} \\ &= \frac{2t^2 \pm 2}{2(1+t^2)} \\ &= \frac{t^2 \pm 1}{t^2+1} \\ &= 1, \frac{t^2-1}{t^2+1} \\ v &= t(u-1) \\ &= t\left(\frac{t^2-1}{t^2+1} - 1\right) \\ &= t\left(\frac{t^2 - 1 - t^2 - 1}{t^2+1}\right) \\ &= -\frac{2t}{t^2+1} \end{aligned}$$

- Can build a dictionary between rational slopes and rational points on $u^2 + v^2 = 1$

$$t \mapsto \left(\frac{t^2-1}{t^2+1}, -\frac{2t}{t^2-1}\right)$$

  Write $t = m/n$ where $m, n \in \mathbb{Z}$

$$\begin{aligned} \frac{t^2-1}{t^2+1} &= \frac{\frac{m^2}{n^2} - 1}{\frac{m^2}{n^2} + 1} \\ &= \frac{m^2 - n^2}{m^2 + n^2} \\ -\frac{2t}{t^2+1} &= \frac{-2\frac{m}{n}}{\frac{m^2}{n^2} + 1} \\ &= \frac{-2mn}{m^2 + n^2} \end{aligned}$$

- From rational points to integer points on $x^2 + y^2 = z^2$

$$\left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{-2mn}{m^2 + n^2}\right) \mapsto \left(\underbrace{m^2 - n^2}_{x}, \underbrace{-2mn}_{y}, \underbrace{n^2 + n^2}_{z}\right)$$

5 Polynomials

Theorem 5.1. *When p (the modulus) is prime, we can have a division algorithm for polynomials*

- Say $f(x)$ is a polynomial with $f(a) \equiv 0 \pmod{p}$, then $f(x) = (x-a)g(x)$
- The degree goes down after division

Polynomials with coefficients in $\mathbb{Z}/p\mathbb{Z}$, p prime

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

Theorem 5.2 (Division Algorithm)**.** *Let $f(x), g(x) \in \mathbb{F}_p[x]$, $g(x)$ nonconstant. There exists $q(x), r(x) \in \mathbb{F}_p[x]$ such that*
$$f(x) = q(x)g(x) + r(x)$$
And $r(x) = 0$ or $\deg r < \deg g$.

Proof. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0, \quad b_m \neq 0$$

If $m > n$, then $q(x) = 0$, $r(x) = f(x)$. If $m \leq n$, then

$$f(n) - \frac{a_n}{b_m}x^{n-m}g(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1 x + c_0$$

Continue to iterate this process until it terminates. The remaining term is $r(x)$, and $q(x) =$ sum of all the terms we multiplied $g(x)$ by. $\square$

- The fact we have a division algorithm means we have a unique factorization in $\mathbb{F}_p[x]$
- Moreover, the division algorithm lets us connect roots of polynomial with linear factors
- Given a polynomial $f(x)$ and that $x - a \mid f(x)$, i.e. there is $g(x) \in \mathbb{F}_p[x]$ with $f(x) = (x-a)g(x)$, then $f(a) = 0$
- The converse is true as well

Theorem 5.3. *Let $f(x) \in \mathbb{F}_p[x]$, $a \in \mathbb{F}_p$. If $f(a) \equiv 0 \pmod{p}$, then $x - a \mid f(x)$.*

Proof. Apply the division algorithm to get $f(x) = g(x)(x-a)+r(x)$, where $r(x) = 0$ or $\deg(r) < \deg(x-a) = 1$, so $r(x) = b_0$ is a constant. Plugging a into the equation gives $f(a) \equiv (a-a)q(a) + b_0 \pmod{p}$, so $b_0 \equiv 0 \pmod{p}$. This means that $r(x) = 0$, so $f(x) = g(x)(x-a)$. $\square$

- Notice if we write
$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_k)g(x)$$
Then $\deg f \geq k$.

Theorem 5.4. *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. Induct on degree.

Base case: degree 0, 1 are clear.

Inductive step: Say the result is true if $\deg = n$ and consider $f(x)$ with degree $n+1$.

- If f has no roots, then we're done
- If $f(x)$ has a root a, then by the previous theorem, we can write

$$f(x) = (x - a)g(x)$$

  and $\deg f = 1 + \deg g$. Knowing $\deg f = n + 1$, I know that $\deg g = n$. By IH the number of roots with multiplicity of $g(x)$ is $\leq n$, so the number of roots with multiplicity of $f(x)$ is $\leq n + 1$.

$\square$

6 Euler's Totient Function

Consider $x^p - x \pmod{p}$

- Observe that $x^p - x = x(x^{p-1} - 1)$
- Everything is a root
- For $a \not\equiv 0 \pmod{p}$, $a^{p-1} \equiv 1 \pmod{p}$

Group of units modulo n

- For $n > 1$,

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\} = \text{invertible elements modulo } n$$

1. If $x, y \in (\mathbb{Z}/n\mathbb{Z})^*$, then $xy \in (\mathbb{Z}/n\mathbb{Z})^*$. Moreover, this product is associative and commutative
2. For all $x \in (\mathbb{Z}/n\mathbb{Z})^*$, $1 \cdot x \equiv x \pmod{n}$
3. For all $x \in (\mathbb{Z}/n\mathbb{Z})^*$, there exists $y \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $xy \equiv 1 \pmod{n}$, i.e. inverses exist

Def. Define a function on the positive integers by

$$\begin{aligned} \phi(1) &= 1 \\ \phi(n) &= |(\mathbb{Z}/n\mathbb{Z})^*| \quad \text{for } n > 1 \end{aligned}$$

This is called the **Euler ϕ-function**.

- For p prime, $\phi(p) = p - 1$
- For $a \in (\mathbb{Z}/n\mathbb{Z})^*$, define a function

$$\mu_a : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*, \quad x \mapsto ax$$

  - This is a bijection
  - We know there is some $a^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*$ so $\mu_a \circ \mu_{a^{-1}} = \mu_{a^{-1}} \circ \mu_a = \text{identity}$

Theorem 6.1 (Euler)**.** *For $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Proof. Write $(\mathbb{Z}/n\mathbb{Z})^* = \left\{x_1, \dots, x_{\phi(n)}\right\} = \left\{ax_1, \dots, ax_{\phi(n)}\right\}$ (multiplying by a shuffles the order of the set). Multiplying everything together gives

$$\begin{aligned} x_1 \cdots x_{\phi(n)} &\equiv (ax_1) \cdots (ax_{\phi(n)}) \pmod{n} \\ &\equiv a^{\phi(n)}(x_1 \cdots x_{\phi(n)}) \pmod{n} \\ 1 &\equiv a^{\phi(n)} \pmod{n} \end{aligned}$$

The product is commutative because integer multiplication is commutative. □

Corollary 6.1.1 (Fermat's Little Theorem)**.** *For p prime, $a \not\equiv 0 \pmod{p}$, $a^{p-1} \equiv 1 \pmod{p}$.*

Lemma 6.2. *If n, m are coprime, then $\phi(nm) = \phi(n)\phi(m)$*

Proof. By Chinese Remainder Theorem, we have bijections

$$\begin{aligned} \mathbb{Z}/nm\mathbb{Z} &\longleftrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ (\mathbb{Z}/nm\mathbb{Z})^* &\longleftrightarrow (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \end{aligned}$$

$a \in (\mathbb{Z}/N\mathbb{Z})^*$ iff $ax \equiv 1 \pmod{N}$ is solvable.

□

Given an arbitrary n, we can factor

$$n = p_1^{k_1} \cdots p_r^{k_r}$$

and $p_i^{k_i}, p_j^{k_j}$ are coprime if $i \neq j$, so

$$\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r})$$

To compute $\phi(p^k)$, observe that $\gcd(a, p^k) = 1 \iff p \nmid a$. p^k has divisors $1, p, p^2, \ldots, p^k$. So if I want $1 \leq a \leq p^k$ with $\gcd(a, p^k) = 1$, observe that this number is the same as

$$\phi(p^k) = p^k - \left\lfloor \frac{p^k}{p} \right\rfloor = p^k - p^{k-1}$$

Because $\lfloor p^k/p \rfloor$ represents the number of multiples of p in the range $1, \ldots, p^k$, and multiples of p cannot be coprime to p^k.

Theorem 6.3.

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

$$\begin{aligned} \phi(n) &= \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) \\ &= p_1^{k_1 - 1}(p_1 - 1) \cdots p_r^{k_r - 1}(p_r - 1) \end{aligned}$$

- Notice that $p^k - p^{k-1} = p^k(1 - 1/p)$
- Can then write

$$\phi(n) = \left(p_1^{k_1}\left(1 - \frac{1}{p_1}\right)\right) \cdots \left(p_r^{k_r}\left(1 - \frac{1}{p_r}\right)\right) = p_1^{k_1} \cdots p_r^{k_r} \prod_{p \mid n}\left(1 - \frac{1}{p}\right) = n \prod_{p \mid n}\left(1 - \frac{1}{p}\right)$$

- E.g. $n = 13^4 \cdot 3^5 \cdot 19^7$, which is big, but we can compute $\phi(n) = 13^3(13-1) \cdot 3^4(3-1) \cdot 19^6(19-1)$
- E.g. Compute the last 2 digits of 3^{1492}
  - We know that $3^{\phi(100)} \equiv 1 \pmod{100}$
  - If $1492 = q \cdot \phi(100) + r$ for $0 \leq r < \phi(100)$, then $3^{1492} \equiv 3^{q \cdot \phi(100) + r} \equiv 3^r \pmod{100}$.
  - $\phi(100) = 2(2-1) \cdot 5(5-1) = 40$
  - $1492 \equiv 12 \pmod{40}$, so $3^{1492} \equiv 3^{12} \pmod{100}$
  - Successive squaring trick: every number has a binary expansion

    $$m = c_k 2^k + c_{k-1} 2^{k-1} + \cdots + c_1 2 + c_0$$

    where $c_i \in \{0, 1\}$. Then

    $$\begin{aligned} x^m &= x^{c_k 2^k + c_{k-1} 2^{k-1} + \cdots + c_1 2 + c_0} \\ &= \left(x^{2^k}\right)^{c_k} \cdot \left(x^{2^{k-1}}\right)^{c_{k-1}} \cdots \left(x^2\right)^{c_1} \cdot x^{c_0} \end{aligned}$$

  - $12 = 8 + 4$, $3^4 = 81$, $3^8 = 361 \equiv 61 \pmod{100}$
  - Now $3^{12} \equiv 61 \cdot 81 \pmod{100} \equiv 41 \pmod{100}$

Want to solve $x^d \equiv 1 \pmod{n}$

- Say $a^d \equiv 1 \pmod{n}$, then $a^{-1} \equiv a^{d-1} \pmod{n}$

Def. For $a \in (\mathbb{Z}/n\mathbb{Z})^*$, the **order** of a, denoted $\operatorname{ord} a$, is the smallest positive integer d such that $a^d \equiv 1 \pmod{n}$.

- This exists because $a^{\phi(n)} \equiv 1 \pmod{n}$, and most of the times the order $< \phi(n)$

Lemma 6.4. *For $a \in (\mathbb{Z}/n\mathbb{Z})^*$, if $a^m \equiv 1 \mod n$, then $\operatorname{ord} a \mid m$.*

Proof. By division algorithm,

$$m = q \cdot \operatorname{ord} a + r, \quad 0 \leq r < \operatorname{ord} a$$

See that

$$1 \equiv a^m \equiv a^{q \cdot \operatorname{ord} a} \cdot a^r \equiv a^r \pmod{n}$$

By minimality of $\operatorname{ord} a$, r must be 0, and so $\operatorname{ord} a \mid m$.

□

Corollary 6.4.1. *For every $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $\operatorname{ord} a \mid \phi(n)$.*

We know that $x^d \equiv 1 \pmod{n}$ are only solvable if $d \mid \phi(n)$

- Observe that if we want solutions with $\operatorname{ord} a = d$, it is enough to solve this for $d = \phi(n)$
- Want to find an element of order d for every $d \mid \phi(n)$

Lemma 6.5. *We can always find an order d element for $d \mid \phi(n)$ iff we can find an order $\phi(n)$ element.*

If we 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

$$A^e \pmod{N}$$

where $\gcd(e, \phi(N)) = 1$. By Bezout

$$ef + \phi(N)h = 1$$

Then

$$\begin{aligned}
A' &\equiv A^{ef+\phi(N)h \pmod{N}} \\
&\equiv A^{ef}\left(A^{\phi(N)}\right)^h \pmod{N} \\
&\equiv (A^e)^f \pmod{N}
\end{aligned}$$

Notice that

$$(\mathbb{Z}/N\mathbb{Z})^* = \left\{1, g, g^2, \ldots, g^{\phi(n)-1}\right\}$$

The existence of a generator gives us a "discrete logarithm" to each $a \in (\mathbb{Z}/N\mathbb{Z})^*$, i.e. there is a unique $0 \leq k \leq \phi(N) - 1$ such that $g^k \equiv a \pmod{N}$, so $k = \log_g(a)$.

- This matters because log "linearizes" equiation

$$\log(A^e) = e \log A$$

7 Primitive Roots

Def. We say $g \in (\mathbb{Z}/n\mathbb{Z})^*$ is a **primitive root** if $\operatorname{ord} g = \phi(n)$.

Lemma 7.1. *For* $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $\operatorname{ord} a = \left|\left\{a^k \mid k \geq 0\right\}\right|$.

Proof. Define a map

$$\{1, \ldots, \operatorname{ord} a\} \to \left\{a^k \mid k \geq 0\right\}, \quad k \mapsto a^k$$

This is surjective by the division algorithm. To see that this is injective, if $a^i \equiv a^j \pmod{n}$, say $i > j$, then $a^{i-j} \equiv 1 \pmod{n}$, but $0 \leq i - j < \operatorname{ord} a$, so $i = j$.

□

For the polynomial $x^d - 1$, if $a \in (\mathbb{Z}/p\mathbb{Z})^*$ of order d, then all powers of a, i.e. $\left\{1, a, a^2, \ldots, a^{d-1}\right\}$ are all distinct roots of $x^d - 1$.

- This list has no repeats
- Since $x^d - 1$ has $\leq d$ roots, and the list contains exactly d roots, the set of elements of order d is some subset of this list

Lemma 7.2. *Let* $a \in (\mathbb{Z}/p\mathbb{Z})^*$ *have order* d*. Then* $\operatorname{ord}(a^k) = d/\gcd(d,k)$*,* $k \geq 1$.

Proof.

$$\begin{aligned}(a^k)^{\frac{d}{\gcd(d,k)}} &\equiv a^{\frac{k}{\gcd(d,k)} \cdot d} \\ &\equiv 1 \pmod{n}\end{aligned}$$

Say that $(a^k)^j \equiv 1 \pmod{n}$, so $d \mid kj$. Then

$$\begin{aligned} &\frac{d}{\gcd(d,k)} \mid \frac{k}{\gcd(d,k)} \cdot j \\ \implies &\frac{d}{\gcd(d,k)} \mid j \qquad \text{By lemma (coprime)}\end{aligned}$$

So as long as $j > 0$, $j \geq \frac{d}{\gcd(d,k)}$.

□

Corollary 7.2.1. $\operatorname{ord}(a^k) = \operatorname{ord}(a)$ *iff* $\gcd(\operatorname{ord}(a), k) = 1$.

Lemma 7.3. *In* $(\mathbb{Z}/p\mathbb{Z})^*$*, there are either 0 elements of order* d*, or there are* $\phi(d)$*.*

Proof. Write $\eta(d) = \#$ of order d elements in $(\mathbb{Z}/p\mathbb{Z})^*$. Observe that

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

Which aggregates elements of every possible order, counting each element once, which results in $|(\mathbb{Z}/p\mathbb{Z})^*| = \phi(p)$. If any $\eta(d) = 0$, then the sum would be $< p - 1$.

- Technique: if $0 \leq a_n \leq b_n$ and $\sum a_n = \sum b_n$, then $a_n = b_n$ for all n
- a_n is $\eta(d)$, which represents the count of elements in $(\mathbb{Z}/p\mathbb{Z})^*$ of order d
- b_n is $\phi(d)$, which represents the theoretical maximum number of elements in $(\mathbb{Z}/p\mathbb{Z})^*$ of order d

□

Theorem 7.4 (Gauss)**.** *For any $m \geq 1$,*

$$\sum_{d|m} \phi(d) = m$$

Proof. Consider $\mathbb{Z}/m\mathbb{Z}$ and for each $d \mid m$, look at

$$S_d = \{x \in Z/m\mathbb{Z} \mid dx \equiv 0 \pmod{m} \land lx \not\equiv 0 \pmod{m} \quad \forall l < d\}$$

This is the set of smallest $\mathbb{Z}/m\mathbb{Z}$ elements that when multiplied by d results in multiples of m. Observe that $S_{d_1} \cap S_{d_2} = \varnothing$ for $d_1 \neq d_2$, because $d_1 x \equiv 0 \equiv d_2 x \pmod{m}$ for any $x \in S_{d_1} \cap S_{d_2}$, so $d_1 \leq d_2 \leq d_1 \implies d_1 = d_2$. Also observe that for every $x \in \mathbb{Z}/m\mathbb{Z}$, $x \in S_d$ for some $d \mid m$ (by division algorithm, since every x can be "multiplied" to $0 \pmod{m}$). Therefore

$$\mathbb{Z}/m\mathbb{Z} = \bigsqcup_{d|m} S_d$$

Take the cardinality of both sides give

$$m = \sum_{d|m} |S_d|$$

Say $x \in S_d$ such that $dx \equiv 0 \pmod{m}$, or equivalently, $m \mid dx$, therefore $\frac{m}{d} \mid x$. Can then write $x = \frac{m}{d}t$ for some $t \in \mathbb{Z}$. We claim that $\gcd(t, d) = 1$, which we can see because

$$x = \frac{m}{d/\gcd(d,t)} \cdot \frac{t}{\gcd(d,t)}$$

Therefore

$$\frac{d}{\gcd(d,t)} x \equiv 0 \pmod{m}$$

But since $x \in S_d$, $d \leq \frac{d}{\gcd(d,t)} \leq d$ (first $\leq$ is by minimality of d), so $d = \frac{d}{\gcd(d,t)}$, which means that $\gcd(d,t) = 1$. Then

$$S_d = \left\{\frac{m}{d}t : 0 \leq t \leq d-1 \land \gcd(t,d) = 1\right\}$$

This means $|S_d| = \phi(d)$, which completes the proof.

□

Theorem 7.5. *Primitive roots exist mod p.*

Proof. We know that

$$\sum_{d|p-1} \eta(d) = p - 1 = \sum_{d|p-1} \phi(d)$$

Since $\eta(d) \leq \phi(d)$, we have $\eta(d) = \phi(d)$. In particular, $\eta(p-1) = \phi(p-1) > 0$, so there is at least one primitive root.

□

Further observation

$$\begin{aligned}
\phi(n) &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) \\
&= n \sum_{p|n} \frac{\mu(d)}{d} \\
&= \sum_{d|n} \mu(d) \frac{n}{d}
\end{aligned}$$

If p is not prime, then primitive root may not exist:

- $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$
  - $1^2 = 1, 3^2 = 1, 5^2 = 1, 7^2 = 1$, and so there are no primitive roots
- $(Z/4p\mathbb{Z})^*$
  - $(\mathbb{Z}/4p\mathbb{Z})^* \longleftrightarrow (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$
  - $a \longleftrightarrow (b, c)$, $a^k \longleftrightarrow (b^k, c^k)$
  - Then $a^{p-1} \equiv 1 \pmod{4p}$ for all a
  - But $\phi(4p) = 2(p-1)$, so there are no primitive roots

Lemma 7.6. *For $n \mid m$, the reduction map*

$$\begin{aligned} (\mathbb{Z}/m\mathbb{Z})^* &\to (\mathbb{Z}/n\mathbb{Z})^* \\ [x]_m &\mapsto [x]_n \end{aligned}$$

is surjective.

Proof. Say $1 \leq x \leq n$, $\gcd(x, n) = 1$ (i.e. take $x \in (\mathbb{Z}/n\mathbb{Z})^*$). If $y \in \mathbb{Z}/m\mathbb{Z}$ with $y = x \pmod{n}$, then for any other $y' \in \mathbb{Z}/m\mathbb{Z}$, $y' \equiv x \pmod{n}$, $y' = y + nt$, so the elements in $\mathbb{Z}/m\mathbb{Z}$ above x are $x + at$. If $\gcd(x, m) = 1$, then we're good. Otherwise, there are primes $p \mid m$ with $p \mid x$. Note that $m = (m/n) \cdot n$. Since $\gcd(x, n) = 1$, we're forced to conclude that $p \mid (m/n)$.

Pick t to "interfere" with these primes, i.e. take t to be the product of $p \mid (m/n)$ but $p \nmid x$. Then we claim that $\gcd(x + nt, m) = 1$. Take a prime $p \mid (m/n)$. If $p \mid x$, then $p \mid x + nt_0$ implies $p \mid nt_0$, so $p \mid t_0$, which is a contradiction (beacuse this would divide x). And, if $p \nmid x$, then by construction $p \mid t_0$, so $p \mid x + nt_0$ implies $p \mid x$, which is a contradiction. Therefore we have shown that $\gcd(x + nt_0, m) = 1$.

□

Lemma 7.7. *Let $n \mid m$. If $(\mathbb{Z}/n\mathbb{Z})^*$ has a primitive root, then so does $(\mathbb{Z}/m\mathbb{Z})^*$.*

Proof. Call the reduction map $\pi : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ and say that g is a primitive root mod m. Take $h \equiv \pi(g) \pmod{n}$, then for any $x \in (\mathbb{Z}/m\mathbb{Z})^*$, I know there is some $y \in (\mathbb{Z}/m\mathbb{Z})^*$ with $\pi(y) = x \pmod{n}$. But since $y \equiv g^k \pmod{m}$ for some $k \geq 0$, and that π preserves multiplication, I see that $h^k \equiv \pi(g)^k \equiv \pi(g^k) \equiv \pi(y) \equiv x \pmod{n}$. Therefore h is a primitive root mod n.

□

Theorem 7.8 (Obstruction)**.** *If $8 \mid n$ or $4p \mid n$ for p an odd prime, then $(\mathbb{Z}/n\mathbb{Z})^*$ has no primitive root. Also, if $pq \mid n$ for distinct odd primes p, q, then there is no primitive root.*

- $(\mathbb{Z}/pq\mathbb{Z})^* \longleftrightarrow (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$
- Exercise: $a^{(p-1)(q-1)/2} \equiv 1 \pmod{pq}$ for all $a \in (\mathbb{Z}/pq\mathbb{Z})^*$
- Work separately in mod p and mod q, observe that

$$p - 1 \mid \frac{(p-1)(q-1)}{2} \qquad \text{and} \qquad q - 1 \mid \frac{(p-1)(q-1)}{2}$$

  Since $\phi(pq) = (p-1)(q-1)$, there is no primitive root mod pq

Candidates for having a primitive root (i.e. things not ruled out by obstruction theorem)

- Only possibilities are $n = 1, 2, 4, p^k, 2p^k$ for p an odd prime

Theorem 7.9. *$(\mathbb{Z}/p^k\mathbb{Z})^*$ has a primitive root for p odd, $k \geq 1$.*

Proof. We're done with the case of $k = 1$. Start induction from $k = 2$. Given g a primitive root $\pmod p$, we claim that one of g or $g + p \pmod{p^2}$ is a primitive root. If g is a primitive root, then we're done. Otherwise, $g^{p-1} \equiv 1 \pmod{p^2}$ since if $g^d \equiv 1 \pmod{p^2}$, then $g^d \equiv 1 \pmod p$. So by an order argument, $p-1 \mid d$. So if d is the order of $g \pmod{p^2}$, we know $d \mid \phi(p^2) = p(p-1)$. So $p-1 \mid d \mid p(p-1)$, so $d = p-1$ or $d = p(p-1)$. Since we're assuming that g is not a primitive root mod p^2, we have that $d = p-1$.

$$\begin{aligned}(g+p)^{p-1} &\equiv g^{p-1} + (p-1)g^{p-2}p && \pmod{p^2}\\ &\equiv 1 + (p-1)g^{p-2}p && \pmod{p^2}\end{aligned}$$

If LHS $\equiv 1$, then $p^2 \mid (p-1)g^{p-2}p$, which implies that $p \mid (p-1)g^{p-2}$, but both of those numbers are coprime to p, so LHS $\not\equiv 1$. This means that $g+p$ has order $p(p-1)$, so it is a primitive root.

Now, for induction, claim that if h is a primitive root mod p^k for $k \geq 2$, then it is a primitive root mod p^{k+1}. Say that $d \equiv$ order of $h \pmod{p^{k+1}}$. Then $h^d \equiv 1 \pmod{p^{k+1}}$ so $h^d \equiv 1 \pmod{p^k}$. By an order argument, $\phi(p^k) \mid d$, and $d \mid \phi(p^{k+1})$. We know

$$\phi(p^k) = p^{k-1}(p-1) \qquad \text{and} \qquad \phi(p^{k+1}) = p^k(p-1)$$

So $d = \phi(p^k)$ or $d = \phi(p^{k+1})$. Observe that $\phi(p^k) = p\phi(p^{k-1})$. We know

$$\begin{aligned}h^{\phi(p^{k-1})} &\equiv 1 \pmod{p^{k-1}} && \text{By Euler's Theorem}\\ h^{\phi(p^{k-1})} &\not\equiv 1 \pmod{p^k}\end{aligned}$$

The first equation states that $h^{\phi(p^{k-1})} \equiv 1 + p^{k-1}t$ and the second equation states that $p \nmid t$. Then

$$\begin{aligned}h^{\phi(p^k)} &\equiv \left(h^{\phi(p^{k-1})}\right)^p \pmod{p^{k+1}} && \pmod{p^{k+1}}\\ &\equiv \left(1 + p^{k-1}t\right)^p && \pmod{p^{k+1}}\\ &\equiv 1 + p^k t + \binom{p}{2} p^{2(k-1)}t^2 + \cdots && \pmod{p^{k+1}}\end{aligned}$$

In the "$\cdots$" are the terms that look like $p^{s(k-1)}$, $s \geq 3$. So using $3(k-1) \geq k+1$, I have $2k \geq 4$, and so $k \geq 2$ (and so the inequality is true). This means that all those terms vanish (because they are divisible by the modulus).

$2(k-1)$ is not always $\geq k+1$, but $p \mid \binom{p}{2}$. So the 3rd term is divisible by $2(k-1)+1$, which is $\geq k+1$, so the 3rd term vanishes too.

So our equation becomes

$$h^{\phi(p^k)} \equiv 1 + p^k t \pmod{p^{k+1}} \pmod{p^{k+1}}$$

LHS $\equiv 1 \iff p^k t \equiv 0 \pmod{p^{k+1}} \iff p \mid t$, which is not true. Therefore h is a primitive root mod p^{k+1}. ☐

- If g is a primitive root mod p^2 (p is odd prime), then g is a primitive root mod p^k for any $k \geq 1$
- Can find a primitive root mod 25 and check that it is a primitive root for 5^k, $k = 1, 3, 4, 5$
- $\phi(2p^k) = \phi(p^k)$, so if g is a primitive root mod p^k, then g is a primitive root mod $2p^k$

Corollary 7.9.1. *$(\mathbb{Z}/2p^k\mathbb{Z})^*$ has a primitive root for p odd, $k \geq 0$.*

Proof. $k = 0$ is trivial. For $k \geq 1$, take g to be the primitive root $\pmod{p^k}$. Say g has order d in mod $2p^k$. Then

$$d \mid \phi(2p^k) = \phi(p^k)$$

and

$$g^d \equiv 1 \pmod{2p^k}$$

This implies that $g^d \equiv 1 \pmod{p^k}$, and so $\phi(p^k) \mid d$, therefore $d = \phi(p^k)$. Hence g is a primitive root mod $2p^k$.

One thing to notice is that if g is even, then we can take $g + p^k$ instead.

□

Theorem 7.10. *$(\mathbb{Z}/n\mathbb{Z})^*$ 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 a primitive root mod 9.

- $(\mathbb{Z}/9\mathbb{Z})^* = \{1, 2, 4, 5, 7, 8\}$, which is of order 6
- It suffices to check 2, 5, 8 as they are primitive roots of mod 3
- $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^6 \equiv 1$. By our theorem, 2 is a primitive root for any $(\mathbb{Z}/3^k\mathbb{Z})^*$
- Additionally, we can find solutions to $x^7 = 8 \pmod{81}$
- Can always write $x = 2^y \pmod 8$, so $2^{7y} \equiv 8 \equiv 2^3 \pmod{81}$
- This means $7y \equiv 3 \pmod{\phi(81) = 54}$

Def. If p is prime, h an integer, $k \geq 0$, then $p^k \mid\mid n$ means that $p^k \mid n$ but $p^{k+1} \nmid n$.

Lemma 7.11. *For $n \geq 0$, $2^{n+2} \mid\mid 5^{2^n} - 1$*

Proof. For $n = 0$, $5^{2^n} - 1 = 5 - 1 = 4$, $2^{n+2} = 4$.

Suppose this holds for $n \geq 0$, and consider $5^{2^{n+1}} - 1$. Observe

$$5^{2^{n+1}} = 5^{2 \cdot 2n} = \left(5^{2^n}\right)^2$$

So

$$5^{2^{n+1}} - 1 = \left(5^{2^n} - 1\right)\left(5^{2^n} + 1\right)$$

By induction, $2^{n+2} \mid\mid 5^{2^n} - 1$. Working mod 4 (because we want to check whether this is divisible by higher powers of 2),

$$5^{2^n} + 1 \equiv 1 + 1 \equiv 2 \pmod 4$$

So $2 \mid\mid 5^{2^n} + 1$. Therefore $2^{n+3} \mid\mid 5^{2^{n+1}} - 1$.

□

Theorem 7.12. *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. For 1, because $\phi(2^n) = 2^{n-1}$, we know that $d = \text{ord}(5) = 2^k$ for some $k \geq 0$ (by Euler's). Moreover, we know

$$5^{2^k} - 1 \equiv 0 \pmod{2^n}$$

So

$$2^n \mid 5^{2^k} - 1$$

But by our lemma, $2^{k+2} \mid\mid 5^{2^k} - 1$, so $n \leq k + 2$. We know $(\mathbb{Z}/2^n\mathbb{Z})^*$ has no primitive root, so $k < n - 1$. This means $n - 2 \leq k \leq n - 2$, therefore $k = n - 2$.

For 2, consider the following lists

$$
\begin{aligned}
&5^0, 5^1, \ldots, 5^{2^{n-2}-1}\\
&-5^0, -5^1, \ldots, -5^{2^{n-2}-1}
\end{aligned}
$$

Each have no repeats. If the lists had no overlap together, they would give $2 \cdot 2^{n-2} = 2^{n-1}$ elements, and $|(\mathbb{Z}/2^n\mathbb{Z})^*| = 2^{n-1}$. Suppose for a contradiction that $5^i = -5^j \pmod{2^{n-1}}$, which implies $1 \equiv -1 \pmod 4$, which is a contradiction, and so the lists do not overlap.

$\square$

E.g. $x^7 \equiv 9 \pmod{280}$

- $280 = 7 \cdot 5 \cdot 2^3$
- By CRT we can split this up
  - $x^7 \equiv 2 \pmod 7$
    - By Euler's theorem (Fermat's little theorem, then multiply x on both sides), $x^7 \equiv x \pmod 7$, $x \equiv 2 \pmod 7$ is the only solution
  - $x^7 \equiv 4 \pmod 5$
    - By Euler's theorem, $x^4 \equiv 1 \pmod 5$, therefore $x^3 \equiv 4 \pmod 5$

x	1	2	3	4
x^3	1	3	2	4

    - Therefore $x^3 \equiv 4 \pmod 5$ has only $x \equiv 4 \pmod 5$ as a solution
  - $x^7 \equiv 1 \pmod 8$
    - By Euler's theorem, $x^4 \equiv 1 \pmod 8$, so $x^3 \equiv 1 \pmod 8$
    - By the previous theorem, all elements mod 8 have the form $\pm 5^i$, $i = 0, 1$
    - $(\pm 5^i)^3 \equiv \pm 5^{3i}$. Since $5^3 \equiv 125 \equiv 45 \equiv 5$, we have $\pm 5^{3i} \equiv \pm 5^i \equiv 1 \pmod 8$. Therefore the only solution is $x \equiv 1 \pmod 8$

Quadratic Formula

- Comes from completing the squares

$$
\begin{aligned}
x^2 + bx + c = \left(x + \frac{b}{2}\right)^2 + c - \frac{b^2}{4} = 0\\
x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}
\end{aligned}
$$

- $x^2 \equiv r \pmod p$ has 0, 1, 2 solutions; if s is a solution, then so is $-s$

8 Quadratic Reciprocity

Things we know

1. Divisibility and factorization, e.g. $ax + by = c$
2. Prime factorization
3. Remainders $\mathbb{Z}/n\mathbb{Z}, (\mathbb{Z}/n\mathbb{Z})^*$, Chinese remainder theorem
4. Hensel's lemma

Theorem 8.1 (Quadratic Reciprocity)**.** *Let p, q be distinct odd primes.*

1. *If $p \equiv 0 \pmod 4$ or $q \equiv 1 \pmod 4$, then $x^2 \equiv p \pmod q$ has a solution iff $x^2 \equiv q \mod p$ has a solution*
2. *If $p \equiv q \equiv 3 \pmod 4$, then $x^2 \equiv p \pmod q$ has a solution iff $x^2 \equiv q \pmod p$ does **not** have a solution*

- By quadratic formula, solving quadratic mod p is the same as solving $x^2 \equiv a \pmod p$

The Gaussian integers are $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$

- $x^2 + y^2 = z^2$ can be factored into $(x + iy)(x - iy) = z^2$
  - Notice 2 can be factored into $(1 + i)(1 - i)$
  - 5 can also be factored, i.e. $5 = (2 + i)(2 - i)$
- There are primes which are the sum of two squares, say $p = x^2 + y^2$ for $x, y \in \mathbb{Z}$ regular integers
- $\gcd(x, p) = \gcd(y, p) = 1$

$$x^2 \equiv -y^2 \pmod p \implies \left(\frac{x}{y}\right)^2 \equiv -1 \pmod p$$

$\mathbb{Z}[\sqrt{q}] = \left\{a + b\sqrt{q} \mid a, b \in \mathbb{Z}\right\}$

- $x^2 - qy^2 = z^2$ can be factored into $(x + \sqrt{q}y)(x - \sqrt{q}y) = z^2$
- We could write some prime p as $p = x^2 - qy^2$; when q is a square, the we have the same case as the above

From now on we consider p to be an odd prime.

Def. $a \in \mathbb{Z}, a \not\equiv 0 \pmod p$ is called a **quadratic residue** if the equation $x^2 \equiv a \pmod p$ has a solution. If there are no solutions, then a is called a **non-residue**.

Lemma 8.2. *There are $\frac{p-1}{2}$ quadratic residues mod p, and $\frac{p-1}{2}$ non-residues.*

Proof. Consider the list $1^2, 2^2, 3^2, \ldots, (p-1)^2$. This contains all quadratic residues. Since $(-x)^2 = x^2$, the list $1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$ contains all quadratic residues. There are no duplicates in this list because if $1 \leq a, b \leq \frac{p-1}{2}$ with $a^2 \equiv b^2 \pmod p$, then $(a-b)(a+b) \equiv 0 \pmod p$. Now $p \mid (a-b)(a+b) \implies p \mid a+b \vee p \mid a-b$. Because $2 \leq a+b \leq p-1$, we have $p \nmid a+b$. Therefore $p \mid a-b$. Knowing that $-p < a-b < p$, we must have $a - b = 0$ and so $a = b$.

Since there are exactly $\frac{p-1}{2}$ quadratic residues, anyone not in the list is a non-residue, therefore there are $\frac{p-1}{2}$ non-residues.

$\square$

Def. For $a \not\equiv 0 \pmod p$, denote

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

This is the **Legendre symbol**.

Theorem 8.3. *Let $a, b \in \mathbb{Z}$. Say $a, b \not\equiv 0 \pmod p$. Then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

That is,

$$\begin{aligned} QR \times QR &= QR \\ QR \times NR &= NR \\ NR \times NR &= QR \end{aligned}$$

Proof.
Case 1: $QR \times QR = QR$. Say $a \equiv s_1^2 \pmod p$ and $b \equiv s_2^2 \pmod p$. Then $ab = (s_1 s_2)^2 \pmod p$.

Case 2: $QR \times NR = NR$. Say $a \equiv s^2 \pmod p$ and b is a NR. Suppose that $ab \equiv t^2 \pmod p$. Then $s^2 b \equiv t^2 \pmod p$. Dividing the s^2 gives $b \equiv (t/s)^2 \pmod p$, which is a contradiction. Notice that we can write fraction because the multiplicative inverse of s exists.

Case 3: $NR \times NR = QR$. Say that a is NR. List all the QRs

$$q_1, \ldots, q_{\frac{p-1}{2}}$$

List all the NRs

$$n_1, \ldots, n_{\frac{p-1}{2}}$$

Mulitplying a to the first list, we get

$$aq_1, \ldots, aq_{\frac{p-1}{2}} \tag{*}$$

which only contains non-residues by case 2. They are distinct otherwise we can cancel the as and the qs would be the same. Since there are $\frac{p-1}{2}$ of them, they must be all the non-residues. Now multiply a to the second list

$$an_1, \ldots, an_{\frac{p-1}{2}}$$

which has $\frac{p-1}{2}$ elements, and they are all distinct. Observe that this list is disjoint from (*). Therefore this list is all the QRs. For a NR b, ab is in this list, hence it is a QR.

□

Example: Does $x^2 \equiv 3^4 \cdot 5^7 \cdot 11^3 \pmod{13}$ have a solution?

- Compute the value of the Legendre symbol

$$\left(\frac{3^4 \cdot 5^7 \cdot 11^3}{13}\right) = \left(\frac{3}{13}\right)^4 \cdot \left(\frac{5}{13}\right)^7 \cdot \left(\frac{11}{13}\right)^3 = \left(\frac{5}{13}\right) \cdot \left(\frac{11}{13}\right)$$

- Now find the list of QRs $1^2, 2^2, 3^2, 4^2, 5^2, 6^2$, which is $1, 4, 9, 3, 12, 10$
- Neither 5 nor 11 are in the list, therefore $(-1)(-1) = 1$, so the original equation has a solution

Generally, given $n = \pm q_1^{k_1} \cdots q_r^{k_r}$ with q_j distinct from p:

$$\left(\frac{n}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{q_1}{p}\right)^{k_1} \cdots \left(\frac{q_r}{p}\right)^{k_r} = \left(\frac{\pm 1}{p}\right)\left(\frac{q_1}{p}\right)^{k_1 \pmod 2} \cdots \left(\frac{q_r}{p}\right)^{k_r \pmod 2}$$

- We know that $\left(\frac{1}{p}\right) = 1$ because $1^2 = 1$
- We want to understand $\left(\frac{-1}{p}\right)$ and $\left(\frac{q}{p}\right)$ for primes $q \neq p$

Theorem 8.4 (Euler's Criterion)**.** *For $a \in \mathbb{Z}, a \not\equiv 0 \pmod p$,*

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

Proof. By Fermat's little theorem, the polynomial $x^{p-1} - 1$ has exactly $p - 1$ roots mod p. But since p is odd, $(p-1)/2 \in \mathbb{Z}$ and so we get a difference of squares

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

Both $x^{\frac{p-1}{2}} - 1$ and $x^{\frac{p-1}{2}} + 1$ have exactly $\frac{p-1}{2}$ roots because

- $x^{p-1} - 1$ has $p - 1$ roots
- So factoring it results in a total of $p - 1$ roots
- Each of the factors has at most $\frac{p-1}{2}$ roots because of the degree
- Therefore each factor has exactly $\frac{p-1}{2}$ roots

Consider for $s \not\equiv 0 \pmod p$:

$$\begin{aligned} (s^2)^{\frac{p-1}{2}} - 1 &\equiv s^{p-1} - 1 && \pmod p \\ &\equiv 0 && \pmod p \end{aligned}$$

Therefore the roots of $x^{\frac{p-1}{2}} - 1$ is the set of the quadratic residues. It follows that the roots of $x^{\frac{p-1}{2}} + 1$ is the set of the non-residues. Rewriting this observation:

1. a is a QR $\iff a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$. So for a QR, $a^{\frac{p-1}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod p$
2. a is a NR $\iff a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$. So for a NR, $a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod p$

$\square$

- Observe that this implies the multiplicativeness of the Legendre symbol up to modulo p

$$\begin{aligned} \left(\frac{ab}{p}\right) &\equiv (ab)^{\frac{p-1}{2}} && \pmod p \\ &\equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} && \pmod p \\ &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) && \pmod p \end{aligned}$$

- If p is an odd prime and $\epsilon, \delta \in \{-1, 1\}$ with $\epsilon \equiv \delta \pmod p$, then $\epsilon = \delta$
  - $\epsilon \equiv \delta \pmod p \implies p \mid \epsilon - \delta$

  - $\epsilon - \delta \in \{-2, 0, 2\}$
  - Out of the list, the odd prime p only divides 0
- The above two points imply that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
- E.g. compute $\left(\frac{7}{11}\right)$
  - By Euler, compute $7^{(11-1)/2} = 7^5$

Corollary 8.4.1.

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

Now we want to compute powers modulo p

- Use Fermat's little theorem
  1. Write out a list $x_1, \ldots, x_t$
  2. Observe that $ax_1, \ldots, ax_t$ is the same list
  3. Therefore $x_1 \cdots x_t = ax_1 \cdots ax_t = a^t x_1 \cdots x_t$
- Now consider the list

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

  - $1 \le n \le \frac{p-1}{2}$ stay where they are
  - $\frac{p-1}{2} < n \le p-1$ get subtracted by p
- First consider the positives, and the related list

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

  - E.g. $p = 13, a = 7$:

Original List	1	2	3	4	5	6
Related List	7	1	8	2	9	3
Related List Reduced mod 13	-6	1	-5	2	-4	3

  - Notice that the number of minus signs = number of $1 \le k \le \frac{p-1}{2}$ so that $ka \pmod p > \frac{p-1}{2} \triangleq N$
  - Also observe that

$$(-1)^N 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 7^6 (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6) \implies 7^6 \equiv (-1)^N \pmod{13}$$

    * 7^6 comes from the fact that we are multiplying by 7 to each of the 6 terms
    * $(-1)^N$ comes from the fact that there are N terms with -1 in front of them

Theorem 8.5 (Gauss' Criterion)**.** *Let $a \not\equiv 0 \pmod p$. Let N be the number of $1 \le k \le \frac{p-1}{2}$ such that $ka \pmod p > \frac{p-1}{2}$. Then*

$$a^{\frac{p-1}{2}} \equiv (-1)^N \pmod p$$

and as a result

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

Proof. Start with the list $1, 2, \dots, \frac{p-1}{2}$ and consider the related list $a, 2a, \dots, \frac{p-1}{2}a$. We know for each $1 \le k \le \frac{p-1}{2}$, we can write $ka \equiv \epsilon_k y_k \pmod{p}$ for $1 \le y_k \le \frac{p-1}{2}$ and $\epsilon = \pm 1$ (i.e. every element in the list looks like $1, 2, \dots, \frac{p-1}{2}$ up to a sign). As a result, the product of elements in the second list is

$$a(2a)(3a)\cdots\left(\frac{p-1}{2}a\right) \equiv a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$$

On the other hand,

$$a(2a)(3a)\cdots\left(\frac{p-1}{2}a\right) \equiv (\epsilon_1 y_1)\cdots\left(\epsilon_{\frac{p-1}{2}} y_{\frac{p-1}{2}}\right) \equiv \prod_{i=1}^{\frac{p-1}{2}} \epsilon_i \prod_{i=1}^{\frac{p-1}{2}} y_i \equiv (-1)^N y_1 \cdots y_{\frac{p-1}{2}} \pmod{p}$$

If the following holds, then we're done:

$$\left\{y_1, \dots, y_{\frac{p-1}{2}}\right\} = \left\{1, \dots, \frac{p-1}{2}\right\}$$

We first show that the y_ks are all distinct. Suppose $y_i = y_j$, then it follows that

$$ia \equiv \epsilon_i y_i \equiv \epsilon_i y_j \equiv \pm ja \pmod{p}$$

So $a(i \mp j) \equiv 0 \pmod{p}$. Because $a \not\equiv 0 \pmod{p}$, we have $p \mid i \mp j$. Because $1 \le i, j \le \frac{p-1}{2}$, this forces $i \mp j = 0$ so $i = \pm j$ and that $i = j$ because both i, j are nonnegative. It follows that $y_1, \dots, y_{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$, so

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

Which implies that $a^{\frac{p-1}{2}} \equiv (-1)^N \pmod{p}$. ∎

- We sometimes use $\mu(a, p)$ to denote N given a, p
- Assume a odd (since the symbol is multiplicative, we can reduce to this case). Notice that there are unique $q_k, r_k \in \mathbb{Z}$ such that $ka = q_k p + r_k$ where $-\frac{p-1}{2} \le r_k \le \frac{p-1}{2}$
  - Observe $\frac{ka}{p} = q_k + \frac{r_k}{p}$ where $-\frac{1}{2} < \frac{r_k}{p} < \frac{1}{2}$
  - Therefore
  $$\left\lfloor \frac{k_q}{p} \right\rfloor = \begin{cases} q_k, & \text{if } r_k \ge 0 \\ q_k - 1, & \text{if } r_k < 0 \end{cases}$$
  - Consequently
  $$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^{\frac{p-1}{2}} q_k - \mu(a, p)$$

Theorem 8.6. *Let p be an odd prime, a be odd, $a \not\equiv 0 \pmod{p}$. Then*

$$\mu(a, p) \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \pmod{2}$$

Proof. From before:

$$\mu(a, p) \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} q_k \pmod{2}$$

Since a, p are odd, we have

$$
\begin{aligned}
ka &\equiv q_k p + r_k \pmod 2 \\
k &\equiv q_k + r_k \pmod 2
\end{aligned}
$$

Therefore

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

The list of r_ks is exactly $\epsilon \cdot 1, \epsilon \cdot 2, \ldots, \epsilon_{\frac{p-1}{2}} \frac{p-1}{2}$, where $\epsilon_i = \pm 1$. Notice that $\pm 1 \equiv 1 \pmod 2$. So

$$\sum_{k=1}^{\frac{p-1}{2}} r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} k \pmod 2$$

And so

$$\sum_{k=1}^{\frac{p-1}{2}} q_k \equiv 2 \sum_{k=1}^{\frac{p-1}{2}} k \equiv 0 \pmod 2$$

$\square$

- E.g. $a = 7, p = 11, 1 \le k \le 5$

  $$\left\lfloor \frac{1 \cdot 7}{11} \right\rfloor = 0 \quad \left\lfloor \frac{2 \cdot 7}{11} \right\rfloor = 1 \quad \left\lfloor \frac{3 \cdot 7}{11} \right\rfloor = 1 \quad \left\lfloor \frac{4 \cdot 7}{11} \right\rfloor = 2 \quad \left\lfloor \frac{5 \cdot 7}{11} \right\rfloor = 3$$

  Their sum is 7, which is odd
- Computing $\mu(7, 11)$ in the traditional way gets

  $$7 \equiv 7 \quad 14 \equiv 3 \quad 21 \equiv 10 \quad 28 \equiv 6 \quad 35 \equiv 2$$

  3 of which are ≥ 5, and so $\mu(7, 11) = 3$, which is odd
- Geometric perspective
  - $\left\lfloor \frac{ka}{p} \right\rfloor$ counts the integers $1 \le m < \frac{ka}{p}$
  - Back to $a = 7, p = 11$ example
  - If m satisfies $1 \le m < \frac{ka}{p}$, we indicate $\times$; otherwise we indicate $\cdot$

    $$
    \begin{array}{c|ccccccc}
    4 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
    3 & \cdot & \cdot & \cdot & \cdot & \cdot & \times & \cdot \\
    2 & \cdot & \cdot & \cdot & \cdot & \times & \times & \cdot \\
    1 & \cdot & \cdot & \times & \times & \times & \times & \cdot \\
    0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
    \hline
    m/k & 0 & 1 & 2 & 3 & 4 & 5 & 6
    \end{array}
    $$
  - If we draw a vertex at $(p/2, a/2)$ and draw a triangle from the origin, then only the $\times$ are in the triangle (we don't count the points on the boundary)

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor = \#\text{ of lattice points inside the triangle} \triangleq T(p, q)$$

Theorem 8.7. *Let p be an odd prime. Then*

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

Proof. Want to use Gauss' Criterion, so we compute $\mu(2,p)$. We know that for $1 \le k \le \frac{p-1}{2}$, $2 \le 2k \le p-1$. So $2k \pmod p = 2k$. So

$$\begin{aligned}
\mu(2,p) &= \left|\left\{1 \le k \le \frac{p-1}{2} : 2k > \frac{p-1}{2}\right\}\right| \\
&= \left|\left\{1 \le k \le \frac{p-1}{2}\right\} : k > \frac{p-1}{4}\right| \\
&= \left|\left\{\frac{p-1}{4} < k \le \frac{p-1}{2}\right\}\right|
\end{aligned}$$

Case 1: $p \equiv 1 \pmod 4$. So $\frac{p-1}{4}$ is an integer and

$$\begin{aligned}
\mu(2,p) &= \left|\left\{\frac{p-1}{4} < k \le \frac{p-1}{2}\right\}\right| \\
&= \frac{p-1}{2} - \frac{p-1}{4} \\
&= \frac{p-1}{4}
\end{aligned}$$

Case 2: $p \equiv 3 \pmod 4$. Then $\frac{p-1}{4} = \frac{p-3}{4} + \frac{1}{2}$. So $\frac{p-1}{4} < k \iff \frac{p-3}{4} + 1 \le k$. Hence

$$\begin{aligned}
\mu(2,p) &= \left|\left\{\frac{p-3}{4} + 1 \le k \le \frac{p-1}{2}\right\}\right| \\
&= \frac{p-1}{2} - \left(\frac{p-3}{4} + 1\right) + 1 \\
&= \frac{3p-2}{4} - \frac{p-3}{4} \\
&= \frac{p+1}{4}
\end{aligned}$$

Now to finish, we need to compute $(-1)^{\mu(2,p)}$. This is a condition on $p \pmod 8$ and there are 4 cases to consider:

Case 1: $p \equiv 1 \pmod 8$. This gives $p \equiv 1 \pmod 4$ so $\mu(2,p) = \frac{p-1}{4}$, which is *even*.

Case 2: $p \equiv 5 \pmod 8$. This gives $p \equiv 1 \pmod 4$ so $\mu(2,p) = \frac{p-1}{4}$, which is *odd*.

Case 3: $p \equiv 3 \pmod 8$. This gives $p \equiv 3 \pmod 4$ so $\mu(2,p) = \frac{p+1}{4}$, which is *odd*.

Case 4: $p \equiv 7 \pmod 8$. This gives $p \equiv 3 \pmod 4$ so $\mu(2,p) = \frac{p+1}{4}$, which is *even*.

Notice that being 1 or 3 mod 4 only gives integrality, only mod 8 gives parity.

□

Theorem 8.8 (Quadratic Reciprocity)**.** *Let p, q be distinct odd primes. Then*

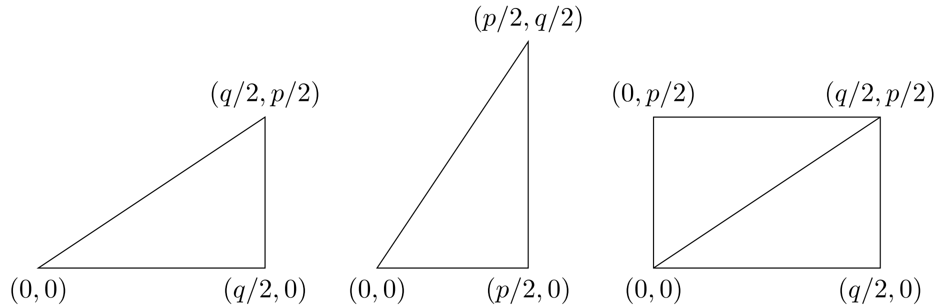
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Proof.

$$\begin{aligned}
\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\mu(p,q)}(-1)^{\mu(q,p)} \\
&= (-1)^{\mu(p,q)+\mu(q,p)} \\
&= (-1)^{T(p,q)+T(q,p)}
\end{aligned}$$

From the triangle argument, we can use some symmetry:

- For $T(p, q)$, the hypotenuse is $y = \frac{p}{q}x$
- For $T(q, p)$, the hypotenuse is $y = \frac{q}{p}x$
- They have reciprocal slopes, and their side lengths are the same
- Can "click" the two triangles together to form a rectangle



- The rectangle has height and width $p/2$ and $q/2$
- Observe that no lattice points lie on the diagonal

Hence $T(p, q) + T(q, p)$ is the number of interior points of the rectangle, which is $\frac{p-1}{2} \cdot \frac{q-1}{2}$

$\square$

Example: let p be an odd prime, $p \neq 5$. When is $x^2 \equiv 5 \pmod{p}$ solvable?

- Compute $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)(-1)^{\frac{p-1}{2}\cdot\frac{5-1}{2}} = \left(\frac{p}{5}\right)$
- $1^2 \equiv 1, 2^2 \equiv 4 \pmod{5}$. Therefore $\left(\frac{p}{5}\right)$ is -1 if $p \equiv 2, 3 \pmod{5}$; 1 if $p \equiv 1, 4 \pmod{5}$

Example: compute $\left(\frac{7}{p}\right)$

- $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)(-1)^{\frac{p-1}{2}\frac{7-1}{2}} = \left(\frac{p}{7}\right)(-1)^{\frac{p-1}{2}}$
- $\frac{p-1}{2}$ is governed by a mod 4 condition; $\left(\frac{p}{7}\right)$ is governed by a mod 7 condition; CRT tells us that the product is governed by a mod 28 condition
- $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 2 \pmod{7}$. Therefore $\left(\frac{p}{7}\right)$ is 1 if $p \equiv 1, 2, 4 \pmod{7}$; -1 if $p \equiv 3, 5, 6 \pmod{7}$
- $(-1)^{\frac{p-1}{2}}$ is 1 if $p \equiv 1 \pmod{4}$; -1 if $p \equiv 3 \pmod{4}$
- The product is 1 if the two are the same; -1 if the two are different

9 Sums of Two Squares

Overarching question: which primes can be written as a sum of 2 squares? i.e. $p = x^2 + y^2;\ x, y \in \mathbb{Z}$

- If $p = 2$, we can do $2 = 1^2 + 1^2$
- We are interested in the odd p case

Lemma 9.1. *If p is an odd prime and $p = x^2 + y^2$, then $p \equiv 1 \pmod 4$.*

Proof. Working mod 4:

x	0	1	2	3
x^2	0	1	0	1

So $x^2 + y^2 \equiv 0, 1, 2 \pmod 4$ (2 comes from $1 + 1$). But p is odd, so $p \equiv 1 \pmod 4$ □

- Recall
$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \end{cases}$$
- If $p \equiv 1 \pmod 4$, there is some a with $a^2 \equiv -1 \pmod p$, or equivalently, $p \mid a^2 + 1$, which we can write $a^2 + 1^2 = pk$ for some $k \in \mathbb{Z}$

Lemma 9.2. $(u^2 + v^2)(A^2 + B^2) = (vA - uB)^2 + (uA + vB)^2$

Lemma 9.3. *If $x^2 + y^2 = zw^2$, then z is a sum of squares if $w \mid x$ and $w \mid y$, i.e.*
$$z = \left(\frac{x}{w}\right)^2 + \left(\frac{y}{w}\right)^2$$

Lemma 9.4. *If we can write $A^2 + B^2 = pk$ for some $1 \le k < p$, then we can write $x^2 + y^2 = p$.*

Proof. (by descent procedure) Input: write $A^2 + B^2 = pk$, $1 \le k < p$

1. If $k = 1$, $A^2 + B^2 = p$. End.
2. Find $-k/2 \le u, v \le k/2$, with $u \equiv A \pmod k$ and $v \equiv B \pmod k$
   - By division algorithm, A and B are congruent to some u, v modulo k
3. Notice $u^2 + v^2 \equiv A^2 + B^2 \equiv 0 \pmod k$. So write $u^2 + v^2 = kt$
   - $kt = u^2 + v^2 \le k^2/4 + k^2/4 = k^2/2$
   - This means $t \le k/2 < k$
   - Because k, u^2, v^2 are nonnegative, $t \ge 0$
   - Suppose for a contradiction that t is 0, then $u, v = 0$, so $k \mid A$ and $k \mid B$. Since $A^2 + B^2 = pk$, we get $A = ka, B = kb$ for some a, b. So $k^2(a^2 + b^2) = A^2 + B^2 = pk$. So $k \mid p$, which means $k = 1$, which contradicts the fact that we did not halt on step 1
   - Therefore $t \ge 1$
4. Multiply $k^2pt = kt \cdot pk = (u^2 + v^2)(A^2 + B^2) = (vA - uB)^2 + (uA + vB)^2$
5. Notice $k \mid (vA - uB)$ and $k \mid (uA + vB)$, so $pt = \left(\frac{vA - uB}{k}\right)^2 + \left(\frac{uA + vB}{k}\right)^2$
   - $vA - uB \equiv BA - AB \equiv 0 \pmod k$
   - $uA + vB \equiv A^2 + B^2 \equiv 0 \pmod k$

□

Theorem 9.5. *If $p \equiv 1 \pmod 4$, then $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.*

Proof. We know that we can write $a^2 + 1^2 = pk$ for some $a \in \mathbb{Z}$ and $1 \le k < p$. Apply the descent procedure until it terminates with $p = x^2 + y^2$.

□

10 Arithmetic Functions

Example: let $W(n)$ be the number of prime divisors of n

- $W(3) = 1$
- $W(12) = 2$

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

Def. An arithmetic function f is **multiplicative** if two conditions are satisfied:

1. $f(1) = 1$
2. If $\gcd(n, m) = 1$, then $f(nm) = f(n)f(m)$

- E.g. Euler's phi function is multiplicative

Theorem 10.1. *Let f be multiplicative. For $n > 1$, $n = p_1^{k_1} \cdots p_n^{k_n}$. Then $f(n) = f(p_1^{k_1}) \cdots f(p_n^{k_n})$*

Proof. WTS by induction if $m_1, \ldots, m_t$ are pairwise coprime, then $f(m_1 \cdots m_t) = f(m_1) \cdots f(m_t)$. The idea is that since m_1 is coprime to all of $m_2, \ldots, m_t$, we can pull out m_1. Then we can pull out m_2, and so on. $\square$

Def. An arithmetic function f is **totally multiplicative** if two conditions are satisfied:

1. $f(1) = 1$
2. $f(nm) = f(n)f(m)$ (no coprime assumption)

- E.g. the Legendre symbol $\left(\frac{\cdot}{n}\right)$ is totally multiplicative

Theorem 10.2. *Let f be totally multiplicative. For $n > 1$, $n = p_1^{k_1} \cdots p_n^{k_n}$. Then $f(n) = f(p_1)^{k_1} \cdots f(p_n)^{k_n}$*

Theorem 10.3. *Let $n, m \in \mathbb{N}$ where $\gcd(n, m) = 1$. For every positive divisor $d \mid nm$, there exists unique positive divisors $d_1 \mid n$, $d_2 \mid m$ such that $d = d_1 d_2$.*

Proof. Take $d_1 = \gcd(d, n)$. Then $d_1 \mid n$. Take $d_2 = d/d_1$. Then $d = d_1 d_2$. To show that $d_2 \mid m$, by gcd property $\gcd(d/d_1, n/d_1) = 1$. The first term is d_2 and so it's coprime to n/d_1. Since $d_1 d_2 = d \mid nm$, we have $d_2 \mid nm/d_1 = m$ because d_2 is coprime to n/d_1.

For uniqueness, suppose there exists $e_1 \mid n$, $e_2 \mid m$ with $d = e_1 e_2$. Then $d_1 d_2 = d = e_1 e_2$. Observe if a, b are coprime, then divisors of a and divisors of b are coprime by prime factorization. This means $\gcd(e_1, d_2) = 1$. Since $e_1 \mid d_1 d_2$, we have $e_1 \mid d_1$. By symmetry $d_1 \mid e_1$, and so $e_1 = \pm d_1$. Since they are all positive, we have $e_1 = d_1$. By symmetry $e_2 = d_2$. $\square$

- Observe that there is a bijection

$$\{\text{positive divisors of } n\} \times \{\text{positive divisors of } m\} \to \{\text{positive divisors of } nm\}$$
$$(d_1, d_2) \mapsto d_1 d_2$$

Lemma 10.4. *$\tau(n)$ and $\sigma(n)$ are multiplicative, where $\tau(n) = \sum_{d \mid n} 1$ is the number of divisors of n, and $\sigma(n) = \sum_{d \mid n} d$ is the sum of divisors of n*

Proof. $\tau(1) = \sigma(1) = 1$ because 1 is the single divisor of 1. Now take n, m to be coprime.

$$\begin{aligned}
\tau(nm) &= \sum_{d|nm} 1 \\
&= \sum_{d_1|n} \sum_{d_2|m} 1 && \text{By previous theorem} \\
&= \sum_{d_1|n} 1 \sum_{d_2|m} 1 && \text{Since multiplication and addition distribute over one another} \\
&= \tau(n)\tau(m) \\
\sigma(nm) &= \sum_{d|nm} d \\
&= \sum_{d_1|n} \sum_{d_2|m} d_1 d_2 && \text{By previous theorem, also because } d = d_1 d_2 \\
&= \sum_{d_1|n} d_1 \sum_{d_2|m} d_2 \\
&= \sigma(n)\sigma(m)
\end{aligned}$$

□

Lemma 10.5 (Generative series)**.**

$$\left(\sum_{n=0}^{\infty} a_n z^n\right)\left(\sum_{m=0}^{\infty} b_m z^m\right) = \sum_{k=0}^{\infty}\left(\sum_{i+j=k} a_i b_j\right) z^k$$

- We consider the series to be absolutely convergent
- Riemann zeta function:
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$
- Dirichlet series:
$$\begin{aligned}
D(s) &= \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \\
E(s) &= \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \\
D(s)E(s) &= \sum_{n=1}^{\infty} \underbrace{\left(\sum_{ab=n} f(a)g(b)\right)}_{\sum_{d|n} f(d)g(n/d)} \frac{1}{n^s} && \text{Inside the parentheses is called } \textbf{Dirichlet convolution}
\end{aligned}$$

Def. **Dirichlet convolution** is an arithmetic function $f * g$ defined by $(f * g)(n) = \sum_{d|n} f(d)g(n/d)$

- E.g. $(1 * 1)(n) = \sum_{d|n} 1(d)1(n/d) = \sum_{d|n} 1 = \tau(n)$ (1 is the constant function that always output 1)
- E.g. $(I * 1)(n) = \sum_{d|n} I(d)1(n/d) = \sum_{d|n} d = \sigma(n)$ (I is the identity function)

Theorem 10.6. *If f, g are multiplicative, then $f * g$ is multiplicative.*

Proof. $(f * g)(1) = \sum_{d|1} f(d)g(1/d) = f(1)g(1) = 1$. Now let n, m be coprime. Then

$$\begin{aligned}
(f * g)(nm) &= \sum_{d|nm} f(d)g\left(\frac{nm}{d}\right) \\
&= \sum_{d_1|n} \sum_{d_2|n} f(d_1 d_2) g\left(\frac{n}{d_1} \cdot \frac{m}{d_2}\right) \\
&= \sum_{d_1|n} \sum_{d_2|m} f(d_1) f(d_2) g\left(\frac{n}{d_1}\right) g\left(\frac{m}{d_2}\right) && n, m \text{ coprime implies their divisors coprime} \\
&= \sum_{d_1|n} f(d_1) g\left(\frac{n}{d_1}\right) \sum_{d_2|m} f(d_2) g\left(\frac{m}{d_2}\right) \\
&= (f * g)(n) \cdot (f * g)(m)
\end{aligned}$$

□

- Follow-up question: since $f * g$ is a "product", is there a "division"?
- Define $i(n) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{elsewise} \end{cases}$

Lemma 10.7. *If f is an arithmetic function, then $f * i = f$.*

Proof.

$$\begin{aligned}
(f * i)(n) &= \sum_{d|n} f(d) i\left(\frac{n}{d}\right) \\
&= f(n) \cdot 1 && \text{Since all } d \neq n \text{ terms vanish} \\
&= f(n)
\end{aligned}$$

□

- Now we want to know whether given f, can we find a g such that $f * g = i$
- E.g. $f = 1$ the constant function. For g to be an inverse, we need $1 * g = i$; or equivalently, $\sum_{d|n} g(d) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{elsewise} \end{cases}$
  - Plug $n = 1$: $g(1) = 1$
  - Plug $n = 2$: $g(1) + g(2) = 0$. This implies $g(2) = -1$
  - Plug $n = 3$: $g(1) + g(3) = 0$. This implies $g(3) = -1$
  - Plut $n = 4$: $g(1) + g(2) + g(4) = 0$. This implies $g(4) = 0$
  - In general, for $n > 1$, $g(n) + \sum_{\substack{d|n \\ d<n}} g(d) = 0$

Def. The **Mobius function** is defined as

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

Lemma 10.8.

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

Proof. The RHS function is i, which is multiplicative. Since $\mu(n)$ is multiplicative, the LHS is also multiplicative. Using the fact that $f = g \iff f(p^k) = g(p^k)$ for all primes, it suffices to check that this equality holds for $n = p^k$, p prime, $n \geq 1$.

$$\begin{aligned} \sum_{d|p^k} \mu(d) &= \sum_{j=0}^{k} \mu(p^j) \\ &= \sum_{j=0}^{1} \mu(p^j) && \text{Since all non-square-free terms are 0} \\ &= \mu(1) + \mu(p) \\ &= 1 + (-1) \\ &= 0 \end{aligned}$$

□

Theorem 10.9 (Mobius Inversion Formula). *Let f, g be arithmetic functions. Then*

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

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

$$\begin{aligned} \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right) &= \sum_{d|n} \left(\sum_{e|d} g(e)\right) \mu\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \sum_{e|d} g(e)\mu\left(\frac{n}{d}\right) \\ &= \sum_{e|n} g(e) \sum_{d|n,\, e|d} \mu\left(\frac{n}{d}\right) \\ &= \sum_{e|n} g(e) \sum_{d'|n/e} \mu\left(\frac{n}{ed'}\right) && \text{Write } d = ed' \text{ so } d \mid n,\ e \mid d \implies d' \mid n/e \\ &= \sum_{e|n} g(e) \sum_{d'|n/e} \mu\left(\frac{n/e}{d'}\right) \\ &= \sum_{e|n} g(e) i\left(\frac{n}{e}\right) \\ &= g(n) \end{aligned}$$

" $\Longleftarrow$ " Follows from a similar argument.

□

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

11 Probability

Question: if I pick two positive integers n, m *at random*, how *likely* is it that they are coprime?

- How do we pick two positive integers at random?

Question: If I pick two positive integers n, m at random from $\{1, 2, \dots, N\}$, how likely is it that they are coprime?

- $\Pr(A \text{ happens}) = \frac{\#\text{ of outcomes where } A \text{ happens}}{\#\text{ of outcomes}}$
- If we call this probability p_N, then the limit $\lim_{N\to\infty} p_N$ (if it exists) is the answer to the first question
- E.g. estimate p_{100}

Size	**Probability**
40	0.5
100	0.494
1000	0.639
10000	0.609

- Compute p_N
  - Total # outcomes = total number of pairs $(n, m) \quad = \quad N^2$
  - Total # pairs n, m such that $\gcd(n, m) = 1 \quad = \quad \sum_{\substack{n,m\le N\\ \gcd(n,m)=1}} 1$
- Recall Lemma 10.8

$$\underbrace{\sum_{d\mid M}\mu(d) = \begin{cases}1, & \text{if } M = 1\\ 0, & \text{elsewise}\end{cases}}_{\text{Lemma 10.8}} \implies \sum_{d\mid\gcd(n,m)}\mu(d) = \begin{cases}1, & \text{if } \gcd(n,m) = 1\\ 0, & \text{elsewise}\end{cases}$$

- Then

$$\begin{aligned}\sum_{\substack{n,m\le N\\ \gcd(n,m)=1}} 1 &= \sum_{n,m\le N}\sum_{d\mid\gcd(n,m)}\mu(d)\\ &= \sum_{d\le N}\mu(d)\,(\#\text{ of pairs } (n,m) \text{ with } d\mid n \text{ and } d\mid m)\\ &= \sum_{d\le N}\mu(d)\left\lfloor\frac{N}{d}\right\rfloor^2 \qquad \text{Because } \#\text{ integer between 1 and } N \text{ divisible by } d \text{ is } \left\lfloor\frac{N}{d}\right\rfloor\\ &= \sum_{d\le N}\mu(d)\left(\frac{N}{d} - \left\{\frac{N}{d}\right\}\right)^2\\ &= \sum_{d\le N}\mu(d)\left(\frac{N^2}{d^2} - 2\frac{N}{d}\left\{\frac{N}{d}\right\} + \left\{\frac{N}{d}\right\}^2\right) \qquad (*)\end{aligned}$$

- Notice that

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

  Therefore

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

- Back to (*):

$$\sum_{\substack{n,m\le N\\ \gcd(n,m)=1}} 1 = \sum_{d\le N}\mu(d)\left(\frac{N^2}{d^2} - 2\frac{N}{d}\left\{\frac{N}{d}\right\} + \left\{\frac{N}{d}\right\}^2\right) \tag{*}$$

$$= \sum_{d\le N}\mu(d)\frac{N^2}{d^2} + \mathcal{O}\left(N\sum_{d\le N}\frac{1}{d}\right)$$

$$= N^2\sum_{d\le N}\frac{\mu(d)}{d^2} + \mathcal{O}\left(N\sum_{d\le N}\frac{1}{d}\right)$$

$$= N^2\sum_{d\le N}\frac{\mu(d)}{d^2} + \mathcal{O}\left(N\log N\right)$$

- Now we can compute p_N:

$$p_N = \frac{\sum\limits_{\substack{n,m\le N\\ \gcd(n,m)=1}} 1}{N^2}$$

$$= \sum_{d\le N}\frac{\mu(d)}{d^2} + \mathcal{O}\left(\frac{\log N}{N}\right)$$

- As we take $N \to \infty$,

$$p_N \to \sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} = \frac{6}{\pi^2}$$

Theorem 11.1 (Basel Problem)**.**

$$\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$$

Theorem 11.2 (Probability of coprimality)**.**

$$\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} = \frac{6}{\pi^2}$$

Proof. Notice that

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}\cdot\sum_{n=1}^{\infty}\frac{1}{n^s} = \sum_{n=1}^{\infty}\frac{(\mu * 1)(n)}{n^s} = 1 \qquad \text{1 is the constant function 1}$$

Knowing that $\sum\limits_{n=1}^{\infty}\frac{1}{n^s} = \zeta(s)$, we have the other sum as $\frac{1}{\zeta(s)}$. Knowing that $\zeta(2) = \frac{\pi^2}{6}$ (Basel problem) completes the proof.

□

Observe that

$$\prod_{p\text{ prime}}\frac{1}{1-1/p} = \prod_{p}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)$$

$$= \left(1+\frac{1}{2}+\frac{1}{2^2}+\cdots\right)\left(1+\frac{1}{3}+\frac{1}{3^2}+\cdots\right)\cdots$$

$$= \sum_{n=1}^{\infty}\frac{1}{n}$$

- If there are finitely many primes, then LHS would be a finite product, however the RHS diverges to infinity

Lemma 11.3. *If f is multiplicative, then*

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

If f is totally multiplicative, then

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

Notice that

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

Going back to the previous chapter, we have

$$\frac{6}{\pi^2} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \prod_p \left(1 - \frac{1}{p^2}\right)$$

- Each of the product terms is the probability that n, m are not both divisible by p

Question: If I pick two positive integers n, m at random, how likely is it that $m \mid n$?

- Start with the question

$$q_N = \frac{\#\text{ of } (n,m) \text{ with } n, m \le N \text{ where } m \mid n}{N^2}$$

- E.g. if $N = 10$, try to count pairs

$(1, m)$	$\tau(1)$ pairs
$(2, m)$	$\tau(2)$ pairs
$\vdots$	$\vdots$
$(10, m)$	$\tau(10)$ pairs

- Then

$$\begin{aligned}\sum_{\substack{n,m \le N \\ m \mid n}} 1 &= \sum_{n \le N} \sum_{\substack{m \le N \\ m \mid n}} 1 \\ &= \sum_{n \le N} \sum_{m \mid n} 1 \\ &= \sum_{n \le N} \tau(n)\end{aligned}$$

- Knowing that $\frac{1}{N} \sum\limits_{n \le N} \tau(n) \approx \log N$ from homework, we have

$$q_N = \frac{\sum\limits_{n \le N} \tau(n)}{N^2} \approx \frac{\log N}{N} \to 0 \qquad \text{as } N \to \infty$$

12 Fermat's Last Theorem

Pythagorean equation: find solutions to $x^2 - y^2 = z^2$ with $\gcd(x,y,z) = 1$

- This is equivalent to $\gcd(x,y) = \gcd(x,z) = \gcd(y,z) = 1$
- This means exactly 2 of x, y, z are odd, let x, z be odd and y even
- Then $(x-y)(x+y) = z^2$
- Observe that

$$\begin{aligned}
\gcd(x-y, x+y) &= \gcd(x-y, 2y) && \text{Since } x+y = x-y+2y \text{ and } \gcd(a,b) = \gcd(a, b+at) \\
&= \gcd(x-y, y) && \text{Since } x-y \text{ is odd} \\
&= \gcd(x,y) && \text{Since } x = x-y+y \\
&= 1
\end{aligned}$$

- Writing $z = p_1^{k_1} \cdots p_r^{k_r}$, then

$$z^2 = p_1^{2k_1} \cdots p_r^{2k_r}$$

so

$$(x-y)(x+y) = p_1^{2k_1} \cdots p_r^{2k_r}$$

- As a result, there are coprime odd s and t with

$$\begin{aligned}
x - y &= s^2 & & x = \frac{(x+y)+(x-y)}{2} = \frac{s^2+t^2}{2} \\
x + y &= t^2 & \implies \quad & y = \frac{(x+y)-(x-y)}{2} = \frac{t^2-s^2}{2} \\
z &= st & & z = st
\end{aligned}$$

- Writing $x^2 = y^2 + z^2$, we found all solutions to the Pythagorean equation

Consider $x^3 + y^3 = z^3$ with $\gcd(x,y,z) = 1$

$$\begin{aligned}
x^3 &= y^3 - z^3 \\
&= (y-z)(y^2 + yz + z^2)
\end{aligned}$$

- At this step, we're stuck

Back to Pythagoras

$$\begin{aligned}
&x^2 + y^2 = z^2 \\
&x^2 - (iy)^2 = z^2 && \text{Since } i^2 = -1 \\
&(x-iy)(x+iy) = z^2
\end{aligned}$$

- We are now working with the Gaussian integers $\mathbb{Z}[i]$

Back to the cubic case

- Take $\omega = e^{2\pi i/3}$, where $\omega^3 = 1$ and $\omega \neq 1$ (3rd root of unity)

$$x^3 - 1 = (x-1)(x^2+x+1)$$

  ω is a root of the LHS. ω is not a root of $(x-1)$. Therefore ω is a root of x^2+x+1.

- Now

$$
\begin{aligned}
z^3 &= x^3 + y^3 \\
&= (x+y)(x+\omega y)(x+\omega^2 y)
\end{aligned}
$$

- Since ω is not a Gaussian integer, we're now working with the Eisenstein integers $\mathbb{Z}[\omega]$
- Both the Gaussian and Eisenstein integers have *unique factorization*
- For an odd prime p, there is $\zeta_p = e^{2\pi i/p}$ with $\zeta_p^p = 1$ and $\zeta_p^{p-1}, \zeta_p^{p-2}, \ldots, \zeta_p^2, \zeta_p \neq 1$

$$
z^p = x^p + y^p = (x+y)(x+\zeta_p y)(x+\zeta_p^2 y)\cdots(x+\zeta_p^{p-1} y)
$$

- We're now working with $\mathbb{Z}[\zeta_p]$, however unique factorization fails in this domain

$$
6 = (1+\sqrt{5})(1-\sqrt{5}) = 2 \cdot 3
$$

  - In equation $x^2 + 5y^2 = z^2$, we would have $(x - \sqrt{-5}y)(x + \sqrt{-5}y) = z^2$, which does not have unique factorization

Theorem 12.1 (Fermat's Last Theorem)**.** *For $n \geq 3$, there are no positive integer solutions to $x^n + y^n = z^n$.*