Math 437 Notes

Henry Xia

December 1, 2017

Contents

1 Divisibility

Consider $a, b \in \mathbb{Z}, a > 0$. There exists uniquely $q, r \in \mathbb{Z}$ such that

$$\begin{cases} b = aq + r \\ 0 \leq r < a \end{cases}$$

Corollary 1.0.1. $a \mid b \iff r = 0$.

Definition 1.1. Let $a, b \in \mathbb{Z}$, not both 0. Then there exists a finite set of common divisors of both a and b. Denote greatest common divisor of a and b as $\gcd(a, b) = (a, b)$.

Proposition 1.1. Let $D = \gcd(a, b)$, then

1. if $d \mid a$ and $d \mid b$, then $d \mid D$.
2. D is the least positive integer of the form $ax + by$, for some $x, y \in \mathbb{Z}$.

Proof of (2) $\implies$ (1). $D = ax_0 + by_0, d \mid ax_0 + by_0 = D$

Proof of (2). Let $S = \{ax + by > 0 : x, y \in \mathbb{Z}\}$. Clearly S is nonempty. Let $s = \min S$. Since $D \mid ax + by$, so $D \mid s \implies D \leq s$.
Claim: $s \mid a$ and $s \mid b$. It suffices to prove $s \mid a$. We divide a by s so that $a = sq + r$ and $0 \leq r < s$. It suffices to prove that $r = 0$. Since a is a linear combination of a and b, and s is a combination of a and b, then $r = a - sq$ must be a combination of a and b. But $r < s$ so $r \notin S$ so r cannot be positive. Therefore $r = 0$.

Now since $s \mid a$ and $s \mid b$, then $s \mid D \implies s \leq D$. Therefore $s = D$. □

Proposition 1.2 (i)**.** Let $c \in \mathbb{N}$, then $\gcd(ac, bc) = c \gcd(a, b)$.

Proposition 1.3 (ii)**.** Let $d \in \mathbb{Z}$ s.t. $d \mid a$ and $d \mid b$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \gcd(a, b)/d$.

Proof of (1) $\implies$ (2). $d \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \gcd(a, b)$

Proof of (1). $\gcd(ac, bc) =$ least positive integer of the form $acx + bcy$
$= c$(least positive integer of the form $ax + by$) $= c \gcd(a, b)$. □

Proposition 1.4. $\gcd(a, b) = \gcd(\pm a, \pm b) = \gcd(a, b + ac)$ for any $c \in \mathbb{Z}$.

Proof. Any linear combination of a and b is a linear combination of a and $b + ac$ since $ax + (b + ac)y = a(x + cy) + by$.

Proof. $\begin{bmatrix} a \\ b + ac \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 \\ -c & 1 \end{bmatrix}$. This is a reversible transformation. □

Corollary 1.0.2. *We can use the Euclidean Algorithm to find* $\gcd(a, b)$ *and write* $\gcd(a, b)$ *as a linear combination of* a *and* b.

1.1 Greatest Common Divisor

Definition 1.2. Let $a_1, \dots, a_n \in \mathbb{Z}$, not all 0. We define $\gcd(a_1, \dots, a_n)$ to be the greatest common divisor of all a_i.

Property 1.1 (i)**.** If $d \mid a_i$ for $i = 1, \dots, n$, then $d \mid \gcd(a_1, \dots, a_n)$.

Property 1.2 (ii)**.** $\gcd(a_1, \dots, a_n)$ is the least positive integer which can be written as $\sum_{i=1}^{n} a_i x_i$ for $x_i \in \mathbb{Z}$.

Theorem 1.1. *If $(a, b) = 1$ and $(a, c) = 1$, then $(a, bc) = 1$.*

Proof. Since $(a, b) = 1, \exists x, y \in \mathbb{Z}$ such that $ax + by = 1$. Also, $\exists z, t \in \mathbb{Z}$ such that $az + ct = 1$.

$$(ax + by)(az + ct) = 1 \implies a(axz + xct + zby) + bc(yt) = 1 \implies \gcd(a, bc) = 1.$$

□

Theorem 1.2. *If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.*

Proof. $\exists x, y \in \mathbb{Z}$ such that $ax + by = 1 \mid c \implies acx + bcy = c$. Since $a \mid acx$ and $a \mid bcy$, then $a \mid c$. □

1.2 Least Common Multiple

Definition 1.3. Let $a, b \in \mathbb{Z} \setminus \{0\}$. We define the $\operatorname{lcm}[a, b]$ be the least positive integer which is a common multiple of a and b. Similarly define $\operatorname{lcm}[a_1, \dots, a_n]$.

Proposition 1.5. Let $M = \operatorname{lcm}[a, b]$.

1. If m is a common multiple of a and b, then $M \mid m$.
2. If $c \in \mathbb{N}$, then $\operatorname{lcm}[ac, bc] = c \cdot \operatorname{lcm}[a, b]$.
3. $\gcd(a, b) \cdot \operatorname{lcm}[a, b] = |ab|$.

Proof of 1. We divide m by M to get $m = Mq + r$ such that $0 \leq r < M$. It suffices to prove that $r = 0$. We know $a \mid M \implies Mq$ and $a \mid m$ therefore $a \mid r$. Similarly, $b \mid r$. Therefore r is a common multiple of a and b and we must have $r = 0$ because there does not exist a common multiple of a and b between 1 and $M - 1$ inclusive. □

Proof of 2. Let $M_1 = \operatorname{lcm}[ac, bc]$. We want $M_1 = c \cdot M$. We have $a \mid M \implies ac \mid c \cdot M$ and similarly $bc \mid c \cdot M$. Therefore $M_1 = \operatorname{lcm}[ac, bc] \mid c \cdot M$. We also have $c \mid ac \mid M_1 \implies M_1 = cx$ for some $x \in \mathbb{Z}$. Then $ac \mid M_1 = cx \implies a \mid x$. Similarly $b \mid x$. Then x is a common multiple of a and b so $\operatorname{lcm}[a, b] \mid x \implies c \cdot \operatorname{lcm}[a, b] \mid M_1$. Now we have both $M_1 \mid c \cdot M$ and $c \cdot M \mid M_1$, and $c \cdot M = M_1$. □

Proof of 3. Let $d = (a, b)$ and $M = [a, b]$. Without loss of generality assume $a, b > 0$.
Look at the lcm. $dM = d \operatorname{lcm}[a, b] = \operatorname{lcm}[da, db]$. Since $d \mid a$ and $d \mid b$, then $db \mid ab$ and $da \mid ab$, so $\operatorname{lcm}[da, db] \mid ab \implies dM \mid ab$.
Look at the gcd. $dM = \gcd(a, b)M = \gcd(aM, bM)$. Since $ab \mid aM$ and $ab \mid bM$, then $ab \mid \gcd(aM, bM) \implies ab \mid dM$.
Now we have both $ab \mid dM$ and $dM \mid ab$ so $dM = ab$. □

1.3 Primes

Definition 1.4. An integer $n > 1$ is called prime if its only positive divisors are 1 and itself.

Lemma 1.3. *If $n > 1$ is an integer, then there exists a prime p dividing n.*

Proof. Proof by induction.
Case $n = 2$: obvious.
Case $n > 2$: We assume that the statement holds for all $k = 2, \ldots, N - 1$. Suppose that N is prime, then $N \mid N$ and we are done. Otherwise there exists some integer d such that $1 < d < N$ and $d \mid N$. Since there exists a prime p such that $p \mid d$, we must have $p \mid d \mid N$. □

Theorem 1.4. *There exists infinitely many prime numbers*

Proof. Suppose that there exists only finitely many prime numbers $p_1, \ldots, p_k$. Consider $N = \prod_{i=1}^{k} p_i + 1$. By the lemma, there exists some prime q such that $q \mid N$. Since q is prime, let $q = p_j$. Then $p_j \mid \prod_{i=1}^{k} p_i + 1$ and $p_j \mid \prod_{i=1}^{k} p_i$. It follows that $p_j \mid 1$ and we have a contradiction. □

Proposition 1.6 (i)**.** If p is prime, $a \in \mathbb{Z}$, then $\gcd(a, p) \in \{1, p\}$ and $\gcd(a, p) = p \iff p \mid a$.

Proposition 1.7 (ii)**.** p is prime, $a, b \in \mathbb{Z}$. If $p \mid ab$ then $p \mid a$ or $p \mid b$.

idea for Proof of (i). p only has divisors 1 and p.

Proof of (ii). Assume that $p \nmid a$. Then $\gcd(a, p) = 1$, so $p \mid b$, and we are done. □

Corollary 1.4.1. *If p is prime and $p \mid \prod_{i=1}^{n} a_i$, then $p \mid a_i$ for some $i = a_1, \ldots, a_n$.*

Theorem 1.5 (**Fundamental Theorem of Arithmetic**)**.** *Any integer $n > 1$ can be written uniquely as a product of primes if we disregard the order of factors.*

Proof. **Claim 1**: $n > 1$ can be written as a product of primes.

Proof of Claim 1: Proof by induction. Clearly $n = 2$ works. There exists some integer d such that $1 < d < N$ and $d \mid N$. Then $N = d \cdot \frac{N}{d}$ and we are done.

Claim 2: If p_i and q_j are primes and $p_1 \cdots p_n = q_1 \cdots q_m$, then $n = m$ and there exists a permutation σ of $\{1, \ldots, n\}$ such that $p_i = q_{\sigma(i)}$.

Proof of Claim 2: Assume that there exists some positive integer N that can be written as a product of primes in two ways. That is $p_1 \cdots p_n = q_1 \cdots q_m$. Without loss of generality, assume that $n + m$ is minimum among all possible products of primes. It follows that $p_i \neq q_j$ for $1 \leq i \leq n$ and $1 \leq j \leq m$ because otherwise we can divide both sides by the repeated primes. Then it follows that $p_1 \mid \prod_{i=1}^{n} p_i$ but $p_1 \nmid \prod_{j=1}^{m} q_j$. □

2 Congruences

Definition 2.1. For $m \in \mathbb{Z} \setminus \{0\}$ and $a, b \in \mathbb{Z}$ we say that a is congruent with b modulo m, that is $a \equiv b \pmod{m}$, if $m \mid a - b$.

For $m \in \mathbb{Z} \setminus \{0\}$ and $a \in \mathbb{Z}$, we denote by $\bar{a}$ the residue class of a modulo m.

Property 2.1 (i)**.** $a \equiv a \pmod{m}$.

Property 2.2 (ii)**.** If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

Property 2.3 (iii)**.** if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Property 2.4. Given $m \in \mathbb{N}$, for any $a \in \mathbb{Z}, \exists k \in \{0, 1, \ldots, m-1\}$ such that $\bar{a} = \bar{k}$.

Proof. By the division algorithm, $\exists q \in \mathbb{Z}$ and $k \in \{0, 1, \ldots, m-1\}$ such that $a = mq + k$. This implies $a \equiv k \pmod{m}$. □

Property 2.5. If $d \mid m$ and $a \equiv b \pmod{m}$, then $a \equiv b \pmod{d}$.

Proof. $a \equiv b \pmod{m} \implies m \mid a - b \implies d \mid a - b \implies a \equiv b \pmod{d}$.

Property 2.6. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$.

Proof. $m \mid a - b$ and $m \mid c - d \implies m \mid (a + c) - (b + d)$. □

Property 2.7. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$

Proof. $a \equiv b \pmod{m} \implies a - b = mx$ for some $x \in \mathbb{Z}$, and $c \equiv d \pmod{m} \implies c - d = my$ for some $y \in \mathbb{Z}$. Then $ac = (mx + b)(my + d) = m^2xy + m(dx + by) + bd \implies ac \equiv bd \pmod{m}$. □

Definition 2.2. $\mathbb{Z}/m\mathbb{Z} = \left\{\overline{0}, \overline{1}, ..., \overline{m-1}\right\}$ is a complete set of residues modulo m.

Definition 2.3. We say that $a \in \mathbb{Z}$ is invertible modulo $m \in \mathbb{Z} \setminus \{0\}$ if there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$.

Definition 2.4. $(\mathbb{Z}/m\mathbb{Z})*$ is the set of residues $\bar{i}$ such that $\bar{i}$ is invertible.

Proposition 2.1. Let $m_1, \ldots, m_r \in \mathbb{Z} \setminus \{0\}$, then $x \equiv y \pmod{m_i}$ for $i = 1, \ldots, r$ if and only if $x \equiv y \pmod{\text{lcm}[m_1, \ldots, m_r]}$.

Proposition 2.2. $ax \equiv ay \pmod{m} \iff x \equiv y \pmod{\frac{m}{\gcd(a,m)}}$.

Proof. Let $d = \gcd(a, m)$. Then $a = da_1$ and $m = dm_1$ and $\gcd(a_1, m_1) = 1$. It follows that

$$\begin{aligned} ax \equiv ay \pmod{m} &\iff m \mid a(x - y) \\ &\iff dm_1 \mid da_1(x - y) \\ &\iff m_1 \mid a_1(x - y) \\ &\iff m_1 \mid x - y \iff x \equiv y \pmod{m_1}. \end{aligned}$$

Proposition 2.3. Let $f \in \mathbb{Z}[x]$. If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

Proof. Write $f(x) = \sum_{i=0}^{r} c_i x^i$. Then

$$f(a) \equiv f(b) \pmod{m} \iff \sum_{i=0}^{r} c_i a^i \equiv \sum_{i=0}^{r} c_i b^i \pmod{m}.$$

It suffices to show $a^i \equiv b^i \pmod{m}$.

Let $N = \overline{a_n a_{n-1} ... a_0} = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0$ where $a_i \in \{0, \ldots, 9\}$.

- $2 \mid N \iff 2 \mid a_0$.
- $4 \mid N \iff 4 \mid 10a_1 + a_0 = \overline{a_1 a_0}$.
- $5 \mid N \iff 5 \mid a_0$.
- $3 \mid N \iff 3 \mid \sum a_i$ because $10 \equiv 1 \pmod{3} \implies 10^k \equiv 1 \pmod{3}$.
- $9 \mid N \iff 9 \mid \sum a_i$ similarly to 3.
- $11 \mid N \iff 11 \mid \sum (-1)^i a_i$ similarly to 9.

2.1 Fermat's Little Theorem, Euler's Theorem, Wilson's Theorem

Theorem 2.1 (Fermat's (Little) Theorem)**.** *Let p be a prime and $a \in \mathbb{Z}$ such that* $\gcd a, p = 1$*. Then a is invertible modulo p and $a^{p-1} \equiv a \pmod{p}$.*

Proof. Let $S = \left\{\overline{1}, \overline{2}, ..., \overline{p-1}\right\}$. Let $f_a : S \to S$ such that $f_a(\overline{k}) = \overline{ak}$. This is well defined because $p \nmid a$ and $p \nmid k$, then p cannot divide ak.
Claim: f_a is bijective.
It suffices to prove that f_a is injective. This is true because

$$\overline{ai} = \overline{aj} \implies p \mid ai - aj \implies p \mid i - j \implies \overline{i} = \overline{j}.$$

Since $p \nmid (p-1)!$, it follows that from the claim that

$$\overline{1} \cdot \overline{2} \cdots \overline{p-1} = \overline{a \cdot 1} \cdot \overline{a \cdot 2} \cdots \overline{a \cdot (p-1)} \implies (p-1)! \equiv (p-1)! \cdot a^{p-1} \pmod{p}.$$

Then $a^{p-1} \equiv 1 \pmod{p}$. $\square$

Definition 2.5. Let $m \in \mathbb{N}$. Then Euler's function $\phi(m)$ is the cardinality of $\{0 \leq i < m : \gcd(i, m) = 1\}$.

- $\phi(1) = 1$.
- If p is prime, then $\phi(p) = p - 1$.
- If p is prime, then $\phi(p^n) = p^n - p^{n-1}$.

Theorem 2.2 (Euler's Theorem)**.** *Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that* $\gcd(a, m) = 1$*. Then*

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

Proof. Let $S = \left\{\overline{i} : 0 \leq i \leq m-1, \gcd(i, m) = 1\right\}$. Then $\phi(m) = \#S$.

Let $f_a : S \to S$ defined by $f_a(\overline{i}) = \overline{a \cdot i}$. This function is well defined because

$$\gcd(i, m) = 1 \text{ and } \gcd(a, m) = 1 \implies \gcd(a \cdot i, m) = 1.$$

Now we prove that f_a is bijective (it suffices to prove that f_a is injective). Observe that

$$f_a(\overline{i}) = f_a(\overline{j}) \implies a \cdot i \equiv a \cdot j \pmod{m} \implies m \mid a(i-j) \implies m \mid (i-j).$$

It follows that $\overline{i} = \overline{j}$ and f_a must be bijective.

Now let $P = \prod_{k \in S} k$. Observe that P is coprime with m because each $k \in S$ is coprime with m. Then

$$P \cdot a^{\phi(m)} \equiv P \pmod{m} \implies a^{\phi(m)} \equiv 1 \pmod{m}.$$

$\square$

Theorem 2.3 (Wilson's Theorem)**.** *Let p be a prime. Then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. We claim that $\forall i \in \{2, \ldots, p-2\}, \exists! j \in \{2, \ldots, p-2\}$ such that $ij \equiv 1 \pmod{p}$, and $i \neq j$.

First we check that the inverse of i cannot be 1 or -1. If $j = 1$, then $ij \equiv i \pmod{p} \implies i \equiv 1 \pmod{p}$. If $j = -1$, then $ij \equiv -i \implies i \equiv p - 1 \pmod{p}$.

Now $j \neq i$ because if $j = i$, then $i^2 \equiv 1 \pmod{p} \implies p \mid (i-1)(i+1)$. Contradiction.

It follows that

$$(p-1)! = (1 \cdot (p-1)) \cdot (i_1 \cdot j_1) \cdots (i_{\frac{p-3}{2}} \cdot j_{\frac{p-3}{2}}) \equiv -1 \pmod{p}.$$

$\square$

Proposition 2.4 (i)**.** If $p \equiv 1 \pmod{4}$ is prime, then

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

Proposition 2.5 (ii)**.** If $p \equiv 3 \pmod{4}$ is prime, then

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

Proof. Wilson's Theorem gives

$$\begin{aligned}
(p-1)! &\equiv -1 \pmod{p} \\
1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2}\right) \cdots (p-1) &\equiv -1 \pmod{p} \\
\left(\frac{p-1}{2}\right) \cdot (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right) &\equiv -1 \pmod{p}
\end{aligned}$$

If $p \equiv 1 \pmod{4}$, then $\frac{p-1}{2}$ and the result follows. If $p \equiv 3 \pmod{4}$, then $\frac{p-1}{2}$ is odd and the result follows. $\square$

2.2 Sum of two squares

Theorem 2.4 (i)**.** *If $p \equiv 1 \pmod{4}$, then there exists 2 distinct residue classes $\overline{x}$ such that $x^2 \equiv -1 \pmod{p}$.*

Theorem 2.5 (ii)**.** *If $p \equiv 3 \pmod{4}$, then there exists no integer x such that $x^2 \equiv -1 \pmod{p}$.*

Proof of (i). There exists two residue classes $\overline{\pm\left(\frac{p-1}{2}\right)!}^2 \equiv -1 \pmod{p}$. These are the only two residue classes.

If $x^2 \equiv y^2 \pmod{p}$, then $(x-y)(x+y) \equiv 0 \pmod{p}$ so $x \equiv y \pmod{p}$ and $x \equiv -y \pmod{p}$. $\square$

Proof of (ii). Assume $\exists x \in \mathbb{Z}$ such that $x^2 \equiv -1 \pmod{p}$. This implies $\gcd(x, p) = 1$. Therefore

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

because $\frac{p-1}{2}$ is odd. $\square$

Corollary 2.5.1. *Let $p \equiv 3 \pmod{4}$ be a prime. If $p \mid a^2 + b^2$, then $p \mid a$ and $p \mid b$.*

Proof. Suppose that $p \mid a^2 + b^2$ and $p \nmid a$. Then $p \nmid b$. Since p is prime, there exists $c \in \mathbb{Z}$ such that $bc \equiv 1 \pmod{p}$. Then $a^2 + b^2 \equiv 0 \pmod{p} \implies (ac)^2 + (bc)^2 \equiv 0 \pmod{p} \implies (ac)^2 \equiv -1 \pmod{p}$. □

Definition 2.6. For any prime p and any positive integer n, we define $\exp_p(n)$ be the exponent of p in the prime factorization of n.

Proposition 2.6. Let $p \equiv 3 \pmod{4}$ be a prime. If $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ such that $n = a^2 + b^2$, then $\exp_p(n)$ is even.

Proof. If $p \nmid n$, we are done. So assume $p \mid n$. Then $p \mid a$ and $p \mid b \implies p^2 \mid n$. Then we let $\alpha = \min\left\{\exp_p(a), \exp_p(b)\right\}$, without loss of generality let $\exp_p(a) = \alpha$. Then $p^{2\alpha} \mid n \implies n = p^{2\alpha}m$ for some $m \in \mathbb{N}$. Now let $a = p^\alpha c$ and $b = p^\alpha d$ for some $c, d \in \mathbb{N}$. Then $m = c^2 + d^2$. Now $p \nmid m$ because $p \nmid c$. Therefore $\exp_p(n) = 2\alpha$. □

Proposition 2.7. $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.

Proposition 2.8. Let $p \equiv 1 \pmod{4}$ be a prime. There exists $a, b \in \mathbb{N}$ such that $a^2 + b^2 = p$.

Proof. Let $S = \left\{c \in \mathbb{N} : \exists a, b \in \mathbb{N}, a^2 + b^2 = c \cdot p\right\}$. Now S is nonempty because $p \in S$ because $p \cdot p = p^2 + 0^2$.

Consider $c_0 = \min S$. It suffices to show that $c_0 = 1$.

Lemma 1: $c_0 < p$.

proof. There exists $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \pmod{p}$. Let $x \in \{0, 1, \ldots, p-1\}$. Now $x^2 + 1 \leq (p-1)^2 + 1 < p^2$. Then $x^2 + 1 = kp$ and $k < p$ so $k \in S$.

— END LEMMA —

Let $a_0, b_0 \in \mathbb{N} \cup \{0\}$ such that $a_0^2 + b_0^2 = c_0 \cdot p$.

Lemma 2: $\gcd(a_0, c_0) = \gcd(b_0, c_0) = 1$.

proof. It suffices to prove that $\gcd(a_0, c_0) = 1$ by symmetry. Suppose that there exists a prime q such that $q \mid a_0$ and $q \mid c_0$. Then $q \mid c_0 \cdot p = a_0^2 + b_0^2 \implies q \mid b_0$. Now since $q \leq c_0 < p$ (Lemma 1), we must have $q \nmid p$. Then

$$a_0^2 + b_0^2 = c_0 \cdot p \implies \left(\frac{a_0}{q}\right)^2 + \left(\frac{b_0}{q}\right)^2 = \frac{c_0}{q^2} \cdot p$$

and we get a contradiction.

— END LEMMA —

Now we proceed by contradiction. Assume that $c_0 > 1$.

There exists

$$a_1, b_1 \in \mathbb{Z} \text{ such that } \begin{cases} a_0 \equiv a_1 \pmod{c_0} \text{ and } b_0 \equiv b_1 \pmod{c_0} \\ |a_1| \leq \frac{c_0}{2} \text{ and } |b_1| \leq \frac{c_0}{2} \\ |a_1| \neq 0 \text{ and } |b_1| \neq 0 \end{cases}$$

Part 2 can be shown by listing the residue classes. Part 3 can be shown by considering Lemma 2 and the assumption $c_0 > 1$. Now

$$c_0 \mid a_0^2 + b_0^2 \text{ and } a_1^2 + b_1^2 \equiv a_0^2 + b_0^2 \pmod{c_0} \implies a_1^2 + b_1^2 = c_0 \cdot c_1.$$

It follows that $c_1 < c_0$ because

$$a_1^2 + b_1^2 \le \left(\frac{c_0}{2}\right)^2 + \left(\frac{c_0}{2}\right)^2 < c_0^2.$$

Now we get

$$\begin{aligned}
(a_0^2 + b_0^2)(a_1^2 + b_1^2) &= p \cdot c_0^2 \cdot c_1 \\
(a_0 a_1 + b_0 b_1)^2 + (a_0 b_1 - a_1 b_0)^2 &= p \cdot c_0^2 \cdot c_1 \\
\left(\frac{a_0 a_1 + b_0 b_1}{c_0}\right)^2 + \left(\frac{a_0 b_1 - a_1 b_0}{c_0}\right)^2 &= p \cdot c_1
\end{aligned}$$

It follows that $c_1 \in S$ and $c_1 < c_0$, contradicting the minimality of c_0.

Therefore c_0 must be 1. □

Question: What positive integers can be written as a sum of 2 squares?

$$n = 2^\alpha \cdot \prod_{i=1}^{r} p_i^{\beta_i} \cdot \prod_{j=1}^{s} q_j^{\gamma_j}$$

where $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$. Now since 2 and each p_i can be written as a sum of two squares. It suffices that $\prod_{j=1}^{s} q_j^{\gamma_j}$ is a square, that is γ_j is even for all j.

2.3 Chinese Remainder Theorem

Theorem 2.6 (Chinese Remainder Theorem). *Let $m_1, \ldots, m_r \in \mathbb{Z} \setminus \{0\}$ be pairwise coprime integers. Let $a_1, \ldots, a_r \in \mathbb{Z}$ be arbitrary. Then the system of congruences*

$$x \equiv a_1 \pmod{m_1}$$

$$\vdots x \equiv a_r \pmod{m_r}$$

has a unique solution modulo $\prod_{i=1}^{r} m_i$.

Proof. Let $M_i = \prod_{j \neq i} m_j$ for each $i = 1, \ldots, r$. Then since $\gcd(m_i, M_i) = 1$, there exists

$$y_i \in \mathbb{Z} \text{ such that } y_i M_i \equiv 1 \pmod{m_i}.$$

Then $x = \sum_{i=1}^{r} a_i y_i M_i$ is a solution to the system. Consider x modulo m_j.

$$\begin{aligned}
\sum_{i=1}^{r} a_i y_i M_i &\equiv a_j y_j M_j + \sum i \neq j a_i y_i M_i \pmod{m_j} \\
&\equiv a_j y_j M_j \mod m_j \\
&\equiv a_j \pmod{m_j}
\end{aligned}$$

If $x' \in \mathbb{Z}$ is another solution to the system of congruences, then $x - x' \equiv 0 \pmod{m_i}$ for all $i = 1, \ldots, r$. This is equivalent to $\operatorname{lcm}[m_1, \ldots, m_r] = \prod_{i=1}^{r} m_i \mid x - x'$. However our mod is $\prod_{i=1}^{r} m_i$ so the solution x must be unique. □

2.4 Euler's Totient Function ϕ

The function $\phi : \mathbb{N} \to \mathbb{N}$ is defined as follows $\phi(n) = \#\{0 \leq i \leq n-1 : \gcd(i,n) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^*$.

Proposition 2.9. If $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Proof. Observation: $\gcd(i,mn) = 1 \iff \gcd(i,m) = 1$ and $\gcd(i,n) = 1$.

Let $f : (\mathbb{Z}/mn\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ defined as $f(\bar{i}) = (i \mod m, i \mod n)$. This function is well defined (if direction of the observation).

For any i, j such that

$$\begin{cases} 0 \leq i \leq m-1 \text{ and } \gcd(i,m) = 1 \\ 0 \leq j \leq n-1 \text{ and } \gcd(j,n) = 1 \end{cases}$$

then CRT yeilds the existence of a unique x modulo mn such that

$$\begin{cases} x \equiv i \pmod m \\ x \equiv j \pmod m \end{cases}$$

Then $f(\overline{x}) = (i \mod m, j \mod n)$. Now f is both surjective and injective. Therefore f is bijective so $\phi(mn) = \phi(m)\phi(n)$. ☐

Since Euler's function is multiplicative, then

$$\begin{aligned} \phi\left(n = \prod_{i=1}^{r} p_i^{\alpha_i}\right) &= \prod_{i=1}^{r} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) \\ &= n\left(1 - \frac{1}{p_i}\right) \end{aligned}$$

Definition 2.7. For the function $f : \mathbb{N} \to \mathbb{C}$, we say that f is multiplicative if $f(mn) = f(m)f(n)$ whenever $\gcd(m,n) = 1$. If we do not need the condition $\gcd(m,n) = 1$, we call f completely multiplicative.

Proposition 2.10. The function $d(n) = \#\{\text{positive divisors of } n\}$ is multiplicative.

Proof. If $\gcd(m,n) = 1$ and $d \mid mn$, then $d = \gcd(d,m)\gcd(d,n)$. ☐

3 The congruence $f(x) \equiv 0 \pmod{p^\alpha}$

In this section p will always be prime.

Proposition 3.1. Let $f \in \mathbb{Z}[x]$ and for each nonzero $m \in \mathbb{Z}$, we let $N_f(m)$ be the number of solutions to the congruence $f(x) \equiv 0 \pmod m$. Then $N_f : \mathbb{N} \to \mathbb{N} \cup \{0\}$ is multiplicative.

Proof. Suppose $\gcd(m,n) = 1$, then $f(x) \equiv 0 \pmod{mn} \iff f(x) \equiv 0 \pmod m$ and $f(x) \equiv 0 \pmod n$. Now if x_1 is a solution to $f(x) \equiv 0 \pmod m$ and x_2 is a solution to $f(x) \equiv 0 \pmod n$, then there exists a unique $x \mod mn$ such that $x \equiv x_1 \pmod m$ and $x \equiv x_2 \pmod n$ (by CRT). Then $f(x) \equiv 0 \pmod{mn}$. It suffices to count the solutions. ☐

Now suppose we want to solve the congruence $f(x) \equiv 0 \pmod n$. We should write $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. Then it suffices to solve

$$\begin{cases} f(x) \equiv 0 \pmod{p_i^{\alpha_i}} \\ \vdots \\ f(x) \equiv 0 \pmod{p_r^{\alpha_r}} \end{cases}$$

By CRT, we can solve these congruences independently.

Definition 3.1. A degree n polynomial f is monic if $f(x) = \sum_{i=0}^{n} a_n x^n$ and $a_n = 1$.

Proposition 3.2. Let $f \in \mathbb{Z}[x] \setminus \{0\}$ of degree $n \geq 0$. Without loss of generality, let f be monic. Then for any prime p, there exists at most n solutions to $f(x) \equiv 0 \pmod{p}$.

Proof. We prove this by induction on n.

Case $n = 0$: We want to solve $f(x) = 1 \equiv 0 \pmod{p}$. There are 0 solutions and $0 \leq 0$, so we are done.

Now assume that the proposition is true for all monic polynomials of degree less than n. Suppose there exists some x_1 such that $f(x_1) \equiv 0 \pmod{p}$. We can write $f(x) = (x - x_1)g(x) + R(x)$ where $R(x)$ has degree less than 1. It follows that $r = f(x_1) \equiv 0 \pmod{p}$.

Now solving $f(x) \equiv 0 \pmod{p}$ is equivalent to solving $(x - x_1)g(x) \equiv 0 \pmod{p}$. Suppose $x_2 \not\equiv x_1 \pmod{p}$ is another solution to $f(x) \equiv 0 \pmod{p}$. Then $(x_2 - x_1)g(x) \equiv 0 \pmod{p}$. Since $p \nmid x_2 - x_1$, then we must have $p \mid g(x) \implies g(x) \equiv 0 \pmod{p}$.

Observe that g is monic and $\deg(g) = n - 1 < n$. Then by induction, there are at most $n - 1$ solutions to the congruence $g(x) \equiv 0 \pmod{p}$. It follows that $f(x) \equiv 0 \pmod{p}$ has at most n solutions. $\square$

Proposition 3.3. Given any $f \in \mathbb{Z}[x]$ of degree $n \geq 0$, we can find a $g \in \mathbb{Z}[x]$ with less that p such that $f(x) \equiv g(x) \pmod{p}$.

Proof. For any $x \in \mathbb{Z}$, we have $x^p \equiv x \pmod{p}$. Then $f(x) = (x^p - x)Q(x) + R(x)$ where $\deg(R) < p$. Then $f(x) \equiv 0 \pmod{p} \iff R(x) \equiv 0 \pmod{p}$.

Observe that f has p solutions if and only if $R(x) \equiv 0 \pmod{p}$ for all $x \in \mathbb{Z}$. $\square$

3.1 Hensel's Lemma

Theorem 3.1 (Hensel's Lifting Lemma). *Let $f \in \mathbb{Z}[x]$, let p be a prime and let*

$$x_1 \in \mathbb{Z} \text{ such that } f(x_1) \equiv 0 \pmod{p} \text{ and } f'(x_1) \not\equiv 0 \pmod{p}.$$

Then for any $n \in \mathbb{N}$, there exists a unique solution x_n to the congruence

$$f(x) \equiv 0 \pmod{p^n} \text{ and } x_n \equiv x_1 \pmod{p}.$$

Proof. It suffices to show that if $f(x_n) \equiv 0 \pmod{p^n}$ and $x_n \equiv x_1 \pmod{p}$, then there exists a unique solution x_{n+1} to $f(x) \equiv 0 \pmod{p^{n+1}}$ and $x_{n+1} \equiv x_n \pmod{p^n}$.

We write

$$
\begin{aligned}
f(x) &= \sum_{i=0}^{d} c_i x^i \\
x_{n+1} &= x_n + p^n k \\
f(x_{n+1}) &= f(x_n + p^n k) = \sum_{i=0}^{d} c_i (x_n + p^n k) \\
&= \sum_{i=0}^{d} c_i \sum_{j=0}^{i} \binom{i}{j} x_n^j (p^n k)^{i-j} \\
&= \left(\sum_{i=0}^{d} c_i x_n^i \right) + \left(p^n k \sum_{i=1}^{d} i c_i x_n^{i-1} \right) + p^{2n} A \\
&= f(x_n) + p^n k f'(x_n) \equiv 0 \pmod{p^{n+1}}
\end{aligned}
$$

Now since $f(x_n) \equiv 0 \pmod{p^n} \iff f(x_n) = p^n b$, it

$$
p^n b + p^n k f'(x_n) \equiv 0 \pmod{p^{n+1}} \iff b + k f'(x_n) \equiv 0 \pmod{p}.
$$

Then by the assumption that $x_n \equiv x_1 \pmod{p}$, we get $f'(x_n) \equiv f'(x_1) \not\equiv 0 \pmod{p}$, so $f'(x_n)$ is invertible modulo p. Then we can uniquely solve for k modulo p.

Therefore we get a unique solution $x_{n+1} = x_n + p^n k$ modulo p^{n+1}. □

Theorem 3.2 (Refined Hensel's Lemma)**.** *If x_0 is a solution to $f(x_0) \equiv 0 \pmod{p}$ and*

$$
\exp_p(f(x_0)) > 2 \exp_p(f'(x_0)),
$$

then it always lifts.

Example: $x^2 + x + 37 \equiv 0 \pmod{7}$. Everything lifts to level 2, only some lift to level 3.

Example: $x^2 + 2x + 50 \equiv 0 \pmod{7}$. Everything lifts to level 2, nothing lift to level 3.

3.2 The Congruence $a^n \equiv 1 \pmod{m}$

Definition 3.2. Let $m \in \mathbb{Z} \setminus \{0\}$ and let $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$. We define the order of a modulo m, denoted $\operatorname{ord}_m(a)$ be the least positive integer d such that $a^d \equiv 1 \pmod{m}$.

Since $a^{\phi(m)} \equiv 1 \pmod{m}$, we have $\operatorname{ord}_m(a) \leq \phi(m)$.

Lemma 3.3. *If p is a prime and $d \in \mathbb{N}$ divides $p - 1$, then there are exactly d solutions to*

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

Proof. Let $k = \frac{p-1}{d} \in \mathbb{N}$. Now

$$
\underbrace{x^{p-1} - 1}_{\text{exactly } p-1 \text{ solutions}} = (x^d - 1) \underbrace{(x^{d(k-1)} + x^{d(k-2)} + \cdots + 1)}_{\text{at most } d(k-1) = p-d \text{ solutions}}.
$$

It follows that $x^d - 1 \equiv 0 \pmod{p}$ has at least d solutions because modulo prime.

However, since $\deg(x^d - 1) = d$, it cannot have more than d solutions. Therefore, $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions. □

Lemma 3.4. *For any $n \in \mathbb{N}$ such that $a^n \equiv 1 \pmod{m}$, we have $ord_m(a) \mid n$.*

Proof. Let $d = \operatorname{ord}_m(a)$. Let q and r be the quotient and remainder respectively when we divide n by d. That is $n = dq + r$ with $0 \le r < d$. It suffices to show $r = 0$.

$$1 \equiv a^n \equiv a^{dq+r} \equiv (a^d)^q a^r \equiv a^r \pmod{m}.$$

It follows that $r = 0$, implying that $d \mid n$. ☐

Lemma 3.5. *Let $d = ord_m(a)$. If $k \in \mathbb{Z}$, then $ord_m(a^k) = \frac{d}{\gcd(k,d)}$*

Proof. Let $D = \gcd(d,k)$ and let $d = l\gcd(d,k) = Dl$. Now we need to show that $\operatorname{ord}_m(a^k) = l$.

$$(a^k)^l \equiv a^{\frac{k}{D}Dl} \equiv (a^d)^{\frac{k}{D}} \equiv 1 \pmod{m}.$$

So, $\operatorname{ord}_m(a^k) \mid l$. Furthermore,

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

so $\operatorname{ord}_m(a) = d \mid kd_1 \implies \frac{d}{D} \mid \frac{k}{D}d_1 \implies l \mid d_1$. ☐

Lemma 3.6. *If $d_1 = ord_m(a_1)$ and $d_2 = ord_m(a_2)$ and $\gcd(d_1, d_2) = 1$, then $ord_m(a_1a_2) = d_1d_2$.*

Proof. Let $d = \operatorname{ord}_m(a_1a_2)$.

$$(a_1a_2)^{d_1d_2} \equiv (a_1^{d_1})^{d_2}(a_2^{d_2})^{d_1} \equiv 1 \pmod{m}$$

so $d \mid d_1d_2$.

$$1 \equiv ((a_1a_2)^d)^{d_1} \equiv (a_1a_2)^{dd_1} \equiv (a_1^{d_1})^d a_2^{dd_1} \equiv a_2^{dd_1} \pmod{m}$$

so $d_2 \mid dd_1 \implies d_2 \mid d$. Similarly, we must have $d_2 \mid d$. Therefore $d_1d_2 \mid d$ so we must have $d = d_1d_2$. ☐

Lemma 3.7. *Let p, q be primes and $\alpha \in \mathbb{N}$ such that $q^\alpha \mid p-1$. Then there exist exactly $q^\alpha - q^{\alpha-1}$ residue classes of integers a such that $ord_p(a) = q^\alpha$.*

Proof. Since $q^\alpha \mid p-1$, there exist exactly q^α solutions to the congruence

$$x^{q^\alpha} \equiv 1 \pmod{p}.$$

For each solution a of this congruence, we must have $\operatorname{ord}_p(a) \mid q^\alpha$, that is $\operatorname{ord}_p(a) = q^\beta$ where $0 \le \beta \le \alpha$.

Consider the case where $\beta < \alpha$. This implies

$$a^{q^{\alpha-1}} \equiv 1 \pmod{p}.$$

Now since $q^{\alpha-1} \mid p-1$, there are exactly $q^{\alpha-1}$ solutions to this congruence.

The lemma follows. ☐

Theorem 3.8. *Let p be a prime, then there exists $a \in \mathbb{Z}$ such that $ord_p(a) = p-1$.*

Proof. For $p = 2$, we can choose $a = 1$.

For $p > 2$, let $p - 1 = \prod_{i=1}^{l} q_i^{\alpha_i}$. By the previous lemma, for each $i = i, \ldots, l$, let $a_i \in \mathbb{Z}$ such that $\operatorname{ord}_p(a_i) = q_i^{\alpha_i}$. Now let $a = \prod_{i=1}^{l} a_i$, $\operatorname{ord}_p(a) = p-1$. ☐

Definition 3.3. If $\operatorname{ord}_p(a) = p - 1$, then a is a primitive root modulo p.

Corollary 3.8.1. *There exist exactly $\phi(p-1)$ primitive roots modulo p.*

Proof. We know there exists one primitive root g modulo p. Now we can write all nonzero residue classes of p as g^α.
Claim: $\{g^\alpha : 0 \leq \alpha \leq p-2\} = \left\{\overline{1}, \overline{2}, ..., \overline{p-1}\right\}$
It suffices to prove that $g^\alpha \not\equiv g^\beta \pmod{p}$ if $0 \leq \alpha < \beta \leq p-2$. If $g^\alpha \equiv g^\beta \pmod{p}$, then $g^{\beta-\alpha} \equiv 1 \pmod{p}$. Now this is a contradiction because $\beta - \alpha < p - 1 = \operatorname{ord}_p(g)$.

Observe that we want $\gcd(\alpha, \operatorname{ord}_p(g)) = 1$ in order for g^α to be a primitive root.

$$\operatorname{ord}_p(g^\alpha) = \frac{\operatorname{ord}_p(g)}{\gcd(\alpha, \operatorname{ord}_p(g))} = p - 1 \iff \gcd(\alpha, p-1) = 1.$$

It follows that there are exactly $\phi(p-1)$ primitive roots. $\square$

Lemma 3.9. *Let $a, b \in \mathbb{Z}, m \in \mathbb{Z} \setminus \{0\}$ and let $d = \gcd(a, m)$. Consider the congruence*

$$ax \equiv b \pmod{m}.$$

(a) If $d \mid b$, then there exists exactly d solutions.

(b) If $d \nmid b$, then there exists no solution.

Proof. To see that d must divide b in order for there to be solutions, observe that

$$m \mid ax - b \implies d \mid ax - b \implies d \mid b.$$

Now let $a = da_1, b = db_1, m = dm_1$. Now $ax \equiv b \pmod{m} \iff a_1 x \equiv b_1 \pmod{m_1}$. There exists a unique x_0 modulo m_1 that is the solution to $a_1 x \equiv b_1 \pmod{m_1}$. Then the solutions to $ax \equiv b \pmod{m}$ are

$$x_0,\ x_0 + m_1,\ ...,\ x_0 + (d-1)m_1,$$

a total of d solutions. $\square$

Theorem 3.10. *Let p be a prime and $a \in \mathbb{Z}$ not divisible by p and $n \in \mathbb{N}$. Let $d = \gcd(n, p-1)$.*

(a) If $a^{\frac{p-1}{d}} \not\equiv 1 \pmod{p}$, then there is no solution to $x^n \equiv a \pmod{p}$.

(b) If $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, then there exist d solutions to $x^n \equiv a \pmod{p}$.

Proof. Let g be some primitive root modulo p. Then there exists some $\alpha \in \{1, \ldots, p-2\}$ such that $a \equiv g^\alpha \pmod{p}$. Now any solution x to $x^n \equiv a \pmod{p}$ can be written as g^β where $\beta \in \{1, \ldots, p-2\}$. Then the congruence becomes

$$\begin{aligned}
(g^\beta)^n \equiv g^\alpha \pmod{p} &\iff g^{n\beta} \equiv g^\alpha \pmod{p} \\
&\iff g^{|n\beta - \alpha|} \equiv 1 \pmod{p} \\
&\iff p - 1 = \operatorname{ord}_p(g) \mid n\beta - \alpha.
\end{aligned}$$

Now this last divisibility is equivalent to the congruence

$$n\beta \equiv \alpha \pmod{p}.$$

By the previous lemma, we are done. $\square$

Corollary 3.10.1. *If p is an odd prime and $a \in \mathbb{Z}$ not divisible by p, then*

(a) If $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, then there is no solution to $x^2 \equiv a \pmod{p}$.

(b) If $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, then there are 2 solutions to $x^2 \equiv a \pmod{p}$.

3.3 Primitive Roots

Theorem 3.11. *Let p be an odd prime and $\alpha \in \mathbb{N}$. Then there is a primitive root g modulo p^α, that is*

$$ord_{p^\alpha}(g) = \phi(p^\alpha) = p^{\alpha-1}(p-1).$$

Proof. We know there exists $g_1 \in \mathbb{Z}$ such that $ord_p(g_1) = p-1$. We construct $g_2 \in \mathbb{Z}$ such that $\mathrm{ord}_{p^2}(g_2) = p(p-1)$. Now if $g_2 \equiv g_1 \pmod p$, then $\mathrm{ord}_p(g_2) = \mathrm{ord}_p(g_1) = p-1$. Now we must have $p-1 \mid \mathrm{ord}_{p^2}(g_2)$ because we need $g_2^n \equiv 1 \pmod p$ if we want $g_2^n \equiv 1 \pmod{p^2}$.

By Euler's Theorem, we get $\mathrm{ord}_{p^2}(g_2) \mid \phi(p^2) = p(p-1)$, hence it suffices to show that there exists some g_2 such that

$$\mathrm{ord}_{p^2}(g_2) \neq p-1.$$

Now if $\mathrm{ord}_{p^2}(g_2) = p-1$, this means $g^{p-1} \equiv 1 \pmod{p^2}$. Hence $g_2^p \equiv g_2 \pmod{p^2}$. We can write $g_2 = g_1 + pk$ and get

$$\begin{aligned} g_2^p &= (g_1+pk)^p \\ &= g_1^p + \sum_{i=1}^{p} g_1^{p-i}(pk)^i \\ &\equiv g_1^p \pmod{p^2} \end{aligned}$$

Now this is equivalent to

$$g_2 \equiv g_2^p \equiv g_1^p \equiv g_1 + pk \pmod{p^2}.$$

This means

$$(g_1^p - g_1) - pk \equiv 0 \pmod{p^2}$$

which is true for at most one residue class k. Therefore there exist $p-1$ residue classes modulo p^2 such that $\mathrm{ord}_{p^2}(g_2) \neq p-1$. Hence we must have $\mathrm{ord}_{p^2}(g_2) = p(p-1)$.

This proves that there is a primitive root modulo p^2.

Claim: g_2 is a primitive root modulo p^α for any $\alpha \geq 1$. We already know that the claim is valid for $\alpha \leq 2$.

We prove this claim by induction on α. Suppose that g_2 is a primitive root for all $\beta \leq \alpha$ for some $\alpha \geq 2$.

We want to show $\mathrm{ord} p^{\alpha+1}(g_2) = p^\alpha(p-1) = \phi(p^{\alpha+1})$. Observe that

$$g_2^{\mathrm{ord}_{p^{\alpha+1}}(g_2)} \equiv 1 \pmod{p^\alpha} \implies \mathrm{ord}_{p^\alpha}(g_2) \mid \mathrm{ord}_{p^{\alpha+1}}(g_2).$$

This means $p^{\alpha-1}(p-1) \mid \mathrm{ord}_{p^{\alpha+1}}(g_2)$. Hence suffices to prove that $\mathrm{ord}_{p^{\alpha+1}}(g_2) \neq p^{\alpha-1}(p-1)$, that is

$$g_2^{p^{\alpha-1}(p-1)} \not\equiv 1 \pmod{p^{\alpha+1}}.$$

Now since we are dealing with orders, we get

$$g_2^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$$

$$g_2^{p^{\alpha-2}(p-1)} \equiv 1 \pmod{p^{\alpha-1}}$$

Hence we write

$$g_2^{p^{\alpha-2}(p-1)} = 1 + p^{\alpha-1}k$$

where $p \nmid k$.

Therefore we can compute

$$\begin{aligned}
\text{Let } q &= g_2 p^{\alpha-2} \\
\text{Let } h &= g^{\alpha-1} \\
q^p &= (1+hk)^p \\
&= 1 + \binom{p}{1} hk + \binom{p}{2}(hk)^2 + \cdots + (hk)^p \\
&= 1 + p^\alpha k + \sum_{i=2}^{p} \binom{p}{i}(hk)^i
\end{aligned}$$

Now for $i = 2, \dots, p-1$, we have

$$\exp_p\left(\binom{p}{i}(p^{\alpha-1}k)^i\right) = 1 + i(\alpha-1) \geq 1 + 2(\alpha-1) \geq \alpha+1$$

and for $i = p$, we have

$$\exp_p((p^{\alpha-1}k)^p) = p(\alpha-1) \geq 3(\alpha-1) \geq \alpha+1.$$

Now we are done. $\square$

Lemma 3.12. *If $\alpha \geq 3$, there is no primitive root modulo 2^α.*

Proof. We prove that if x is odd, then

$$x^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}.$$

We already know this is true for $\alpha = 3$. We use induction on α.

Assume that this is true for α and prove the result for $\alpha+1$. We can compute

$$x^{2^{\alpha-1}} = (x^{2^{\alpha-2}})^2 = (1+2^\alpha k)^2 = 1 + 2^{\alpha+1}k + 2^{2\alpha}k^2 \equiv 1 \pmod{2^{\alpha+1}}.$$

(The reason is the exponent is not large enough) $\square$

Lemma 3.13. *Let $m, n \in \mathbb{N}$ such that $\gcd(m,n) = 1$. If a is a primitive root modulo mn, then*

(a) a is a primitive root modulo m and modulo n.

(b) $\gcd(\phi(m), \phi(n)) = 1$.

Proof. Let $d_1 = \mathrm{ord}_m(a)$ and $d_2 = \mathrm{ord}_n(a)$.

$$a^{d_1 d_2} \equiv (a^{d_1})^{d_2} \equiv 1 \pmod{m}$$
$$a^{d_1 d_2} \equiv (a^{d_2})^{d_1} \equiv 1 \pmod{n}$$

Since $\gcd(m,n) = 1$, we have $a^{d_1 d_2} \equiv 1 \pmod{nm}$. Hence

$$\phi(mn) = \mathrm{ord}_{mn}(a) \mid d_1 d_2 \mid \phi(m)\phi(n) = \phi(mn).$$

Now this means $d_1 = \phi(m)$ and $d_2 = \phi(n)$, and part (a) follows.

Replacing $d_1 d_2$ with $\mathrm{lcm}[d_1, d_2]$ gives part (b) because we get

$$\phi(mn) = \mathrm{ord}_{mn}(a) \mid \mathrm{lcm}[d_1, d_2] \mid d_1 d_2 \mid \phi(m)\phi(n) = \phi(mn).$$

Then $\mathrm{lcm}[d_1, d_2] = d_1 d_2$ so $\gcd(\phi(m), \phi(n)) = 1$. $\square$

CONCLUSION: n admits a primitive root if

- $n = 2^\alpha$, where $\alpha \leq 2$.
- $n = p^\alpha$, where p is an odd prime.
- $n = 2 \cdot p^\alpha$, where p is an odd prime.

Claim: If a is some primitive root p^α, then either a or $a + p^\alpha$ is a primitive root modulo $2 \cdot p^\alpha$.

Proof. Without loss of generality, a is odd. Then $\text{ord}_{2\cdot p^\alpha}(a) = \phi(p^\alpha)$ is divisible by $\text{ord}_{p^\alpha}(a) = \phi(p^\alpha)$. $\square$

4 Quadratic Reciprocity

4.1 Quadratic Residues and the Legendre Symbol

Recall the congruence

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

Then there are two possibilities:

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \implies x^2 \equiv a \pmod{p} \text{ has 2 solutions,}$$

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \implies x^2 \equiv a \pmod{p} \text{ has 0 solutions.}$$

Recall that the congruence

$$x^2 \equiv -1 \pmod{p}$$

is solvable if $p \equiv 1 \pmod{4}$ and not solvable if $p \equiv 3 \pmod{4}$.

Definition 4.1. Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol is

$$\left(\frac{a}{p}\right) \text{ is } \begin{cases} 0, \text{ if } p \mid a \\ 1, \text{ if } p \nmid a \text{ and } a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ -1, \text{ if } p \nmid a \text{ and } a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \end{cases}$$

Remark 4.1. Observations for odd primes p.

1. If $\left(\frac{a}{p}\right) \in \{0, 1\}$, then a is called a quadratic residue modulo p (square mod p).
2. There are $\frac{p-1}{2}$ nonzero quadratic residues modulo p. They are $1^2, 2^2, ..., (\frac{p-1}{2})^2$.
3. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Proof of observation 2. It suffices to show that the residue classes are distinct. That is if $1 \leq i < j \leq \frac{p-1}{2}$ then $i^2 \not\equiv j^2 \pmod{p}$. Suppose that there exists $i^2 \equiv j^2 \pmod{p}$ for contradiction. Then

$$(i-j)(i+j) \equiv 0 \pmod{p} \iff i \equiv j \pmod{p} \text{ or } i + j \equiv 0 \mod p.$$

This cannot be true. $\square$

Lemma 4.1. *If p is an odd prime, then*

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

Proof. Observe that

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

Now this means

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

□

Remark 4.2. More observations.

1. $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
2. If $p \nmid a$, then $\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n$.
3. If $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Theorem 4.2 (Quadratic Reciprocity)**.** *If $p \neq q$ are odd primes, then*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Equivalently,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Proof. First we outline the very enlightening proof.

1. Polynomials and Irreducibility
2. Roots of Unity
3. Character Sums
4. Quadratic Reciprocity

□

Theorem 4.3. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod 8 \text{ and } \left(\frac{2}{p}\right) = -1 \iff p \equiv \pm 3 \pmod 8.$$

Proof. For each $i = 1, ..., \frac{p-1}{2}$, there exist unique $\varepsilon(i) \in \{0, 1\}$ and $f(i) \in \left\{1, ..., \frac{p-1}{2}\right\}$ such that

$$2 \cdot i \equiv (-1)^{\varepsilon(i)} \cdot f(i) \pmod p.$$

We claim that f is bijective. Since f is from a set to itself, it suffices to prove that it is injective.
Case 1: $\varepsilon(i) = \varepsilon(j)$. Then

$$2i \equiv (-1)^{\varepsilon(i)} f(i) \equiv (-1)^{\varepsilon(j)} f(j) \equiv 2j \pmod p \implies i \equiv j \pmod p \implies i = j.$$

Case 2: $\varepsilon(i) \neq \varepsilon(j)$. Then

$$2i \equiv (-1)^{\varepsilon(i)} f(i) \equiv -(-1)^{\varepsilon(j)} f(j) \equiv -2j \pmod p \implies p \mid 2(i+j) \implies p \mid i+j.$$

This leads to a contradiction.

Now take the products (same trick as Euler's Theorem)

$$\prod_{i=1}^{\frac{p-1}{2}} (2i) \equiv \prod_{i=1}^{\frac{p-1}{2}} (-1)^{\varepsilon(i)} f(i) \pmod p$$
$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^l \left(\frac{p-1}{2}\right)! \pmod p$$

Now, $l = \# \left\{1 \leq i \leq \frac{p-1}{2} : 2i > \frac{p-1}{2}\right\}$.

We can consider the two cases $p = 4k+1$ and $p = 4k+3$ to get that l is even if and only if $p \equiv \pm 1 \pmod 8$. $\square$

Observe that we can write $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

4.2 Polynomials and Commutative Algebra

We want to prove that the pth cyclotomic polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible.

Proposition 4.1. Let $f, g, h \in \mathbb{Z}[x]$, and $f(x) = g(x) \cdot h(x)$. If there exists a prime p dividing each coefficient of f, then p devidies each coefficient of g or each coefficient of h.

Proof with algebra. We can reduce the polynomials modulo p, that is

$$\overline{f}, \overline{g}, \overline{h} \in \mathbb{R}_p[x].$$

Now if the proposition is not true, we can consider the product of the following nonzero polynomials

$$\overline{g}(x) = \overline{a_m} x^m + \cdots$$
$$\overline{h}(x) = \overline{b_n} x^n + \cdots$$

which is nonzero. $\square$

Proof. We prove this by contradiction.

Let m, n be maximal such that if

$$g(x) = \sum_{i=0}^{\deg(g)} a_i x^i$$

$$h(x) = \sum_{i=0}^{\deg(h)} b_i x^i$$

then $a_m \not\equiv 0 \pmod p$ and $b_n \not\equiv 0 \pmod p$. Now consider the coefficient of x^{m+n} in $f(x)$, then

$$\sum_{i+j=m+n} a_i b_j \equiv a_m b_n \pmod p.$$

Now we are done because $a_m b_n \not\equiv 0 \pmod p$. $\square$

Definition 4.2. We first define irreducibility.

1. $f \in \mathbb{Q}[x]$ is irreducible if $\nexists g, h \in \mathbb{Q}[x]$ such that $f = g \cdot h$ and $\deg(g), \deg(h) < \deg(f)$.
2. $f \in \mathbb{Z}[x]$ is irreducible if $\nexists g, h \in \mathbb{Z}[x]$ such that $f = g \cdot h$ and $\deg(g), \deg(h) < \deg(f)$.

Proposition 4.2 (Gauss's Lemma)**.** Let $f \in \mathbb{Z}[x]$. Then f is irreducible in $\mathbb{Q}[x]$ if and only if f is irreducible in $\mathbb{Z}[x]$.

Proof. Since $\mathbb{Z} \subset \mathbb{Q}$, the implication follows.

For the converse, we prove that if f is reducible in $\mathbb{Q}[x]$, then f is reducible in $\mathbb{Z}[x]$. There exists $g, h \in \mathbb{Q}[x]$ such that $f = g \cdot h$ and $\deg(g), \deg(h) < \deg(f)$.

Let $D(g) \in \mathbb{Z} \setminus \{0\}$ such that $D(g)g(x) \in \mathbb{Z}[x]$. Similarly define $D(h)$. Let $g_1(x) = D(g)g(x) \in \mathbb{Z}[x]$ and $h_1(x) = D(h)h(x) \in \mathbb{Z}[x]$. Then we have

$$D(g)D(h) \cdot f = g_1 \cdot h_1.$$

Let $N(g_1)$ be the gcd of the coefficients of g_1. Similarly define $N(h_1)$. Let $g_2(x) = \frac{g_1(x)}{N(g_1)} \in \mathbb{Z}[x]$ and $h_2(x) = \frac{h_1(x)}{N(h_1)} \in \mathbb{Z}[x]$. Now we have

$$D(g)D(h) \cdot f = g_1 \cdot g_2 = N(g_1)N(h_1) \cdot g_2 \cdot h_2.$$

By the previous lemma, there does not exist a prime p that divides each coefficient of $g_2(x)$ or each coefficient of $h_2(x)$. Otherwise, we contradict gcd.

Let $\frac{N(g_1)N(h_1)}{D(g)D(h)}$ written in lowest terms as $\frac{a}{b}$ (ie. $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$). It suffices to prove that $b = 1$, that is no prime p divides b. By contradiction, suppose that there exists some prime p that divides b. Since $\gcd(a, b) = 1$, then $p \nmid a$. Equivalently,

$$b \cdot f = a \cdot g_2 \cdot h_2.$$

Now p divides each coefficient of $b \cdot f$. Since $p \nmid a$ and p does not divide each coefficient of g_2 or each coefficient of h_2 and we have a contradiction. It follows that $b = 1$. □

Proposition 4.3 (Eisenstein Criterion for Irreducibility)**.** Let p be a prime and let $a_0, \ldots, a_n \in \mathbb{Z}$ such that

1. $p \nmid a_n$,
2. $p \mid a_i$ for $0 \leq i \leq n-1$,
3. $p^2 \nmid a_0$.

Then $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is irreducible.

Proof. We prove this by contradiction. Assume that there exists such a polynomial is reducible, that is $\exists g, h \in \mathbb{Z}[x]$ such that $f = gh$ and $1 \leq \deg(g), \deg(h) < \deg(f)$. Let

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$
$$h(x) = c_l x^l + c_{l-1}x^{l-1} + \cdots + c_1 x + c_0$$

Since $a_0 = b_0c_0$, $p \mid a_0$ and $p^2 \nmid a_0$, we get that p divides exactly one of b_0 and c_0. Without loss of generality, assume that $p \mid b_0$ and $p \nmid c_0$. Now we can prove by induction that $p \mid b_i$ for all $i = 0, \ldots, m$.

We already have the base case. Assume that $p \mid b_j$ for all $j < i$. Then

$$p \mid a_i = b_ic_0 + b_{i-1}c_1 + \cdots + b_0c_i \implies p \mid b_i.$$

It follows that $p \mid a_n$, contradiction. $\square$

Corollary 4.3.1. *Let p be a prime, and let $\Phi_p(x) = x^{p-1} + \cdots + x + 1$, then $\Phi_p(x)$ is irreducible.*

Proof. Observe that $\Phi_p(x+1) = \frac{x^p-1}{x-1}$. Then

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-1}$$

satisfies the Eisenstein criterion for p, so $\Phi_p(x+1)$ is irreducible. Now $\Phi_p(x)$ must be irreducible.

We can see that if $\Phi_p(x) = g(x) \cdot h(x) \implies \Phi_p(x+1) = g(x+1) \cdot h(x+1)$. $\square$

4.3 Primitive Roots of Unity

Consider the roots of $\Phi_p(x)$. These are $e^{i\frac{2\pi l}{p}}, l \in \{1, \ldots, p-1\}$. Let $\xi_p = e^{i\frac{2\pi}{p}}$.

Lemma 4.4. *There exists no nonzero polynomial $g(x) \in \mathbb{Q}[x]$ of degree less than $p-1$ such that $g(\xi_p) = 0$.*

Proof. We can assume that $g \in \mathbb{Z}[x]$ because we can simply clear the denominators. Without loss of generality, assume g has the minimum degree among all polynomials with ξ_p as a root. We divide $\Phi_p(x)$ by $g(x)$ with quotient and remainder

$$\Phi_p(x) = g(x) \cdot Q(x) + R(x)$$

where $Q, R \in \mathbb{Q}[x]$ and $\deg(R) < \deg(g)$.

Now we get $\Phi_p(\xi_p) = g(\xi_p)Q(\xi_p) + R(\xi_p) \implies R(\xi_p) = 0$. By the minimality of g, we get $R(x) = 0$. This implies that $\Phi_p(x) = g(x)Q(x)$ and by Gauss's Lemma, $\Phi_p(x)$ is irreducible. Hence $Q(x)$ is a constant function. $\square$

Corollary 4.4.1. *If $c_1, \ldots, c_p - 1 \in \mathbb{Q}$ such that $c_1\xi_p + c_2\xi_p^2 + \cdots + c_{p-1}\xi_p^{p-1} = 0$, then $c_1 = c_2 = \cdots = c_{p-1} = 0$.*

Proof. Assume $\sum_{i=1}^{p-1} c_i\xi_p^i = 0$. Since $\xi_p \neq 0$, we can divide by ξ_p. Now we get some polynomial of degree less than $p-1$ with a root at ξ_p, so it is identically 0. $\square$

Lemma 4.5. *Let $b \in \mathbb{Z}$. Then*

$$\sum_{i=1}^{p-1} \xi_p^{ib} = \begin{cases} p-1 \text{ if } p \mid b \\ -1 \text{ if } p \nmid b \end{cases}$$

Proof. If $p \mid b$, then $\xi_p^{ib} = 1$ for all i, so $\sum_{i=1}^{p-1} \xi_p^{ib} = p-1$.

If $P \nmid b$, then $\{ib : 1 \le i \le p-1\} = \{1, ..., p-1\}$ modulo p, so

$$\sum_{i=1}^{p-1} \xi_p^{ib} = \sum_{i=1}^{p-1} \xi_p^i = -1.$$

$\square$

Definition 4.3. We define the Gauss sum to be

$$G(p) = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \cdot \xi_p^i.$$

Lemma 4.6. $G(p)^2 = p \cdot \left(\frac{-1}{p}\right) = p \cdot (-1)^{\frac{p-1}{2}}$.

Proof. We expand to get

$$G(p)^2 = \sum_{1 \leq i,j \leq p-1} \left(\frac{i}{p}\right)\left(\frac{j}{p}\right) \xi_p^i \xi_p^j$$

Everything is invertible, so we an let $j = ik$ for some $k \in \{1, ..., p-1\}$.

$$\begin{aligned} G(p)^2 &= \sum_{1 \leq i,j \leq p-1} \left(\frac{ij}{p}\right) \xi_p^{i+j} = \sum_{1 \leq i,k \leq p-1} \left(\frac{i^2 k}{p}\right) \xi_p^{i(k+1)} = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \sum_{i=1}^{p-1} \xi_p^{i(k+1)} \\ &= \left(\sum_{k=1}^{p-2} \left(\frac{k}{p}\right) \sum_{i=1}^{p-1} \xi_p^i\right) + \left(\frac{p-1}{p}\right) \sum_{i=1}^{p-1} \xi_p^0 = \left(\sum_{k=1}^{p-2} \left(\frac{k}{p}\right)(-1)\right) + \left(\frac{p-1}{p}\right)(p-1) \\ &= p\left(\frac{-1}{p}\right) - \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = p\left(\frac{-1}{p}\right) \end{aligned}$$

□

Lemma 4.7. *Let $n \in \mathbb{N}$, $i_1, ..., i_k \in \mathbb{Z}$ and $a_{i_1}, ..., a_{i_k} \in \mathbb{Z}$ such that $n \mid a_{i_j}$ for each $j = 1, ..., k$. Then there exist*

$$\begin{gathered} b_1, ..., b_{p-1} \in \mathbb{Z} \text{ such that } \forall j \in \{1, ..., p-1\}, n \mid b_j \text{ such that} \\ a_{i_1}\xi_p^{i_1} + \cdots + a_{i_k}\xi_p^{i_k} = b_1\xi_p + b_2\xi_p^2 + \cdots + b_{p-1}\xi_p^{p-1} \end{gathered}$$

4.4 Proof of Quadratic Reciprocity

Lemma 4.8. *Let $k \in \mathbb{N}$ and $x_1, \ldots, x_k$ are variables and q is a prime. Then*

$$(x_1 + \cdots + x_k)^q = x_1^q + \cdots + x_k^q + \sum_{i_1 + \cdots i_k = q} c_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k}$$

where each c is divisible by q. That is

$$(x_1 + \cdots + x_k)^q \equiv x_1^q + \cdots + x_k^q \pmod q.$$

Proof. Proof by induction ok k.

Base case $k = 2$: Obvious after expansion.

Inductive step $k > 2$:

$$\begin{aligned} (x_1 + \cdots + (x_k + x_{k+1}))^q &= x_1^q + \cdots + (x_k + x_{k+1})^q + \sum_{i_1 + \cdots + i_k = q} c_{i_1,\ldots,i_k} \cdots (x_k + x_{k+1})^{i_k} \\ &= x_1^q + \cdots + x_{k+1}^q + \sum_{j=1}^{q-1} \binom{q}{j} x_k^j x_{k+1}^{q-j} + \sum c \cdot \cdots \left(\sum \text{binom}\right) \end{aligned}$$

Now we get $(x_1 + \cdots + x_k)^q \equiv x_1^q + \cdots + x_k^q \pmod q$. □

Theorem 4.9 (Quadratic Reciprocity)**.** *If $p \neq q$ are odd primes, then*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Equivalently,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Proof. Consider the Gauss sum.

$$\begin{aligned} G(p) &= \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi_p^i \\ G(p)^2 &= p \cdot \left(\frac{-1}{p}\right) = p \cdot (-1)^{\frac{p-1}{2}} \\ G(p)^q &= G(p) \cdot (G(p)^2)^{\frac{q-1}{2}} \end{aligned}$$

Raising the Gauss sum to the power of q we get

$$\begin{aligned} G(p)^q &= \left(\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi_p^i\right)^q \\ &= \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)^q \xi_p^{iq} + \sum_{i_1,\dots,i_{p-1}} c_{i_1,\dots,i_{p-1}} \left(\prod_{j=1}^{p-1} \left(\left(\frac{j}{p}\right) \xi_p^j\right)^{i_j}\right) \\ &= \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi_p^{iq} + \sum_{i=1}^{p-1} b_i \xi_p^i \\ &= \left(\frac{q}{p}\right) \sum_{i=1}^{p-1} \left(\frac{iq}{p}\right) \xi_p^{iq} + \sum_{i=1}^{p-1} b_i \xi_p^i \\ &= \left(\frac{q}{p}\right) G(p) + \sum_{i=1}^{p-1} b_i \xi_p^i \end{aligned}$$

where $p \mid b_i$ for each i. Now from the other side, we get

$$\begin{aligned} G(p)^q &= G(p) \cdot (G(p)^2)^{\frac{q-1}{2}} \\ &= G(p) \cdot (p \cdot (-1)^{\frac{p-1}{2}})^{\frac{q-1}{2}} \\ &= G(p) \cdot p^{q-1} 2 \cdot (-1)^{\frac{(p-1)(q-1)}{4}} \\ &= G(p) \cdot \left(\left(\frac{p}{q}\right) + ql\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}} \\ &= G(p) \cdot \left(\frac{p}{q}\right) + ql(-1)^{\frac{(p-1)(q-1)}{4}} G(p) \\ &= G(p) \cdot \left(\frac{p}{q}\right) + \sum_{i=1}^{p-1} a_i \xi_p^i \end{aligned}$$

where $q \mid a_i$ for each i.

Equating the two expressions for $G(p)^q$ gives

$$\left(\frac{q}{p}\right)G(p) + \sum_{i=1}^{p-1} b_i \xi_p^i = \left(\frac{p}{q}\right)(-1)^{\frac{(p-1)(q-1)}{4}} G(p) + \sum_{i=1}^{p-1} a_i \xi_p^i$$

$$\left(\left(\frac{q}{p}\right) - \left(\frac{p}{q}\right)(-1)^{\frac{(p-1)(q-1)}{4}} G(p)\right) = \sum_{i=1}^{p-1} (a_i - b_i)\xi_p^i$$

$$\sum_{i=1}^{p-1}\left(\left(\frac{q}{p}\right) - \left(\frac{p}{q}\right)(-1)^{\frac{(p-1)(q-1)}{4}}\right)\left(\frac{i}{p}\right)\xi_p^i = \sum_{i=1}^{p-1}(a_i - b_i)\xi_p^i$$

It follows that for each $i = 1, ..., p-1$ we have

$$q \mid a_i - b_i = \left(\left(\frac{q}{p}\right) - \left(\frac{p}{q}\right)(-1)^{\frac{(p-1)(q-1)}{4}}\right)\left(\frac{i}{p}\right) \in \{-2, 0, 2\}.$$

Hence $a_i = b_i$ and the proof is complete. $\square$

5 Diophantine Equations

Definition 5.1. If $f \in \mathbb{Z}[x_1, ..., x_n]$, then $f(x_1, ..., x_n) = 0$ is a diophantine equation. We search for integer solutions.

The common questions relating to Diophantine equations:

1. Find all solutions.
2. Determine whether there are infinitely many solutions.

Consider the equation

$$Ax^m + By^n + Cz^k = 0$$

where $A, B, C \in \mathbb{Z}$ and $m, n, k \in \mathbb{N}$, and we are looking for solutions in rationals. Then we have three cases.

1. If $\frac{1}{m} + \frac{1}{n} + \frac{1}{k} > 1$, then there are infinitely many solutions.
2. If $\frac{1}{m} + \frac{1}{n} + \frac{1}{k} = 1$, this gives an elliptic curve.
3. If $\frac{1}{m} + \frac{1}{n} + \frac{1}{k} < 1$, then there are finitely many solutions.

Note: There are always finitely many integer solutions on an elliptic curve.
Example on elliptic curves.

$$y^2 + x^3 - 17z^6 = 0$$

We can rewrite this equation as

$$\left(\frac{y}{z^3}\right)^2 + \left(\frac{x}{z^2}\right)^3 - 17 = 0$$

which is a planar curve as follows

$$y^2 = x^3 + 17.$$

How do we generate solutions when we know one solution? We can draw the tangent and find another point on the curve.

5.1 Examples of Diophantine Equations

Example 5.1. Consider the Diophantine equation

$$x^2 + 2y^2 - 8z - 5 = 0.$$

Proof. This is equivalent with the congruence

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

Observe that x is odd, so $x^2 \equiv 1 \pmod 8$. Then the congruence is equivalent to

$$2y^2 \equiv 4 \pmod 8.$$

Now $2 \mid y$ so $4 \mid y^2$, hence $2y^2 \equiv 0 \pmod 8$ and we have a contradiction. Therefore there are no solutions. □

Example 5.2. Consider the Diophantine equation

$$x^2 - 3xy + z^2 - 6xz^3 - 21 = 0.$$

Proof. We reduce this equation modulo 3.

$$x^2 + z^2 \equiv 0 \pmod 3.$$

This means $3 \mid x^2 + z^2$ and since $3 \pmod 4$, we get $3 \mid x$ and $3 \mid z$. Now we get that 9 divides all terms in the equation except -21 and we have a contradiction. Therefore there are no solutions. □

Example 5.3. Consider the Diophantine equation

$$x^2 - 2xy^2 + 5y^4 - 3x + 6y + 10 = 0.$$

Proof. Observe that

$$\begin{aligned} 0 &= \left(\frac{1}{4}x^2 - 2xy^2 + 4y^4\right) + \left(\frac{3}{4}x^2 - 3x + 3\right) + \left(y^4 - 2y^2 + 1\right) + 2y^2 + 6y + 6 \\ &= \left(\frac{1}{2}x - 2y^2\right)^2 + 3\left(\frac{1}{2}x - 1\right)^2 + \left(y^2 - 1\right)^2 + 2\left(y + \frac{3}{2}\right)^2 + \frac{3}{2} \\ &> 0 \end{aligned}$$

□

Example 5.4. Consider the Diophantine equation

$$x^3 + 2y^3 - 7z^3 - 14w^3 = 0.$$

Proof. Consider reducing modulo 7.

$$x^3 + 2y^3 \equiv 0 \pmod 7.$$

Observe that $(n^3)^2 = x^6 \equiv 1 \pmod 7$ so

$$x^3 \equiv \begin{cases} 0 \pmod 7 \\ \pm 1 \pmod 7 \end{cases}$$

It follows that we must have $7 \mid x$ and $7 \mid y$. Now consider the original equation, we must get $7 \mid z^3 + 2w^3$ and hence infinite descent.

If $(0,0,0,0)$ is not the only solution, then there exists a nontrivial solution (x,y,z,w) such that $\gcd(x,y,z,w) = 1$. Then we show that $7 \mid \gcd(x,y,z,w)$ and get a contradiction. □

Example 5.5. Consider the Diophantine equation

$$7x^4 + 11y^4 - z^4 = 0.$$

Proof. Assume that there is a nontrivial solution (x, y, z) such that $\gcd(x, y, z) = 1$.

Consider reducing modulo 7.

$$4y^4 \equiv z^4 \pmod 7$$

This does not give anything when $7 \nmid y$ and $7 \nmid z$.

Consider reducing modulo 11 and suppose that $11 \nmid x$ and $11 \nmid z$.

$$7x^4 \equiv z^4 \pmod 7.$$

No we get $7 \equiv A^4 \pmod{11} \iff 7 \equiv B^2 \pmod{11}$ but $\left(\frac{7}{11}\right) = -1$ and we have a contradiction. □

5.2 Pythagorean Triples

Consider the Diophantine equation

$$x^2 + y^2 = z^2 \text{ where } x, y, z \in \mathbb{Z}.$$

Observation 5.1. If $d \mid \gcd(x, y, z)$, then

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

Observation 5.2. We can assume $\gcd(x, y) = \gcd(y, z) = \gcd(z, x) = 1$.

Observation 5.3. z is odd.

Proof. If z is even, then x and y have the same parity.

If x and y are even, then we contradict the coprimality.

If x and y are odd, then we have

$$0 \equiv z^2 \equiv x^2 + y^2 \equiv 2 \pmod 4.$$

□

Now, since we know that z is odd, then without loss of generality, let x be even and y be odd. Then

$$x = 2x_1; x_1 \in \mathbb{Z}.$$

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

Observation 5.4. If $A, B, C \in \mathbb{N}$ and $n \in \mathbb{N}$, and

$$\begin{cases} A^n = BC \\ \gcd(B, C) = 1 \end{cases}$$

then we must have B and C are both nth powers.

Proof. For each prime p, we have

$$\exp_p(B) + \exp_p(C) = n \cdot \exp_p(A)$$

However, we must have $\exp_p(B) = 0$, or $\exp_p(B) > 0$ and $\exp_p(C) = 0$. Hence, $\exp_p(B) \in \{0, n \cdot \exp_p(A)\}$. Similarly for C. $\square$

Since z and y are both odd, we can let

$$z - y = 2u; u \in \mathbb{N}$$
$$z + y = 2v; v \in \mathbb{N}$$

$$4x_1^2 = 2u \cdot 2v \implies x_1^2 = u \cdot v.$$

Observation 5.5. *u and v are coprime.*

Proof. Since $z = u+v$ and $y = v-u$, if $d \mid u$ and $d \mid v$, then $d \mid y$ and $d \mid z$. Hence $\gcd(u, v) = 1$. $\square$

Now, we get that u and v are perfect squares, that is there exist $a, b \in \mathbb{N}$ such that

$$u = a^2$$
$$v = b^2$$

$$x_1 = a \cdot b.$$

Now we get the solutions

$$x = 2ab$$
$$y = b^2 - a^2$$
$$z = b^2 + a^2$$

for $a, b \in \mathbb{N}$ and $\gcd(a, b) = 1$. These are all the primitive solutions.

$$(2ab, b^2 - a^2, b^2 + a^2) \text{ solves } x^2 + y^2 = z^2$$

Now, any $a, b \in \mathbb{Z}$ would solve the equation. However, we do not recover all solutions like this. To recover all solutions, it suffices to multiply the triple by a constant

$$(2abc, (b^2 - a^2)c, (b^2 + a^2)c)$$

5.2.1 Rational Points on the Unit Circle

Consider rational solutions to the equation

$$x^2 + y^2 = 1.$$

Since we have the integer solutions to $x^2 + y^2 = z^2$, we can simply divide to get

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

for $t = \frac{a}{b}$.

This means that the number of rational solutions of $x^2 + y^2 = 1$ is infinite. Usually we expect the number of rational solutions on a curve is finite.

Theorem 5.1 (Faltings)**.** *Let $f \in \mathbb{Q}[x,y]$, $\deg_x(f), \deg_y(f) \geq 4$ and f is irreducible over $\mathbb{Q}$, then the number of rational solutions to $f(x,y) = 0$ is finite.*

5.2.2 The Equation $x^4 + y^4 = z^4$

Theorem 5.2. *There are no solutions in $\mathbb{N}$ to the equation*

$$x^4 + y^4 = z^4.$$

Proof. Assume that there exist solutions in $\mathbb{N}$ to the equation

$$x^4 + y^4 = z^2.$$

Let (x_0, y_0, z_0) be the solution with the smallest z_0.

Observe that $\gcd(x_0, y_0, z_0) = 1$. If $p \mid x_0$ and $p \mid y_0$, then $p^4 \mid x^4 + y^4 = z^2 \implies p^2 \mid z$. Hence $(\frac{x_0}{p}, \frac{y_0}{p}, \frac{z_0}{p^2}$ is another solution with a smaller z_0. Now we get that $\gcd(x_0, y_0) = \gcd(y_0, z_0) = \gcd(x_0, z_0) = 1$.

Now we can rewrite the original equation as

$$(x_0^2)^2 + (y_0^2)^2 = z_0^2$$

where (x_0^2, y_0^2, z_0) is a primitive Pythagorean triple.

Now we know that z_0 is odd and we may assume that x_0 is even and y_0 is odd. Hence there exist $a, b \in \mathbb{N}$ where $\gcd(a, b) = 1$ such that

$$\begin{aligned} x_0^2 &= 2ab \\ y_0^2 &= b^2 - a^2 \\ z_0 &= a^2 + b^2 \end{aligned}$$

Observe that we have another primitive Pythagorean triple

$$a^2 + y_0^2 = b^2.$$

Now there exist $u, v \in \mathbb{N}$ where $\gcd(u, v) = 1$ such that

$$\begin{aligned} a &= 2uv \\ y_0 &= v^2 - u^2 \\ b &= u^2 + v^2 \end{aligned}$$

Now we need to check that $x_0^2 = 2ab$ is a perfect square. Since x_0 is even, we can write $x_0 = 2x_1$.

$$x_1^2 = uv(u^2 + v^2).$$

Since $\gcd(u, v) = 1$, we get that

$$1 = \gcd(u, v) = \gcd(u, u^2 + v^2) = \gcd(v, u^2 + v^2).$$

Hence u, v, $u^2 + v^2$ are all perfect squares.

Let $c, d, e \in \mathbb{N}$ where c, d, e are pairwise coprime such that

$$\begin{aligned} u &= c^2 \\ v &= d^2 \\ u^2 + v^2 &= e^2 \end{aligned}$$

Now we get the equation

$$c^4 + d^4 = e^2.$$

It suffices to check that $e < z_0$.

$$e \leq e^2 = u^2 + v^2 = b \leq b^2 < a^2 + b^2 = z_0$$

Now we have found a smaller solution in $\mathbb{N}$ to the original equation, contradicting the minimality of z_0. $\square$

5.3 Pell's Equation

Theorem 5.3. *Let $D \in \mathbb{N}$ such that $\sqrt{D} \notin \mathbb{N}$. There exist infinitely many solutions in $\mathbb{N} \times \mathbb{N}$ to $x^2 - Dy^2 = 1$.*

Lemma 5.4. *If there exists a solution $(x_0, y_0) \in \mathbb{N} \times \mathbb{N}$ such that*

$$x^2 - Dy^2 = 1.$$

then there exist infinitely many solutions.

Proof. Assume that

$$\begin{cases} x_0^2 - Dy_0^2 = 1 \\ x_1^1 - Dy_1^2 = 1 \end{cases}$$

We simply multiply the two equations to get

$$\begin{aligned} 1 &= x_0^2 x_1^2 + D^2 y_0^2 y_1^2 - D(x_0^2 y_1^2 + x_1^2 y_0^2) \\ &= x_0^2 x_1^2 + D^2 y_0^2 y_1^2 + 2D x_0 x_1 y_0 y_1 - D(x_0^2 y_1^2 - 2x_0 x_1 y_0 y_1 + x_1^2 y_0^2) \\ &= (x_0 x_1 + D y_0 y_1)^2 - D(x_0 y_1 + x_1 y_0)^2 \\ &= x_2^2 - D y_2^2 \end{aligned}$$

Clearly, $(x_2, y_2) \in \mathbb{N} \times \mathbb{N}$ and x_2, y_2 are not equal to the two solutions we started with. $\square$

Lemma 5.5. *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and $N \in \mathbb{N}$, then there exists $(p, q) \in \mathbb{Z} \times \mathbb{N}$ such that*

$$q \leq N \text{ and } \left| \alpha - \frac{p}{q} \right| < \frac{1}{qN}.$$

Proof. Consider $\{i \cdot \alpha\} \in [0, 1); 0 \leq i \leq N$. We divide the interval $[0, 1)$ into N intervals. Then by the Pigeonhole Principle, there exist $0 \leq j < i \leq N$ such that

$$\begin{aligned} \frac{1}{N} &> |\{i\alpha\} - \{j\alpha\}| \\ &= |(i-j)\alpha - (\lfloor i\alpha \rfloor - \lfloor j\alpha \rfloor)| \\ \frac{1}{(i-j)N} &> \left| \alpha - \frac{\lfloor i\alpha \rfloor - \lfloor j\alpha \rfloor}{i-j} \right| \end{aligned}$$

Now we let $p = \lfloor i\alpha \rfloor - \lfloor j\alpha \rfloor$ and $q = i - j$ to get the desired result. $\square$

Corollary 5.5.1. *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, then there exist infinitely many pairs $(p, q) \in \mathbb{Z} \times \mathbb{N}$ such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Proof. For each $N \in \mathbb{N}$, there exists $(p_N, q_N) \in \mathbb{Z} \times \mathbb{N}$ such that

$$\left|\alpha - \frac{p_N}{q_N}\right| < \frac{1}{q_N N} \leq \frac{1}{q_N^2}.$$

It suffices to show that there is no pair $(p, q) \in \mathbb{Z} \times \mathbb{N}$ such that for infinitely many $N \in \mathbb{N}$, we have $(p_N, q_N) = (p, q)$. Suppose that we have such (p, q), then

$$\left|\alpha - \frac{p}{q}\right| = \left|\alpha - \frac{p_N}{q_N}\right| < \frac{1}{q_N N} \to 0,$$

contradicting the irrationality of α. □

Lemma 5.6. *Let $D \in \mathbb{N}$ such that $\sqrt{D} \notin \mathbb{N}$, then there exists $n_0 \in \mathbb{Z} \setminus \{0\}$ such that the equation*

$$x^2 - Dy^2 = n_0$$

has infinitely many solutions in $\mathbb{N} \times \mathbb{N}$.

Proof. We know there exist infinitely many $(p, q) \in \mathbb{Z} \times \mathbb{N}$ such that

$$\left|\sqrt{D} - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Observe that

$$\left|p^2 - Dq^2\right| = \left|p - \sqrt{D}q\right| \cdot \left|p + \sqrt{D}q\right| = q^2 \cdot \left|\frac{p}{q} - \sqrt{D}\right| \cdot \left|\frac{p}{q} + \sqrt{D}\right| < q^2 \cdot \frac{1}{q^2} \cdot (2\sqrt{D} + 1)$$

Now, for each pair $(p, q) \in \mathbb{Z} \times \mathbb{N}$, we have

$$\left|p^2 - Dq^2\right| < 2\sqrt{D} + 1.$$

There exists $n_0 \in [-2\sqrt{D} - 1, 2\sqrt{D} + 1]$ such that the equation $x^2 - Dy^2 = n_0$ has infinitely many solutions. □

5.3.1 Diophantine Approximation

Lemma 5.7. *Let $D \in \mathbb{N}$ such that $\sqrt{D} \notin \mathbb{N}$, Let $(x_1, y_1) \in \mathbb{N} \times \mathbb{N}$ such that $x_1^2 - Dy_1^2 = 1$ and x_1 is minimal among all such nontrivial solutions, then for any $(\alpha, \beta) \in \mathbb{N} \times \mathbb{N}$ such that $\alpha^2 - D\beta^2 = 1$, there exists a unique $n \in \mathbb{N}$ such that*

$$\alpha + \sqrt{D}\beta = (x_1 + \sqrt{D}y_1)^n$$
$$\alpha - \sqrt{D}\beta = (x_1 - \sqrt{D}y_1)^n$$

Proof. Since x_1 is minimal among all nontrivial solutions to Pell's equation, then $x_1 + \sqrt{D}y_1$ is minimal among all nontrivial solutions. We argue by contradiction that there exists an n such that

$$(x_1 + \sqrt{D}y_1)^n < \alpha + \sqrt{D}\beta < (x_1 + \sqrt{D}y_1)^{n+1}$$
$$1 < (\alpha + \sqrt{D}\beta)(x_1 - \sqrt{D}y_1)^n < x_1 + \sqrt{D}y_1$$

It suffices to show that if $\gamma + \delta\sqrt{D} = (\alpha + \beta\sqrt{D})(x_1 - \sqrt{D}y_1)^n$, then γ and δ are positive, since $\gamma^2 - D\delta^2 = 1$ so we contradict the minimality of $x_1 + \sqrt{D}y_1$.

First observe that γ and δ are nonzero because Pell's equation. By inspection, at least one of γ and δ is positive.

If $\gamma < 0$ and $\delta > 0$, then since $\gamma^2 > D\delta^2$, we have $-\gamma > \sqrt{D}\delta$. Hence $\gamma + \sqrt{D}\delta < 0$, contradicting $\gamma + \sqrt{D}\delta > 1$.

If $\gamma > 0$ and $\delta < 0$, then we get $\gamma + \sqrt{D}\delta = \frac{1}{\gamma - \sqrt{D}\delta} < 1$, contradiction.

Finally we get that $\gamma, \delta > 0$, contradicting the minimality of $x_1 + \sqrt{D}y_1$. □

Lemma 5.8. *There exist infinitely many $(p, q) \in \mathbb{N} \times \mathbb{N}$ such that*

$$\left|\frac{p}{q} - \sqrt{2}\right| < \frac{1}{2\sqrt{2}q^2}$$

Proof. There exist infinitely many solutions to Pell's Equation.

Let $(p, q) \in \mathbb{N} \times \mathbb{N}$ be a solution to Pell's Equation

$$x^2 - 2y^2 = 1.$$

Now we rewrite the approximation as

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

□

Lemma 5.9. *There exist no $(p, q) \in \mathbb{N} \times \mathbb{N}$ such that*

$$\left|\frac{p}{q} - \sqrt{2}\right| \leq \frac{1}{3q^2}.$$

Proof. If $q = 1$, then

$$\left|\frac{p}{q} - \sqrt{2}\right| \geq \min\left\{2 - \sqrt{2}, \sqrt{2} - 1\right\} = \sqrt{2} - 1 > \frac{1}{3}.$$

Now we assume that $q \geq 2$.

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

Now it suffices to prove that

$$\frac{p}{q} < 3 - \sqrt{2}.$$

If $\frac{p}{q} \geq 3 - \sqrt{2}$, then

$$\left|\frac{p}{q} - \sqrt{2}\right| \geq 3 - 2\sqrt{2} > 0.16 > \frac{1}{3q^2}.$$

□

Lemma 5.10. *There exist no $(p, q) \in \mathbb{N} \times \mathbb{N}$ such that*

$$\left|\frac{p}{q} - \sqrt[4]{2}\right| \leq \frac{1}{12q^4}.$$

Proof. We rewrite as

$$\left|\frac{p}{q} - \sqrt[4]{2}\right| = \frac{\left|p - \sqrt[4]{2}q\right|}{q} = \frac{\left|p^4 - 2q^4\right|}{q^4\left(\frac{p}{q} + \sqrt[4]{2}\right)\left(\frac{p^2}{q^2} + \sqrt{2}\right)} \geq \frac{1}{q^4\left(\frac{p}{q} + \sqrt[4]{2}\right)\left(\frac{p^2}{q^2} + \sqrt{2}\right)}.$$

Observe that $1 < \sqrt[4]{2} < \frac{5}{4}$, so $0 < \frac{p}{q} < \frac{3}{2}$. If otherwise, $\frac{p}{q} \geq \frac{3}{2}$, then $\left|\frac{p}{q} - \sqrt[4]{2}\right| > \frac{1}{4} > \frac{1}{12q^4}$. Hence $\frac{p}{q} < \frac{3}{2}$, so $\frac{p}{q} + \sqrt[4]{2} < 3$. Similarly, $\frac{p^2}{q^2} + \sqrt{2} < 4$. □

Another approach that does not involve numerically expressing irrational numbers is as follows. Assume that $\left|\frac{p}{q} - \sqrt[4]{2}\right| < 1$, otherwise it is not a good approximation.

$$\begin{aligned}
\left|\frac{p}{q} + \sqrt[4]{2}\right| &= \left|\frac{p}{q} - \sqrt[4]{2} + \sqrt[4]{2} + \sqrt[4]{2}\right| < 1 + 2\sqrt[4]{2} \\
\left|\frac{p}{q} + i\sqrt[4]{2}\right| &= \left|\frac{p}{q} - \sqrt[4]{2} + \sqrt[4]{2} + i\sqrt[4]{2}\right| < 1 + \left|\sqrt[4]{2} + i\sqrt[4]{2}\right| \\
\left|\frac{p}{q} - i\sqrt[4]{2}\right| &= \left|\frac{p}{q} - \sqrt[4]{2} + \sqrt[4]{2} - i\sqrt[4]{2}\right| < 1 + \left|\sqrt[4]{2} - i\sqrt[4]{2}\right|
\end{aligned}$$

Then we can rewrite the error as

$$\begin{aligned}
\left|\frac{p}{q} - \sqrt[4]{2}\right| &= \frac{\left|p^4 - 2q^4\right|}{q^4\left(\frac{p}{q} + \sqrt[4]{2}\right)\left(\frac{p^2}{q^2} + \sqrt{2}\right)} \\
&= \frac{\left|p^4 - 2q^4\right|}{q^4\left|\frac{p}{q} + \sqrt[4]{2}\right|\left|\frac{p}{q} + i\sqrt[4]{2}\right|\left|\frac{p}{q} - i\sqrt[4]{2}\right|} \\
&> \frac{1}{q^4(1 + \left|\sqrt[4]{2} - (-\sqrt[4]{2})\right|)(1 + \left|\sqrt[4]{2} - (-i\sqrt[4]{2})\right|)(1 + \left|\sqrt[4]{2} - (i\sqrt[4]{2})\right|)}
\end{aligned}$$

5.3.2 Liouville's Theorem

Definition 5.2. A number $\alpha \in \mathbb{C}$ is algebraic if $\exists f \in \mathbb{Z}[x] \setminus \{0\}$ such that $f(\alpha) = 0$. The minimum degree d for such a polynomial is called the degree of α.

Definition 5.3. A number is trancendental if it is not algebraic.

Remark 5.1. Observe the following.

- $d = 1 \iff \alpha \in \mathbb{Q}$.
- The set of all algebraic numbers is countable.
- If $f \in \mathbb{Z}[x]$ is monic, then α is an algebraic integer.

Lemma 5.11. *If α has degree d and $f \in \mathbb{Z}[x]$ has degree d and $f(\alpha) = 0$, then f is irreducible.*

Proof. Otherwise, let $f = g \cdot h; g, h \in \mathbb{Z}[x]$. Then $\deg g, \deg h < \deg f$, contradicting the minimality of $\deg f$. $\square$

Remark 5.2. Let f be the minimal polynomial, then if $\deg(f) \geq 2$, then f has no root which is a rational number.

Remark 5.3. All the roots of f are simple (multiplicity 1).

Proof. Otherwise, f and f' would share a root. The $\gcd(f, f') = g$, where $g \in \mathbb{Q}[x]$ and $\deg g \geq 1$. Then f is reducible, but it cannot be. $\square$

Theorem 5.12 (Liouville's Theorem)**.** *Let α be algebraic of degree $d \geq 2$ and let $f \in \mathbb{Z}[x]$ of degree d such that $f(\alpha) = 0$.*

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0.$$

Let $\alpha_1, \alpha 2, ..., \alpha_d$ be the roots of f. Let $\alpha = \alpha_1$. Let

$$c = \frac{1}{|a_d| \cdot \prod_{i=2}^{d} (1 + |\alpha_i - \alpha 1|}.$$

Then for any $\frac{p}{q} \in \mathbb{Q}$, we have

$$\left| \frac{p}{q} - \alpha \right| > \frac{c}{q^d}.$$

Proof. Let $\frac{p}{q} \in \mathbb{Q}$ and consider

$$\begin{aligned} \left| f(\frac{p}{q}) \right| &= \left| a_d \left(\frac{p}{q} \right)^d + a_{d-1} \left(\frac{p}{q} \right)^{d-1} + \cdots + a_0 \right| \\ &= \frac{\left| a_d p^d + a_{d-1} p^{d-1} q + \cdots + a_0 q^d \right|}{q^d} \\ &\geq \frac{1}{q^d} \end{aligned}$$

Now we look at the roots of f.

$$\left| f(\frac{p}{q}) \right| = \left| a_d \cdot \prod_{i=2}^{d} (\frac{p}{q} - \alpha_i) \right|$$

Now we get the following inequality.

$$\left| \frac{p}{q} - \alpha \right| \geq \frac{1}{q^d \cdot |a_d| \cdot \prod_{i=2}^{d} \left| \frac{p}{q} - \alpha_i \right|}.$$

If $\left| \frac{p}{q} - \alpha \right| \geq 1$, then we are done because $c < 1$.
If $\left| \frac{p}{q} - \alpha \right| < 1$, then for each $i = 2, ..., d$, we have

$$\left| \frac{p}{q} - \alpha_i \right| \leq \left| \frac{p}{q} - \alpha_1 \right| + |\alpha_1 - \alpha_i| < 1 + |\alpha_1 - \alpha_i|.$$

The result of the theorem follows. $\square$

Corollary 5.12.1. *Let* $\beta = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$*, then* β *is trancendental.*

Proof. First observe that $\beta \notin \mathbb{Q}$.

Assume that β is algebraic with degree $d \geq 2$. So $\exists c > 0$ such that for any $\frac{p}{q} \in \mathbb{Q}$, we have

$$\left| \frac{p}{q} - \beta \right| > \frac{c}{q^d}.$$

Let the partial sum of the series be

$$\frac{p_n}{q_n} = \sum_{i=1}^{n} \frac{1}{10^{i!}}.$$

Then we have

$$\begin{aligned} \left| \frac{p_n}{q_n} - \beta \right| &= \sum_{i=n+1}^{\infty} \\ &< \frac{1}{10^{(n+1)!}} \cdot \sum_{i \geq 0} \frac{1}{10^i} = \frac{1}{10^{(n+1)!}} \cdot \frac{1}{1 - \frac{1}{10}} \\ &= \frac{10}{9 \cdot 10^{(n+1)!}} \end{aligned}$$

Now we get the following inequalities,

$$\frac{c}{10^{n! \cdot d}} < \left| \frac{p_n}{q_n} - \beta \right| < \frac{10}{9 \cdot 10^{(n+1)!}}$$

$$\frac{9c}{10} < 10^{n!(d-n-1)} \to 0$$

which is a contradiction. □

5.4 Polynomial-Exponential Equations

Example 5.6. We want to solve the following equation where $m, n \in \mathbb{Z}$.

$$3^m - 2^n = 1.$$

Then $(m, n) = (1, 1), (2, 3)$ are the only solutions

Proof. If $n \geq 2$, then $2^n \equiv 0 \pmod 4$. Then $(-1)^m \equiv 3^m \equiv 1 \pmod 4$, so m is even. Let $m = 2k$. It follows that

$$3^{2k} - 1 = 2^n \implies (3^k - 1)(3^k + 1) = 2^n$$

and the result follows. □

Example 5.7. Another similar equation is

$$3^m - 2^n = -1.$$

Proof. A similar trick but with $3^m = 2^n - 1$ taken modulo 3. □

Example 5.8. Consider the equation

$$n^2017 - 53n + 21) \cdot 10^n + (n+2) \cdot 13^n - (m^4 + 5m + 2) \cdot 6^m - (k^2 + 5k + 2) \cdot 5^k = 2018.$$

Proof. This one will be ugly. □

Example 5.9. Any polynomial-exponential is a linear recurrence sequence.

$$(n^2 + 3) \cdot 2^n + 3^n + (-n + 6) \cdot 12^n$$

gives the recurrence

$$(x-2)^3 \cdot (x-3) \cdot (x-12)^2.$$

Theorem 5.13 (Laurent's Theorem)**.** *The equation*

$$\sum_{i=1}^{l} \sum_{j=1}^{k_i} p_{i,j}(n_i) r_{i,j}^{n_i} = b,$$

where $p_{i,j} \in \mathbb{Z}[x], r_{i,j} \in \mathbb{Z}, n_i \in \mathbb{N}$ are variables, has finitely many solutions if the numbers $r_{i,j}$ are multiplicatively independent. ie. if for some $c_{i,j} \in \mathbb{Z}$, we have $\prod_{i,j} r_{i,j}^{c_{i,j}} = 1$, then $c_{i,j} = 0, \forall i, j$.

Note: The equation could be rewritten as

$$\sum_{i=1}^{l} a_{i,n_i}.$$

Example 5.10. Consider the linear recurrences

$$\begin{aligned}
&\{F_n\}\,; \\
&\{a_0 = 2; a_1 = 3; a_{n+2} = -5a_{n+1} - 2a_n\}\,; \\
&\{b_0 = 1; b_1 = -2; b_2 = 3; b_{n+3} = 7b_{n+2} - 2b_{n+1} + 3b_n\}
\end{aligned}$$

$$F_n + a_m + b_k = 2017.$$

Proof. Laurent's Theorem says this has finitely many solutions. □