A Step to Fermat's Last Theorem

Saiyue Lyu

This is a tiny essay about Lamé's Lemma and Kummer's Lemma using group theory to show a special case of Fermat's Last Theorem : When $\mathbb{Z}[\omega] = \{\sum_{i=1}^{p} a_i\omega^{i-1}\}$ is a unique factorization domain with p being a prime, the equation $x^p + y^p = z^p$ has no integer solution with $p \nmid xyz$. This essay is also based on exercises in Marcus's Number Fields, which is the reference book for PMath 441/641 (Algebraic Number Theory) instructed by Professor Wentang Kuo in my 3A term at University of Waterloo.

For years Fermat's Last Theorem attracts mathematicians, which states that the Diophantine equation

$$x^n + y^n = z^n$$

has no nonzero integer solution (x, y, z) for $n > 2$.

1. Fermat's Last Theorem for cases $n = 1$

It is clear when $n = 1$, $x + y = z$ has a set of integer solutions.

2. Fermat's Last Theorem for cases $n = 2$

When $n = 2$, we would like to find the integer solution of $x^2 + y^2 = z^2$

Up to scalar isomorphism, we may assume $\gcd(x, y, z) = 1$

Define $\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}$ to be the set of Galois integers, it is obvious that $\mathbb{Z}[i]$ is a Euclidean domain, thus a Principle Ideal Domain, a Unique Factorization Domain.

In $\mathbb{Z}[i]$, we have $x^2 + y^2 = (x + iy)(x - iy) = z^2$

Claim : $x + iy$ can be written as $u \cdot \alpha^2$ for some Galois integer α and Galois integer unit u (i.e. $\exists\, v \in \mathbb{Z}[i]$ such that $uv = 1$)

From $(x + iy)(x - iy) = z^2$ and the unique factorization division of $\mathbb{Z}[i]$, it is sufficient to show that $(x + iy)$ and $(x - iy)$ are coprime, i.e. have no common factor. Since if they are coprime and their product is a square, then each of them must be a square).

We suppose for contradiction that Π is a common factor of $(x + iy)$ and $(x - iy)$.

To get the contradiction, we would like to show $\Pi \mid 1$, i.e. Π is a unit.

Since $\Pi|(x + iy)$ and $\Pi|(x - iy)$, we get

$$\Pi \mid (x + iy) + (x - iy) \Rightarrow \Pi \mid 2x$$
$$\Pi \mid (x + iy) \cdot (x - iy) \Rightarrow \Pi \mid z^2$$

Which gives us

$$\Pi \mid \gcd(2x, z^2)$$

By assumption, we have $\gcd(x, y, z) = 1$, thus $\gcd(x, z) = 1$, hence we obtain as long as we prove $\gcd(2, z) = 1$, we would have $\gcd(2x, z^2) = 1$

If $2 \mid z$, we can write $x = 2a+1, y = 2b+1, z = 2c$ for some $a, b, c \in \mathbb{Z}$, then we have

$$x^2 + y^2 = z^2 \Rightarrow 4a^2 + 4a + 4b^2 + 4b + 2 = 4c^2$$

But this is a contradiction since after modulo 4, we have $2 = 0 \mod 4$, hence we must have $2 \nmid z$. Therefore we have $(x+iy)$ and $(x-iy)$ are coprime.

Also consider the Galois integer unit of $\mathbb{Z}[i]$ are ± 1 and $\pm i$, hence we have

$$\begin{aligned} x + yi &= u \cdot (a+bi)^2 \text{ for some } a, b \in \mathbb{Z} \\ &= u \cdot (a^2 - b^2 + 2abi) \end{aligned}$$

Hence we finally obtain the value set of x, y, z :

$$\{x, y\} = \{\pm(a^2 - b^2) \pm 2ab\}, \; z = \pm(a^2 \pm b^2), a, b \in \mathbb{Z}$$

3. Fermat's Last Theorem for cases $n = 3$

When $n = 3$, $x^3 + y^3 = z^3$ has no solution by direct proof

1. Fermat's Last Theorem for cases $n > 3$

Consider when $n \geq 3$, the problem can be reduced to $n = p$, for p being a prime since if $p \mid n$ and $n \neq 2^k$, $x^n + y^n = z^n \iff (x^{n/p})^p + (y^{n/p})^p = (z^{n/p})^p$

Also note when $n = 4$ (also the case for $p = 2$), the equation has no integer solution, which is a direct consequence by the case when $n = 2$.

So now consider the reduced problem when $p > 3$. Define the $p-$th root of unit to be $\omega = e^{2\pi i/p}$. At this stage, we only look at the case when $p \nmid xyz$, which is the famous **Lamé's Lemma** :

Let $p > 3$ be a prime. Assume $\mathbb{Z}[\omega] = \{a_0 + a_1\omega + \cdots + a_{p-1}\omega^{p-1}\}$ is a Unique Factorization Domain (UFD). If $p \nmid xyz$, then $x^p + y^p = z^p$ has no integer solutions.

We proceed by contradiction. Suppose that $x^p + y^p = z^p$ for some nonzero $x, y, z \in \mathbb{Z}$.
Considering that $x^p + y^p = (x+y)(x+y\omega)(x+y\omega^2)\cdots(x+y\omega^{p-1}) = z^p$
Let $y = -1$, we have

$$\begin{aligned} (x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{p-1}) &= x^p + (-1)^p = x^p - 1 \text{ as } p \text{ is odd} \\ &= (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1) \text{ as } p \text{ is odd} \end{aligned}$$

Here $x \neq 1$, otherwise $z^p = 1^p + (-1)^p = 0$ leads to $p \mid xyz$, hence have :

$$(x-\omega)(x-\omega^2)\cdots(x-\omega^{p-1}) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

Now take $x = 1$, we have :

$$(1-\omega)(1-\omega^2)\cdots(1-\omega^{p-1}) = p$$

Claim 1 : $x + y\omega = u\alpha^p$ for some unit $u \in \mathbb{Z}[\omega]$ and $\alpha \in \mathbb{Z}[\omega]$.

Assume Π is a prime element with $\Pi \mid (x + y\omega)$. And suppose for contradiction that $\Pi \mid (x + y\omega^i)$, for some $i = 0,$ or $2 \leq i \leq p - 1$, i.e.

$$\Pi \mid (x + y\omega^i)$$

With the previous condition

$$\Pi \mid (x + y\omega)$$

By modular property, we have :

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

This leads to : $\Pi \mid z$

On the other hand, since $\Pi \mid (x + y\omega^i)$ and $\Pi \mid (x + y\omega)$, have :

$$\Pi \mid \big((x + y\omega) - (x + y\omega^i)\big) \Rightarrow \Pi \mid y\omega(1 - \omega^{i-1})$$

Since $0 \leq i < p, i \neq 1$ by assumption

Then $(1 - \omega^{i-1})$ is one of the factors in the product $(1 - \omega)(1 - \omega^2)\cdots(1 - \omega^{p-1}) = p$

Hence have $y(1 - \omega^{i-1}) \mid yp$, then $\Pi \mid y\omega p$, thus $\Pi \mid yp$ as ω is a unit

Since z and yp are co-prime, then $\exists m, n \in \mathbb{Z}$ such that $zm + ypn = 1$

Consider $\Pi \mid z, \Pi \mid yp$ and $m, n \in \mathbb{Z}$, hence $\Pi \mid (zm + ypn) \Rightarrow \Pi \mid 1$

This contradicting the fact that Π is a prime element.

Therefore $\Pi \nmid (x + y\omega^i), \forall i = 0$ or $2 \leq i \leq p - 1$

Since if $\Pi \mid (x + y\omega)$, then $\Pi \nmid (x + y\omega^i), \forall i = 0,$ or $2 \leq i \leq p - 1$

Then $(x + y\omega)$ and $\prod_{\substack{i \neq 1}}^{0 \leq i \leq p-1} (x + y\omega^i)$ are relatively prime $\forall i = 0,$ or $2 \leq i \leq p - 1$

Note that their product is a pth power and $\mathbb{Z}[\omega]$ is a UFD by assumption.

Since no irreducible factor will appear in $(x + y\omega)$ and $\prod_{\substack{i \neq 1}}^{0 \leq i \leq p-1} (x + y\omega^i)$

Then each factor appearing in $(x + y\omega)$ must appear a multiple of p times.

I.e. must have $x + y\omega$ is a pth power, up to unit multiple.

Therefore $x + y\omega = u\alpha^p$ for some unit $u \in \mathbb{Z}[\omega]$ and $\alpha \in \mathbb{Z}[\omega]$

Now consider dropping the assumption that $\mathbb{Z}[\omega]$ is a UFD but using the fact that ideals factors uniquely (up to order) into prime ideals.

Claim 2 : The principal ideal $< x + y\omega >= I^p$ for some ideal I.

Suppose for contradiction that Δ is a common prime ideal factor of $< x + y\omega >$ and $< x + y\omega^i >$, for some $i = 0, 2 \cdots p - 1$. By equation (1'), also have

$$\Delta \mid < z >^p$$

Since Δ is prime, this forces $\Delta \mid < z >$, i.e.

$$< z > \subset \Delta \tag{1}$$

Since $\Delta \mid < x+y\omega >$, $\Delta \mid < x+y\omega^i >$, then $\Delta \mid \ (< x+y\omega > + < x+y\omega^i >)$, i.e.

$$\begin{aligned}\Delta \supset \ (< x+y\omega > + < x+y\omega^i >) &= < x+y\omega, x+y\omega^i > \\ &= < x+y\omega, (x+y\omega)-(x+y\omega^i) > \\ &= < x+y\omega, y\omega(1-\omega^{i-1}) > \\ &\supset < y\omega(1-\omega^{i-1}) > = < y >< 1-\omega^{i-1} >\end{aligned}$$

Since $0 \le i \le p-1, i \ne 1$ by assumption, then have

$$< 1-\omega^{i-1} > | < 1-\omega >< 1-\omega^2 > \cdots < 1-\omega^{p-1} > = < p >$$
$$< y >< 1-\omega^{i-1} > | < y >< p > = < yp > \implies < y >< 1-\omega^{i-1} > \supset < yp >$$

Hence have :

$$\Delta \supset < yp > \tag{2}$$

Combining (1) and (2), have

$$< z > + < yp > \subset \Delta$$

Since z and yp are relatively prime, then $\exists\, m, n \in \mathbb{Z}$ such that $zm + ypn = 1$, hence

$$1 \in < z > + < yp > \subset \Delta$$

Which is a contradiction since Δ can not contain 1 as a proper ideal
Therefore $< x+y\omega >$ has no common prime ideal factor with $< x+y\omega^i >, \forall i = 0, 2, \cdots, p-1$
Then, $< x+y\omega >$ and $\prod_{i\ne 1}^{0\le i\le p-1} < x+y\omega^i >$ have no common prime ideal factors.
By the **Unique Prime Ideal Factorization** applied to equation (1'),
Each factor appearing in $< x+y\omega >$ must appear a multiple of p times
Note also factors appearing in $< x+y\omega >$ must not appear in $\prod_{i\ne 1}^{0\le i\le p-1} < x+y\omega^i >$
Therefore $< x+y\omega > = I^p$ for some ideal I.

Claim 3 : Every element of $\mathbb{Q}[\omega]$ is uniquely representable in the form

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2} \qquad \forall 0 \le i \le p-2,\ a_i \in \mathbb{Q}$$

When $\omega = e^{2\pi i/p}$, we have :

$$\begin{aligned}\Phi_p(\omega) &= \omega^{p-1} + \omega^{p-2} + \cdots + \omega + 1 \\ &= \frac{\omega^p - 1}{\omega - 1} \qquad\qquad \text{as } \omega \ne 1 \\ &= \frac{(e^{2\pi i/p})^p - 1}{\omega - 1} \\ &= \frac{e^{2\pi i} - 1}{\omega - 1} \\ &= 0\end{aligned}$$

Hence ω is a root of the cyclotomic polynomial $\Phi_p(x)$. Moreover,

$$\begin{aligned}\Phi_p(x+1) &= \frac{(x+1)^p - 1}{(x+1)-1} \\ &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}\end{aligned}$$

Using Eisenstein's Criterion with p as $p \nmid 1, p^2 \nmid \binom{p}{p-1}, p \mid \binom{p}{i}, \forall 1 \le i \le p-1$
Hence $\Phi_p(x+1) \in \mathbb{Q}[x]$ is irreducible, thus so is $\Phi_p(x) \in \mathbb{Q}[x]$
Therefore $\Phi_p(x)$ is the minimal polynomial for ω over $\mathbb{Q}$

By definition, every element in $\mathbb{Q}[\omega]$ can be wrriten as the form

$$\alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \cdots + \alpha_n\omega^n \text{ for some } n \text{ and } \alpha_i \in \mathbb{Q}, \forall i$$

When $n = p-2$, we are done immediately.
When $n < p-2$, we are done by setting $\alpha_j = 0 \in \mathbb{Q}, \forall n+1 \le j \le p-2$
Hence WLOG, we assume $n \ge p-1$
Since $\Phi_p(\omega) = \omega^{p-1} + \omega^{p-2} + \cdots + \omega + 1 = 0$ by above, have

$$\omega^{p-1} = -(\omega^{p-2} + \cdots + \omega + 1)$$

Then any element in $\mathbb{Q}[\omega]$ can be written as

$$\begin{aligned}\alpha_0 + \alpha_\omega + \alpha_2\omega^2 + \cdots + \alpha_n\omega^n &= \alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \cdots + \alpha_{n-1}\omega^{n-1} + \alpha_n\omega^{n-p+1}\omega^{p-1} \\ &= \alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \cdots + \alpha_{n-1}\omega^{n-1} - \alpha_n\omega^{n-p+1}(\omega^{p-2} + \cdots + \omega + 1) \\ &= \beta_0 + \beta_1\omega + \beta_2\omega^2 + \cdots + \beta_{n-1}\omega^{n-1}\end{aligned}$$

where

$$\beta_i = \begin{cases}\alpha_i, & \text{for } 0 \le i < n-p+1 \\ \alpha_i - \alpha_n, & \text{for } n-p+1 \le i \le n-1\end{cases}$$

I.e., $\alpha_0 + \alpha_\omega + \alpha_2\omega^2 + \cdots + \alpha_n\omega^n$ can be written in the form $\beta_0 + \beta_1\omega + \beta_2\omega^2 + \cdots + \beta_{n-1}\omega^{n-1}$
By iteration (or induction), $\alpha_0 + \alpha_\omega + \alpha_2\omega^2 + \cdots + \alpha_n\omega^n$ can be written in the form

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2} \text{ for some } a_i \in \mathbb{Q}, \forall 0 \le i \le p-2$$

Now it remains to show the uniqueness of this representation.
Suppose that some element in $\mathbb{Q}[\omega]$ achieves 2 representation, i.e.

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2} = b_0 + b_1\omega + b_2\omega^2 + \cdots + b_{p-2}\omega^{p-2} \text{ for some } a_i, b_i \in \mathbb{Q}$$

$$(a_0 - b_0) + (a_1 - b_1)\omega + (a_2 - b_2)\omega^2 + \cdots + (a_{p-2} - b_{p-2})\omega^{p-2} = 0$$

Hence ω is a root of $f(x) \in \mathbb{Q}[x]$ where

$$f(x) = (a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 + \cdots + (a_{p-2} - b_{p-2})x^{p-2}$$

Since $\Phi_p(x)$ is the minimal polynomial of ω over $\mathbb{Q}$ by above, then have

$$\Phi_p(x) \mid f(x)$$
$$(1 + x + \cdots + x^{p-2} + x^{p-1}) \mid \left((a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 + \cdots + (a_{p-2} - b_{p-2})x^{p-2}\right)$$

This forces $f(x) = 0$ as $\deg \Phi_p = p - 1 > p - 2 = \deg f$
Hence $a_i = b_i, \forall 0 \leq i \leq p-2$, i.e. the representation is unique.

Therefore every element in $\mathbb{Q}[\omega]$ is uniquely representable in the form

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2} \qquad \forall 0 \leq i \leq p-2,\ a_i \in \mathbb{Q}$$

By the similar steps in **Claim 3**,
we can show that every element in $\mathbb{Z}[\omega]$ can be written in the form

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2} \qquad \forall 0 \leq i \leq p-2,\ a_i \in \mathbb{Z}$$

If $p \mid \alpha$, i.e.$\alpha = p \cdot \beta$ for some $\beta = b_0 + b_1\omega + b_2\omega^2 + \cdots + b_{p-2}\omega^{p-2} \in \mathbb{Z}[\omega]$, then

$$\begin{aligned}
\alpha = a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2} &= p\beta \\
&= p(b_0 + b_1\omega + b_2\omega^2 + \cdots + b_{p-2}\omega^{p-2}) \\
&= pb_0 + pb_1\omega + pb_2\omega^2 + \cdots + pb_{p-2}\omega^{p-2}
\end{aligned}$$

Since the representation of α is unique by the result from **Claim 3**
Then $a_i = pb_i,\ \forall 0 \leq i \leq p-2$
Therefore $\forall 0 \leq i \leq p-2,\ p \mid a_i$

Now define congruence $\mod p$ for $\beta, \gamma \in \mathbb{Z}[\omega]$ as follows:

$$\beta \equiv \gamma \mod p \iff \beta - \gamma = p\delta \text{ for some } \delta \in \mathbb{Z}[\omega]$$

In terms of the language of ideal, this is congruence mod the principal ideal $p\mathbb{Z}[\omega]$

Claim 4 : If $\beta \equiv \gamma$, then $\bar{\beta} \equiv \bar{\gamma}$, where the bar denotes complex conjugation.
By definition of congruence in $\mathbb{Z}[\omega]$, since $\beta \equiv \gamma$, then $\beta - \gamma = p\delta$ for some $\delta \in \mathbb{Z}[\omega]$
Take the conjugate of both sides, we have :

$$\begin{aligned}
\overline{\beta - \gamma} &= \overline{p\delta} \\
\bar{\beta} - \bar{\gamma} &= \bar{p}\bar{\delta} \\
\bar{\beta} - \bar{\gamma} &= p\bar{\delta}
\end{aligned}$$

Also note that

$$\bar{\omega} = e^{\overline{2\pi i}/p} = e^{-2\pi i/p} = e^{-2\pi i/p + 2\pi i} = e^{(p-1)2\pi i/p} = (e^{2\pi i/p})^{p-1} = \omega^{p-1}$$

By the iteration procedure in **Claim 3**,
We have that ω^{p-1} can be written in the form $\beta_0 + \beta_1\omega + \beta_2\omega^2 + \cdots + \beta_{n-1}\omega^{n-1}$

Hence $\bar{\omega} \in \mathbb{Z}[\omega]$
Similarly in **Claim 3**, $\delta \in \mathbb{Z}[\omega]$ can be written in the form $a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2}$
It follows that $\bar{\delta} \in \mathbb{Z}[\omega]$, i.e. $\bar{\beta} \equiv \bar{\gamma} \mod p$ by definition

Claim 5 : $(\beta+\gamma)^p \equiv \beta^p + \gamma^p \mod p$
By definition, it suffices to show that

$$(\beta+\gamma)^p - (\beta^p + \gamma^p) = p\delta \text{ for some } \delta \in \mathbb{Z}[\omega]$$

By Binomial Theorem, we have

$$\begin{aligned}(\beta+\gamma)^p - (\beta^p + \gamma^p) &= \sum_{k=1}^{p-1} \binom{p}{k} \beta^k \gamma^{p-k} \\ &= \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} \beta^k \gamma^{p-k}\end{aligned}$$

Since $p \mid p!, , p \nmid k!(p-k)!$ for all $1 \le k \le p-1$, we have $p \mid \binom{p}{k}$ for all $1 \le k \le p-1$, i.e.

$$(\beta+\gamma)^p - (\beta^p + \gamma^p) = p \cdot \sum_{k=1}^{p-1} \frac{(p-1)!}{k!(p-k)!} \beta^k \gamma^{p-k} \text{ where } \sum_{k=1}^{p-1} \frac{(p-1)!}{k!(p-k)!} \beta^k \gamma^{p-k} \in \mathbb{Z}[\omega]$$

Therefore $(\beta+\gamma)^p \equiv \beta^p + \gamma^p \mod p$

The generalization of this is $(\beta_1 + \cdots + \beta_n)^p \equiv \beta_1^p + \cdots + \beta_n^p$ for all $n \ge 2$
To show this, we proceed by induction on n.
We have proven that the case when $n = 2$ holds.
Assume we have the congruence equation for given n, i.e.

$$(\beta_1 + \cdots + \beta_n)^p \equiv \beta_1^p + \cdots + \beta_n^p$$

Then we consider the case for $n+1$:

$$\begin{aligned}(\beta_1 + \cdots + \beta_n + \beta_{n+1})^p &\equiv (\beta_1 + \cdots + \beta_n)^p + \beta_{n+1}^p && \text{by the case when } n = 2 \\ &\equiv \beta_1^p + \cdots + \beta_n^p + \beta_{n+1}^p && \text{by assumption of case } n\end{aligned}$$

Therefore $(\beta_1 + \cdots + \beta_n)^p \equiv \beta_1^p + \cdots + \beta_n^p$ holds for all $n \ge 2$

Claim 6 : For any $\alpha \in \mathbb{Z}[\omega]$, there exists $a \in \mathbb{Z}$ such that $\alpha^p \equiv a \mod p$
For any $\alpha \in \mathbb{Z}[\omega]$, by **Claim 3** and direct sequence after it, have

$$\alpha = a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2} \text{ with all } a_i \in \mathbb{Z}$$

Hence we have :

$$\begin{aligned}\alpha^p &= (a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2})^p \\ &\equiv a_0^p + a_1^p\omega^p + a_2^p\omega^{2p} + \cdots + a_{p-2}^p\omega^{(p-2)p} \mod p && \text{by the generalized result from } \textbf{Claim 5} \\ &= a_0^p + a_1^p + a_2^p + \cdots + a_{p-2}^p && \text{as } \omega^i\text{'s are } p\text{th roots of unity}\end{aligned}$$

Therefore we have $\alpha^p \equiv a \mod p$ with $a = a_0^p + a_1^p + a_2^p + \cdots + a_{p-2}^p \in \mathbb{Z}$

Now we introduce another lemma to prove **Lamé's Lemma**, which is **Kummer's Lemma**:

If u is a unit in $\mathbb{Z}[\omega]$ and $\bar{u}$ is its complex conjugate, then $u/\bar{u}$ is a power of ω

If all roots of monic polynomial $f(x)$ have absolute value 1, then we have

$$f(x) = (x-1)^k (x+1)^l \text{ where } k+l=n$$

Then the absolute value of the coefficient of x^r is

$$\begin{aligned}\Big| \sum_{i=0}^{r} (-1)^{k-i} \binom{k}{i}\binom{l}{r-i} \Big| &\leq \sum_{i=0}^{r} \Big| (-1)^{k-i} \binom{k}{i}\binom{l}{r-i} \Big| \\ &\leq \sum_{i=0}^{r} \Big| (-1)^{k-i} \binom{k}{i} \Big| \cdot \Big| \binom{l}{r-i} \Big| \\ &= \sum_{i=0}^{r} \binom{k}{i}\binom{l}{r-i} = \binom{n}{r}\end{aligned}$$

Therefore the coefficient of x^r has absolute value $\leq \binom{n}{r}$

Let α be an algebraic integer of degree n and $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n$ be the conjugates
Let $f(x)$ be the minimal polynomial of $\alpha \in \mathbb{A}$. Hence have $f(x) \in \mathbb{Z}[x]$
Consider also $f(x) = \big(x - \sigma_1(\alpha)\big)\cdots\big(x - \sigma_n(\alpha)\big) = (x-\alpha_1)\cdots(x-\alpha_n)$
Hence all roots of $f(x)$ have absolute value 1
By the result from part (i), the coefficient of x^r, say c_r, is $\leq \binom{n}{r}$
Also $c_r \in \mathbb{Z}$, thus there are only finitely many choices for c_r
Let S be the set of such $f(x)$ with degree n and any algebraic integer α of degree n with absolute value 1 is a root of an element in S, i.e.

$$S = \{f(x) \in \mathbb{Z}[x] \mid def\, f = n, f(\alpha) = 0 \text{ for some } \alpha \in \mathbb{A} \text{ with } |\sigma_i(\alpha)| = 1, \forall 1 \leq i \leq n\}$$

Since each coefficient of $x^r, \forall 0 \leq r \leq n$ has only finitely many choices, this forces

$$|S| < \infty$$

Since $def\, f = n < \infty$, hence such f has at most n roots
Now S is a finite set of f with finitely many roots and α is one of those roots
It follows that there are only finitely many such $\alpha \in \mathbb{A}$, i.e. there are only finitely many algebraic integers α of fixed degree n, all of whose conjugates (including α) have absolute value 1 for a fixed n.
Let $\beta = \alpha^s$ be a power of α, thus $\beta \in \mathbb{Q}[\alpha]$, moreover β has degree $\leq n$
Let $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n$ be the conjugates of α with embedding $\sigma_1, \cdots, \sigma_n$ from $\mathbb{Q}[\alpha]$ to $\mathbb{C}$
Hence $\forall 1 \leq i \leq n$, $\sigma_i(\alpha) = \alpha_i$, moreover, it also sends α^s to α_i^s
Thus $\alpha_1^s = \beta, \alpha_2^s, \cdots, \alpha_n^s$ are conjugates of β
Since $deg\, \beta \leq n$, hence there are at most n conjugates of β
Hence all conjugates of α^s are $\alpha_1^s = \beta, \alpha_2^s, \cdots, \alpha_n^s$

Note that the absolute value of α_i^s is $1^s = 1$ as if $\alpha_i = r \cdot e^{i\theta}$ with absolute value $|r| = 1$, then $\alpha_i^s = r^s \cdot e^{is\theta}$ with absolute value $|r^s| = 1$

Now any power β of α has degree $\le n$ and all its conjugates have absolute value 1

By the result in part above, there are finitely many such power of α, then

$$\exists\, p, q \in \mathbb{N} \text{ with } p > q \text{ such that } \alpha^p = \alpha^q$$

Therefore $\alpha^{p-q} = 1$ for some $p - q \in \mathbb{N}$, i.e. α is a root of unity.

This means **an algebraic integer α, all of whose conjugates (including α) have absolute value 1, must be a root of unity.**

Let $\sigma : \mathbb{C} \to \mathbb{C}$ be the complex conjugation, i.e. $\sigma(\omega) = \bar{\omega} = \omega^{-1}$

Hence we have $\sigma \in Gal\big(\mathbb{Q}(\omega)/\mathbb{Q}\big) \cong \big(\mathbb{Z}/p\mathbb{Z}\big)^*$, which is an abelian group

Hence for any $\tau \in Gal\big(\mathbb{Q}(\omega)/\mathbb{Q}\big)$, it commutes with σ, hence we have

$$\begin{aligned} |\tau(u/\bar{u})| = |\tau\big(u/\sigma(u)\big)| &= |\tau(u)/\tau\big(\sigma(u)\big)| \\ &= |\tau(u)/\sigma\big(\tau(u)\big)| \\ &= |\tau(u)|/|\sigma\big(\tau(u)\big)| \\ &= |\tau(u)|/|\tau(u)| = 1 \end{aligned}$$

It follows that all conjugates of $u/\bar{u}$ have absolute value 1.

Also note that $u/\bar{u}$ is an algebraic integer as u is a unit in $\mathbb{Z}[\omega]$

By the result from above, $u/\bar{u}$ is a root of unity

Recall that with p being an odd prime, the only roots of unity in $\mathbb{Q}[\omega]$ are the $2p$–th root of unity, i.e. $\pm\omega^k$ for some k

Therefore $u/\bar{u} = \pm\omega^k$ for some k

Now suppose for contradiction that $u/\bar{u} = -\omega^k$, i.e. $u^p = -\bar{u}^p$

By the result from **Claim 6**, there exists $a \in \mathbb{Z}$ such that

$$u^p \equiv a \mod p$$

By the result from consequence of **Claim 3**,

$$\bar{u}^p \equiv \bar{a} \mod p$$

Hence we have

$$-\bar{u}^p \equiv -\bar{a} \equiv -a \mod p$$

Hence $u^p = -\bar{u}^p$ implies $a \equiv -a \mod p$, i.e. $2a \equiv 0 \mod p$, which is $p \mid 2a$

Since p is odd, this forces $p \mid a$

Thus $u^p \equiv a \mod p$ implies $p \mid u^p$

Which is a contradiction since u^p is a unit while p is not

Therefore in $u/\bar{u} = \pm\omega^k$, only the $+$ holds, i.e. $u/\bar{u}$ is a power of ω.

Now back to our main proof of **Lamé's Lemma**:

Claim 7 : With $p \ge 5$, $x + y\omega \equiv (x + y\omega^{-1})\omega^k \mod p$

By the result of **Claim 2** and the definition of congruencein $\mathbb{Z}[\omega]$, we have

$$x + y\omega \equiv u\alpha^p \mod p \qquad \text{for some unit } u \in \mathbb{Z}[\omega] \text{ and some } \alpha \in \mathbb{Z}[\omega] \tag{3}$$

By the result of **Claim 6**, $\exists\, a \in \mathbb{Z}$ such that

$$\alpha^p \equiv a \mod p \tag{4}$$

Combing (3) &(4), we have :

$$x + y\omega \equiv ua \mod p \tag{5}$$

By Kummer's Lemma, have

$$u = \bar{u}\omega^k \text{ for some } k \in \mathbb{Z} \tag{6}$$

Combing (5) & (6), we have

$$x + y\omega \equiv \bar{u}\omega^k a \mod p \tag{7}$$

By the result of **Claim 5**, taking the congruence of both sides of (5), we have

$$\overline{x + y\omega} \equiv \overline{ua} \mod p \tag{8}$$
$$x + y\omega^{-1} \equiv \bar{u}a \mod p \tag{9}$$

Combing (7) & (9), we have

$$x + y\omega \equiv \bar{u}\omega^k a \equiv (x + y\omega^{-1})\omega^k \mod p$$

I.e., $x + y\omega \equiv (x + y\omega^{-1})\omega^k \mod p$ for some $k \in \mathbb{Z}$

For $k \in \mathbb{Z}$ determined in **Claim 7**, we can write $k = np + s$ for some $0 \le n, 0 \le s < p$
By the result of **Claim 7**, we have $x + y\omega \equiv (x + y\omega^{-1})\omega^k \mod p$, i.e.

$$p \mid \big((x + y\omega) - (x + y\omega^{-1})\omega^k\big)$$

- When $s = 0$, i.e. $k = np$, have

$$\begin{aligned}
(x + y\omega) - (x + y\omega^{-1})\omega^k &= (x - x\omega^{np}) + y(\omega - \omega^{np-1}) \\
&= y(\omega - \omega^{np-1}) \\
&= y(\omega - \omega^{p-1}) && \text{as } \omega^{(n-1)p} \text{ is a } p\text{th roots of unity} \\
&= y(\omega - 1 - \omega - \omega^2 - \cdots - \omega^{p-2}) && \text{by the result of } \textbf{Claim 3} \\
&= y(-1 - \omega^2 - \omega^3 - \cdots - \omega^{p-2})
\end{aligned}$$

Since $p \nmid y$ by assumption, this forces

$$p \mid (-1 - \omega^2 - \omega^3 - \cdots - \omega^{p-2})$$

By the result of consequence after **Claim 3**, this leads to

$$p \mid (-1) \mod p$$

Which contradicts the assumption that $p \geq 5$

- When $s = p-1$, i.e. $k \equiv p-1 \mod p$, have

$$\begin{aligned}(x+y\omega)-(x+y\omega^{-1})\omega^k &= (x - x\omega^{np+p-1}) + y(\omega - \omega^{np+p-1-1}) \\ &= (x - x\omega^{p-1}) + y\omega - y\omega^{p-2} && \text{as } \omega^{np} \text{ is a } p\text{th roots of unity} \\ &= x(1+1+\omega+\cdots+\omega^{p-2}) + y(\omega-\omega^{p-2}) && \text{by the result of } \textbf{Claim 3} \\ &= 2x + (x+y)\omega + x(\omega^2+\cdots+\omega^{p-3}) + (x-y)\omega^{p-2}\end{aligned}$$

By the result of consequence after **Claim 3**, have :

$$p \mid (2x), \ , p \mid (x+y)$$

$$p \mid x \tag{10}$$

$$p \mid (x-y)$$

But (10) contradicts the assumption that $p \nmid x$

- Hence $1 \leq s \leq p-2$

It follows that $\big((x+y\omega)-(x+y\omega^{-1})\omega^k\big)$ can be written in the form

$$\begin{aligned}\big((x+y\omega)-(x+y\omega^{-1})\omega^k\big) &= x + y\omega + y\omega^{k-1} - x\omega^k \\ &= x + y\omega + y\omega^{np+s-1} - x\omega^{np+s} \\ &= x + y\omega + y\omega^{s-1} - x\omega^s \\ &= a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2} \text{ for some } a_i \in \mathbb{Z}\end{aligned}$$

Which by the result of consequence after **Claim 3**, the coefficient of ω^0 and ω^1 must be divisible by p

But have $p \nmid x$ and $p \nmid y$

So the coefficient of ω^0 is not x and the coefficient of ω^0 is not y

This forces $\{\omega^{s-1}, \omega^s\} = \{\omega^0, \omega^1\}$

Hence must have $s-1=0, s=1$

Therefore $k \equiv 1 \mod p$

Hence we have

$$\omega^k = \omega \tag{11}$$

Combing (11) and the result of **Claim 7**, have

$$x + y\omega = (x+y\omega^{-1})\omega^k = (x+y\omega^{-1})\omega = x\omega + y \mod p$$

I.e., $p \mid \big((x-y)+(x-y)\omega\big)$

By the result of (vii), have $p \mid (x-y)$

Therefore $x \equiv y \mod p$

Up till now we get a statement saying with the assumption of **Lamé's Lemma**, we would have $x \equiv y \mod p$

Since $p > 3$ is prime, thus odd, then have

$$x^p + y^p = z^p \iff x^p + (-z)^p = (-y)^p$$

Apply the statement to $(x, -z, -y)$, we have

$$x \equiv -z \mod p$$

Thus $2x^p \equiv x^p + y^p = z^p \equiv (-x)^p \mod p$, which gives

$$3x^p \equiv 0 \mod p$$

Hence $p \mid 3x^p$, which is a contradiction since $p > 3$ and $p \nmid x$.

Therefore we finished the proof of **Lamé's Lemma**, under which circumstance, the equation has no integer solution.

4. Discussion

Note that the assumption of **Lamé's Lemma** that $\mathbb{Z}[\omega]$ is a UFD is very important since $\mathbb{Z}[\omega]$ is not always UFD in fact. For example, when $p = 23$, $\mathbb{Z}[\omega]$ is not a UFD. In the proof above, it drops the assumption that $\mathbb{Z}[\omega]$ is a UFD by using the properties of principle ideal domain.