Cyclotomic Fields and Kummer's Theorem

A short story

Sunil Vittal [1]

Dorm Lecture

Table of Contents

Kummer's Theorem

Kummer's Theorem

For regular primes $p \geq 3$, the equation $x^p + y^p = z^p$ has no solutions.

- A regular prime is a prime that doesn't divide the class number of $\mathbb{Q}[\zeta_p]$

Kummer's Theorem

Kummer's Theorem

For regular primes $p \geq 3$, the equation $x^p + y^p = z^p$ has no solutions.

- A regular prime is a prime that doesn't divide the class number of $\mathbb{Q}[\zeta_p]$
- Two cases: $p \nmid xyz$ and $p \mid xyz$ where x, y, z are pairwise relatively prime. We will do $p \nmid xyz$

Table of Contents

Number Fields, Norms, and the Discriminant

For our purposes, number fields often look like $\mathbb{Q}[\alpha]$ where α is the root of some monic rational polynomial. Today, our Number Field of choice is $K = \mathbb{Q}[\zeta]$ where ζ is a pth root of unity. $(\zeta^p = 1)$

- Its minimum polynomial is $\frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1$

Number Fields, Norms, and the Discriminant

For our purposes, number fields often look like $\mathbb{Q}[\alpha]$ where α is the root of some monic rational polynomial. Today, our Number Field of choice is $K = \mathbb{Q}[\zeta]$ where ζ is a pth root of unity. ($\zeta^p = 1$)

- Its minimum polynomial is $\frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1$
- If $\alpha = a + b\zeta$, $N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{p-1}(a + b\zeta^i)$. The key idea for today will be that there's $p-1$ multiplications occuring.

Number Fields, Norms, and the Discriminant

For our purposes, number fields often look like $\mathbb{Q}[\alpha]$ where α is the root of some monic rational polynomial. Today, our Number Field of choice is $K = \mathbb{Q}[\zeta]$ where ζ is a pth root of unity. $(\zeta^p = 1)$

- Its minimum polynomial is $\frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$
- If $\alpha = a + b\zeta$, $N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{p-1}(a + b\zeta^i)$. The key idea for today will be that there's $p - 1$ multiplications occuring.
- It's Ring of Integers $\mathcal{O}_K = \mathbb{Z}[\zeta]$

Number Fields, Norms, and the Discriminant

For our purposes, number fields often look like $\mathbb{Q}[\alpha]$ where α is the root of some monic rational polynomial. Today, our Number Field of choice is $K = \mathbb{Q}[\zeta]$ where ζ is a pth root of unity. $(\zeta^p = 1)$

- Its minimum polynomial is $\frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1$
- If $\alpha = a + b\zeta$, $N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{p-1}(a + b\zeta^i)$. The key idea for today will be that there's $p-1$ multiplications occuring.
- It's Ring of Integers $\mathcal{O}_K = \mathbb{Z}[\zeta]$
- What is it's discriminant?

How to calculate the Discriminant!

Given a $\mathbb{Q}$ basis $\{\alpha^i\} = \{1, \alpha, \alpha^2, \dots \alpha^{n-1}\}$ for $K = \mathbb{Q}[\alpha]$, and conjugate mappings σ_i,

$$\mathcal{D}_K = \det(\sigma_i(x_j))^2 = \det \begin{pmatrix} 1 & \sigma_1(\alpha) & \sigma_1(\alpha)^2 & \cdots & \sigma_1(\alpha)^{n-1} \\ 1 & \sigma_2(\alpha) & \sigma_2(\alpha)^2 & \cdots & \sigma_2(\alpha)^{n-1} \\ \vdots & & & \cdots & \vdots \\ 1 & \sigma_n(\alpha) & \sigma_n(\alpha)^2 & \cdots & \sigma_n(\alpha)^{n-1} \end{pmatrix}^2$$

Discriminant Formula Continued

This is a Vandermonde Determinant! Famous determinant identity shows us

$$\mathcal{D}_K = \det \begin{pmatrix} 1 & \sigma_1(\alpha) & \sigma_1(\alpha)^2 & \cdots & \sigma_1(\alpha)^{n-1} \\ 1 & \sigma_2(\alpha) & \sigma_2(\alpha)^2 & \cdots & \sigma_2(\alpha)^{n-1} \\ \vdots & & & \cdots & \vdots \\ 1 & \sigma_n(\alpha) & \sigma_n(\alpha)^2 & \cdots & \sigma_n(\alpha)^{n-1} \end{pmatrix}^2 \tag{1}$$

$$= \prod_{i<j}(\sigma_i(\alpha) - \sigma_j(\alpha))^2 \tag{2}$$

More Calculations

Using product tricks and the product rule, we have

$$
\begin{aligned}
& (-1)^{\frac{n(n-1)}{2}} \prod_i (\prod_{j\neq i}(\sigma_i(\alpha) - \sigma_j(\alpha)) && (1)\\
= \quad & (-1)^{\frac{n(n-1)}{2}} \prod_i f'(\sigma_i(\alpha)) && (2)\\
= \quad & (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha)) && (3)
\end{aligned}
$$

Let's apply this Formula

- $\mathbb{Q}[\zeta]$ surely has a power basis $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$, so we can apply this formula.

$$\begin{aligned} x^p - 1 &= (x-1)\Phi_p(x) \qquad (1) \\ \Longrightarrow px^{p-1} &= \Phi_p(x) + (x-1)\Phi_p'(x) \qquad (2) \end{aligned}$$

by taking derivatives.

Let's apply this Formula

- $\mathbb{Q}[\zeta]$ surely has a power basis $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$, so we can apply this formula.

$$\begin{aligned} x^p - 1 &= \quad (x-1)\Phi_p(x) && (1) \\ \implies px^{p-1} &= \Phi_p(x) + (x-1)\Phi_p'(x) && (2) \end{aligned}$$

  by taking derivatives.

- Plugging in ζ and taking norms,

$$N_{K/\mathbb{Q}}(p\zeta^{p-1}) = N_{K/\mathbb{Q}}(\zeta - 1)N_{K/\mathbb{Q}}(\Phi_p'(\zeta)) \tag{3}$$

The Discrminant of $\mathbb{Q}[\zeta]$

- $N_{K/\mathbb{Q}}(\zeta^{p-1}) = N_{K/\mathbb{Q}}(\zeta) = 1 \implies N_{K/\mathbb{Q}}(p\zeta^{p-1}) = p^{p-1}$.

The Discrminant of $\mathbb{Q}[\zeta]$

- $N_{K/\mathbb{Q}}(\zeta^{p-1}) = N_{K/\mathbb{Q}}(\zeta) = 1 \implies N_{K/\mathbb{Q}}(p\zeta^{p-1}) = p^{p-1}$.
- $\zeta - 1$ has minimum polynomial $\Phi_p(x+1) \implies N_{K/\mathbb{Q}}(\zeta - 1) = p$

The Discrminant of $\mathbb{Q}[\zeta]$

- $N_{K/\mathbb{Q}}(\zeta^{p-1}) = N_{K/\mathbb{Q}}(\zeta) = 1 \implies N_{K/\mathbb{Q}}(p\zeta^{p-1}) = p^{p-1}$.
- $\zeta - 1$ has minimum polynomial $\Phi_p(x+1) \implies N_{K/\mathbb{Q}}(\zeta - 1) = p$
- $p^{p-1} = pN_{K/\mathbb{Q}}(\Phi_p'(\zeta)) \implies \mathcal{D}_K = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}$

Table of Contents

First Lemma

Lemma 1

In $\mathbb{Z}[\zeta]$, the numbers $\zeta^k - 1$ are all unit multiples of eachother. Moreover, $\mathfrak{p} = (\zeta - 1)$ is the only prime ideal above (p) for p a rational prime.

First Lemma

Lemma 1

In $\mathbb{Z}[\zeta]$, the numbers $\zeta^k - 1$ are all unit multiples of eachother. Moreover, $\mathfrak{p} = (\zeta - 1)$ is the only prime ideal above (p) for p a rational prime.

Proof.

Note that $\zeta - 1 = \zeta^j - 1$ for some $j \equiv 1 \pmod{p}$. Clearly $\frac{\zeta^k - 1}{\zeta - 1} \in \mathbb{Z}[\zeta]$.

First Lemma

Lemma 1

In $\mathbb{Z}[\zeta]$, the numbers $\zeta^k - 1$ are all unit multiples of eachother. Moreover, $\mathfrak{p} = (\zeta - 1)$ is the only prime ideal above (p) for p a rational prime.

Proof.

Note that $\zeta - 1 = \zeta^j - 1$ for some $j \equiv 1 \pmod{p}$. Clearly $\frac{\zeta^k - 1}{\zeta - 1} \in \mathbb{Z}[\zeta]$.

Note also, $\frac{\zeta - 1}{\zeta^k - 1} = \frac{\zeta^{kk'} - 1}{\zeta^k - 1} \in \mathbb{Z}[\zeta]$ for some $kk' \equiv 1 \pmod{p}$.

First Lemma

Lemma 1

In $\mathbb{Z}[\zeta]$, the numbers $\zeta^k - 1$ are all unit multiples of eachother. Moreover, $\mathfrak{p} = (\zeta - 1)$ is the only prime ideal above (p) for p a rational prime.

Proof.

Note that $\zeta - 1 = \zeta^j - 1$ for some $j \equiv 1 \pmod{p}$. Clearly $\frac{\zeta^k - 1}{\zeta - 1} \in \mathbb{Z}[\zeta]$. Note also, $\frac{\zeta - 1}{\zeta^k - 1} = \frac{\zeta^{kk'} - 1}{\zeta^k - 1} \in \mathbb{Z}[\zeta]$ for some $kk' \equiv 1 \pmod{p}$. Since $\frac{\zeta^k - 1}{\zeta - 1}$ and its reciprocal both lie in $\mathbb{Z}[\zeta]$, $\zeta - 1$ and $\zeta^k - 1$ must be unit multiples of eachother. $\square$

Lemma 1 Continued

Lemma 1

In $\mathbb{Z}[\zeta]$, the numbers $\zeta^k - 1$ are all unit multiples of eachother. Moreover, $\mathfrak{p} = (\zeta - 1)$ is the only prime ideal above (p) for p a rational prime.

Lemma 1 Continued

Lemma 1

In $\mathbb{Z}[\zeta]$, the numbers $\zeta^k - 1$ are all unit multiples of eachother. Moreover, $\mathfrak{p} = (\zeta - 1)$ is the only prime ideal above (p) for p a rational prime.

Proof.

Note that $p = N_{K/\mathbb{Q}}(\zeta - 1) = \prod_{i=1}^{p-1}(\zeta^i - 1)$.

Lemma 1 Continued

Lemma 1

In $\mathbb{Z}[\zeta]$, the numbers $\zeta^k - 1$ are all unit multiples of eachother. Moreover, $\mathfrak{p} = (\zeta - 1)$ is the only prime ideal above (p) for p a rational prime.

Proof.

Note that $p = N_{K/\mathbb{Q}}(\zeta - 1) = \prod_{i=1}^{p-1}(\zeta^i - 1)$. Since $\zeta^i - 1 = u(\zeta - 1)$ for some unit u, we have $p = \prod_{i=1}^{p-1}(\zeta^i - 1) = v(\zeta - 1)^{p-1}$ where v is a product of units.

Lemma 1 Continued

Lemma 1

In $\mathbb{Z}[\zeta]$, the numbers $\zeta^k - 1$ are all unit multiples of eachother. Moreover, $\mathfrak{p} = (\zeta - 1)$ is the only prime ideal above (p) for p a rational prime.

Proof.

Note that $p = N_{K/\mathbb{Q}}(\zeta - 1) = \prod_{i=1}^{p-1}(\zeta^i - 1)$. Since $\zeta^i - 1 = u(\zeta - 1)$ for some unit u, we have $p = \prod_{i=1}^{p-1}(\zeta^i - 1) = v(\zeta - 1)^{p-1}$ where v is a product of units. As ideals, unique factorization indicates that $(p) = (\zeta - 1)^{p-1}$, so $\zeta - 1$ is the only prime ideal above (p). □

Some Theorem of Kronecker's

Lemma 2

If α is a nonzero algebraic integer such that all of its conjugates have absolute value 1, then α is a root of unity.

Some Theorem of Kronecker's

Lemma 2

If α is a nonzero algebraic integer such that all of its conjugates have absolute value 1, then α is a root of unity.

Idea: Use triangle inequality to get bounds on polynomials f such that $f(\alpha) = 0$,

Some Theorem of Kronecker's

Lemma 2

If α is a nonzero algebraic integer such that all of its conjugates have absolute value 1, then α is a root of unity.

Idea: Use triangle inequality to get bounds on polynomials f such that $f(\alpha) = 0$, so there are finitely many polynomials for which the above occurs

Lemma 2

If α is a nonzero algebraic integer such that all of its conjugates have absolute value 1, then α is a root of unity.

Idea: Use triangle inequality to get bounds on polynomials f such that $f(\alpha) = 0$, so there are finitely many polynomials for which the above occurs $\implies$ finitely many α as well.

Lemma 2

If α is a nonzero algebraic integer such that all of its conjugates have absolute value 1, then α is a root of unity.

Idea: Use triangle inequality to get bounds on polynomials f such that $f(\alpha) = 0$, so there are finitely many polynomials for which the above occurs $\implies$ finitely many α as well. Construct a new polynomial with α^k and its conjugates as roots of it.

Some Theorem of Kronecker's

Lemma 2

If α is a nonzero algebraic integer such that all of its conjugates have absolute value 1, then α is a root of unity.

Idea: Use triangle inequality to get bounds on polynomials f such that $f(\alpha) = 0$, so there are finitely many polynomials for which the above occurs $\implies$ finitely many α as well. Construct a new polynomial with α^k and its conjugates as roots of it. Finitely many $\alpha \implies \alpha^k = \alpha$ for some $k > \deg(f)$, and we're done.

Kummer's Lemma

Lemma 3

For $u \in \mathbb{Z}[\zeta]^{\times}$, $u/\overline{u} = \zeta^k$ for some $k > 0$

Kummer's Lemma

Lemma 3

For $u \in \mathbb{Z}[\zeta]^\times$, $u/\overline{u} = \zeta^k$ for some $k > 0$

Proof.

Note that $|u/\overline{u}| = |u|/|\overline{u}|$ but $|u| = |\overline{u}|$, so $|u/\overline{u}| = 1$.

Kummer's Lemma

Lemma 3

For $u \in \mathbb{Z}[\zeta]^\times$, $u/\overline{u} = \zeta^k$ for some $k > 0$

Proof.

Note that $|u/\overline{u}| = |u|/|\overline{u}|$ but $|u| = |\overline{u}|$, so $|u/\overline{u}| = 1$. Taking some conjugate mapping σ, note $\sigma(u)\sigma(\overline{u}) = \sigma(u\overline{u})$, meaning $\sigma(\overline{u}) = \overline{\sigma(u)}$.

Kummer's Lemma

Lemma 3

For $u \in \mathbb{Z}[\zeta]^\times$, $u/\overline{u} = \zeta^k$ for some $k > 0$

Proof.

Note that $|u/\overline{u}| = |u|/|\overline{u}|$ but $|u| = |\overline{u}|$, so $|u/\overline{u}| = 1$. Taking some conjugate mapping σ, note $\sigma(u)\sigma(\overline{u}) = \sigma(u\overline{u})$, meaning $\sigma(\overline{u}) = \overline{\sigma(u)}$. Then $\sigma(u/\overline{u}) = \sigma(u)/\overline{\sigma(u)}$ has absolute value $1 \implies$ all conjugates have absolute value 1.

Kummer's Lemma

Lemma 3

For $u \in \mathbb{Z}[\zeta]^{\times}$, $u/\overline{u} = \zeta^k$ for some $k > 0$

Proof.

Note that $|u/\overline{u}| = |u|/|\overline{u}|$ but $|u| = |\overline{u}|$, so $|u/\overline{u}| = 1$. Taking some conjugate mapping σ, note $\sigma(u)\sigma(\overline{u}) = \sigma(u\overline{u})$, meaning $\sigma(\overline{u}) = \overline{\sigma(u)}$. Then $\sigma(u/\overline{u}) = \sigma(u)/\overline{\sigma(u)}$ has absolute value 1 $\implies$ all conjugates have absolute value 1. By Lemma 1, $u/\overline{u} = \pm\zeta^k$ for some $k > 0$. □

Kummer's Lemma Continued

Lemma 3

For $u \in \mathbb{Z}[\zeta]^\times$, $u/\overline{u} = \zeta^k$ for some $k > 0$

Kummer's Lemma Continued

Lemma 3

For $u \in \mathbb{Z}[\zeta]^\times$, $u/\overline{u} = \zeta^k$ for some $k > 0$

Proof.

Suppose $u = -\zeta^k \overline{u}$. Now, working mod p, we have $u \equiv -\zeta^k \overline{u} \pmod{p}$.

Kummer's Lemma Continued

Lemma 3

For $u \in \mathbb{Z}[\zeta]^\times$, $u/\overline{u} = \zeta^k$ for some $k > 0$

Proof.

Suppose $u = -\zeta^k \overline{u}$. Now, working mod p, we have $u \equiv -\zeta^k \overline{u} \pmod{p}$. Raising everything to the pth power, we have $u \equiv -u \pmod{p}$,

Kummer's Lemma Continued

Lemma 3

For $u \in \mathbb{Z}[\zeta]^\times$, $u/\overline{u} = \zeta^k$ for some $k > 0$

Proof.

Suppose $u = -\zeta^k \overline{u}$. Now, working mod p, we have $u \equiv -\zeta^k \overline{u} \pmod{p}$. Raising everything to the pth power, we have $u \equiv -u \pmod{p}$, meaning $p \mid 2u \implies p \mid 2$ or $p \mid u$, neither of which are possible. Contradiction, $u = \zeta^k \overline{u}$. $\square$

Kummer's Lemma Continued

Lemma 3

For $u \in \mathbb{Z}[\zeta]^\times$, $u/\overline{u} = \zeta^k$ for some $k > 0$

Proof.

Suppose $u = -\zeta^k \overline{u}$. Now, working mod p, we have $u \equiv -\zeta^k \overline{u} \pmod{p}$. Raising everything to the pth power, we have $u \equiv -u \pmod{p}$, meaning $p \mid 2u \implies p \mid 2$ or $p \mid u$, neither of which are possible. Contradiction, $u = \zeta^k \overline{u}$. $\square$

Remark

You can actually show that $u = \zeta^k v$ for some totally real unit v. In fact, $\mathbb{Q}[\zeta]$ has a maximal real subfield $L = \mathbb{Q}[\zeta + \zeta^-]$, and $v \in \mathcal{O}_L^\times$.

Table of Contents

Our Lemmas and the Theorem

Lemma 1

In $\mathbb{Z}[\zeta]$, the numbers $\zeta^k - 1$ are all unit multiples of eachother. Moreover, $\mathfrak{p} = (\zeta - 1)$ is the only prime ideal above (p) for p a rational prime.

Kummer's Lemma

For $u \in \mathbb{Z}[\zeta]^\times$, $u/\overline{u} = \zeta^k$ for some $k > 0$

Kummer's Theorem

For regular primes $p \geq 3$, the equation $x^p + y^p = z^p$ has no solutions.

Step 1: Showing $x + \zeta^i y$ are pairwise coprime

Kummer's Theorem

For regular primes $p \geq 3$, the equation $x^p + y^p = z^p$ has no solutions.

Proof.

We have $x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta^i y) = z^p$.

Step 1: Showing $x + \zeta^i y$ are pairwise coprime

Kummer's Theorem

For regular primes $p \geq 3$, the equation $x^p + y^p = z^p$ has no solutions.

Proof.

We have $x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta^i y) = z^p$. We'd like to show that the $(x + \zeta^i y)$ are pairwise coprime.

Step 1: Showing $x + \zeta^i y$ are pairwise coprime

Kummer's Theorem

For regular primes $p \geq 3$, the equation $x^p + y^p = z^p$ has no solutions.

Proof.

We have $x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta^i y) = z^p$. We'd like to show that the $(x + \zeta^i y)$ are pairwise coprime. Assuming $i > j$, if they weren't we have $x + \zeta^i y - x - \zeta^j y = y\zeta^j(\zeta^{i-j} - 1) \in \mathfrak{p}$ for some prime ideal $\mathfrak{p}$

Step 1: Showing $x + \zeta^i y$ are pairwise coprime

Kummer's Theorem

For regular primes $p \geq 3$, the equation $x^p + y^p = z^p$ has no solutions.

Proof.

We have $x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta^i y) = z^p$. We'd like to show that the $(x + \zeta^i y)$ are pairwise coprime. Assuming $i > j$, if they weren't we have $x + \zeta^i y - x - \zeta^j y = y\zeta^j(\zeta^{i-j} - 1) \in \mathfrak{p}$ for some prime ideal $\mathfrak{p}$ Using Lemma 1, we have $y\zeta^j(\zeta^{i-j} - 1) = uy(\zeta - 1) \in \mathfrak{p}$.

Step 1: Showing $x + \zeta^i y$ are pairwise coprime

Kummer's Theorem

For regular primes $p \geq 3$, the equation $x^p + y^p = z^p$ has no solutions.

Proof.

We have $x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta^i y) = z^p$. We'd like to show that the $(x + \zeta^i y)$ are pairwise coprime. Assuming $i > j$, if they weren't we have $x + \zeta^i y - x - \zeta^j y = y\zeta^j(\zeta^{i-j} - 1) \in \mathfrak{p}$ for some prime ideal $\mathfrak{p}$ Using Lemma 1, we have $y\zeta^j(\zeta^{i-j} - 1) = uy(\zeta - 1) \in \mathfrak{p}$. Wait! This implies $yp \in \mathfrak{p}$.

Step 1: Showing $x + \zeta^i y$ are pairwise coprime

Kummer's Theorem

For regular primes $p \geq 3$, the equation $x^p + y^p = z^p$ has no solutions.

Proof.

We have $x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta^i y) = z^p$. We'd like to show that the $(x + \zeta^i y)$ are pairwise coprime. Assuming $i > j$, if they weren't we have $x + \zeta^i y - x - \zeta^j y = y\zeta^j(\zeta^{i-j} - 1) \in \mathfrak{p}$ for some prime ideal $\mathfrak{p}$ Using Lemma 1, we have $y\zeta^j(\zeta^{i-j} - 1) = uy(\zeta - 1) \in \mathfrak{p}$. Wait! This implies $yp \in \mathfrak{p}$. At the same time, $z^p \in \mathfrak{p}$, but $\gcd(yp, z^p)$ is 1, so $\mathfrak{p}$ must be trivial, meaning all the $(x + \zeta^i y)$ are pairwise coprime. □

Step 2: Using Regular Primes

Kummer's Theorem

For regular primes $p \geq 3$, the equation $x^p + y^p = z^p$ has no solutions.

Proof.

Using Unique Factorization of Ideals, $z = \prod_{i=1}^{k} \mathfrak{p}_i^{\alpha_i}$, so setting $\mathfrak{p}_i^{\alpha_i} = \mathfrak{a}_i$ Since the $x + \zeta^i y$ are pairwise coprime and $\prod_{i=0}^{p-1}(x + \zeta^i y) = (z)^p$, we have $(x + \zeta^i y) = \mathfrak{a}_i^p \implies [\mathfrak{a}_i^p] \sim [(1)]$ in $Cl(\mathbb{Q}[\zeta])$. By Lagrange's Theorem, we should have $p \mid |Cl(\mathbb{Q}[\zeta])|$, but p is regular, so $\mathfrak{a}_i$ must've been trivial in the first place. Now we know, $x + \zeta^i y = ua^p$ for some unit u and some $a \in \mathbb{Z}[\zeta]$. $\square$

Step 3: Using Kummer's Lemma and Working mod p

Kummer's Theorem

For regular primes $p \geq 3$, the equation $x^p + y^p = z^p$ has no solutions.

Proof.

By using Kummer's Lemma, we have $u/\overline{u} = \zeta^k$ for some $k > 0$. Moreover, fix $i = 1$, so $x + \zeta y = \zeta^k \overline{u} a^p$. Note that $a^p \equiv \overline{a}^p \pmod{p}$ (Why?), so $x + \zeta y \equiv \zeta^k \overline{ua}^p \equiv \zeta^k(x + \zeta^{p-1} y) \pmod{p}$. It follows that $p \mid (x + \zeta y - \zeta^k x - \zeta^{k-1} y)$. Note that $\zeta \neq 1$ and $\zeta^k \neq \zeta^{k-1}$. As a result, we have one of the following: $1 = \zeta^{k-1}$, $1 = \zeta^k$, or $\zeta = \zeta^{k-1}$. □

Step 4: Casework!

Kummer's Theorem

For regular primes $p \geq 3$, the equation $x^p + y^p = z^p$ has no solutions.

Proof.

Going in order, let $\zeta^{k-1} = 1$, then we have $x + \zeta y - \zeta x - y \equiv 0 \pmod{p}$.
Factoring, we have $(x - y)(1 - \zeta) \equiv 0 \pmod{p} \implies x \equiv y \pmod{p}$.
Why is this a contradiction?
If $\zeta^k = 1$, we have $x + \zeta y - x - \zeta^{-} y \equiv y(\zeta - \zeta^{-}) \pmod{p} \implies p \mid y$.
Contradiction.
Lastly, if $\zeta = \zeta^{k-1}$, we have $x(1 - \zeta^2) \equiv 0 \pmod{p} \implies p \mid x$.
Contradiction. $\square$