Special Case of Fermat's Last Theorem

Joseph Cleary

Fermat's Last Theorem

Theorem

The equation $x^n + y^n = z^n$ has no nontrivial integer solutions for $n \geq 3$.

We can reduce to the case when n is a prime number.

Theorem

The equation $x^p + y^p = z^p$ has no nontrivial integer solutions for $p \geq 3$, with p a prime.

We will only sketch a proof a special case, with additional restrictions.

Pythagorean Theorem Example

Here we introduce the ring of the Gaussian Integers:

Definition

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

Using this, we want to classify all primitive Pythagorean Triples, i.e. pairwise coprime integers x, y, z satisfying

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

Now that we are working in this ring, we can factor the equation into

$$(x + yi)(x - yi) = z^2$$

1. $(x + yi)$ and $(x - yi)$ are coprime.
2. $x + yi = (m + ni)^2 = (m^2 - n^2) + 2mni$
3. $x = m^2 - n^2, y = 2mn, z = m^2 + n^2$, m, n relatively prime and not both odd.

The Special Case

In the previous example, unique factorization of elements was our main tool. We want to apply this strategy to $p \geq 3$, but there is a problem, because not all number rings have unique factorization of elements.

Theorem

Suppose p is an odd prime and p does not divide the class number of the field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive pth root of unity. Then

$$x^p + y^p = z^p, \qquad \gcd(xyz, p) = 1$$

has no nontrivial integer solutions.

The restriction on xyz means that p does not divide x, y, and z.

Number Fields

Definition

A **number field** is a subfield of $\mathbb{C}$ having finite dimension as a vector space over $\mathbb{Q}$.

- $\mathbb{Q}[\sqrt{m}]$ where m is a nonsquare integer.
- $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$
- We will use later that $\mathbb{Q}[\zeta_p]$ where $\zeta_p = e^{2\pi i/p}$ with p a prime. (This is the primitive pth root of unity.)

$$\mathbb{Q}[\zeta_p] = \left\{a_0 + \cdots + a_{p-2}\zeta_p^{p-2} : a_i \in \mathbb{Q}\right\}$$

Number Rings

Definition

An element in a number field is called **integral** if it is the root of some monic polynomial with coefficients in $\mathbb{Z}$.
Call the set of integral elements in $\mathbb{C}$ the set of **algebraic integers**, denoted it as $\mathbb{A}$.
Define a **number ring** to be $\mathbb{A} \cap K$, where K is a number field.

- If $K = \mathbb{Q}[i]$, then $\mathbb{A} \cap K = \mathbb{Z}[i]$
- If $K = \mathbb{Q}[\zeta_p]$, then $\mathbb{A} \cap K = \mathbb{Z}[\zeta_p]$. This is not a trivial fact.

Operation of Ideals

Let A be a Noetherian domain. We can define the **product** of ideals to be

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J \right\}$$

The set of ideals of A only forms a monoid with A as the identity, so we introduce a generalized concept of ideals.

Definition

Let K be the fraction field of A. A A-submodule of K, M is called a **fractional ideal** if there exists a nonzero $a \in K$ such that $aM \subset A$. The set of fractional ideals are denoted $\mathcal{J}_A$.

With the inverse defined as $I^{-1} = \{a \in K \mid aI \subset A\}$, $\mathcal{J}_A$ becomes an abelian group.

Dedekind Domain

For number rings, $\mathcal{J}_A$ has a nice description. Any ideal in a number ring is of the form

$$I = \prod_{i=1}^{r} P_i^{e_i} = \prod_{P \text{ prime ideal}} P^{e_P} \text{ with } e_P \in \mathbb{Z}_{\geq 0}, e_P = 0 \ a.e.$$

The $e_P = 0$ *a.e.* means that $e_P \neq 0$ for only finitely many prime ideals, because this is a product over all primes. A ring satisfying this unique factorization of ideals is called a **Dedekind domain**.

$$\mathcal{J}_A = \left\{ I \;\middle|\; I = \prod_{P \text{ prime ideal}} P^{e_P} \text{ with } e_P \in \mathbb{Z}, e_P = 0 \ a.e. \right\}$$

Ideal Class Group

Definition

A fractional ideal of A that is generated by an element $a \in K$ is called a **principal ideal**. It is usually denoted (a) or aA. The set of principal fractional ideals is denoted $\mathcal{I}_A$.

$\mathcal{I}_A$ is a subgroup of $\mathcal{J}_A$.

Definition

The **ideal class group** is the quotient group $\mathcal{C}_A = \mathcal{J}_A / \mathcal{I}_A$. The **class number** is the order of the group $\mathcal{C}_A$.

It is not so easy to prove that class numbers are finite.

Our Special Case

Theorem

Suppose p is an odd prime and p does not divide the class number of the field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive pth root of unity. Then

$$x^p + y^p = z^p, \qquad \gcd(xyz, p) = 1$$

has no solutions in rational integers.

The restriction on xyz means that p does not divide x, y, and z.

We factor the equation $x^p + y^p = z^p$ into

$$\prod_{i=0}^{p-1}(x + \zeta_p^i y) = z^p \qquad \text{(elements)}$$

Let $\zeta = \zeta_p$. Here we consider as a multiplicative problem in the ring $\mathbb{Z}[\zeta]$, using ideals. We then get an equality of ideals

$$\prod_{i=0}^{p-1}(x + \zeta^i y) = (z)^p \qquad \text{(ideals)}$$

Proposition

Let $I_1, \ldots, I_n, J$ be ideals of a Dedekind domain A, and $I_1, \ldots, I_n$ be pairwise disjoint. If

$$I_1 \cdots I_n = J^m$$

then $I_i = K_i^m$ for some ideal $K_i \subset A$.

Lemma

The ideals $(x + \zeta^i y), i = 0, 1, \ldots, p-1$ are pairwise relatively prime.

These ideals are pairwise disjoint. By the proposition, each must be the pth power of another ideal A_i in $\mathbb{Z}[\zeta]$:

$$(x + \zeta^i y) = A_i^p$$

Lemma

If G is a group of order n and $x \in G$, where $x^p = e \in G$ and $p \not| n$, then $x = e$

1. $A_i^p I_{\mathbb{Q}[\zeta]} = (x + \zeta^i y) I_{\mathbb{Q}[\zeta]} = I_{\mathbb{Q}[\zeta]} \in Cl_Q(\zeta)$ because $(x + \zeta^i y)$ is principal.
2. Because $A_i^p I_{\mathbb{Q}[\zeta]} = I_{\mathbb{Q}[\zeta]}$, and we have that $p \not| \# Cl_Q(\zeta)$, by Lemma, we conclude that $A_i I_{\mathbb{Q}[\zeta]} = I_{\mathbb{Q}[\zeta]}$, so $A_i \in I_{\mathbb{Q}[\zeta]}$ and each A_i is a principal ideal.
3. Thus we can rewrite each $(x + \zeta^i y) = (\alpha_i^p)$ as ideals, so then we have an equality of elements $x + \zeta^i y = u \cdot \alpha_i^p$, with u a unit.
4. From here, we can do slightly long case-by-case checking and get a contradiction.