A Special Case of Fermat's Last Theorem

Hikmet Burak Özcan

İzmir Institute of Technology

MCBÜ Algebra Workshop

17 September 2019

Overview

Primitive Pythagorean Triples

- Algebraic number theory is essentially the study of number fields.
- Such fields can be useful in solving problems which at first appear to involve only rational numbers.
- Consider, for example, the following problem:

Problem

Find all **primitive Pythagorean triples**: i.e., integer solutions of

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

having no common factor.

Solution

- Assume that we have such a triple (x, y, z).
- z must be odd.
- We factor the left side of the equation

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

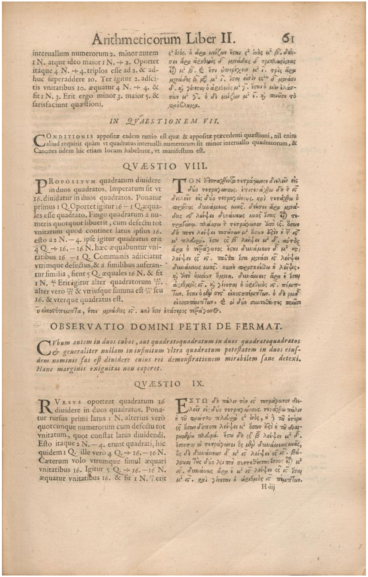
- It is a multiplicative problem in the number field $\mathbb{Q}(i)$ and in fact in the ring of Gaussian integers $\mathbb{Z}[i]$.
- $\mathbb{Z}[i]$ is a UFD.
- Since $x + iy$ and $x - iy$ have no common prime factor,

$$x + yi = u\alpha^2$$

  for some unit $u \in \mathbb{Z}[i]$ and non-zero $\alpha \in \mathbb{Z}[i]$.
- If $\alpha = m + ni$, then we obtain that

$$\{x, y\} = \{\pm(m^2 - n^2), \pm 2mn\} \quad \textit{and} \quad z = \pm(m^2 + n^2).$$

Arithmetica



Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVAESTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hîc etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto à 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

H iij

Fermat's Last Theorem

Fermat's Last Theorem

There are no solutions of the equation

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

in the set of non-zero integers whenever $n > 2$.

- This was first conjectured by **Pierre de Fermat** in 1637 in the margin of a copy of **Arithmetica**.
- Fermat added that he had a proof that was too large to fit in the margin.
- After 358 years of effort by mathematicians, the first successful proof was released in 1994 by **Andrew Wiles**.

- Using our result on primitive Pythagorean triples, we can show that Fermat was right for $n = 4$ and hence (automatically) also for any multiple of 4.
- Therefore, it is sufficient to consider only the case in which n is an odd prime p, since if no solutions exist when $n = p$, then no solutions exist when n is a multiple of p.
- Thus, **Fermat's Conjecture** is the following problem:

Fermat's Conjecture

If p is an odd prime, then

$$x^p + y^p = z^p$$

has no solution in nonzero integers x, y, z.

Two Cases

- Suppose, for some odd prime p, there is a solution $x, y, z \in \mathbb{Z} \setminus \{0\}$.
- We may assume that x, y, z have no common factor (divide it out if there is one).
- We have two following cases:

Case 1

p divides none of x, y, z.

Case 2

p divides exactly one of them. (If p divided more than one, then it would divide all three, which is impossible.)

In this talk, we will consider only case 1.

$p = 3$

- Suppose that (x, y, z) is a solution of the equation

$$x^3 + y^3 = z^3.$$

- If x, y and z are not multiples of 3, then each of these cubes is equivalent to ± 1 $(mod\ 9)$.
-

$$x^3 + y^3 \not\equiv z^3 \ (mod\ 9).$$

$p > 3$

- Now, assume $p > 3$; x, y and z are not multiples of p; and

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

- Factoring the left side, we obtain

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

where w is the p<u>th</u> root of unity $e^{2\pi i/p}$.

- Now, we have a multiplicative problem in the number field $\mathbb{Q}[w]$, and in fact in the subring $\mathbb{Z}[w]$.

Kummer's Approach

- Kummer attempted to prove Fermat's conjecture by considering whether the unique factorization property of $\mathbb{Z}$ and $\mathbb{Z}[i]$ generalizes to the ring $\mathbb{Z}[w]$.
- Unfortunately, $\mathbb{Z}[w]$ is not a UFD for some prime p. For example, it is not a UFD for $p = 23$.
- However, it is a UFD for all primes less than 23. For these primes it is not difficult to show that

$$x^p + y^p = z^p$$

has no **case** 1 solutions.

Proof.

- Assume that
$$x^p + y^p = z^p,$$
where x, y and z are not a multiple of p.
- Assume that $\mathbb{Z}[w]$ is a UFD.
- Recall that we have the following multiplicative problem in $\mathbb{Z}[w]$:
$$(x+y)(x+yw)(x+yw^2)\cdots(x+yw^{p-1}) = z^p, \qquad (*)$$
where w is the p$\underline{\text{th}}$ root of unity $e^{2\pi i/p}$.
- Since all factors in the right side of equation $(*)$ have no common prime divisor,
$$x + yw = u\alpha^p,$$
where $\alpha \in \mathbb{Z}[w]$ and a unit $u \in \mathbb{Z}[w]$.
- $x \equiv y \ (mod\ p)$.

(continued)

- Similarly, writting
$$x^p + (-z)^p = (-y)^p$$
we obtain $x \equiv -z \ (mod \ p)$.
- Then,
$$2x^p \equiv x^p + y^p = z^p \equiv -x^p \ (mod \ p).$$
- It implies that $p|3x^p$.
- Since $p \nmid x$ and $p \neq 3$, this is a contradiction. $\square$

What about other primes?

- Unique factorization in $\mathbb{Z}[w]$ was needed only to obtain that

$$x + yw = u\alpha^p.$$

Might it not be possible to deduce this in some other way?

<u>Answer:</u> "yes" for certain values of p, including for example $p = 23$.

- This results from Dedekind's amazing discovery of the generalization of unique factorization.
- Although the elements of $\mathbb{Z}[w]$ may not factor uniquely into irreducible elements, the ideals in this ring always factor uniquely into prime ideals.

* Using this, for certain prime p, called **"regular"** primes

$$(x + yw) = I^p = (\alpha)^p = (\alpha^p).$$

- Thus, again we have

$$x + yw = u\alpha^p.$$

- As before, this implies

$$x \equiv y \ (mod \ p)$$

  and the contradiction follows.

* Regular Primes

There is an equivalence relation $\sim$ on the set of ideals of $\mathbb{Z}[w]$, defined as follows: for ideals A and B

$$A \sim B \quad \text{iff} \quad \alpha A = \beta B \quad \text{for some } \alpha, \beta \in \mathbb{Z}[w].$$

- There are only finitely many equivalence classes of ideals under $\sim$.
- The number of classes is called the **class number** of the ring $\mathbb{Z}[w]$, and is denoted by the letter h_p.

Definition

A prime p is **regular** iff $p \nmid h_p$.

Proposition

If p is a regular prime, then the ideal I (in the equation $(x + yw) = I^p$*) must be principal.*

Proof.

- First, note that the ideal classes can be multiplied in the obvious way: the product of two ideal classes is obtained by selecting an ideal from each; multiplying them; and taking the ideal class which contains the product ideal. This is well-defined.
- The ideal classes form a finite abelian group with this multiplication.
- The identity element is the class C_0 consisting of all principal ideal.

(continued)

We claim that if p is regular, then clearly this group contains no element of order p, and it follows that if I^p is principal then so is I:

- Let C be the ideal class containing I; then C^p is the class containing I^p, which is C_0
- C_0 is the identity in the ideal class group and C cannot have order p
- It follows that $C = C_0$, which shows that I is principal. □

Result

The equation

$$x^p + y^p = z^p$$

has no case 1 solutions (i.e, solutions for which $p \nmid xyz$) when p is a regular prime.

- Furthermore, It is also possible, although somewhat more difficult, to show that no case 2 solutions exist for regular primes.
- Thus, **Fermat's Last Theorem** can be proved for all regular primes p, hence for all integers n which have at least one regular prime factor.
- Unfortunately, irregular primes exist (e.g. 37, 59, 67). In fact, there are infinitely many. On the other hand, it is not known whether there are infinitely many regular primes.

Conclusion

In any case, our attempt to prove **Fermat's Last Theorem** leads us to consider various questions about the ring $\mathbb{Z}[w]$.

Questions

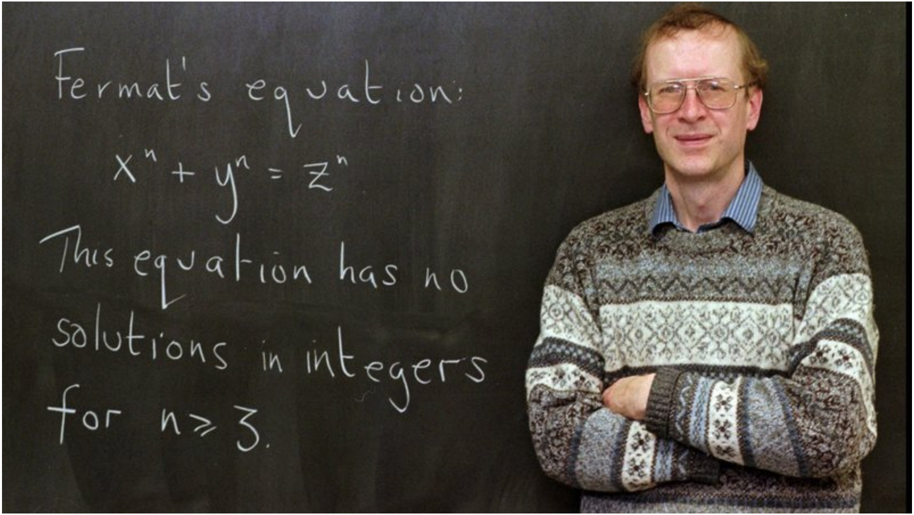
- What are the units in this ring?
- What are the irreducible elements?
- Do elements factor uniquely?
- If not, what can we say about the factorization of ideals into prime ideals?
- How many ideal classes are there?

The investigation of such problems forms a large portion of **algebraic number theory**.

References

Daniel A. Marcus, Number Fields, Springer, 1991

Thank You!!!



Fermat's equation:
$x^n + y^n = z^n$
This equation has no
solutions in integers
for $n \geq 3$.