AN ADVENTURER'S GUIDE TO DIVIDING THE PRIMES

LIGHT EDIAND

Abstract: In this paper we show how partitioning the primes into various sums allows us to factorise them in a subring of the complex numbers.

1. Introduction

This story begins on a late summer evening last year. I was reading the manga Stone Ocean by Hirohiko Araki (apologies to those JoJo fans not up to date with the story as this does contain spoilers), and to my delight I found that one of the characters, Enrico Pucci, was fond of the prime numbers. Pucci's admiration comes from the fact that primes are indivisible, and this indivisibility gives him strength, so he recites them to calm himself and regain his composure. Though in spite of all this, he dies. He is defeated. His supposed strength he found in the primes was not enough to save him. What if, this is because primes are not as strong and indivisible as he anticipated? What if primes *were* divisible, and we had just not found the right numbers to divide them yet? Thus, I present to you, An Adventurer's Guide to Dividing The Primes, where we uncover the secret factors that lie beneath, that caused our dear Pucci to meet his unpleasant fate.

2. Arithmetic of Complex Numbers

Before we can begin with finding our factors, we must first define complex numbers and how to do some essential arithmetic operations with them. Without further ado, a complex number is made up of two parts, a real part denoted x, and an imaginary part denoted yi, where y is a real number and i is the square root of -1. However, it is useful to make note of the following equivalent definition of i, as it will come in handy later on!

$$i^2 = -1.$$

Hence a complex number, z, is

$$z = x + yi, \text{ where } x, y \in \mathbb{R}.$$

We define the sum and product of two complex numbers as follows.

$$z_1 + z_2 = (x_1 + y_1 i) + (x_2 + y_2 i) = x_1 + x_2 + (y_1 + y_2)i.$$

$$z_1 \cdot z_2 = (x_1 + y_1 i) \cdot (x_2 + y_2 i) = x_1 x_2 + x_1 y_2 i + x_2 y_1 i - y_1 y_2.$$

3. A Complicated Difference of Two Squares

There is a short formula we come across in algebra known as the difference of two squares. For two real numbers a and b we have,

$$(a + b)(a - b) = a^2 + ab - ab - b^2 = a^2 - b^2.$$

Instead of a real binomial, we are going to use a fake one, or rather, a complex number, which is made up of two parts as explained above. Rewriting the difference of two squares formula with bi instead of plain b, we obtain,

$$(a + bi)(a - bi).$$

Multiplying these two brackets together gives us this:

$$a^2 + abi - abi - (bi)^2 = a^2 - (bi)^2.$$

Finally,

$$a^2 - (bi)^2 = a^2 - (b^2)(i^2) = a^2 - (b^2)(-1) = a^2 + b^2.$$

Aha!

4. A Sum of Two Squares

So as you can see from above, when we multiply two complex numbers together with opposite signs, the result is a sum, not a difference! You may be wondering, 'How does this relate to prime numbers?' Well, some, not all, but *some* prime numbers can be rewritten as the sum of two squares.

As prime numbers are infinite, I will be limiting this paper to all the prime numbers under 50, which gives us plenty to mess around with for demonstration purposes without being too overwhelming.

$$\mathbb{P}_{50} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}.$$

Let us first consider 2. Quite elegantly, we have $2 = 1 + 1$, where our sum is of the two squares 1 and 1. Our next job is to factorise the sum $1 + 1$, which can be done by substituting them as values a and b in our sum of two squares formula, recalled below.

$$(a + bi)(a - bi) = a^2 + b^2.$$

Working backwards, we arrive at the following:

$$1^2 + 1^2 = (1 + i)(1 - i).$$

And there we have it! Factors of 2 are $(1 + i)$ and $(1 - i)$. Not so prime after all, is it? Let's see which other numbers in $\mathbb{P}_{50}$ can be written as a sum of two squares. We have,

$$\begin{aligned} 5 &= 4 + 1 \\ 13 &= 9 + 4 \\ 17 &= 16 + 1 \\ 29 &= 25 + 4 \\ 37 &= 36 + 1 \\ 41 &= 25 + 16. \end{aligned}$$

An interesting thing to note about these sum of two square primes is that they are all congruent to 1 modulo 4, that is they are primes of the form

$$p = 4n + 1 \text{ where } n \in \mathbb{N}.$$

They are known as Pythagorean Primes [4] and in fact, Fermat stated that an odd prime can be written as the sum of two squares *if and only if* they have this congruence property! This is known as Fermat's Two Squares Theorem.

In particular, primes of the form n^2+1 where n is a natural number [5], such as 2, 5, 17 and 37, caught the attention of Landau. One day, he brought forward four questions, and the last of these questions was, "Are there infinitely many primes of the form $n^2 + 1$?" It has been proven there are infinitely many primes, and we know there are infinitely many numbers of the form $n^2 + 1$, but whether or not there are infinitely many *primes* of the form $n^2 + 1$ remains a complete mystery! This little mystery left me completely mesmerised, it's what set in stone my love and fascination for number theory, and is the reason I am writing this to you today, even if I don't have an answer!

Returning to the task at hand, factorising in turn each of our sums by substituting them into our sum of two squares formula, we find our factors are as follows.

$$\begin{aligned}
5 &= 4+1 = 2^2+1^2 = (2+i)(2-i)\\
13 &= 9+4 = 3^2+2^2 = (3+2i)(3-2i)\\
17 &= 16+1 = 4^2+1^2 = (4+i)(4-i)\\
29 &= 25+4 = 5^2+2^2 = (5+2i)(5-2i)\\
37 &= 36+1 = 6^2+1^2 = (6+i)(6-i)\\
41 &= 25+16 = 5^2+4^2 = (5+4i)(5-4i).
\end{aligned}$$

I should point out that since integer addition is commutative, factors will represent this. For example 5 is 4+1, but it is also 1+4, which means that it can additionally be factorised to $(1+2i)(1-2i)$. Nonetheless, I have only listed one set of factors for each prime in this paper, but there are in fact, countless, many factors contained within prime numbers.

Unfortunately, not all primes can be divided with this method. The prime 3 can only be written as 2+1 or 1+2, which is not two squares. Whatever will we do to complete our quest of dividing the primes?

5. Inventing a New Type of Number to Solve Problems

May I present to you the (first) most wonderful set of numbers in existence: The Surd Squares, $\mathbb{SS}$. Surd Squares are the integer multiples of the square root of a prime number, squared. The square root of a prime number is the surd part. Using set notation:

$$\mathbb{SS} = \left\{(n\sqrt{p})^2 : n \in \mathbb{N}, p \in \mathbb{P}\right\} = \left\{n^2 p : n \in \mathbb{N}, p \in \mathbb{P}\right\}.$$

Technically, the invention of these numbers gives factors to all primes simply by setting $n = 1$ and the prime we want to factorise as p. However, what's the fun in that? Literally none. Zero, zip, zilch, nada. In order to fully appreciate the existence of $\mathbb{SS}$, we must use as little of $\mathbb{SS}$ as possible. We have established that $3 = 2 + 1$, so we are going to apply a restriction to $\mathbb{SS}$, such that we only use the Surd Squares made using 2. As indexing begins at 0, it follows that $\mathbb{SS}_0$ is the set made using 0 primes. That is, it only contains n^2 and is therefore equal to the set of square numbers.

You may be wondering why I have referred to $\mathbb{SS}$ as only the *first* most wonderful set, as opposed to being the most wonderful. This is because $\mathbb{N}$, where 0 is *naturally* a member of this set, is the zeroth most wonderful. It creates a beautiful monoid under addition, and there is nothing more mathematically beautiful than a monoid. These days, far too many heretics like to exclude 0, but I am taking a stand against them! We must demand justice for zero, justice for the monoidal beauty of the natural numbers, and justice for proper indexing that begins at zero; a natural way to start anything!

In conclusion $\mathbb{SS}_0$ contains the Surd Squares made using no primes, ie the squares; $\mathbb{SS}_1$ contains the Surd Squares made using the prime 2; $\mathbb{SS}_2$ uses 2 and 3; and so on.

$$\mathbb{SS}_1 = \left\{\left(n\sqrt{2}\right)^2 : n \in \mathbb{N}\right\} = \{2, 8, 18, 32, ...\}.$$

With $\mathbb{SS}_1$ in mind, 3 can be factorised as follows:

$$3 = 2 + 1 = \left(\sqrt{2}\right)^2 + 1^2 = \left(\sqrt{2} + i\right)\left(\sqrt{2} - i\right).$$

Reviewing the elements of $\mathbb{SS}_1$ and the primes in $\mathbb{P}_{50}$ that have yet to be factorised,

$$\begin{aligned}11 &= 9+2 = 3^2 + \left(\sqrt{2}\right)^2 = \left(3+i\sqrt{2}\right)\left(3-i\sqrt{2}\right)\\ 19 &= 18+1 = \left(3\sqrt{2}\right)^2 + 1^2 = \left(3\sqrt{2}+i\right)\left(3\sqrt{2}-i\right)\\ 43 &= 25+18 = 5^2 + \left(3\sqrt{2}\right)^2 = \left(5+3i\sqrt{2}\right)\left(5-3i\sqrt{2}\right).\end{aligned}$$

6. When life gives you lemons, add more Surd Squares to the mix

Let's see how many more primes in $\mathbb{P}_{50}$ we can factorise by using $\mathbb{SS}_2$! We begin by establishing the elements of the set:

$$\mathbb{SS}_2 = \left\{(n\sqrt{p})^2 : n \in \mathbb{N}, p \in \{2,3\}\right\} = \{2,3,8,12,18,27,32,48,...\}.$$

With $\mathbb{SS}_2$, we are able to factorise a further two primes, as shown below.

$$\begin{aligned}7 &= 4+3 = 2^2 + \left(\sqrt{3}\right)^2 = \left(2+i\sqrt{3}\right)\left(2-i\sqrt{3}\right)\\ 31 &= 27+4 = \left(3\sqrt{3}\right)^2 + 2^2 = \left(3\sqrt{3}+2i\right)\left(3\sqrt{3}-2i\right).\end{aligned}$$

That leaves only 23 and 47 from $\mathbb{P}_{50}$ that have yet to be factorised. I am delighted to inform you that we only need to go to $\mathbb{SS}_3$ to add Surd Squares also made using 5 to complete our task.

$$\mathbb{SS}_3 = \left\{(n\sqrt{p})^2 : n \in \mathbb{N}, p \in \{2,3,5\}\right\} = \{2,3,5,8,12,18,20,27,32,45,48,...\}.$$

Finally, we factorise our remaining primes.

$$\begin{aligned}23 &= 18+5 = \left(3\sqrt{2}\right)^2 + \left(\sqrt{5}\right)^2 = \left(3\sqrt{2}+i\sqrt{5}\right)\left(3\sqrt{2}-i\sqrt{5}\right)\\ 47 &= 45+2 = \left(3\sqrt{5}\right)^2 + \left(\sqrt{2}\right)^2 = \left(3\sqrt{5}+i\sqrt{2}\right)\left(3\sqrt{5}-i\sqrt{2}\right).\end{aligned}$$

In summary:

$$\begin{aligned}
2 &= (1+i)(1-i)\\
3 &= \left(\sqrt{2}+i\right)\left(\sqrt{2}-i\right)\\
5 &= (2+i)(2-i)\\
7 &= \left(2+i\sqrt{3}\right)\left(2-i\sqrt{3}\right)\\
11 &= \left(3+i\sqrt{2}\right)\left(3-i\sqrt{2}\right)\\
13 &= (3+2i)(3-2i)\\
17 &= (4+i)(4-i)\\
19 &= \left(3\sqrt{2}+i\right)\left(3\sqrt{2}-i\right)\\
23 &= \left(3\sqrt{2}+i\sqrt{5}\right)\left(3\sqrt{2}-i\sqrt{5}\right)\\
29 &= (5+2i)(5-2i)\\
31 &= \left(3\sqrt{3}+2i\right)\left(3\sqrt{3}-2i\right)\\
37 &= (6+i)(6-i)\\
41 &= (5+4i)(5-4i)\\
43 &= \left(5+3i\sqrt{2}\right)\left(5-3i\sqrt{2}\right)\\
47 &= \left(3\sqrt{5}+i\sqrt{2}\right)\left(3\sqrt{5}-i\sqrt{2}\right).
\end{aligned}$$

7. Wait. That's illegal!

The definition of primes is: a natural number greater than 1 that is not a product of two smaller natural numbers [6]. When we have to use complex numbers to divide them, it is breaking several, *several* rules. We cannot actually divide the primes in $\mathbb{N}$, because if we could, they wouldn't be primes in $\mathbb{N}$, which means we have created *quite* the paradox here!

To solve this paradox, we can change from $\mathbb{N}$ to somewhere else where our divisors can exist. $\mathbb{C}$ might be the ideal place to go to since our factors are complex numbers, however, we don't actually need *all* of $\mathbb{C}$. As you will recall from earlier we applied restrictions to $\mathbb{SS}$ and used as little of the Surd Squares as possible to divide our primes. So it follows on from this that we use as little of $\mathbb{C}$ as possible: a subring of $\mathbb{C}$ that only contains the complex numbers made using integers and the surds we used for our Surd Squares; that is $\mathbb{Z}$, $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{5}$.

Let A be the ring

$$A = \mathbb{Z}\left[\sqrt{2}, \sqrt{3}, \sqrt{5}\right].$$

Then $A[i]$ is a subring of $\mathbb{C}$ and

$$A[i] = \{a + bi : a, b \in A\}.$$

Now $A[i]$ is the smallest place where we can happily divide the primes under 50, without breaking any rules! Thus concludes An Adventurer's Guide to Dividing the Primes.

To be continued...

There is something strange going on with the Surd Squares. I can't quite put my finger on it. Though once I have figured it out, there will be a sequel to this paper called: *Surd Squares and the Mysterious Modulos*. Until next time, friends!

Acknowledgements

A huge thank you to all my lovely friends in arithmetic geometry and number theory, who helped me in my endeavours to divide the primes and start my mathematical career as a number theorist. Your support and encouragement will forever be cherished.

References

[1] An Adventurer's Guide to Number Theory by Friedberg
[2] Complex Numbers from A to Z by Andreescu and Andrica
[3] JoJo's Bizaare Adventure by Hirohiko Araki (Though only Stone Ocean is referenced here, I highly recommend you read all the previous manga to fully appreciate the story as intended. Don't skip parts!)
[4] Sequence A002144 on the Online Encyclopedia of Integer Sequences (Pythagorean Primes)
[5] Sequence A002496 on the Online Encyclopedia of Integer Sequences (Primes of the form $n^2 + 1$)
[6] Prime numbers: https://en.wikipedia.org/wiki/Prime_number

---

Published to *ediand.xyz* July 27, 2022
Revised December 18, 2023