Are primes really primes...?

Sachin Kumar
University of Waterloo, Faculty of Mathematics

Introduction

There is a very real sense in which 5 isn't a prime number because, one can write $5 = (2 + i)(2 - i)$, ie., one can write it as a product of two complex numbers. This reveals something very interesting whether a number is a prime depends on the universe of numbers you're living in. Visually, normally we work over the $\mathbb{Z}$, that's the number line, but now we're working in a lattice in the $\mathbb{C}$, ie., consisting of all complex numbers with integer coordinates.

Our basic question is as follows: how do the rules of number theory change, when you extend your universe of numbers beyond the integers? The field of mathematics that deals with this question is called algebraic number theory. We'll first introduce the basic concepts of the subject, this will allow us to enter one of the most beautiful branches of the theory of numbers called Iwasawa theory, this is the branch of math that does number theory in infinite towers. The culmination of this essay is the foundational result of this subject, which very loosely describes how numbers factor into primes as you climb the layers of a certain infinite tower. It's honestly one of the beautiful theorems in number theory,

$$\begin{gathered} \mathbb{Z}[\zeta_p] - \mathbb{Z}[\zeta_{p^2}] - \mathbb{Z}[\zeta_{p^3}] \cdots \\ \text{power of } p \text{ in class \# of } \mathbb{Z}[\zeta_{p^n}] = p^{\lambda n + \nu} \end{gathered}$$

Number Rings

Before we delve deep, We will now introduce some terminology, the number system we saw earlier is, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, this is an example of something called a number ring. A number ring is a universe of numbers like the integers. The main theme when studying number systems like these is that many thing we take for granted over the integers aren't true over number rings, like 5 is no longer a primes, another one which is more serious over the integers, is the fact that every number can be factored uniquely as a product of prime numbers (Fundamental Theorem of Arithmetic), this fails quite spectacularly in the other number systems.

For example, consider the ring, $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. One can factor,

$$\begin{aligned} 6 &= 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \\ 21 &= 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5}) \end{aligned}$$

I want to stress the problem here isn't that you can't factor numbers into primes, you totally can but you can't do so uniquely. This somehow suggests that looking at numbers and factoring them into prime numbers isn't the right way to look at things, the starting insight of algebraic number theory is instead of looking at a single number look at the set of all multiples of that number at the same time. To gain intuition, let's consider a trivial example, $2 \cdot 3 = 6$. Instead of looking at 2, look at the set of all multiples of two at the same time, $A = \{2a \mid a \in \mathbb{Z}\}$, similarly look at the set, $B = \{3b \mid b \in \mathbb{Z}\}$. Now, if you multiply all the numbers in A with all the numbers in B in all possible combinations, you will get the set, $C = \{6c \mid c \in \mathbb{Z}\}$, ie., the set of all multiples of 6. This allows us to interpret $2 \cdot 3 = 6$ in a different way.

Over the integers, I agree that this is a totally bizzare way to look at numbers, but this perspective is crucial to how we're going to think about multiplication in higher number systems. To see how it generalizes, we'll look at the properties of the set, A and make it into a definition. Notice that it satifies these properties: $0 \in A$, closed under $+$ and $-$, closed under taking multiples. This motivates the following theory.

Ideals, Unique factorization and Class Numbers

Definition 0.1 (Ideal)**.** *Let R be any number ring. $I \subseteq R$ is an ideal, if and only if I satisfies the following properties:*

1. $0 \in I$.
2. *I is closed under $+$ and $-$*
3. *If $x \in I$, then $rx \in I$, for all $r \in R$.*

Orginally,

$$\text{Number} \longrightarrow \text{Factor as product of prime numbers}$$

but now,

$$\text{Ideal} \longrightarrow \text{Factor as product of prime ideals}$$

For the first, we saw that unique factorization isn't true. The point is for the bottom, unique factorization is true every ideal can be written uniquely as a product of prime ideals, that's the motivation to introducing ideals in the first place. For example, the set A is an ideal, denoted as (2), for another example consider $\mathbb{Z}[i]$, and consider a point $1+i$, because an ideal is closed under addition, any ideal containing this point has to contain twice that number, 0 and all the integer multiples of that number, and as well it should also contain i times that number and all integer multiples of that number, it should also contain all possible sums of these numbers, and filling in these gaps, we cover the entire plane. This is the ideal denoted as $(1+i)$, it is the set of all multiples of $1+i$.

A word of warning both examples we have seen, ie., (2) and $(1+i)$, have been the set of all multiples of a single number, but its not true in general that all ideals have to be of that form. For example, we looked at the ring, $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Visually, consider two points 3 and $1 + \sqrt{-5}$, what is the smallest ideal containing them? Well if it contains 3, then it should contain all integer multiples of 3 and if it contains $1+\sqrt{-5}$, it should contain all integer multiples of it, so if you fill in the gaps, what would you get? Think!. This is a ideal, denoted as $(3, 1+\sqrt{-5})$, the ideal generated by 3 and $1+\sqrt{-5}$. Let's see how factoring into ideals as opposed to numbers fixes our older example, so we saw that you can factor 6 in two ways: $2 \cdot 3$ and $(1+\sqrt{-5})(1-\sqrt{-5})$, but now instead of factoring the number, 6, lets factor the ideal, (6). It factors as a product of four different prime ideals,

$$\begin{aligned}(6) &= \big((2, 1+\sqrt{-5})(2, 1-\sqrt{-5})\big)\big((3, 1+\sqrt{-5})(3, 1-\sqrt{-5})\big) = (2)(3)\\ &= \big((2, 1+\sqrt{-5})(3, 1+\sqrt{-5})\big)\big((2, 1-\sqrt{-5})(3, 1-\sqrt{-5})\big) = (1+\sqrt{-5})(1-\sqrt{-5})\end{aligned}$$

So the whole time, the two factorizations of 6, weren't actually different, there was just a deeper underlying factorization into ideals and we were just grouping the terms in different ways.

So lets summarize, we've seen that certain number rings fail to have unique factorization into prime numbers, the fix was instead of factoring numbers into prime numbers, we will factor ideal into prime ideals and the way it fixes things is whenever unique factorization into numbers happens to fail, there is always a deeper factorization into ideals that works.

Here is an interesting question, given an number ring, how badly does the unique factorization into prime numbers fail? This question will lead us to the puch line of this essay. To answer this, I would like to introduce some helpful terminology,

Definition 0.2 (Principal and Non-principal Ideal)**.** *An ideal is generated by one number if and only if it is a principal ideal. For example,* (2)*. An ideal is generated by more than one number if and only if it is a non-principal ideal. For example,* $(3, 1+\sqrt{-5})$*.*

Non-principal ideals are not as trivial to understand as principal ideals, they are things that you add in order to restore the unique factorization. Before we answer the previous question, we will ask a more precise question, given a number ring, how many non-priciple ideals does it have? Intuitively, how many new ideals did you have to add in order to restore the unique factorization? Now, as it stands this is not a well defined question because a number ring could have infinitely many non-principal ideals. But there is a better way to quantify this. Consider the two prime ideals, $(2, 1+\sqrt{-5})$ and $(3, 1+\sqrt{-5})$. It turns out that these ideals are scalar multiples of each other,

$$\alpha(2, 1+\sqrt{-5}) = (3, 1+\sqrt{-5})$$
$$\frac{1+\sqrt{-5}}{2}(2, 1+\sqrt{-5}) = (3, 1+\sqrt{-5})$$

Likewise, it turns out that this ideal on the right is also some constant alpha times the first ideal. In fact, every non-principal ideal in this ring is a scalar multiple of this one. This ring has infinitely many non-principal ideals but they are all of the same kind, so to speak they all address the same illness in the underlying ring, but that's not always true. Consider the ring, $\mathbb{Z}[\sqrt{82}]$ and if you consider the two ideals, $(2, \sqrt{82})$ and $(3, 1+\sqrt{82})$, they are not scalar multiples of each other, ie., there does not exist any constant α, that makes the equation, $\alpha(2, \sqrt{82}) = (3, 1+\sqrt{82})$ hold true. They are genuinely different kinds of ideals. So for this ring you have to add more than one kind of ideal in order to rescue unique factorization.

Definition 0.3 (Class Number)**.** *The number of kinds of ideals in a number ring is called a class number of that ring.*

The class number answers our question, how many non-pricipal ideals do we have to add to recover unique factorization? It's kind of a proxy for how screwed up the underlying number system is. In general, the class number can get extremely large. For example, if you take $\mathbb{Z}[-3449]$, the class number is 100 (refer LMFDB and OEIS for more amazing examples). But by far the most intricate number rings of all are, $\mathbb{Z}[\zeta_n] = \{a_0 + a_1\zeta_n + \cdots + a_{n-1}\zeta_n^{n-1} \mid a_i \in \mathbb{Z}\}$, where ζ_n is the n-th root of unity, the complex number sitting one n-th, (angle of $\frac{2\pi}{n}$) of the way around the unit circle in the complex plane. Now, if there is one thing I want to emphasize here is that nobody knows how to compute the class numbers, because to calculate them you have essentially understand all the ideals in the number ring, which ideals are multiple of others and which ones aren't. To underscore this, to calculate the class number of few number rings, we have to consider the assumption of the generalized Riemann hypothesis.

Iwasawa Theory

BUT that all changed in the 1950's when Kenkichi Iwasawa entered the scene. Instead of calculating the class number of just one number ring, he actually looked at an infinite tower of number rings and calculated all of their class numbers in one go. Specifically, he considered the following tower:

$$\mathbb{Z}[\zeta_p] - \mathbb{Z}[\zeta_{p^2}] - \mathbb{Z}[\zeta_{p^3}] \cdots$$

He noticed that if you looked at the class numbers in this tower a pattern emerged. Take the case $p = 37$, this is $\mathbb{Z}[\zeta_{37}] + \mathbb{Z}[\zeta_{37^2}] - \cdots$, and finding class numbers of these rings is very hard but if you just look at the powers of 37 appearing in the class number, you can see a exponential curve, ie., the power of 37 appearing in the class number increases exponentially fast as you climb the layers of this tower. So lets take another prime $p = 11$, lets look at the power of 11 appearing in the class number. In this case, it is actually identically zero, ie., 11 never divides the class number of any number ring in this tower. So this is what Iwasawa was able to prove in general, his theorem was the following:

Theorem 0.4. *The power of p dividing the class number # of $\mathbb{Z}[\zeta_{p^n}] = p^{\lambda n+\nu}$.*

The proof is non-trivial, it uses very sophisticated techniques from group theory, representation theory, class field theory and much more. The basic idea is that if you arrange the rings in an infinite tower, you can look at all of their ideals at once and this object has many more algebraic symmetries than the ideals at any finite layer.

Unfortunately, there existed an the error term in Iwasawa's theorem, μ_{p^n}, for some $\mu \in \mathbb{Z}$, which was absolutely gigantic, it was an exponential of an exponential and it completely over shadowed the main term. In numerical computation of these class numbers, Iwasawa noticed that for all primes, $p \leq 4001$, $\mu = 0$, that this term wasn't actually there. But it turned out to be very difficult to prove this for all primes p and it took almost 30 years and it was finally proved in 1979, by Bruce Ferrero and Lawrence C. Washington, in the paper "The Iwasawa invariant μ_p vanishes for abelian number fields". They proved that for all primes p, the μ invariant of the p-th cyclotomic field was zero, but this theorem in this place we could then remove this invariant.

References

1. An unorthodox introduction to algebraic number theory.

2. Introduction to Cyclotomic Fields by Lawrence Washington (Iwasawa Theory)