Algebraic Number Theory – Lecture 1

Lee Butler

> "Stand firm in your refusal to remain conscious during algebra. In real life, I assure you, there is no such thing as algebra."
>
> – Fran Lebowitz

Some Books

Algebraic Number Theory – Ian Stewart and David Tall.
Intended for senior undergraduates or postgraduates, it covers all the basics but skips some of the more interesting proofs. Features plenty of history for the easily distracted.

Algebraic Number Theory – Jürgen Neukirch.
Starts with "$2 = 1 + 1$", which is nice. It's thorough and eschews short but opaque 'trick' proofs in favour of ones that extend to more complicated situations.

Number Theory – Z.I. Borevich and I.R. Shafarevich.
Features the proofs that Stewart and Tall omit.

http://www.jmilne.org/math/ – Features Milne's online lecture notes on Algebraic Number Theory, as well as notes on other useful topics.

1. What is Algebraic Number Theory?

Depending on where you place the hyphen, algebraic number theory may be read in two ways, either it's the Theory of Algebraic Numbers, or else it's Number Theory studied via Algebra. Considering the presence of Analytic Number Theory (which is not the study of analytic numbers) it's tempting to read it in that second way. However, there are at least three good reasons to read it the first way:

(1) Just using algebraic tools limits us somewhat and would prevent us from seeing some of the finest results in this field.
(2) The study of algebraic numbers involves – indirectly and directly – using algebra and answers questions about number theory in general, so nothing is lost.
(3) Transcendental number theory is not – despite our demi-god like status – the study of number theory using tools that transcend mere mortals; it's the study of transcendental numbers, and algebraic number theory has more in common with this part of maths than analytic number theory.

So, for now at least, algebraic number theory is the study of algebraic numbers. Or more generally of algebraic number fields – but Mike will tell us all about them next week.

2. A Little History

Algebraic number theory first attracted mass attention about a hundred and fifty years ago with respect to Fermat's last theorem. But – almost predictably – it was Gauss who achieved the first major results at the turn of the nineteenth century. He was working on extending his pet result on quadratic reciprocity. Recall that a number q is called a quadratic residue of p if there is a number x such that $x^2 \equiv q \pmod{p}$. Writing

$$\left(\frac{q}{p}\right) = \begin{cases} 1 \text{ if } q \text{ is a quadratic residue of } p \\ -1 \text{ if not,} \end{cases}$$

then the law of quadratic reciprocity says that for distinct odd primes p and q:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}.$$

Disentangling this it gives conditions on p being a quadratic residue of q assuming we know whether q is a quadratic residue of p and what p and q are mod 4.

Gauss adored this result and gave numerous proofs of it; he also sought similar results for higher powers than squares. He found laws of cubic reciprocity (cubes instead of squares) but in the process realised his calculations became much easier by considering numbers of the form $a+b\omega$ for integers a and b and where $\omega = e^{2\pi i/3}$ is a complex cube root of unity. Similarly he found a law of biquadratic reciprocity (fourth powers instead of squares), which was much easier to prove by considering numbers of the form $a + bi$ for integers a and b. During his work he proved that every number of the form $a + bi$ can be uniquely factorised into primes, just like the normal integers can be, although the notion of what a prime number has to be extended to this new setting. The set of these numbers

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

is now called the set of Gaussian integers in Gauss' honour.

Given that any $a_0 \in \mathbb{Z}$ can be uniquely factorised into primes, and given Gauss proved numbers of the form $a_0 + a_1 i \in \mathbb{Z}[i]$ may also be uniquely factorised, one might rashly assume that if $\zeta = e^{2\pi i/n}$ is a complex nth root of unity then numbers of the form $a_0 + a_1\zeta + \ldots + a_{n-1}\zeta^{n-1} \in \mathbb{Z}[\zeta]$ will factor uniquely into primes as well. And indeed in 1847 the French mathematician Gabriel Lamé proved Fermat's last theorem assuming this result for prime n.

The astute and awake among you might recall that Andrew Wiles was the one who proved Fermat's last theorem, and so suspect some kind of English conspiracy to oppress Lamé's result. In fact – as Liouville pointed out – the unique factorisation into primes result had been proved for $n = 1, 2, 3, 4$, but not for general rings of the above type. First year undergraduates might be satisfied that if something is true for n from 1 to 4 then it must be true for all n, but we know better. In fact, as Ernst Kummer had proved a few years before Lamé's 'proof', unique factorisation works in these rings for all primes up to $n = 19$, but fails for every prime number $n \geqslant 23$.

Remark 1. In a unique factorisation domain, one has, for every prime p, $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. Now let $\zeta = e^{2\pi i/23}$ and consider the ring $\mathbb{Z}[\zeta]$. General elements of this ring are of the form

$$a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_{21}\zeta^{21}.$$

One can check that 2 is a prime in $\mathbb{Z}[\zeta]$, and that

$$2 \nmid 1 + \zeta^2 + \zeta^4 + \zeta^5 + \zeta^6 + \zeta^{10} + \zeta^{11} =: \alpha,$$

and

$$2 \nmid 1 + \zeta + \zeta^5 + \zeta^6 + \zeta^7 + \zeta^9 + \zeta^{11} =: \beta.$$

But

$$\alpha\beta = 2(\zeta^5 + \zeta^6 + \zeta^7 + \zeta^9 + \zeta^{10} + 3\zeta^{11} + \zeta^{12} + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^{17}).$$

And so $\mathbb{Z}[\zeta]$ cannot be a unique factorisation domain.

Kummer then rubbed salt into Lamé's wounds by proving Fermat's last theorem for exponents that are 'regular primes'[1]. He used what he called 'ideal numbers', in effect he suggested that when unique factorisation fails it is because there are hidden common factors lurking behind the scenes, and these hidden numbers he called ideal numbers. For example, in $\mathbb{Z}[\sqrt{-5}]$ we don't have unique factorisation because

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Kummer proposed that there was some hidden common factor of 2 and $1 + \sqrt{-5}$ that, while not actually present in $\mathbb{Z}[\sqrt{-5}]$, existed in some higher setting and caused the apparent lack of unique factorisation.

Remark 2. The idea of some ethereal ideal numbers lurking behind-the-scenes may sound fatuous, but it makes sense. Consider the following artifice. Let

$$S = 3\mathbb{Z} + 1 = \{n \in \mathbb{Z} \mid n \equiv 1 \pmod 3\}.$$

In S, then, we have

$$220 = 4 \cdot 55 = 10 \cdot 22,$$

with $4, 55, 10$, and 22 all irreducible in S, and so it is not a unique factorisation domain. What goes wrong? Well we know that behind-the-scenes in $\mathbb{Z}$ none of these numbers are actually irreducible, in fact $220 = 2^2 \cdot 5 \cdot 11$. But none of these prime numbers is actually in S hence the failure to factorise uniquely. What Kummer did was to postulate that something similar was happening in the more general setting and introduced new 'ideal numbers' in place of our primes $2, 5$, and 11.

[1] It's conjectured that $e^{-1/2} \approx 61\%$ of all primes are regular, but so far it is not even known that there are infinitely many such primes, only that infinitely many primes are irregular.

The fact Kummer called his numbers ‘ideal’ perchance alerts you to what they formed the basis of, and you’d be wrong. What Kummer did had a lot more to do with Kurt Hensel’s p-adic numbers than what we now call ‘ideals’, but Dedekind did reformulate Kummer’s work and this reformulation led to the modern theory of ideals. Ideals are where it’s at. Unique factorisation often fails for rings of integers but never for ideals.

Kummer and Dedekind’s work led to a flourish of activity and a realisation that vast tracts of number theory could be reformulated in terms of algebraic numbers. Hilbert urged the use of this point of view 111 years ago, and what Hilbert says goes. Which is why we study algebraic number theory today.