Introduction to Algebraic Number Theory
Lecture 1

Andrei Jorza

2014-01-15

Today's lecture is an overview of the course topics.

Let me start by saying provocatively that the purpose of this course is to do the following problem:

Problem 1. Compute

$$\int_0^1 \frac{\log(1+x^{2+\sqrt{3}})}{1+x}dx$$

We can use all the technical ingredients of this course to compute this integral as

$$\frac{\pi^2}{12}(1-\sqrt{3})+\log 2\cdot\log(1+\sqrt{3})$$

Algebraic number theory, to some extent, is concerned with the study of an algebraic closure $\overline{\mathbb{Q}}$ of the rationals. We are interested in:

1. Its subfields $\mathbb{Q}\subset F\subset\overline{\mathbb{Q}}$, in particular those which are finite extensions of $\mathbb{Q}$ (these are called number fields);

2. Its subrings $\mathbb{Z}\subset R\subset\overline{\mathbb{Q}}$, in particular those which are finitely generated (these are called number rings). For example we'd like to classify them, perhaps enumerate them.

3. Multiplication in these subfields and subrings:

   - what are the units, i.e., the invertible elements?
   - what are the primes?
   - can one decompose any number into primes?
   - is this decomposition unique?
   - can one predict patterns for decompositions into prime factors?

For example, Problem 1 relies on the fact that in the ring $\mathbb{Z}[\sqrt{3}]$ (generated by $\mathbb{Z}$ and $\sqrt{3}$) the exponent $2+\sqrt{3}$ of x is a unit (i.e., it is invertible, with inverse $2-\sqrt{3}$) and factorization into primes numbers is unique.

How can decomposition into primes fail? Here is a simple example: in $\mathbb{Z}[\sqrt{-5}]$ the number 6 decomposes in two ways:

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

and each factor is a prime number. In general unique factorization fails, but here is an example where it holds: $\mathbb{Z}[i]$, the so-called Gaussian integers. Here is an application:

Problem 2. If x, y, z are integers such that $x^2 + y^2 = z^2$ then, up to reordering, one can write

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2 \end{aligned}$$

for integers m and n

Proof. First, we may assume that x, y, z do not have a common factor, since otherwise we can simplify the equation. Next, if x and y are both even, then z is even so they have a common factor. If x and y are both odd, then x^2 and y^2 are $\equiv 1 \pmod 4$ and so $z^2 \equiv 2 \pmod 4$ which cannot happen and so we may assume that x is odd and y is even (up to reordering).

Rewrite $x^2 + y^2 = z^2$ as $(x + iy)(x - iy) = z^2$. The factors $x + iy$ and $x - iy$ cannot have any common prime divisors (if it did, then it would divide their sum $2x$ and it cannot divide x because otherwise it would also divide y and thus z; thus it would have to divide 2 which would contradict the fact that x is odd) and so $x + iy$ and $x - iy$ are both perfect squares times a unit.

Say $x + iy = u(m + ni)^2$ where u is a unit, in which case u can only be one of $1, -1, i, -i$. Then $x + iy = u(m^2 - n^2 + 2imn)$ and up to reshuffling we obtain the desired result. □

The proof of Problem 2 highlighted two important themes in algebraic number theory:

1. Modular arithmetic is extremely useful and often working modulo well-chosen primes simplifies the problem immensely (here is another example: show that $x^2 + x - 2y^2 = 1$ has no integer solutions).

2. Working with factorizations is very useful and we will spend a significant amount of time to find the correct language for unique factorization to hold (we will replace decomposition into prime numbers with decomposition into prime ideals). In this language, failure of unique factorization into prime *numbers* is captured by an integer, often denoted h, called the **class number** (this number is the cardinality of a group called the class group).

One stunning, but fairly straightforward, application of this correct language for unique factorization is the following (a different phrasing is if p does not divide the class number of the cyclotomic field $\mathbb{Q}(\zeta_p)$):

Problem 3 (Kummer)**.** Suppose p is a prime number which does not divide the first $p-3$ Taylor coefficients of

$$\operatorname{cotan}(x) = \frac{1}{x} - \frac{x}{3} - \frac{x^3}{45} - \frac{2x^5}{945} - \cdots$$

Then Fermat's Last Theorem holds for p, i.e., $x^p + y^p = z^p$ has no nonzero integer solutions.

An important technical tool in studying factorizations in number fields is **Galois theory** which captures the symmetries of elements in the number field (such as complex conjugation, or $2 + \sqrt{3}$ going to $2 - \sqrt{3}$). Galois theory also bridges the conceptual gap between factorization and modular arithmetic: how far we get studying a number ring working modulo a prime is captured by the concept of ramification (we'd say that a number ring is unramified at a prime if working modulo that prime we capture essentially all the arithmetic information) and the manifestation of ramification in Galois theory captures a lot of interesting phenomena. Going in the other direction, one application of algebraic number theory to Galois theory is the computation of Galois groups of polynomials with integer coefficients by reducing modulo (unramified) prime numbers:

Theorem 4. *If $f \in \mathbb{Z}[X]$ is an irreducible polynomial and p is a prime decompose $f(X) \mod p$ into prime factors $f_1(X) \cdots f_d(X)$. Suppose all the irreducible polynomials $f_1, \ldots, f_d$ are distinct (which happens for all except for finitely many p). Then the Galois group of f contains an element (thought of as a permutation of the roots of f) with cycle decomposition* $\deg f_1, \ldots, \deg f_d$.

Some related topics:

1. Quadratic reciprocity and its uses in cryptography;

2. How a prime in a number field factors in a bigger number field;

A huge topic in number theory is solving diophantine equations. One can ask whether a diophantine equation has solutions; if yes, what are they? perhaps estimate how many solutions there exist. This connects algebraic number theory with arithmetic geometry, complex geometry, topology, dynamics, analysis and even logic. Here is a simple example where one can count solutions precisely:

Problem 5. A positive integer n can be written as $n = x^2+y^2$ where x and y are integers in $4(d_+(n)-d_-(n))$ ways where $d_\pm(n)$ is the number of divisors of n which are $\equiv \pm 1 \pmod 4$.

Other questions are: in how many ways can one write n as $x^2 + xy + y^2$? How about a general quadratic form? This last problem has a subtle application, to a formula in the style of those found by Ramanujan:

Problem 6. Show that

$$\sum_{m,n}(q^{m^2+mn+6n^2} - q^{2m^2+mn+3n^2}) = q\prod_{n\geq 1}((1-q^n)(1-q^{23n}))$$

The LHS of this equation is an example of a Θ-function which, using Fourier analysis, can be shown to satisfy certain arithmetic functional equations (making them the most basic examples of modular forms). This leads to deep connections between simple combinatorial questions such as "how to write an exponent as $m^2 + mn + 6n^2$" and analysis. Remark: here the exponent 23 is the negative of the discriminant of $x^2 + xy + 6y^2$.

Analysis shows up again in a remarkable connection with the class number (this is a very special case of the million dollar Birch and Swinnerton-Dyer conjecture). The Riemann ζ-function

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

makes sense as a convergent series when $\operatorname{Re} s > 1$ and one can make sense of $\zeta(s)$ as having a Taylor expansion around $s = 1$ of the form

$$\frac{1}{s-1} + a_0 + a_1(s-1) + \cdots$$

(here a_0 is the Euler constant γ) and the simple pole at $s = 1$ gives the approximation $x/\log(x)$ for the number of primes less than x. There exist analogues for all number fields, still with Taylor expansion

$$\frac{A}{s-1} + a_0 + a_1(s-1) + \cdots$$

but now the constant A depends on the units in the ring of integers, the roots of unity and the class number. This is known as the Class Number Formula and is an ingredient of Problem 1.

Some more examples of problems where we will think analytically:

1. Dirichlet's theorem on the number of units in a number ring.

2. Dirichlet's theorem on the number of primes $\equiv a \pmod n$,

3. Classifying and counting number rings (Gauss composition laws),

4. Special values of the ζ-function (a special example being $\zeta(2) = \pi^2/6$). It turns out ζ at negative integers is always a rational number, which has immense implications to modern number theory.

Where does this course leave you? By the end you have the tools to venture into other number theory related topics:

1. Class field theory, which describes ramification in great detail.

2. Representations of Galois groups;
3. Modular forms;
4. Elliptic curves and algebraic geometry;
5. Applied math: cryptography, randomness;

Not to mention you'll know how to do Problem 1!