MATH 361: NUMBER THEORY — FIRST LECTURE

This lecture previews Math 361. After a brief introduction, some beginning ideas from algebraic number are illustrated by example, specifically in connection with primes that are the sum of two squares ($p = x^2 + y^2$) and Pythagorean triples ($x^2 + y^2 = z^2$). Some related ideas are also touched on in the process.

Contents

1. Introduction

As a provisional definition, view number theory as the study of the properties of the positive integers,

$$\mathbb{Z}^+ = \{1, 2, 3, \dots\}.$$

Of particular interest, consider the *prime* numbers, the noninvertible positive integers divisible only by 1 and by themselves,

$$\mathcal{P} = \{2, 3, 5, 7, 11, \dots\}.$$

Euclid (c.300 B.C.) and Diophantus (c.250 A.D.) posed and solved number theory problems, as did Archimedes. In the middle ages the Indians and perhaps the Chinese knew further results. Fermat (early 1600's) got a copy of Diophantus and revived the subject. Euler (mid-1700's), Lagrange, Legendre, and others took it seriously. Gauss wrote *Disquisitiones Arithmeticae* in 1799.

Example questions:

- (*The perfect number problem.*) The numbers $6 = 1 + 2 + 3$ and $28 = 1+2+4+7+14$ are *perfect numbers*, the sum of their proper divisors. Are there others? Which numbers are perfect? This problem is not completely solved.
- (*The congruent number problem.*) Consider a positive integer n. Is there a rational right triangle of area n? That is, is there a right triangle all three of whose sides are rational, that has area n? This problem is not completely solved, but very technical 20th century mathematics has reduced it to a problem called the *Birch and Swinnerton-Dyer Conjecture*, one of the so-called Clay Institute Millennium Problems, each of which carries a million

dollar prize. The book **Introduction to Elliptic Curves and Modular forms** by Neal Koblitz uses the congruent number problem to introduce the relevant 20th century mathematics.

- (*A representation problem.*) Let n be a positive integer. Which primes p take the form
$$p = x^2 + ny^2$$
for some $x, y \in \mathbb{Z}$? This problem is solved by modern mathematical ideas, specifically complex multiplication and class field theory. The book **Primes of the Form $\mathbf{x^2 + ny^2}$** by David Cox uses the representation problem in its title to introduce these subjects.
- (*The distribution of primes.*) Are there infinitely many primes? If so, can we say more than *infinitely many*? If $\pi(x)$ denotes the number of primes $p \leq x$ then how does $\pi(x)$ grow as x grows? Questions like this lead quickly into *analytic number theory*, where, for example, ideas from complex analysis or Fourier analysis are brought to bear on number theory. The Euler–Riemann zeta function
$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots, \quad s \in \mathbb{C},\ \mathrm{Re}(s) > 1$$
extends by complex analytic means to all $s \in \mathbb{C}$, with the extension no longer defined to be the sum. The behavior of the extended zeta function is crucial to proving the *Prime Number Theorem*, that asymptotically
$$\pi(x) \sim x/\ln(x)$$
The rate of asymptotic convergence depends on the famous *Riemann hypothesis*, another unsolved problem.
- (*More on the distribution of primes.*) Are there infinitely many $4k + 1$ primes? Infinitely many $28k + 9$ primes? Infinitely many $nk + a$ primes whenever n and a share no factors? If so, can we say more than *infinitely many*? Dirichlet's theorem on primes in an arithmetic progression answers these questions affirmatively. Its proof again uses complex analytic objects; further, these are fully cogent only if we think about the field $\mathbb{Q}(\zeta_n)$ where $\zeta_n = e^{2\pi i/n}$ is the first complex nth root of unity.
- (*The Goldbach Conjecture.*) Is every even integer $n \geq 4$ the sum of two primes? This problem is unsolved.

For all of these problems, the answer is either unknown or requires mathematical structures larger than $\mathbb{Z}^+$ and its arithmetic. On the other hand, plenty can be done working entirely inside $\mathbb{Z}^+$ as well.

So, loosely speaking, there are two options for a first course in number theory, *elementary* or *nonelementary*. (Here elementary doesn't mean *easy*, but rather refers to a course set entirely in $\mathbb{Z}$.) And again speaking loosely, a nonelementary course can be *algebraic* or *analytic*. This course will be nonelementary, with more emphasis on algebra than on analysis, although I hope to introduce some analytical ideas near the end of the semester to demonstrate their interaction with the algebra. Despite the emphasis on algebra in this class, the abstract algebra course is not prerequisite. This course is equally a good venue for practicing with algebra or for beginning to learn it.

Our text, by Ireland and Rosen, is well-suited to the emphasis of the course. We will cover its first nine chapters and a selection of its later material.

Many books are on reserve for this course as well, e.g., Cox, Hardy and Wright, Koblitz, Marcus, Silverman and Tate, Niven and Zuckerman and Montgomery, and so on. Many of these books are mostly about subjects that we will only touch on. Feel welcome to come see me for guidance about reading beyond the course.

2. The Gaussian Integers

As an example of an algebraic structure larger than the integers, the ring of *Gaussian integers* is

$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\},$$

with its rules of addition and multiplication inherited from the field of complex numbers. The Gaussian integers form a ring rather than a field, meaning that addition, subtraction, and multiplication are well-behaved, but inversion is not: the reciprocal of a Gaussian integer in general need not exist within the Gaussian integers.

As a ring, the Gaussian integers behave similarly to the rational integers $\mathbb{Z}$. The *units* (multiplicatively invertible elements) of the Gaussian integers are

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\},$$

a multiplicative group. Every nonzero Gaussian integer factors uniquely (up to units) into prime Gaussian integers. And so on.

Prime numbers in $\mathbb{Z}$ are called *rational primes* to distinguish them from prime numbers in the Gaussian integers. The somewhat awkward phrase *odd prime* means any prime p *other* than 2.

3. Prime Sums of Two Squares via the Gaussian Integers

Theorem 3.1 (Prime Sums of Two Squares)**.** *An odd rational prime p takes the form $p = a^2 + b^2$ (where $a, b \in \mathbb{Z}$) if and only if $p \equiv 1 \bmod 4$.*

(Note: The notation $p \equiv 1 \bmod 4$ means that $p = 4k + 1$ for some k. In general, the language x *is* y *modulo* n means that x and y have the same remainder upon division by n, or equivalently, that n divides $y - x$.)

Proof. ($\Longrightarrow$) This direction is elementary. An odd rational prime p is 1 or 3 modulo 4. If $p = a^2 + b^2$ then $p \equiv 1 \bmod 4$ because each of a^2 and b^2 is 0 or 1 modulo 4.

($\Longleftarrow$) This direction uses the Gaussian integers. For now, take for granted a fact about their arithmetic:

$$p \equiv 1 \bmod 4 \implies p \text{ factors in } \mathbb{Z}[i].$$

Granting the fact, we have

$$\begin{aligned} p \equiv 1 \bmod 4 &\implies p \text{ factors in } \mathbb{Z}[i] \\ &\implies p = (a+ib)(c+id), \quad a+ib, c+id \notin \mathbb{Z}[i]^\times \\ &\implies p^2 = p\overline{p} = (a^2+b^2)(c^2+d^2) \\ &\implies p = a^2+b^2 = c^2+d^2. \end{aligned}$$

So the arithmetic of the Gaussian integers has made the problem easy, but now we need to establish their arithmetic property that p factors in $\mathbb{Z}[i]$ if $p \equiv 1 \bmod 4$. To do so structurally, we quote a fact to be shown later in this course,

$$\{1, 2, 3, \ldots, p-1\} = \{1, g, g^2, \ldots, g^{p-2}\} \quad \text{for some } g\text{, working modulo } p.$$

That is, some element g of the multiplicative group $\{1, 2, 3, \ldots, p-1\}$ (again, working modulo p) *generates* the group. Equivalently, the group is *cyclic*. The generator g need not be unique, but choose some g that generates the group, and define

$$h = g^{(p-1)/4}.$$

This definition is sensible because $p \equiv 1 \bmod 4$. Then $h^2 = -1$, still working modulo p. That is, in the mod p world, -1 has a square root. Now work in the ordinary integers again, where we have $h^2 \equiv -1 \bmod p$. That is, letting the symbol "$\,|\,$" mean *divides* (and then moving back up to the Gaussian integers),

$$p \mid 1 + h^2 = (1 + ih)(1 - ih).$$

But if $p \mid 1 + ih$ then also $p = \overline{p} \mid 1 - ih$, so $p \mid 2$ in $\mathbb{Z}[i]$, so $p \mid 2$ in $\mathbb{Z}$, contradicting the fact that p is odd. Similarly, $p \nmid 1 - ih$. We conclude that p is not prime in $\mathbb{Z}[i]$, because when a prime divides a product, it divides at least one of the factors. Thus p factors in $\mathbb{Z}[i]$ as desired.

However, this argument leaves us with a loose end. Does *prime* mean

doesn't decompose as a product

(i.e., *divisible only by itself, up to units*), or does *prime* mean

doesn't decompose as a factor

(i.e., *if it divides a product then it must divide at least one multiplicand*)? We will discuss this issue soon. Overall, the purpose of this argument that $p \equiv 1 \bmod 4$ implies $p = a^2 + b^2$ is to illustrate the importance of algebraic structure results ($\{1, 2, 3, \ldots, p-1\}$ is cyclic) and algebraic questions (how do two notions of *prime* relate?), not yet to be fully persuasive. □

4. Pythagorean Triples via the Gaussian Integers

Suppose that we have a primitive Pythagorean triple,

$$x^2 + y^2 = z^2, \quad x, y, z \in \mathbb{Z}^+, \ \gcd(x, y, z) = 1.$$

It follows that in fact x, y, and z are pairwise coprime. We normalize the triple by taking x odd, y even, and z odd. (Inspection modulo 4, as in the beginning of the proof just given, shows that the case where x and y are odd and z is even cannot arise.)

Working in the Gaussian integers, the sum of squares factors,

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

For now, take for granted the fact that consequently

$$x + iy \text{ is a perfect square in } \mathbb{Z}[i].$$

Granting the fact, we have

$$x + iy = (r + is)^2 = r^2 - s^2 + i2rs,$$

so that the primitive normalized Pythagorean triple takes the form

$$x = r^2 - s^2, \quad y = 2rs, \quad z = r^2 + s^2,$$

where

$$0 < s < r, \quad \gcd(r, s) = 1, \quad \text{one of } r,\, s \text{ is even.}$$

Incidentally these conditions show that $y \equiv 0 \bmod 4$, and then that $x, z \equiv \pm 1 \bmod 8$ or $x, z \equiv \pm 3 \bmod 8$. Also, the conditions on r and s do ensure that the Pythagorean triple (x, y, z) is primitive: if some prime p divides x and y and z, then p divides $z + x = 2r^2$ and $z - x = 2s^2$. So $p = 2$ because r and s are coprime, but the conditions on r and s make x odd, so this is impossible. Now we can systematically write down all primitive normalized Pythagorean triples in a table. The table begins as follows.

	$r = 2$	$r = 3$	$r = 4$	$r = 5$	$r = 6$	$r = 7$
$s = 1$	$(3, 4, 5)$		$(15, 8, 17)$		$(35, 12, 37)$	
$s = 2$		$(5, 12, 13)$		$(21, 20, 29)$		$(45, 28, 53)$
$s = 3$			$(7, 24, 25)$			
$s = 4$				$(9, 40, 41)$		$(33, 56, 65)$
$s = 5$					$(11, 60, 61)$	
$s = 6$						$(13, 84, 85)$

So the question is why $x + iy$ is a perfect square in $\mathbb{Z}[i]$. Suppose that some prime $\pi \in \mathbb{Z}[i]$ divides $x + iy$ an odd number of times. Recall that $z^2 = (x + iy)(x - iy)$, so that π divides z^2, all of whose prime power divisors must occur an even number of times, and so also π divides $x - iy$. Now we have

$$\pi \mid x \pm iy, z \implies \pi \mid 2x, z \implies \pi\overline{\pi} \mid 4x^2, z^2$$

The last two divisibilities $\pi\overline{\pi} \mid 4x^2, z^2$ hold in $\mathbb{Z}[i]$ if and only if they hold in $\mathbb{Z}$. They fail in $\mathbb{Z}$ because of the primitive normalized Pythagorean triple conditions that $\gcd(x, z) = 1$ and z is odd. So the condition that π divides $x + iy$ an odd number of times is impossible, and $x + iy$ is a unit times a square in $\mathbb{Z}[i]$. If the unit is ± 1 then $x + iy$ is a square. If the unit is $\pm i$ then $i(x + iy) = -y + ix$ is a square $(r + is)^2$, but this makes $x = 2rs$ even, contradicting that x is odd, so this case can't occur. This completes the argument that $x + iy$ is a perfect square in $\mathbb{Z}[i]$.

5. Rational Parametrization of the Circle

Let k denote any field, and let K be any extension field of k, possibly $K = k$. These fields are completely general; for example, k could be the field of p elements for some prime p and K could be the field of $q = p^e$ elements for some positive integer e.

Consider the y-axis and the unit circle in $K \times K$,

$$\mathcal{L} : x = 0,$$
$$\mathcal{C} : x^2 + y^2 = 1,$$

and consider a particular point of C_k,

$$P = (-1, 0),$$

the only point of C_k having first coordinate -1. Given a point $Q = (x_Q, y_Q) \in \mathcal{C}_K$ other than P, so that $x_Q \neq -1$, the corresponding point on $\mathcal{L}_K$ is

$$R = \left(0, \frac{y_Q}{x_Q + 1}\right).$$

Conversely, given a point $R = (0, y_R) \in \mathcal{L}_K$, let $t = y_R$. We seek a point $Q = (x, y) \in \mathcal{C}_K$ with $y = t(x+1)$, other than P. The condition $x^2 + y^2 = 1$ is $(x+1-1)^2 + t^2(x+1)^2 = 1$, and because $x+1 \neq 0$ this simplifies to $(1+t^2)(x+1) = 2$, giving $x + 1 = 2/(1+t^2)$. Because $y = t(x+1)$ it follows that $y = 2t/(1+t^2)$, so that finally,

$$Q = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right).$$

6. Pythagorean Triples Again

Again consider a primitive Pythagorean triple,

$$(x, y, z) \in \mathbb{Z}^3, \quad x^2 + y^2 = z^2, \quad x, y, z \in \mathbb{Z}^+, \ \gcd(x, y, z) = 1, , \ x \text{ odd}, \ y \text{ even}.$$

Let $\widetilde{x} = x/z$ and $\widetilde{y} = y/z$. Then $(\widetilde{x}, \widetilde{y})$ is a point of $\mathcal{C}_{\mathbb{Q}}$,

$$(\widetilde{x}, \widetilde{y}) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right), \quad t = s/r \in \mathbb{Q}.$$

It follows that

$$(\widetilde{x}, \widetilde{y}) = \left(\frac{r^2 - s^2}{r^2 + s^2}, \frac{2rs}{r^2 + s^2} \right), \quad s, r \in \mathbb{Z}.$$

Here we take $0 < s < r$, $\gcd(r, s) = 1$. If in addition, r and s have opposite parities then the quotients will be in lowest terms, so that as before,

$$x = r^2 - s^2, \quad y = 2rs, \quad z = r^2 + s^2.$$

7. An Application From Calculus

Let θ denote the angle to a point $(x, y) \in \mathcal{C}_{\mathbb{R}}$. Then the quantity t in section 5 is

$$t = \tan(\theta/2).$$

Thus $\theta = 2\arctan(t)$, giving the third of the equalities

$$\cos(\theta) = \frac{1-t^2}{1+t^2}, \quad \sin(\theta) = \frac{2t}{1+t^2}, \quad \mathrm{d}\theta = \frac{2\,\mathrm{d}t}{1+t^2}.$$

These relations show that the rational parametrization of the circle gives rise to the substitution in elementary calculus that reduces any integral of a rational function of the transcendental functions $\cos(\theta)$ and $\sin(\theta)$ of the variable of integration θ to the integral of a rational function of the variable of integration t,

$$\int R(\cos(\theta), \sin(\theta))\,\mathrm{d}\theta = \int \widetilde{R}(t)\,\mathrm{d}t.$$

In the abstract, this last integral can be evaluated by the method of partial fractions, but doing so in practice requires factoring the denominator of the integrand.

8. Cubic Curves

Rather than a conic curve, we could consider a cubic curve, e.g.,

$$\mathcal{E} : y^2 = x^3 - g_2 x - g_3 \quad \text{where } g_2 \text{ and } g_3 \text{ are constants.}$$

If the curve $\mathcal{E}$ has a rational point (x, y) then one of the magical phenomena of mathematics arises: the curve carries the structure of an abelian group. The subtleties of the group give rise to applications in connection with number theory and cryptography. Relevant references here are the book by Silverman and Tate, and the book by Washington.

9. Cyclotomic Integer Rings

Finally, here is another example of the utility of an algebraic structure larger than the rational integer ring $\mathbb{Z}$.

Let p be an odd prime. Let $\zeta_p = e^{2\pi i/p} = \cos(2\pi/p) + i\sin(2\pi/p)$ denote the usual "first" complex pth root of unity. Consider the ring $\mathbb{Z}[\zeta_p]$ of polynomials in ζ_p having integer coefficients. Because $1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = 0$, the elements of $\mathbb{Z}[\zeta_p]$ take the form

$$a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}, \quad a_0, a_1, \ldots, a_{p-2} \in \mathbb{Z}.$$

Like the ring of Gaussian integers, this ring of so-called cyclotomic integers has many properties similar to the ring of rational integers. In this ring p factors essentially as $(1-\zeta_p)^p$. For some odd primes p, but not all, one can show by working in the ring $\mathbb{Z}[\zeta_p]$ that the Fermat equation

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

has no solutions (x, y, z) in the rational integers such that $p \nmid xyz$. The starting point to the argument is that in $\mathbb{Z}[\zeta_p]$ we have the factorization

$$x^p + y^p = \prod_{j=0}^{p-1}(x + \zeta_p^j y).$$

This is perhaps most easily seen by noting that because p is odd, $x^p + y^p = 0$ exactly when $x = -\zeta_p^j y$ for some $j \in \{0, 1, \ldots, p-1\}$. For more on this topic, see the *An easy case of Fermat's Last Theorem* writeup for this class or its more general source in chapter 1 of the book **Cyclotomic Fields** by Washington.