Introduction to Number Theory (Fall 2009)
My notes

Kimball Martin

September 2, 2009

Warning: These are my notes for lecture *for myself*, and are not a substitute for the text, or the lectures, or you taking your own notes. Consequently, some details in the lecture and text will not appear here (particularly many examples and some details of proofs), but I am posting them as a *supplementary* reference for the text. (They contain several remarks from lecture that are not in the text.) I also do not know if I will have time to type up notes for the whole semester. However, I will make a point of typing notes for any material not covered in the text.

1 Natural Numbers and Integers

1.1 Natural Numbers

Definition 1.1. *The* natural numbers *are* $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Definition 1.2. *We say* a divides n *(or* a *is a* divisor *of* n*), and write* $a|n$*, if* $n = ab$*, where* n, a, b *are natural numbers.*

Exercise 1.1. *Using the definition, prove that if* $a|b$ *and* $b|c$*, then* $a|c$ *(transitivity).*

Note for any n, both 1 and n are divisors of n.

Definition 1.3. *A natural number* p *is* prime *if it has only 2 divisors:* 1 *and* p*. (Note this excludes 1.) E.g.,* $2, 3, 5, 7, 11, 13, 17, \ldots$

The biggest mystery of number theory is that the primes—fundamental building blocks of natural numbers—individually appear almost completely random, while at the same time, as a group follow certain patterns with complete regularity.

First result: Infinitude of Primes (see two proofs from Lecture 1 notes)

Exercise 1.2. *While there is no known simple way to generate an arbitrary number of primes, certain polynomials are known to produce prime numbers up to a certain point. Let* $p(n) = n^2+n+11$*. Compute* $p(n)$ *for* $0 \le n \le 20$*. For which of these values is* $p(n)$ *prime? (Cf. Exercises in 1.1 the text for a similar question.)*

1.2 Induction

Example. *Show* $3|k^3 + 2k$ *for any natural number* k*.*

Exercise 1.3. *Prove by induction:* $3|2k^3 + k$ *for any natural number* k*.*

1.3 Integers

Definition 1.4. *The* integers *are* $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

Advantage of $\mathbb{Z}$ over $\mathbb{N}$: can subtract any two numbers. This provides more algebraic structure, which makes it easier to work with.

Example. *Describe the set S of numbers of the form $4m + 7n$ (1) where $m, n \in \mathbb{N}$; and (2) where $m, n \in \mathbb{Z}$.*

(1) $S = \{11, 15, 18, 19, 22, 23, 25, 26, 27\} \cup \{29, 30, 31, 32, 33, 34, \ldots\}$
Check ≤ 32 by hand.

$$\begin{aligned} 29 = 4 \cdot 2 + 7 \cdot 3 &\implies 29 + 4m \in S \\ 30 = 4 \cdot 4 + 7 \cdot 2 &\implies 30 + 4m \in S \\ 31 = 4 \cdot 6 + 7 \cdot 1 &\implies 31 + 4m \in S \\ 32 = 4 \cdot 1 + 7 \cdot 4 &\implies 32 + 4m \in S \end{aligned}$$

(2) $S = \mathbb{Z}$
$1 = 4 \cdot 2 + 7 \cdot (-1) \implies n = 4 \cdot (2n) + 7 \cdot (-n) \in S$

Exercise 1.4. *1.3.1, 1.3.3 (can use 1.3.2 without doing it), 1.3.4–1.3.6*

1.4 Division with Remainder

Given $a, b \in \mathbb{N}$, we can repeatedly subtract b from a, say q times, until we get a number $0 \leq r < a$. This gives a unique representation

$$a = qb + r, \;\; 0 \leq r < b$$

where q is the *quotient* and r is the *remainder*. Note $r = 0 \iff b|a$.

Example. $a = 35$, $b = 11$.

1.5 Binary Notation

Repeated division of $n \in N$ by $b \in N$ leads naturally to the b-*ary representation* of n. We will just do examples in the standard (decimal) case of $b = 10$ and the binary case of $b = 2$.

Example. $n = 1234$, $b = 10$.

Example. $n = 43$, $b = 2$.

101011

In general the b-ary representation of n is $a_k a_{k-1} \cdots a_1 a_0$ if

$$n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \cdots + a_1 \cdot b + a_0$$

where $0 \leq a_i < b$. It is well-defined and unique for $n \geq 0$.

$$1234 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4$$
$$43 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1$$

Number of operations. Observe we can use binary representation to drastically reduce the number of operations required to do things like exponentation, which is useful in computation-intensive work.

Example. *Compute* 3^{43}.

$$3^{43} = 3^{2^5} \cdot 3^{2^3} \cdot 3^2 \cdot 3^1$$

Now don't compute 3^{2^5} as 3^{32}, but by *repeated squaring*:

$$\begin{aligned} 3^2 &= 9 \\ 3^{2^2} &= 9^2 = 81 \\ 3^{2^3} &= 81^2 = 6561 \\ 3^{2^4} &= 6561^2 = 43046721 \\ 3^{2^5} &= 43046721 = 1853020188851841 \\ &\text{(5 operations)} \end{aligned}$$

Then

$$3^{43} = 1853020188851841 \cdot 6561 \cdot 9 \cdot 3. \text{ (3 operations)}$$

This is a total of 8 operations, instead of 43. (Here the operation being multiplying 2 numbers.) Note $\lfloor \log_2 43 \rfloor = 5$ and you can always do exponentation with exponent e using between ℓ (best case: binary rep. is $100 \cdots 0$) and 2ℓ (worst case: binary rep. is $111 \cdots 1$) operations where $\ell = \lfloor \log_2 e \rfloor$, instead of $e \approx 2^\ell$ operations.

Exercise 1.5. *Write 19 in binary. Exercises 1.5.1, 1.5.3, 1.5.5.*

1.6 Diophantine Equations

Algebra is concerned with solutions of equations. Finding solutions in radicals, e.g., a la the quadratic formula, is one kind of problem. This is the subject of *Galois theory* and relies on the algebraic notions of *groups* and *fields*.

Another is finding solutions in integers, which is the subject of *number theory*. This relies upon the algebraic notions of *ideals* and *rings*, which we will introduce in the latter part of the course.

One might also consider solutions in natural numbers. As exhibited in Section 1.3, problems in natural numbers may be more complicated than problems in integers, owing to the lack of subtraction. In other cases, these two kinds of problems are equivalent (see the Pythagorean triples below). In any case, problems in natural numbers are a restrictive case of problems in integers, and considered part of number theory. Also in practice, it often makes sense to consider the problem in integers first.

Of course, another natural question is to consider solutions in rational numbers. Multiplying through by denominators allows us to consider integer solutions of a related equations, so these problems are also subsumed in our definition of number theory. However, just like the distinction between natural numbers and integers, problems in rational are sometimes much easier than problems in integers because of the added struction division affords. (For example, consider the question: what natural numbers are of the form $x^3 + y^3 + z^3$. If we want $x, y, z \in \mathbb{Z}$, this is unsolved (#14 of the quiz); but if we allow $x, y, z \in \mathbb{Q}$, then it is not too difficult to show the answer is all natural numbers.) But it many cases, they end up being equivalent (e.g., the congruent number problem, #15 of the quiz).

Definition 1.5. *A* **Diophantine equation** *is an equation of the form (or an equivalent form to)* $f(x_1, \ldots, x_m) = 0$ *where* $f(x_1, \ldots, x_m)$ *is a polynomial with integer coefficients.*

Important examples are:

- The Pythagorean equation $x^2 + y^2 = z^2$. Solutions are called *Pythagorean triples.*
- The Pell equation $x^2 - ny^2 = 1$ where n is not a square.
- The Bachet equation $y^3 = x^2 + n$ for $n > 0$. (Examples of elliptic curves.)
- The Fermat equation $x^n + y^n = z^n$ for $n > 2$.

We will study the above equations, at least in part, in the course of the semester.

For the Pythagorean equation, Euclid showed around 300BC that the solutions in $\mathbb{N}$ are precisely

$$x = (u^2 - v^2)w, \quad y = 2uvw, \quad z = (u^2 + v^2)w,$$

where $u, v, w \in \mathbb{N}$. It is clear that these all give solutions:

$$x^2 + y^2 = (u^2 - v^2)^2 w^2 + 2(u^2 v^2) w^2 = (u^2 + v^2)^2 w^2 = z^2,$$

but it is not clear why these should be all of the solutions. We give a proof (more or less) by elementary means in the next section, and present an algebraic number theory proof in Section 6.6.

1.7 The Diophantus Chord Method

Another classical kind of question in number theory (and arithmetic or algebraic geometry) is, given a curve C, what are its *rational points*, i.e., what points on C have rational coordinated? The Diophantus chord method, also called the *rational slope method*, is one method we can use in many cases.

Namely, suppose you know one rational point Q on C. If R is another rational point on C, then the line through P and Q must have rational slope t (or possibly $t = \infty$). This suggests the following way to find all rational points on a curve, which we illustrate for the circle $C : X^2 + Y^2 = 1$. There are 4 obvious rational points on C, we pick $Q = (-1, 0)$. The line through Q with slope t is given by

$$Y = t(X + 1).$$

Hence other any rational point R on C must lie on one of these lines for some *rational* t (it is clear geometrically we don't need to worry about the vertical line through Q). Substitute in $Y = t(X+1)$ in the equation for C to get

$$X^2 + t^2(X + 1)^2 = 1,$$

i.e.,

$$X^2(1+t^2) + 2t^2X + t^2 - 1 = 0.$$

The quadratic formula gives the solutions $X = -1$ (which gives Q) and

$$X = \frac{1-t^2}{1+t^2} \implies Y = \frac{2t}{1+t^2}.$$

Since X and Y are rational when t is, this gives another rational point R. In fact, this parametrizes all rational points on the circle:

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \text{ for } t \text{ rational and (-1,0) (the “}t = \infty\text{” case).}$$

How is this related to Pythagorean triples? (Stillwell glosses over the details, but I think it is good to go through at least most of them.) Write $X = \frac{x}{z}$ and $Y = \frac{y}{z}$ where z. Then the equation for C is precisely the Pythagorean equation $x^2 + y^2 = z^2$. Now write $t = \frac{v}{u}$, where $u, v \in \mathbb{Z}$. Then

$$\frac{x}{z} = X = \frac{u^2 - v^2}{u^2 + v^2}, \quad \frac{y}{z} = Y = \frac{2uv}{u^2 + v^2}.$$

One would like to say that this implies

$$x = (u^2 - v^2), \quad y = 2uv, \quad z = (u^2 + v^2).$$

It is clear this may not be true. It is more reasonable to hope that

$$x = (u^2 - v^2)w, \quad y = 2uvw, \quad z = (u^2 + v^2)w, \tag{1}$$

for some $w \in \mathbb{N}$ (which also seems more reasonable because it agrees with Euclid's solution.) However, even this is not necessarily true:

$$x = 4, \quad y = 3, \quad z = 5, \quad u = 3, \quad v = 1$$

gives

$$\frac{x}{z} = \frac{4}{5} = \frac{u^2 - v^2}{u^2 + v^2} = \frac{8}{10}, \quad \frac{y}{z} = \frac{3}{5} = \frac{2uv}{u^2 + v^2} = \frac{6}{10}$$

but

$$x = 4 \neq u^2 - v^2 = 8, \quad y = 3 \neq 2uv = 6, \quad z = 5 \neq u^2 + v^2 = 10.$$

This example shows even requiring all our fractions $\frac{x}{z}, \frac{y}{z}$ and $\frac{v}{u}$ be in lowest terms is not sufficient to make this happen.

Nevertheless, it is not difficult to show that if we assume our $\frac{v}{u}$ is in reduced terms, then either

$$x = (u^2 - v^2)w, \quad y = 2uvw, \quad z = (u^2 + v^2)w.$$

or

$$x = \frac{(u^2 - v^2)w}{2}, \quad y = uvw, \quad z = \frac{(u^2 + v^2)w}{2},$$

for some $w \in \mathbb{N}$. (The idea is that if u and v share no common divisors, uv and $u^2 + v^2$ also share no common divisors, so it must be that the reduced form for $\frac{2uv}{u^2+v^2}$ is $\frac{2uv}{u^2+v^2}$ or $\frac{uv}{(u^2+v^2)/2}$. This implies either $z = (u^2 + v^2)w$ or $z = (u^2 + v^2)w/2$ for some w, which gives the corresponding equations for x and y.) In the first case we are done; in the second case, the change of variables $u' = u + v$, $v' = u - v$ gives

$$x = 2u'v'w, \;\; y = (u'^2 - v'^2)w, \;\; z = (u'^2 + v'^2)w,$$

which is the *form* we wanted with x and y reversed. Thus, up to switching x and y any *integer* solutions to the Pythagorean equation are of the form (1) for $u, v, w \in Z$. This implies any *natural number* solutions to the Pythagorean equation are also of the form (1) gives Euclid's solution to the Pythagorean triple problem (where of course now one requires $u, v, w \in \mathbb{N}$ with $u > v$). □

Note that one can easily go back and forth between *integer* and *rational* solutions to $x^2 + y^2 = z^2$ simply by multiplying in or out any denominators. This is possible because the equation is *homogeneous*, i.e., all terms have the same degree (2 in this case).

The rational slope method is also useful in finding rational points on *ellipic curves*

$$y^2 = x^3 + ax + b.$$

However, because this is inhomogeneous, the nature of the integer and rational solutions are quite different (one cannot scale an old solution to get a new one). See Exercises in 1.7.

Exercise 1.6. *Use the rational slope method to find all rational points on the ellipse $X^2 + 2Y^2 = 1$.*

1.8 Gaussian Integers

Note that the elementary solution above required some trickery. I previously suggested introducing the *Gaussian integers,*

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

would lead to an elegant solution due to the factorizations

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

This idea will lead to several other results as well as be indicative of more general methods.

Gauss noticed that $\mathbb{Z}[i]$ has similar properties to $\mathbb{Z}$—for one, they are both closed under $+, -$ and ×. We first prove a modest result.

Two square identity. Products of sums of two squares are sums of two squares.

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2$$

Proof. Note we can rewrite this as

$$(a_1 - b_1i)(a_1 + b_1i)(a_2 - b_2i)(a_2 + b_2i) = (a_1a_2 - b_1b_2 - (a_1b_2 + b_1a_2)i)(a_1a_2 - b_1b_2 + (a_1b_2 + b_1a_2)i),$$

which is the RHS. (Here we multiplied the 1st and 4th and 2nd and 3rd terms on the left.) □

Corollary 1.6. *If (a_1, b_1, c_1) and (a_2, b_2, c_2) are Pythagorean triples, so is $(a_1a_2 - b_1b_2, a_1b_2 + b_1a_2, c_1c_2)$.*

Proof.

$$c_1^2c_2^2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2$$

by the two square identity. □

This can of course be proved without resorting to complex numbers, and must have first been, as Stillwell suggests it was known to Diophantus and possibly the Babylonians. However, it is more naturally seen when viewed from the complex numbers $\mathbb{C}$. For any $z = a + bi \in C$ $(a, b \in \mathbb{R})$, define the *norm* of z

$$N(z) = |z|^2 = |a + bi|^2 = a^2 + b^2.$$

Then it is clear from the absolute value expression that $z = z_1 z_2$ implies

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = N(z_1)N(z_2) = |z_1|^2|z_2|^2 = |z|^2 = N(z) = a^2 + b^2$$

where $z_k = a_k + b_k i$. This is precisely the two square identity above, since one computes

$$z_1 z_2 = (a_1 + b_1 i)(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i \implies a = a_1 a_2 - b_1 b_2, \;\; b = a_1 b_2 + b_1 a_2.$$

Hence the two square identity follows from the fact that $\mathbb{Z}[i]$ is closed under multiplication and the norm map is *multiplicative*, i.e., $N(z_1)N(z_2) = N(z_1 z_2)$.

As mentioned in Lecture 1, one has similar notions of divisibility and prime for $\mathbb{Z}[i]$ as with $\mathbb{Z}$. This suggests the following approach to the Pythagorean triple problem. Suppose (x, y, z) is a *primitive* Pythagorean triple, meaning x, y and z have no common factors (in $\mathbb{Z}$). Now using $\mathbb{Z}[i]$, we factor

$$z^2 = x^2 + y^2 = (x - yi)(x + yi).$$

Since x and y have no common factors in $\mathbb{Z}$, it is reasonable to guess that $x - yi$ and $x + yi$ have no common factors in $\mathbb{Z}[i]$ (whatever this means). But then for the LHS to be a square, both $x - yi$ and $x + yi$ would have to be *squares in* $\mathbb{Z}[i]$, i.e.,

$$x - yi = (u - vi)^2 = (u^2 - v^2) - 2uvi$$

for some $u, v \in \mathbb{Z}$. This means

$$x = u^2 - v^2, \;\; y = 2uv \implies z = u^2 + v^2.$$

Then we can easily go from primitive Pythagorean triples to all Pythagorean triples by multiplying each of x, y and z by w to get Euclid's solution as above. All of this will be made precise in Chapter 6. □

In principle, we could move directly on to the material in Chapter 6 and do this now, but to get a better appreciation for the development of the subject, we will tackle things in order and do some elementary number theory first.

Exercise 1.7. *Exercises 1.8.4, 1.8.5, 1.8.6.*

1.9 Discussion

The Pythagorean triple question—essentially, when is $x^2 + y^2$ a square?—leads to another question: what values does the *quadratic form* $x^2 + y^2$ take? i.e., what numbers are sums of two squares? i.e., which n can we write as $n = x^2 + y^2$? One natural geometric interpretation (assuming $x, y \in \mathbb{N}$) is: what are the possible hypoteni of right triangles whose base and height are integer lengths?

As suggested earlier, it's easier to first consider the problem over $\mathbb{Z}$, and then not too hard to obtain the solution over $\mathbb{N}$. The Exercises in 1.8 imply that if $n = x^2 + y^2$, it cannot be of the form $4k+3$. Around 1640, Fermat answered this question, as well as similar questions for the forms x^2+2y^2 and x^2+3y^2.

In 1798, at the ripe age of 21, Gauss finished his finished his landmark work in number theory, *Disquisitiones Arithmeticae*, which thoroughly treated general binary (here meaning two-variable) quadratic forms $ax^2+bxy+cy^2$, after being previously studied by such greats as Euler, Lagrange and Legendre.

Disquistiones was very hard to penetrate, and the leading 19th century number theorists essentially developed algebraic number theory and much of modern algebra—in particular, rings, ideals and abelian groups—in order to understand it.

The basic idea of algebraic number theory—introducing other number systems—goes back at least to Euler and Lagrange around 1770. For example, Euler determined the integer solutions to $y^3=x^2+2$ by using $\mathbb{Z}[\sqrt{-2}]=\left\{a+b\sqrt{-2}:a,b\in\mathbb{Z}\right\}$ factoring to get $y^3=(x+\sqrt{-2})(x-\sqrt{-2})$, and *assuming* $\mathbb{Z}[\sqrt{-2}]$ behaves sufficiently like $\mathbb{Z}$. Similarly one can use $\mathbb{Z}[\sqrt{-2}]$ to study the form x^2+2y^2.

Gauss rejected this argument, and in fact as he may have known, not all number systems $\mathbb{Z}[\sqrt{-d}]$ have the same properties as $\mathbb{Z}$—in particular, unique factorization into primes may fail. He did however prove that $\mathbb{Z}[i]$ has unique factorization. Subsequently, Kummer and Dedekind, resolved the issue of unique factorization through the concept of *ideals* (which are closely related to quadratic forms), and understanding this will be one of the main goals of the course.