Introduction to Number Theory (Fall 2009)
Lecture 1: What is number theory?

Kimball Martin

August 19, 2009

Basic Terminology: The *natural numbers* are $1, 2, 3, \ldots$. The *integers* are $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$. *Primes* are natural numbers which have precisely 2 factors: 1 and itself; i.e., $2, 3, 5, 7, 11, 13, \ldots$. (Note for technical reasons 1 is typically excluded.)

1 The dictionary answer

What is number theory?

It is usually defined as the study of the integer solutions to polynomial equations with integer coefficients (called *Diophantine equations*). Some examples are $x^2+y^2=z^2$, $3x-5y=7$, $y^2=x^3+12x+5$ and $x^2+y^2+z^2+w^2=10$. You may recognize the first equation as the Pythagorean theorem (variables suitably interpreted). In other words, the question "what are the integer solutions to $x^2+y^2=z^2$" is equivalent to asking what are all the integral Pythagorean triples, i.e., what are the possibilities for right-angled triangles with integral length sides. It is easy to find some—you probably remember from high school that $x=3, y=4, z=5$ or $x=5, y=12, z=13$ work—but how to determine all (integral) solutions is a more advanced problem.

An elegant way to solve this problem is through the use of complex numbers. In particular, define the *Gaussian integers* to be the set of numbers of the form $a+bi$ where a and b are integers and $i=\sqrt{-1}$. Thinking in terms of Gaussian integers we can factor the left hand side of the equation $x^2+y^2=z^2$ to get

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

Here $\alpha = x+iy$ and $\beta = x-iy$ are by definition Gaussian integers. Just like integers can be factored into primes, the Gaussian integer z^2 (which is also an integer) can be factored into what are called Gaussian primes, and this can be used to determine the possibilities for $\alpha = x+iy$ and $\beta = x-iy$, and hence the possibilites for x and y.

It may be helpful to illustrate the idea of using prime factorization in a simpler context. Suppose you want to find the solutions $mn=30$ (m, n integers). The prime factorization of 30 is $30 = 2\cdot3\cdot5$, so we can list all possible solutions as

$$30 = 1\cdot30 = 30\cdot1 = 2\cdot15 = 15\cdot2 = 6\cdot5 = 5\cdot6 = 10\cdot3 = 3\cdot10.$$

The idea is that working we can solve the equation $\alpha\beta = z^2$ in Gaussian integers in a similar way, which leads to the complete solution (in integers) of our original equation $x^2+y^2=z^2$. This idea is also described in Section 1.8, and we will do this properly in Chapter 6 of the text. This is considered an *algebraic* approach. There are also so-called *elementary* approaches to this problem, as were discovered by the ancient Greeks (cf. Sections 1.6 and 1.7).

Above, I said that number theory is usually defined as the study of the integer solutions of these equations. However, it is also much more this. In fact the above Pythagorean triple example illustrates several important features pervasive through number theory:

- Number theory is arguably the *oldest branch* of mathematics, beginning with counting. For a long time, mathematics was essentially just number theory and geometry.
- As questions about integer solutions can be boiled down to problems about prime numbers, perhaps the most central topic in number theory is the study of **primes** (both the familiar and more generalized notions such as Gaussian primes).
- Many questions in number theory have **geometric interpretations**, just as the Pythagorean triple question is a question about right-angled triangles.
- Many questions in number theory which are very simple to state are in fact very challenging to solve. In fact, unlike a course in Calculus or Linear Algebra, where most basic questions you can ask are fairly simple to solve and the subject (at its basic levels) is thought of as a "closed book," **most** basic questions you might think to ask are **still unsolved**. This has to do with the mysterious nature of prime numbers, and the richly hidden patterns in nature and numbers.

  In many cases where a solution is found, the solution will require tools from seemingly unrelated areas of mathematics. (Or rather it's often the case is that by trying to solve these problems, new areas of mathematics are discovered. It has been said that the two driving forces within modern mathematics are Number Theory and Calculus. For instance, most of Modern Algebra was developed out of studying problems in Number Theory.) Moreover, the problem is often beautiful in how simple the answer is but how the solution itself requires a new kind of cleverness or way of thinking (as we will see is true for the Pythagorean triple question in Chapter 6).

All of these things have made number theory the branch of mathematics that, more so than any other, have fascinated amateurs and professionals throughout the ages.

2 Answered with questions

Another way to answer "what is number theory" is by giving you a representative sample of the kinds of problems studied in number theory. I hope this will make apparent the "living" nature of number theory (i.e., that people are still actively discovering new things about it), and in particular the "easy to state, hard to solve" nature of the field mentioned above which draws many mathematicians and non-mathematicians to it. Here I will describe several interesting and well known classical problems below in the form of a quiz. Some of these have been solved long ago, some not until recently and some are still unsolved. These are very roughly ordered by flavor, and not by difficulty. For each of these, I would like you to guess which have been solved long ago, which were solved recently (say within the last 50 years) and which are still unsolved.

Bear in mind that all of these problems are well founded. In other words, while some may seem random at first, they were well thought out in advance based on numerical evidence.

The quiz

All numbers are assumed to be integers in the problems below, unless stated otherwise.

1. How many primes are there?

2. Find a formula for the n-th prime number.

3. Are there infinitely many primes of the form $4n + 1$?

4. Are there infinitely many primes of the form $n^2 + 1$?

5. Note that 3 and 5, as well as 5 and 7, 11 and 13, etc. are *twin primes*, i.e., they differ by 2. Are there infinitely many twin primes?

6. An *arithmetic progression* is a sequence of numbers which increase by the same amount each time. For example, $3, 5, 7$ and $11, 17, 23, 29$ are arithmetic progressions of primes, of lengths 3 and 4 respectively. Are there arbitrarily long arithmetic progressions of primes?

7. Is every even integer greater than 2 is the sum of two primes?

8. $8 = 2^3$ and $9 = 3^2$ are consecutive numbers which are both powers (squares, cubes, fourth powers, etc.) of integers. Are there others?

9. Start with any positive n. If it is even divide by two. If it is odd take $3n + 1$. Repeat with the new number. If repeated sufficiently many times, does one eventually get down to 1 for any initial number n?

10. Find a simple characterization of all numbers which are sums of two squares (i.e., of the form $x^2 + y^2$).

11. Find a simple characterization of all numbers of the form $x^2 + y^2 + 10z^2$.

12. Find a simple characterization of all numbers which are sums of 4 squares (i.e., of the form $x^2 + y^2 + z^2 + w^2$).

13. Find a simple characterization of all natural numbers which are sums of 2 cubes of *rational numbers*.

14. Find a simple characterization of all natural numbers which are sums of 3 cubes of *rational numbers*.

15. Which numbers occur as areas of right triangles whose sides are all integer lengths?

16. Are there solutions in the positive integers to $x^n + y^n = z^n$ for $n > 2$?

17. Given a Diophantine equation, devise an algorithm to determine whether it has integer solutions or not in a finite number of steps.

3 Solutions and non-solutions

1. How many primes are there?

   Status: Easy. Solved by Euclid (ca. 300 BC). There are infinitely many primes. However, this seemingly basic question goes much deeper than this. A more refined way of asking this is: for any x, how many primes are less than x? Conjectured in 1796 by Legendre, and proved independently exactly 100 years later by Hadamard and de la Vallée Poussin, we in fact know the asymptotic distribution of prime numbers,

   $$\#\{\text{primes } \leq x\} \sim \frac{x}{\log x}.$$

   This result is known as the Prime Number Theorem and was proved using complex analysis and so-called the Riemann zeta function. Since many proofs (all quite difficult, but some not requiring complex analysis) have been found, until a relatively simple proof was found in 1980 by Newman (using complex analysis). The Prime Number Theorem is only a first-order asymptotic, and the "best possible" bound on the error term ($\sqrt{x}\log(x)/(8\pi)$) is equivalent to the famous (still conjectural) *Riemann hypothesis*. All of this is a central topic in *analytic number theory*.

2. Find a formula for the n-th prime number.

   Status: There is no known formula (in a sense of easily computable) to generate the prime numbers, nor is it believed that there is one (at least in a simple sense). Note that such a formula would be equivalent to an exact formula for $\pi(x)$, which is quite complicated as indicated above.

3. Are there infinitely many primes of the form $4n + 1$?

   Status: Yes. In fact if $p(n) = an + b$ where a and b have no common factors, then $p(n)$ is prime infinitely often. This is known as *Dirichlet's theorem on arithmetic progressions* and was proved in 1837 by Dirichlet. In the course of proving this Dirichlet developed much basic groundwork used in both *algebraic* and *analytic number theory*. We will get to the specific case of $4n + 1$ at the end of Chapter 6.

4. Are there infinitely many primes of the form $n^2 + 1$?

   Status: Unsolved. It is easy to see that no (non-constant) polynomial can be prime for all n. However it is not known if there exists *any* quadratic (or cubic, quartic, etc.) polynomial which gives prime values infinitely often. Aside: in 1772, Euler observed that the polynomial $p(n) = n^2 + n + 41$ gives prime numbers for all $0 \leq n < 40$, but not for $n = 40$.

5. Note that 3 and 5, as well as 5 and 7, 11 and 13, etc. are *twin primes*, i.e., they differ by 2. Are there infinitely many twin primes?

   Status: Still unsolved. Generally believed the answer is yes. In 1966, Chen used analytic methods to show that there are infinitely many primes p such that $p + 2$ is either prime or a product of two primes.

6. An *arithmetic progression* is a sequence of numbers which increase by the same amount each time. For example, $3, 5, 7$ and $11, 17, 23, 29$ are arithmetic progressions of primes, of lengths 3 and 4 respectively. Are there arbitrarily long arithmetic progressions of primes?

Status: Recently solved! This was a big theorem proved by Green and Tao in 2004 using combinatorial and analytic methods (56 pages).

7. Is every even number greater than 2 is the sum of two primes?

   Status: Unsolved, though much work has been done, and the answer is believed to be yes. This was conjectured by Goldbach in a weaker form in 1742 and refined by Euler to the present form. Much progress has been made by *analytic* methods, specifically using *sieve* techniques. In 1975, Montgomery and Vaughan showed that *most* even numbers are sums of two primes. In 1995, Ramaré show that every even number is the sum of at most six primes.

8. $8 = 2^3$ and $9 = 3^2$ are consecutive numbers which are both powers (squares, cubes, fourth powers, etc.) of integers. Are there others?

   Status: Recently solved! The answer is no. This was conjectured by Catalan in 1844 and proved by Mihailescu in 2002 using *algebraic number theory* techniques (28 pages).

9. Start with any positive n. If it is even divide by two. If it is odd take $3n+1$. Repeat with the new number. If repeated sufficiently many times, does one eventually get down to 1 for any initial number n?

   Status: Unsolved, though much work has been done. This is called the $3n+1$ or the *Collatz problem*, proposed by Collatz in 1937. The iterated nature of the problem makes this a part of what might be called *arithmetic dynamics*, a crossroads of dynamical systems and number theory.

10. Find a simple characterization of all numbers which are sums of two squares (i.e., of the form $x^2 + y^2$).

    Status: Solved in 1640 by Fermat, one of the founding fathers of modern number theory (who was in fact an amateur mathematician—his profession was a judge), though not an easy problem. The solution comes by way of solving the simpler question of which *primes* are sums of two squares. The answer is precisely 2 and the primes of the form $4n + 1$! This will be our main result in Chapter 6. This question, concerning squares as it does, can be interpreted geometrically, and is a starting point for the very rich area of number theory known as *quadratic forms* (meaning expressions such as $x^2 + y^2$, $x^2 + y^2 + 10z^2$, etc., where all terms are quadratic).

11. Find a simple characterization of all numbers of the form $x^2 + y^2 + 10z^2$.

    Status: Unsolved, but recent progress. This form is known as Ramanujan's form and the following answer was by the famous Indian mathematician in 1916. He had a partial answer, and in 1997 Ono and Soundararajan showed that the (still conjectural) generalized Riemann hypothesis implies the following answer: all even numbers not of the form $4^k(16m + 6)$ and all odd numbers except 3, 7, 21, 31, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391, 679, 2719. This is a famous problem in the theory of *quadratic forms*, and Ono and Soundararajan show it is intimately related to *analytic number theory* as well as *algebraic number theory* and *geometry* via *elliptic curves*.

12. Find a simple characterization of all numbers which are sums of 4 squares (i.e., of the form $x^2 + y^2 + z^2 + w^2$).

Status: Solved. Even though you might guess that it looks harder than Ramanujan's form because of the extra variable, it's much easier, as is the answer: all integers This was proved by Lagrange in 1770, and we will use some simple techniques from *algebraic number theory* to prove this result in Chapter 8. (Note: this problem is also easier than the case of 3 squares: $x^2 + y^2 + z^2$ which was dealt with by Legendre and Gauss decades later.)

13. Find a simple characterization of all natural numbers which are sums of 2 cubes of *rational numbers.*

    Status: Unsolved! In 1995 Villegas and Zagier showed that the theory of *elliptic curves* and *modular forms* classifies, in a simple way, which primes are sums of 2 cubes, under the assumption of the Birch–Swinnerton-Dyer (BSD) conjecture, the second most famous outstanding conjecture in number theory. The result for primes may lead to the result for all natural numbers, as in the case of the sum of 2 squares.

14. Find a simple characterization of all natural numbers which are sums of 3 cubes of *rational numbers.*

    Status: Solved by Richmond in 1923. This question is not too hard (unlike the previous), however this problem (and likely the previous) is much harder if we ask which numbers are sums of 3 cubes of *integers.* The smallest unknown case is 33. Computational work is ongoing. On the other hand, *analytic methods* have been recently applied to show that *most* numbers are sums of 3 cubes without giving any information which ones are. As both the status of this and the previous problem indicate, while the theory of quadratic forms is very rich, the theory of *cubic forms* (polynomial expressions where each term is of degree three) is as yet very primitive, though there has been spectacular development within the past 50 years.

15. Which numbers occur as areas of right triangles whose sides are all integer lengths?

    Status: Unsolved! This is known as the *congruent number problem*, which seems to go back to the ancient Greeks. Interestingly enough, in 1983 Tunnell gave an elegant solution *assuming* the same conjecture Villegas and Zagier took for granted in their work on the sum of 2 cubes, the BSD conjecture.

16. Are there solutions in the positive integers to $x^n + y^n = z^n$ for $n > 2$?

    Status: Recently solved! You've probably heard of this. The answer's no and it's called Fermat's Last Theorem. Wiles, with help from Taylor, proved it in 1995 using some heavy-duty *algebraic number theory* techniques (129 pages). This proof also involves a lot of geometry via what are called *elliptic curves* and their relation to *modular forms*, which stand at a crossroads of *algebraic* and *analytic number theory.* While it would take several years of serious study to understand the complete proof, we will be able to tackle the case of $n = 3$ with some simple algebraic number theory in Chapter 7. (The cases $n = 4$, $n = 5$ and $n = 7$ are also relatively easy.)

17. Given a Diophantine equation, devise an algorithm to determine whether it has integer solutions or not in a finite number of steps.

    Status: Solved! Sort of. Fairly recently. In 1900, Hilbert presented a famous list of 23 problems, saying that once all of these are solved, we will know all that there is to know about mathematics. (Some are more ambitious than others, and some are rather vague: The 6th is axiomatize all of physics. The 8th was the aforementioned Riemann hypothesis together with Goldbach's conjecture. Of the 23, 6 are pure number theory, and 2 of these 6 are resolved. In total, somewhere between 10 and 13 have been resolved, depending on interpretation.) This problem was Hilbert's 10th. It was proved in 1959 by Davis and Putnam showed that no such algorithm exists!

Let me remark the person(s) I attribute to solving the problem are for reference purposes only. A good mathematical problem gets considered by many individuals (sometimes working together, which is much more common nowadays) and the solution evolves through the effort of many people over decades or possibly centuries. In the community, people who make important contributions are usually (often?) appropriately acknowledged, but here I only mention the person(s) who completed the solution (who do of course typically deserve a lion's share of the credit). Similarly, while I occasionally gave the number of pages for the paper with the solution to give you an idea of how much it involves, bear in mind that these paper build upon previous papers, so in some sense this is just how long the "last step" of the solution is.

4 Main branches of number theory

Number theory can be divided into many different branches, typically delineated by the kinds of problems studied as well as the techniques used. I think most mathematicians would agree on the following as the 3 main categories of number theory, though the actual lines between them are rather blurry.

- **Elementary number theory.** While all of the problems stated in the quiz were stated in an "elementary" way—their statement requires no advanced mathematics—very few of them can be tackled in an elementary way. One of the main ideas here is to use the idea of divisibility and some cleverness to prove some results, which one can do for things like the infinitude of primes (Euclid's answer to #1 on the quiz), the Pythagorean triple question (cf. Sections 1.6 and 1.7 for the elementary approach—the one we suggested using Gaussian integers is the "algebraic" approach) or which numbers are sums of squares (#10 on the quiz). A typical undergrad first course in number theory focuses on elementary number theory.

- **Algebraic number theory.** The basic idea of algebraic number theory is to use other number systems to study the integers and primes, as in the example of introducing the Gaussian integers for the Pythagorean triple question. (This problem, as well as others, are included in both the elementary and algebraic categories because there are different ways to solve it.) We could also consider problems #3, #8, and #10–#16 in the realm of algebraic number theory.

- **Analytic number theory.** It turns out that calculus and complex analysis are very powerful tools which can be applied to number theory problems such as the Prime Number Theorem (cf. #1, #2). This is rather striking as on the surface these subjects seem very far removed from one another, but the basic idea is to consider appropriate series for studying the problem at hand. One might say that the problems #3—#7 are in the realm of analytic number theory, though it also has plays a role in problems such as #10–#16.

As the methods from elementary number theory tend to be rather limited, most number theory research nowadays involves algebraic or analytic number theory, if not both. For example, the theory of *quadratic forms* mentioned above contains aspects of each of elementary, algebraic and analytic number theory.

Two of the most important tools in modern number theory, as seen in applications to to #11, #13, #15 and #16 above, are:

- **Modular** (or **automorphic) forms.** These arise at a crossroads of algebraic and analytic number theory. Here at OU (and OSU), our number theory research group specializes more on the algebraic side (involving *groups* and *representations*) of things—in particular Ralf Schmidt and I often work on the more algebraic aspects of modular and automorphic forms (which in practice involves a lot of series and integrals).

- **Elliptic curves.** These are related to modular forms, and lie at an intesection of algebraic number theory and algebraic geometry. Elliptic curves are also an active area of research, with the BSD conjecture being one of the biggest problems in the field. While no one at OU currently works explicitly on elliptic curves (or is an expert in the area), via modular forms it is related to some of the work we do here.

This semester might be considered a course in elementary algebraic number theory. We will start with some basic elementary methods, (a la Chapters 1–5, omitting 4), gently introducing methods of algebraic number theory with the Gaussian integers in Chapter 6, quadratic integers in Chapter 7, prove Lagrange's four squares theorem using quaternions in Chapter 8, cover quadratic reciprocity—the crowning achievement of elementary number theory— in Chapter 9, and then develop the basic building blocks of algebraic number theory—rings and ideals—in Chapters 10–11, and explore a generalized notion of primes in Chapter 12.

Some possibilities for the second semester are i) more serious (but not too serious) algebraic number theory, ii) basic analytic number theory, iii) quadratic forms and iv) elliptic curves. Any of these could potentially lead into a graduate course on modular forms the subsequent year, though I am currently leaning towards a combination of algebraic number theory and quadratic forms, which would be a natural continuation of the material this semester.

5 Postscript: an example of elementary and analytic techniques

While I partially sketched an example of some simple algebraic number theory by introducing the Gaussian integers into the Pythagorean triple question, I haven't really given you any examples of elementary or analytic number theory techniques. I will illustrate each by giving two proofs of the infinitude of primes.

Theorem. There are infinitely many primes.

Elementary Number Theory Proof. (Euclid, ca. 300BC; also see Section 1.1 of text) This is an example of a proof by contradiction, which you should be comfortable with. Suppose on the contrary there are only finitely many primes. Label them $p_1, p_2, \ldots, p_k$. Let $n = p_1 p_2 \cdots p_k + 1$. Then n divided by p_i has remainder 1 for any $i = 1, 2 \ldots k$, i.e., none of the p_i's are factors of n. This leaves two possibilities: either n itself is prime (if it has no factors besides 1 and n), or it is not. If n is prime, we have our contradiction and are done.

If n is not prime, $n = ab$ for some $1 < a, b < n$. Since no p_i is a factor of n, no p_i is a factor of a either. Now we repeat our argument for n with a: either a is prime, or not. It a is prime, we are done. If not, we apply the argument again with a smaller factor of a. Now this process must terminate in a finite number of steps (less than n), because we are working with smaller and smaller integers between 1 and n. Thus we will eventually end with a prime factor of n, contradicting the assumption that there were only finitely many primes. (This process of going down from n to a and so on is called *descent*; cf. Section 1.2.) $\square$

Analytic Number Theory Proof. (Euler, ca. 1735) The key idea of Euler is to observe that

$$\left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots\right)\left(1 + \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \cdots\right)\left(1 + \frac{1}{5} + \frac{1}{5^2} + \frac{1}{5^3} + \cdots\right)\cdots$$
$$= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n},$$

where the product on the left is a product of the quantities

$$1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots$$

as p ranges over all primes. Note that this series is a geometric series with ratio less than 1, so it is evaluated by

$$1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots = \frac{1}{1 - 1/p}.$$

(If you forgot this, multiply through by the denominator of the right hand side, and the left hand side telescopes down to 1.) Hence we have

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_p \frac{1}{1 - 1/p} = \infty$$

since the left hand side is the harmonic series which diverges. Since each term in the product over primes is a finite number, for this product to diverge, it must be infinite. I.e., there must be infinitely many primes! In other words, the infinitude of primes is equivalent to the divergence of the harmonic series! $\square$

While the analytic proof may seem unnecessarily complicated (in that it involves some calculus—it is not actually longer), i) it is certainly beautiful, and ii) the basic ideas in this proof can be pushed much much further to get strong results like the Prime Number Theorem, which one can't do with Euclid's proof. While we will not pursue these ideas this semester, if you are interested in learning more about them, look up the *Riemann zeta function.*