MA357 — Elementary Number Theory

Spring, 2020

Fernando Q. Gouvêa

People have always been fascinated by numbers and their properties. Number theory is the natural outgrowth of that fascination. Already in ancient times one finds questions about "properties of numbers." Since then, number theory has become an important part of mathematics. Because it deals with patterns that are easily observed empirically, it sometimes has the feel of experimental science. On the other hand, the proofs that these patterns hold (or that they don't) are often hidden so deeply that one needs extremely sophisticated mathematical tools to make any progress at all. It is perhaps this blend of simplicity (in the questions) and depth (in the answers) that has led mathematicians such as Gauss to proclaim number theory "the Queen of Mathematics."

During most of its history, number theory was famous for being the purest of "pure mathematics." Even as late as 1982, when Jean Dieudonné wrote his *Panorama of Pure Mathematics* (check it out, it's in the library), he could claim that there were no contacts between number theory and the physical sciences. That has all changed, quite suddenly, over the last few decades, when two new realms of application became more and more important. The first is computer science, where number theory has come to play a crucial role—there is a lot of number theory in Knuth's *The Art of Computer Programming*, for example. The best known applications have to do with the problems of encoding data and of encrypting data. The second area of application is theoretical physics, where recent developments in string theory and related ideas have led to surprising connections with number theory. (It's not clear if the result will be good physics, but it is certainly interesting mathematics.) Of course, it never was quite true that number theory had no applications: in any situation that is discrete, one is bound to run into number-theoretical problems, and one can mention several examples beginning in the mid-nineteenth century. The difference, I think, is that those examples involved application of relatively elementary number theory, while modern-day applications have grown increasingly subtle and have in fact motivated new work in the field.

This course will pay some attention to the applications of number theory, especially those related to cryptography, but our main focus will be on the theory itself. Nevertheless, I will try to give you pointers to significant applications as we reach the relevant portions of the course.

So what is number theory about? It is about (whole or rational) numbers, but in a special sense. Number theory isn't really too interested in specific problems about particular numbers (that's arithmetic); instead, it focuses on *general* patterns.

Some theorems of number theory are known by everyone: "the sum of two odd numbers is even" is a general property of numbers. But most patterns are harder. For example, one of the theorems we will prove says that a prime number can be written as a sum of two squares if and only if it leaves a remainder of 1 when it is divided by 4. We will discuss a number of questions of this type in our first class meeting.

This course will be an introduction to elementary number theory. The word "elementary" here has a technical meaning: it indicates that we won't be using more advanced theories (such as complex analysis or algebraic geometry) to study number-theoretical patterns. This means the course has few pre-requisites, but it does *not* mean that the material is easy—in fact, many of the theorems we'll be thinking about are quite subtle.

One way to approach elementary number theory is to keep away from "heavy" mathematical concepts from, say, abstract algebra or analysis. To do this, one chooses simple but tricky methods to prove the basic theorems. Unfortunately, this suggests that number theory is all about finding incredibly tricky elementary arguments. That's just not true! So we're going to try something different, choosing arguments and ideas that link to bigger mathematical themes. We will do this in two ways: by linking number theory to geometry and by introducing some elementary bits of abstract algebra when they are helpful. This way, I hope you will see how number theory fits into the rest of mathematics. Perhaps it'll also help convince you that those other ideas are useful!

I think number theory is fun. I hope you'll come to agree.

Course web site: Please visit and bookmark this page:

`http://personal.colby.edu/personal/f/fqgouvea/357/`

Assignments will be posted there as well as other useful information.

Goals of this Course: What do I expect you to be able to do after this course? Of course, I want you to know the content. But here are some other goals:

- I hope you will further develop your ability to read, understand, and create mathematical arguments.
- I hope you will leave the course more confident in your ability to think creatively and to find solutions to problems without having a "road map" in advance.
- I hope you will improve your ability to think precisely.
- I hope you will improve your ability to *write* about mathematics.
- I hope you will realize that things can be fascinating and fun despite being difficult (maybe even *because* they are difficult).

- I hope you will have a better sense of this area of mathematics: know its central themes, be able to use some of its basic methods, be able to enjoy new ideas and discoveries.
- Finally, I hope you will have a stronger desire to learn more mathematics!

Where to find me: My office is Davis 208; my phone extension is 5836; my email address is `fqgouvea@colby.edu`. If you need to reach me when I'm not in my office, email is the best method. If you prefer, feel free to call and leave a message—but sometimes I take a while to notice the little red light. In any case, see the note on email below.

Office hours: You are encouraged to come see me. Talking to your professors is part of your education, and one of your privileges as a Colby student. I can help you with the course, talk about your mathematics courses in general, or talk about whatever else you would like.

My office hours this semester will be on **Mondays and Wednesdays** from 1:30 to 3:30 PM. What this means is that at these times I will be in my office and will not be busy with anything but students. You may arrive at my office to find me busy with another student. If so, please be patient; I'll try to make sure that everyone gets a chance to see me.

You may find me in my office at other times, but it is only at the times above that I can guarantee that I'll be available. Feel free to ask me if I can talk, but please allow me to say "no" if I am busy with other things.

You can always reach me by email, and if necessary we can make an appointment. Notice, however, that I am usually not on campus on Thursdays.

Texts: Our textbook will be *Number Theory and Geometry*, by Álvaro Lozano Robledo. This is an elementary introduction to number theory that keeps its sight firmly on the more advanced area known as "arithmetic(al) algebraic geometry." I hope to cover chapters 1–10 and then go on to do at least part of 11–14.

We have a second required book, John Derbyshire's *Prime Obsession*. This is not a textbook; rather, it's a "popular math" book. I hope you'll find it readable. Our approach to Number Theory will emphasize the algebraic and geometric sides of number theory. Derbyshire's book will give us a glimpse of another branch of advanced number theory, known as "analytic number theory."

Other books: It's important to remember that Colby does have a good library. We have many books on number theory, and it's quite possible that one of them will fit your personal style and so prove to be a useful complement to our textbook. The number theory books live in the sections of the library numbered QA241–247. Go look.

Here are some books that might be worth a look:

- Joe Silverman has a book called *A Friendly Introduction to Number Theory*; it really is friendly, though the price is not.
- *Elementary Number Theory: Primes, Congruences, and Secrets*, by Stein, uses *Sage*. (Stein is the creator of *Sage*.) Colby's library has this as an e-book, so you can access it easily.
- *The Elements of Number Theory*, by John Stillwell, is the textbook I used the last time I taught this course.
- *Number Theory in Science and Communication*, by M. R. Schroeder, is a good account of some of the easier applications of number theory.
- Weissman's *An Illustrated Theory of Numbers* is amazing: every topic is treated in a strongly visual fashion. It's a bit too hard for a textbook, but definitely interesting.

Reading mathematics books is hard, but you can often get some good insights simply by reading introductions and first chapters and then browsing a bit. Of course, if you find the book interesting, read more.

Technology: Number theory has an experimental side: one can detect number patterns by computing a large number of examples. You will probably find it helpful (or even necessary) to use a computer to construct examples, test conjectures, and experiment. There are two very useful (and free) programs you should learn to use: *Sage* and GP. On the course web site there is a handout with a (very) short introduction to these programs.

Assignments: In any math course, the real action is in the problem sets and assignments. You just can't learn mathematics passively. So there will be a variety of assignments during the course:

- **Automathography by email:** your first assignment is to send me a short email message introducing your mathematical self to me. Tell me about courses you have taken, about ideas that you've found exciting, about things you've found boring or difficult, about your goals as a student. If you have taken MA274, I'd like to know what that was like and how much you remember. If you have worries about any special problems or needs, let me know. You are encouraged to be creative in your response; don't just answer the questions above, but include whatever else you wish. This email message is due no later than **Wednesday, February 12**.
- **First writing assignment: review a book.** There will be two writing assignments. The first will be based on John Derbyshire's *Prime Obsession*. You will be asked to read the book and then write a review. Your review should

describe the content of the book, discuss the quality of the expository writing, and give your reaction to both the mathematics and the history that Derbyshire explains. More details about this assignment will be provided during the first week of classes. This assignment will be due **Friday, March 13** (so start reading!).

- **Second writing assignment: a mathematical exploration.** The second writing assignment will involve some expository mathematical writing of your own. I will provide you with a list of possible topics, all of which will consist either of a significant theorem or a problem (solved or unsolved) that requires some exploration. (It's ok for you to choose your own topic, of course, but check with me first.) This paper has a dual goal: to understand a small bit of mathematics as thoroughly as possible, and then to explain it as clearly as possible. More details of this assignment will be provided later. This assignment will be due **Friday, April 24**.

- **Problem Sets:** Problem sets will be passed out **every Friday** and will be **due the following Friday**. They will include a few routine practice problems and a few more interesting problems that will require some thought and creativity. These problems can be freely discussed with other students and with professors, but please do not go searching for solutions online. Once you have solved the problems, however, you are to "write up" the solutions yourself.

  These problem sets *will* take several days to complete: don't leave them for the last day!

  We will grade the problem sets as follows: I will (semi) randomly choose four of the problems to be graded. Each problem will be worth two points. An additional two points "for style" are available; typically you will get one style point if your assignment is well written, formatted well, and easy to deal with. The second style point is reserved for special situations. You should think of the "perfect score" as being 9 points, even though it is possible to get more than that.

Exams: We will have one midterm exam, in the week of March 16–20 (the week before spring break), and also a final exam. Both exams will be take-home exams. While working on them, you will be allowed to use your textbook, your notes, mathematical software tools such as *Sage* or GP, and to talk to your professor. No other sources of help will be allowed. In particular, you may not discuss the problems with others and you may not search for solutions online. I will provide more information as we get nearer to the exam dates.

Attendance: You are expected to come to class. Should you be unable to come to class on a particular day, please contact me. Unexcused absences *will* have an effect on your grade for the course. Many unexcused absences may lead to your being asked to withdraw from the course.

Grading: Your grade will be computed as follows:

problem sets	25%
first writing assignment	10%
second writing assignment	20%
midterm exam	20%
final exam	25%

On reading your textbook: I expect you to read your textbook. This doesn't mean that you have to learn everything by yourself, but it does mean that I will often concentrate on the central ideas of an argument when the book contains all the details. Of course, you should feel free to ask questions about what's in the book when we discuss the material in class.

Reading a mathematics book is not like reading other texts. First of all, it's slow. Mathematicians tend to write in a very compressed, terse style, and reading it takes lots of "unpacking." As you read, have paper and pencil in hand, and be careful to work out examples, fill in details, check assertions. Second, one reading is not going to be enough. I suggest that before each class you try to read the relevant sections of the book. In this first reading, you should try to get the overall structure of the argument, without worrying too much about the details. Then, after class, re-read the section, comparing with what we discussed in class and filling in all the details you can. If necessary, compare with other books. Discuss the material with other people, and with me. Then read again.

Working with others: Mathematics is a social activity. Mathematicians are always talking to each other, explaining questions and theorems and saying things like "what's really going on here is…", "do you know whether…" and "I have a conjecture…." You'll enjoy this course more if you can find a small group of people to work with, not only doing the homework together, but talking about the material. The more you invest, the more you'll profit.

An outline: Trying to schedule a mathematics course amounts to me predicting how fast my students will learn. I don't know how to predict that. So instead of a week-by-week schedule, here is an outline of what I'm planning to do.

a. We'll start with an axiomatic description of the integers.

b. The first big theme will be how to find rational and integral points on lines. The rational case is easy, but solving the integer case will require a lot of material on divisibility, prime numbers, greatest common divisors, congruences, modular arithmetic, and so on.

c. Modular arithmetic turns out to be so interesting that we will stop for an extended tour, using them to introduce the language of fields and rings, some simple group theory, and so on.

d. At this point we should be able to discuss how prime factorizations allow us to construct a method to keep messages secret.

e. The next big theme will be finding rational and integer solutions to quadratic equations. That will lead to several important ideas, including the most important elementary theorem in number theory, known as “quadratic reciprocity.”

f. At that point we’ll be close to the end of chapter 10 in the textbook; we will see then which topics to consider next.

Academic Honesty & Consequences for Academic Dishonesty

Honesty, integrity, and personal responsibility are cornerstones of a Colby education and provide the foundation for scholarly inquiry, intellectual discourse, and an open and welcoming campus community. These values are articulated in the *Colby Affirmation* below. I will expect you to behave accordingly. You are expected to demonstrate academic honesty in all aspects of this course. If you are clear about course expectations, give credit to those whose work you rely on, and submit your best work, you are highly unlikely to commit an act of academic dishonesty.

Academic dishonesty includes, but is not limited to: violating clearly stated rules for taking an exam or completing homework; plagiarism (including material from sources without a citation and quotation marks around any borrowed words); claiming another's work or a modification of another's work as one's own; buying or attempting to buy papers or projects for a course; fabricating information or citations; knowingly assisting others in acts of academic dishonesty; misrepresentations to faculty within the context of a course; and submitting the same work, including an essay that you wrote, in more than one course without the permission of the instructors.

Academic dishonesty is a serious offense against the college. Sanctions for academic dishonesty are assigned by an academic review board and may include failure on the assignment, failure in the course, or suspension or expulsion from the College. For more on recognizing and avoiding plagiarism, see the library guide: `libguides.colby.edu/avoidingplagiarism`.

The Colby Affirmation:

Colby College is a community dedicated to learning and committed to the growth and well-being of all its members.

As a community devoted to intellectual growth, we value academic integrity. We agree to take ownership of our academic work, to submit only work that is our own, to fully acknowledge the research and ideas of others in our work, and to abide by the instructions and regulations governing academic work established by the faculty.

As a community built on respect for ourselves, each other, and our physical environment, we recognize the diversity of people that have gathered here and that genuine inclusivity requires active, honest, and compassionate engagement with one another. We agree to respect each other, to honor community expectations, and to comply with college policies.

As a member of this community, I pledge to hold myself and others accountable to these values.