Number Theory
Instructor’s suggestions for use of Number Theory notes

Goal. Our goal is to inspire students to be actively engaged in mathematical thought. We want them to discover ideas on their own, grapple with challenging new concepts, and learn various techniques of thought through repeated exposure throughout the course. Many students entering this course do not arrive with an understanding of mathematical thinking. Most students in this course do not have experience with proving theorems independently and making conjectures independently. Our goal is to give students the chance to explore mathematical questions on their own. As they do so, they will develop methods of proving theorems and exploring mathematics.

The basic method. Fundamentally the method of instruction consists of the students working on the questions and theorems in the notes and presenting their work at the board. On a typical day, the students’ assignment is to work on the next five theorems or questions and to be prepared to present their answers or proofs at the next class.

There are several challenges to using this method.

• get all students to participate actively in the process,
• not letting the class be dominated by just a few students,
Number Theory and Mathematical Thinking

One of the great steps in the development of a mathematician is becoming an independent thinker. Every mathematician can look back and see a time when mathematics was mostly a matter of learning techniques or formulas. Later, the challenge was to learn some proofs. But at some point, the successful mathematics student becomes a more independent mathematician. Formulating ideas into definitions, examples, theorems, and conjectures becomes part of daily life.

The following notes have two equally significant goals. One goal is to help you develop independent mathematical thinking skills. The second is to help you understand some of the fundamental ideas of number theory.

You will develop skills of formulating and proving theorems. Mathematics is a participatory sport. Just as a person learning to play tennis would expect to play tennis, people seeking to learn to think like a mathematician should expect to do those things that mathematicians do. Also, in analogy to learning a sport, making mistakes and then making adjustments are clear parts of the experience.

Number theory is an excellent subject for learning the ways of mathematical thought. Every college student is familiar with basic properties of numbers, and yet the study of those familiar numbers leads us into waters of extreme depth. Many simple observations about small, whole numbers can be collected, formulated, and proved. Other simple observations about small, whole numbers can be formulated into conjectures of amazing richness. Many simple-sounding questions remain unanswered after literally thousands of years of thought. Other questions have recently been settled after being unsolved for hundreds of years.

Throughout these notes, we will continue to emphasize the dual goals of developing mathematical thinking skills and developing an understanding of number theory. The two goals are inextricably entwined throughout and seeking to disentangle the two would be to miss the essential strategy of this two-pronged approach.

The mathematical thinking skills developed here include being able to

- look at examples and formulate definitions and questions or conjectures;
- prove theorems using various strategies;
- determine the correctness of a mathematical argument independently without having to ask an authority.

Clearly these thinking skills are applicable across all mathematical topics and outside mathematics as well.
Note on the approach. The book is divided into modules. Each module begins with a brief introductory statement about the topic. The module then contains definitions, examples and some questions, statements of lemmas, and statements of theorems. Definitions are generally preceded by examples and discussion that make that definition a natural consequence of the experience of the examples and the line of thinking presented. We want you to see the development of mathematics as a natural exploration of a realm of thought. Never should mathematics seem to be a mysterious collection of definitions, theorems, and proofs that arise from the void and must be memorized for a test. Theorem statements arise as crystallized observations. Proofs are clear reasons that the statements are true. Most sections end with a Big Picture Question which may be an open-ended question or other question that seeks to have you gather the threads of the module into one coherent strand.

While looking at numbers and finding patterns among them, it will be natural to develop an understanding of various ways to give convincing arguments. These different styles of proofs will become familiar and logically sound. We do not present these methods of proof in the abstract, but instead develop them as naturally occurring methods of stating logically correct reasons for the truth of statements.

Number theory contains within it some of the most fascinating insights in mathematics. We hope you will enjoy your exploration of this intriguing domain.
Outline for an introduction to number theory and mathematical thinking

The course contains two threads—number theory and mathematical thinking. Methods of thought, proof, and analysis are not facts to be learned once, but they are developed into useful tools as they appear recurrently in different contexts.

Some methods of thought, proof, and analysis are:

- Finding patterns and formulating conjectures.
- Making precise definitions.
- Making precise statements.
- Learning basic logic including taking negations and contrapositives.
- Understanding examples.
- Relating examples to the general case.
- Generalizing from examples.
- Measuring complexity.
- Looking for elementary building blocks.
- Following consequences of assumptions.
- Methods of proof:
  - induction,
  - method of descent,
  - method of ascent,
  - reducing complexity,
  - contradiction,
  - taking reasoning that works in a special case and making it general.

1. Division algorithm, Euclidean algorithm, linear Diophantine equations, introduction to modular arithmetic
2. Primes
   Basic Diophantine equations—Pythagorean triples, Fermat’s methods of ascent and descent, basic remarks about Pell’s equation, \( x^4 + y^4 = z^4 \), Fermat’s Last Theorem.

Section II: Modular arithmetic and applications in RSA cryptography.

- Modular arithmetic—definition, basic theorems about congruences under arithmetic operations, linear Diophantine equations.
- Diophantine equations revisited using congruents to show that certain Diophantine equations have no solutions.
- Chinese Remainder Theorem and applications.
• Lagrange’s Theorem about number of roots of equations mod $p$, efficient algorithm to take exponents.
• Fermat’s Little Theorem, Euler’s $\phi$-function, Euler’s Theorem, consequences for taking modular exponents.
• RSA cryptography.

Section III: Primitive roots, quadratic reciprocity, and sums of squares.
• Euler’s $\phi$-function is multiplicative, sum of $\phi(d)(d|n)$.
• Order of elements mod $p$ and $n$, ord$(a)|(p - 1)$, primitive roots.
• Squares mod $p$, quadratic reciprocity.
• Primes as sums of squares, sums of squares.

Section IV: Rational and irrational numbers.
• Introduction to rational and irrational numbers.
• Farey fractions.
• Irrationality of $\sqrt{n}$ and related numbers.
• Irrationality of $e$, discussion of $\pi$, open questions.

Section V: Diophantine approximation.
• Dirichlet’s Theorem, rational approximation of irrationals.
• Continued fractions.
• Quadratic irrationals and Pell’s equation revisited.
• Algebraic and transcendental numbers, Liouville’s Theorem, and a proof that transcendental numbers exist.
• Discussion of Roth’s Theorem and its implications to Diophantine equations.
1. Division Algorithm, Euclidean Algorithm, Linear Diophantine Equations and Introduction to Modular Arithmetic

**Introduction and Goals.** How can one natural number be expressed as the product of smaller natural numbers? This innocent sounding question leads to a vast field of interconnections among the natural numbers that mathematicians have been exploring for literally thousands of years. The adventure begins by recalling the arithmetic from our youth and looking at it afresh. In this section we will explore the Division Algorithm, greatest common divisors, the Euclidean Algorithm, and some consequences of these to finding integer solutions to linear equations. We will develop skills in proving theorems by induction and other means.

Many experiences in everyday life are cyclical—hours in the day, days in a week, motions of the planets. This concept of cyclicity gives rise to the idea of modular arithmetic, which develops the notion of numbers on a cycle. In this section, we will introduce the basic idea of modular arithmetic, which we will develop further in future sections.

**Definitions.**

1. The natural numbers are the numbers \( \{1, 2, 3, 4, \ldots\} \).
2. The integers are \( \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \).
3. Suppose \( a \) and \( d \) are integers, then \( d \) divides \( a \), denoted \( d | a \), if and only if there is an integer \( k \) such that \( a = kd \).
4. Suppose that \( a, b \), and \( n \) are integers, \( n > 0 \). We say that \( a \) and \( b \) are **congruent modulo** \( n \) if and only if \( n | (a - b) \). We denote this relationship as \( a \equiv b \pmod{n} \)

and read these symbols as “\( a \) is congruent to \( b \) (mod \( n \)).”

We begin now with the first set of questions. “Theorem” denotes a mathematical statement to be proved by you. For example,

**Example Theorem.** \( 3 | -9 \).

Then you would supply the proof, write it up clearly, and be prepared to present your proof at the board. Your write-up might look like this:

**Example Proof.** By definition, \( 3 | -9 \) means that there exists an integer \( k \) such that \( -9 = 3k \). So to prove that this definition is satisfied, we need to find an integer \( k \) such that \( -9 = 3k \). Since \( -9 = 3 \cdot (-3) \), the definition is satisfied, so \( 3 | -9 \) is true. \( \square \)
Example Theorem. $3 \equiv 7 \pmod{2}$.

Example Proof. $-4 = 2(-2)$. So, by definition, $2|(-4)$. So $2|(3 - 7)$. But $2|(3 - 7)$ is the definition of $3 \equiv 7 \pmod{2}$, so the theorem is proved. \[ \square \]

Note: In giving proofs, rely on the definitions of terms and symbols, and feel free to use results that you have previously proved. Avoid using statements that you ‘know,’ but which we have not yet proved.

1.1. Theorem. Let $a$, $b$, and $c$ be integers. If $a|b$ and $a|c$, then $a|(b + c)$.

1.2. Theorem. Let $a$, $b$, and $c$ be integers. If $a|b$ and $a|c$, then $a|(b - c)$.

1.3. Theorem. Let $a$, $b$, and $c$ be integers. If $a|b$ and $a|c$, then $a|bc$.

1.4. Question. Can you weaken the hypothesis of the previous theorem and still prove the theorem? Can you replace the conclusion by $a\div b$ and still prove the theorem?

1.5. Formulate your own theorem along the lines of the above theorems and prove it.

1.6. Theorem. Let $a$, $b$, and $c$ be integers. If $a|b$, then $a|bc$.

1.7. Examples. Prove your answers. Is $45 \equiv 9 \pmod{4}$? Is $37 \equiv 2 \pmod{5}$? Is $37 \equiv 3 \pmod{5}$? Is $31 \equiv -3 \pmod{5}$?

1.8. Exercise. For each of the following congruences, characterize all the numbers $m$ that satisfy that congruence.

$$
egin{align*}
m &\equiv 0 \pmod{3}, \\
m &\equiv 1 \pmod{3}, \\
m &\equiv 2 \pmod{3}, \\
m &\equiv 3 \pmod{3}, \\
m &\equiv 4 \pmod{3}.
\end{align*}
$$

1.9. Theorem. Let $a$ and $n$ be integers with $n > 0$. Then $a \equiv a \pmod{n}$.

1.10. Theorem. Let $a$, $b$, and $n$ be integers with $n > 0$. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

1.11. Theorem. Let $a$, $b$, $c$, and $n$ be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
Note: If you are familiar with equivalence relations, you may note that the previous three theorems establish that congruence modulo \( n \) defines an equivalence relation on the set of integers. In the question before those theorems, 1.8, you described the equivalence classes modulo 3.

1.12. Theorem. Let \( a, b, c, d, \) and \( n \) be integers with \( n > 0 \). If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then \( a + c \equiv b + d \pmod{n} \).

1.13. Theorem. Let \( a, b, c, d, \) and \( n \) be integers with \( n > 0 \). If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then \( a - c \equiv b - d \pmod{n} \).

1.14. Theorem. Let \( a, b, c, d, \) and \( n \) be integers with \( n > 0 \). If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then \( ac \equiv bd \pmod{n} \).

1.15. Theorem. Let \( a, b, k, \) and \( n \) be integers with \( n > 0 \) and \( k > 0 \). If \( a \equiv b \pmod{n} \), then \( a^k \equiv b^k \pmod{n} \).

1.16. Question. Illustrate each of the above theorems with an example using actual numbers.

1.17. Theorem. Let a natural number \( n \) be expressed in base 10 as

\[
n = a_ka_k - 1 \cdots a_1a_0 .
\]

Then if \( m = a_k + a_{k-1} + \cdots + a_1 + a_0 \), \( n \equiv m \pmod{3} \).

1.18. Theorem. A natural number that is expressed in base 10 is divisible by 3 if and only if the sum of its digits is divisible by 3.

1.19. Question. Devise and prove other divisibility criteria similar to the preceding one.

**Well-Ordering Axiom for the Natural Numbers.** Let \( S \) be any non-empty set of natural numbers, then \( S \) has a smallest element.

We will just assume that the Well-Ordering Axiom for the Natural Numbers is true. So feel free to use it whenever you wish.

**The Division Algorithm.** Let \( n \) and \( m \) be natural numbers. Then (existence part) there exist integers \( q \) (for quotient) and \( r \) (for remainder) such that

\[
m = nq + r \text{ and}
\]
0 \leq r \leq n - 1 \ (r \ is \ greater \ than \ or \ equal \ to \ 0 \ but \ less \ than \ or \ equal \ to \ n - 1). \ Moreover, \ (uniqueness \ part) \ if \ q, \ q' \ and \ r, \ r' \ are \ any \ integers \ that \ satisfy \ m = nq + r = nq' + r' \ with \ 0 \leq r, r' \leq n - 1, \ then \ q = q' \ and \ r = r'.

1.20. Illustrate the division algorithm for \( m = 22, \ n = 11; \) \( m = 33, \ n = 45; \) \( m = 277, \ n = 4. \)

1.21. Prove the existence part of the Division Algorithm. (Hint: Given \( n \) and \( m, \) how will you define \( q? \) Once you choose this \( q, \) then how is \( r \) chosen? Then show that \( 0 \leq r \leq n - 1. \))

1.22. Prove the uniqueness part of the Division Algorithm. (Hint: If \( nq + r = nq' + r', \) then \( nq - nq' = r' - r. \) Use what you know about \( r \) and \( r' \) as part of your argument that \( q = q'. \))

1.23. Theorem. Let \( a, \ b, \) and \( n \) be nonnegative integers with \( n > 0. \) Then \( a \equiv b \ (\text{mod} \ n) \) if and only if \( a \) and \( b \) have the same remainder when divided by \( n. \) Equivalently, \( a \equiv b \ (\text{mod} \ n) \) if and only if when \( a = nq_1 + r_1 \ (0 \leq r_1 \leq n - 1) \) and \( b = nq_2 + r_2 \ (0 \leq r_2 \leq n - 1), \) then \( r_1 = r_2. \)

Definitions. 1. The greatest common divisor of two integers \( a \) and \( b \) is the largest integer \( d \) such that \( d|a \) and \( d|b. \) The greatest common divisor of two integers \( a \) and \( b \) is denoted \( \gcd(a, b) \) or \( (a, b). \)

2. If \( \gcd(a, b) = 1, \) then \( a \) and \( b \) are said to be relatively prime.

1.24. Question. Find \((36, 22), (45, -15), (296, -88), (0, 256), \) and \((15, 28). \)

1.25. Theorem. Let \( a, \ n, \ b, \) and \( k \) be integers. If \( a = nb + r \) and \( k|a \) and \( k|b, \) then \( k|r. \)

1.26. Theorem. Let \( a, \ n_1, \ b, \ r_1, \ n_2, \) and \( r_2 \) be integers. If \( a = n_1b + r_1, \) then \( (a, b) = (b, r_1). \) Similarly, if \( b = n_2r_1 + r_2, \) then \( (b, r_1) = (r_1, r_2). \)

1.27. Question. As an illustration of the above theorem, note that

\[
\begin{align*}
51 &= 3 \cdot 15 + 6 \\
15 &= 2 \cdot 6 + 3 \\
6 &= 2 \cdot 3 + 0.
\end{align*}
\]

Show that if \( a = 51 \) and \( b = 15, \) then \( (51, 15) = (6, 3) = 3. \)
1.28. Question (Euclidean Algorithm). Using the previous theorem and the Division Algorithm successively, devise a procedure for finding the greatest common divisor of two integers.

1.29. Use the Euclidean Algorithm to find (96, 112), (288, 166), and (175, 24).

1.30. Using your work from 1.29, find integers $x$ and $y$ such that $175x + 24y = 1$.

1.31. Theorem. Let $a$ and $b$ be integers. The greatest common divisor of $a$ and $b$ equals 1 (i.e., $(a, b) = 1$) if and only if there exist integers $x$ and $y$ such that $ax + by = 1$.

(Note: This theorem is an ‘if and only if’ theorem, so you must prove two theorems: (1) If $(a, b) = 1$, then there exist integers $x$ and $y$ such that $ax + by = 1$. And (2) If there exist integers $x$ and $y$ with $ax + by = 1$, then $(a, b) = 1$. The hint for the first part is to use the Euclidean Algorithm. Do some examples by taking some pairs of relatively prime integers, doing the Euclidean Algorithm, and seeing how to find the $x$ and $y$. It is a good idea to start with an example where the Euclidean Algorithm takes just one step, then do an example where the Euclidean Algorithm takes two steps, then three steps, then look for a general procedure.)

1.32. Theorem. For any integers $a$ and $b$, there are integers $x$ and $y$ such that $ax + by = (a, b)$.

1.33. Theorem. Let $a$, $b$, and $c$ be integers. If $a|bc$ and $(a, b) = 1$, then $a|c$.

Theorems 1.30 and 1.31 begin to address the question: Given integers $a$, $b$, and $c$, when do there exist integers $x$ and $y$ that satisfy the equation $ax + by = c$? When we seek integer solutions to an equation, the equation is called a Diophantine equation.

1.34. Question. Suppose there is a solution to the linear Diophantine equation $ax + by = c$. What condition does $c$ satisfy in terms of $a$ and $b$?

1.35. Question. Make a conjecture by completing the following theorem statement. Conjecture. Given integers $a$, $b$, and $c$, there exist integers $x$ and $y$ that satisfy the equation $ax + by = c$ if and only if _______. Prove your conjecture.

1.36. Theorem. Given integers $a$, $b$, and $c$, there exist integers $x$ and $y$ that satisfy the equation $ax + by = c$ if and only if $(a, b)|c$. 

11
1.37. **Question.** For integers $a$, $b$, and $c$, consider the linear Diophantine equation $ax + by = c$. Suppose integers $x_0$ and $y_0$ satisfy the equation, that is, $ax_0 + by_0 = c$. What other values, $x = x_0 + h$ and $y = y_0 + k$, also satisfy $ax + by = c$? Formulate a conjecture that answers this question. Devise some numerical examples to ground your exploration. For example, $6(-2) + 15 \cdot 2 = 18$. Can you find other integers $x$ and $y$ such that $6x + 15y = 18$? How many other pairs of integers $x$ and $y$ can you find? Can you find infinitely many other solutions?

1.38. **Question (Euler).** A farmer lays out the sum of 1,770 crowns in purchasing horses and oxen. He pays 31 crowns for each horse and 21 crowns for each ox. What are the possible numbers of horses and oxen that the farmer bought?

1.39. **Theorem.** Let $a$, $b$, $c$, $x_0$, and $y_0$ be integers such that $ax_0 + by_0 = c$. Then the integers $x = x_0 + \frac{b}{(a,b)}$ and $y = y_0 - \frac{a}{(a,b)}$ also satisfy the linear Diophantine equation $ax + by = c$.

1.40. **Question.** If $a$, $b$, and $c$ are integers and the linear Diophantine equation $ax + by = c$ has at least one integer solution, find a general expression for all the integer solutions to that equation. Prove your conjecture.

1.41. **Theorem.** Let $a$, $b$, $c$, be integers. Then the equation $ax + by = c$ has a solution if and only if $(a, b)|c$. If $x_0, y_0$ is a solution, that is, $ax_0 + by_0 = c$, then for every integer $k$, the integers $x = x_0 + \frac{kb}{(a,b)}$ and $y = y_0 - \frac{ka}{(a,b)}$ also satisfy the linear Diophantine equation $ax + by = c$. Moreover, every solution to the linear Diophantine equation $ax + by = c$ is of this form.

1.42. **Theorem.** If $a$ and $b$ are integers and $k$ is a natural number, then $\gcd(ka, kb) = k \gcd(a, b)$.

1.43. **Formulate a definition.** For natural numbers $a$ and $b$, give a suitable definition for the least common multiple of $a$ and $b$, denoted $\text{lcm}(a, b)$. Your definition should reflect the words “least common multiple.” Construct and compute some examples.

1.44. **Theorem.** If $a$ and $b$ are natural numbers, then $\gcd(a, b) \text{lcm}(a, b) = ab$.

1.45. **Corollary.** If $a$ and $b$ are natural numbers, then $\text{lcm}(a, b) = ab$ if and only if $\gcd(a, b) = 1$.

1.46. **Big Picture Question:** How are the ideas of greatest common divisor and solutions to linear Diophantine equations related?