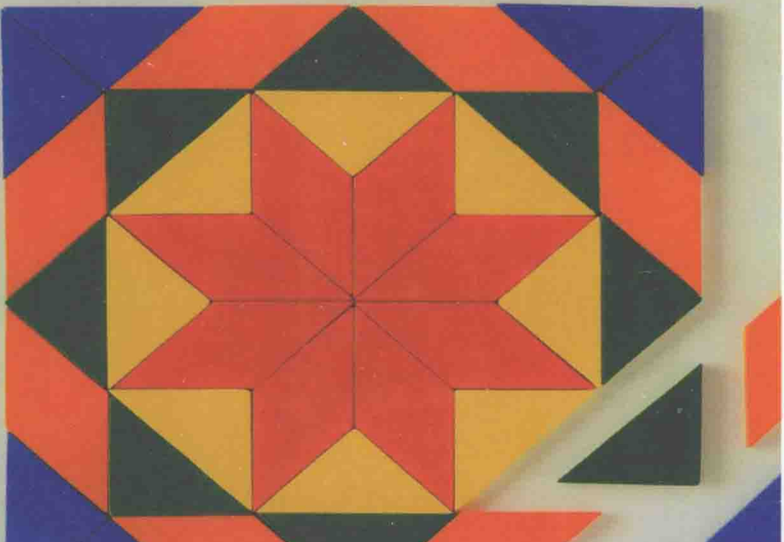
经　典　原　版　书　库

数论概论

（英文版 · 第3版）

A FRIENDLY INTRODUCTION TO NUMBER THEORY

THIRD EDITION



（美） Joseph H. Silverman 著
布朗大学

机械工业出版社
China Machine Press

经 典 原 版 书 库

数论概论

（英文版 · 第3版）

A Friendly Introduction to Number Theory

(Third Edition)

（美） Joseph H. Silverman 著
布朗大学

机械工业出版社
China Machine Press

本书版权登记号：图字：01-2006-3141

图书在版编目（CIP）数据

数论概论（英文版·第3版）/（美）西尔弗曼（Silverman, J. H.）著. －北京：机械工业出版社，2006.8

（经典原版书库）

书名原文：A Friendly Introduction to Number Theory, Third Edition

ISBN 7-111-19611-2

Ⅰ.数…　Ⅱ.西…　Ⅲ.数论－教材－英文　Ⅳ.O156

中国版本图书馆CIP数据核字（2006）第080893号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）
责任编辑：迟振春
北京京北制版厂印刷·新华书店北京发行所发行
2006年8月第1版第1次印刷
170mm × 242mm · 27.75印张
定价：52.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换
本社购书热线：（010）68326294

Preface

The 1990s saw a wave of calculus reform whose aim was to teach students to think for themselves and to solve substantial problems, rather than merely memorizing formulas and performing rote algebraic manipulations. This book has a similar, albeit somewhat more ambitious, goal; to lead you to think mathematically and to experience the thrill of independent intellectual discovery. Our chosen subject, Number Theory, is particularly well suited for this purpose. The natural numbers 1, 2, 3, ... satisfy a multitude of beautiful patterns and relationships, many of which can be discerned at a glance; others are so subtle that one marvels they were noticed at all. Experimentation requires nothing more than paper and pencil, but many false alleys beckon to those who make conjectures on too scanty evidence. It is only by rigorous demonstration that one is finally convinced that the numerical evidence reflects a universal truth. This book will lead you through the groves wherein lurk some of the brightest flowers of Number Theory, as it simultaneously encourages you to investigate, analyze, conjecture, and ultimately prove your own beautiful number theoretic results.

This book was originally written to serve as a text for Math 42, a course created by Jeff Hoffstein at Brown University in the early 1990s. Math 42 was designed to attract nonscience majors, those with little interest in pursuing the standard calculus sequence, and to convince them to study some college mathematics. The intent was to create a course similar to one on, say, "The Music of Mozart" or "Elizabethan Drama," wherein an audience is introduced to the overall themes and methodology of an entire discipline through the detailed study of a particular facet of the subject. Math 42 has been extremely successful, attracting both its intended audience and also scientifically oriented undergraduates interested in a change of pace from their large-lecture, cookbook-style courses.

The prerequisites for reading this book are few. Some facility with high school algebra is required, and those who know how to program a computer will have fun generating reams of data and implementing assorted algorithms, but in truth the reader needs nothing more than a simple calculator. Concepts from calculus are mentioned in passing, but are not used in an essential way. However, and the reader is hereby forewarned, it is not possible to truly appreciate Number Theory without an eager and questioning mind and a spirit that is not afraid to experiment, to make mistakes and profit from them, to accept frustration and persevere to the ultimate triumph. Readers who are able to cultivate these qualities will find themselves richly rewarded, both in their study of Number Theory and their appreciation of all that life has to offer.

Acknowledgments for the First Edition

There are many people I would like to thank for their assistance—Jeff Hoffstein, Karen Bender, and Rachel Pries for their pioneering work in Math 42; Bill Amend for kindly permitting me to use some of his wonderful FoxTrot cartoons; the creators of PARI for providing the ultimate in number theory computational power; Nick Fiori, Daniel Goldston, Rob Gross, Matt Holford, Alan Landman, Paul Lockhart, Matt Marcy, Patricia Pacelli, Rachel Pries (again), Michael Schlessinger, Thomas Shemanske, Jeffrey Stopple, Chris Towse, Roger Ware, Larry Washington, Yangbo Ye, and Karl Zimmerman for looking at the initial draft and offering invaluable suggestions; Michael Artin, Richard Guy, Marc Hindry, Mike Rosen, Karl Rubin, Ed Scheinerman, John Selfridge, and Sam Wagstaff for much helpful advice; and George Lobell and Gale Epps at Prentice Hall for their excellent advice and guidance during the publication process.

Finally, and most important, I want to thank my wife Susan and children Debby, Daniel, and Jonathan for their patience and understanding while this book was being written.

Acknowledgments for the Second Edition

I would like to thank all those who took the time to send me corrections and suggestions that were invaluable in preparing this second edition, including Arthur Baragar, Aaron Bertram, Nigel Boston, David Boyd, Seth Braver, Michael Catalano-Johnson, L. Chang, Robin Chapman, Miguel Cordero, John Cremona, Jim Delany, Lisa Fastenberg, Nicholas Fiori, Fumiyasu Funami, Jim Funderburk, Andrew Granville, Rob Gross, Shamita Dutta Gupta, Tom Hagedorn, Ron Jacobowitz, Jerry S. Kelly, Hershy Kisilevsky, Hendrik Lenstra, Gordon S. Lessells, Ken Levasseur, Stephen Lichtenbaum, Nidia Lopez Jerry Metzger, Jukka Pihko, Carl Pomerance, Rachel Pries, Ken Ribet, John Robeson, David Rohrlich, Daniel Silverman, Alfred Tang, and Wenchao Zhou.

Acknowledgments for the Third Edition

I would like to thank Jiro Suzuki for his beautiful translation of my book into Japanese. I would also like to thank all those who took the time to send me corrections and suggestions that were invaluable in preparing this third edition, including Bill Adams, Autumn Alden, Robert Altshuler, Avner Ash, Joe Auslander, Dave Benoit, Jürgen Bierbrauer, Andrew Clifford, Keith Conrad, Sarah DeGooyer, Amartya Kumar Dutta, Laurie Fanning, Benji Fisher, Joe Fisher, Jon Graff, Eric Gutman, Edward Hinson, Bruce Hugo, Ole Jensen, Peter Kahn, Avinash Kalra, Jerry Kelly, Yukio Kikuchi, Amartya Kumar, Andrew Lenard, Sufatrio Liu, Troy Madsen, Russ Mann, Gordon Mason, Farley Mawyer, Mike McConnell, Jerry Metzger, Steve Paik, Nicole Perez, Dinakar Ramakrishnan, Cecil Rousseau, Marc Roth, Ehud Schreiber, Tamina Stephenson, Jiro Suzuki, James Tanton, James Tong, Chris Towse, Roger Turton, Fernando Villegas, and Chung Yi.

Email and Electronic Resources

All the people listed above have helped me to correct numerous mistakes and to greatly refine the exposition, but no book is ever free from error or incapable of being improved. I would be delighted to receive comments, good or bad, and corrections from my readers. You can send mail to me at

`jhs@math.brown.edu`

Additional material, including an errata sheet, links to interesting number theoretic sites, and downloadable versions of various computer exercises, are available on the *Friendly Introduction to Number Theory* Home Page:

`www.math.brown.edu/~jhs/frint.html`

Joseph H. Silverman

Contents

Introduction

Euclid alone
Has looked on Beauty bare. Fortunate they
Who, though once only and then but far away,
Have heard her massive sandal set on stone.
Edna St. Vincent Millay (1923)

The origins of the natural numbers 1, 2, 3, 4, 5, 6, ... are lost in the mists of time. We have no knowledge of who first realized that there is a certain concept of "threeness" that applies equally well to three rocks, three stars, and three people. From the very beginnings of recorded history, numbers have inspired an endless fascination—mystical, aesthetic, and practical as well. It is not just the numbers themselves, of course, that command attention. Far more intriguing are the relationships that numbers exhibit, one with another. It is within these profound and often subtle relationships that one finds the Beauty[1] so strikingly described in Edna St. Vincent Millay's poem. Here is another description by a celebrated twentieth-century philosopher.

> Mathematics, rightly viewed, possesses not only truth, but supreme beauty—a beauty cold and austere, like that of sculpture, without appeal to any part of our weaker nature, without the gorgeous trappings of paintings or music, yet sublimely pure, and capable of a stern perfection such as only the greatest art can show. (Bertrand Russell, 1902)

The Theory of Numbers is that area of mathematics whose aim is to uncover the many deep and subtle relationships between different sorts of numbers. To take a simple example, many people through the ages have been intrigued by the square numbers 1, 4, 9, 16, 25, ... If we perform the experiment of adding together pairs

[1] Euclid, indeed, has looked on Beauty bare, and not merely the beauty of geometry that most people associate with his name. Number theory is prominently featured in Books VII, VIII, and IX of Euclid's famous *Elements*.

of square numbers, we will find that occasionally we get another square. The most famous example of this phenomenon is

$$3^2 + 4^2 = 5^2,$$

but there are many others, such as

$$5^2 + 12^2 = 13^2, \quad 20^2 + 21^2 = 29^2, \quad 28^2 + 45^2 = 53^2.$$

Triples like $(3, 4, 5)$, $(5, 12, 13)$, $(20, 21, 29)$, and $(28, 45, 53)$ have been given the name Pythagorean triples.[2] Based on this experiment, anyone with a lively curiosity is bound to pose various questions, such as "Are there infinitely many Pythagorean triples?" and "If so, can we find a formula that describes all of them?" These are the sorts of questions dealt with by number theory.

As another example, consider the problem of finding the remainder when the huge number

$$32478543^{743921429837645}$$

is divided by 54817263. Here's one way to solve this problem. Take the number 32478543, multiply it by itself 743921429837645 times, use long division to divide by 54817263, and take the remainder. In principle, this method will work, but in practice it would take far longer than a lifetime, even on the world's fastest computers. Number theory provides a means for solving this problem, too. "Wait a minute," I hear you say, "Pythagorean triples have a certain elegance that is pleasing to the eye, but where is the beauty in long division and remainders?" The answer is not in the remainders themselves, but in the use to which such remainders can be put. In a striking turn of events, mathematicians have shown how the solution of this elementary remainder problem (and its inverse) leads to the creation of simple codes that are so secure that even the National Security Agency[3] is unable to break them. So much for G.H. Hardy's singularly unprophetic remark that "no one has yet discovered any warlike purpose to be served by the theory of numbers or relativity, and it seems very unlikely that anyone will do so for many years."[4]

The land of Number Theory is populated by a variety of exotic flora and fauna. There are square numbers and prime numbers and odd numbers and perfect numbers (but no square-prime numbers and, as far as anyone knows, no odd-perfect

[2] In fairness, it should be mentioned that the Babylonians compiled large tables of "Pythagorean" triples many centuries before Pythagoras was born.

[3] The National Security Agency (NSA) is the arm of the United States government charged with data collection, code making, and code breaking. The NSA, with a budget larger than that of the CIA, is the single largest employer of mathematicians in the world.

[4] *A Mathematician's Apology*, §28, G.H. Hardy, Camb. Univ. Press, 1940.

numbers). There are Fermat equations and Pell equations, Pythagorean triples and elliptic curves, Fibonacci's rabbits, unbreakable codes, and much, much more. You will meet all these creatures, and many others, as we journey through the Theory of Numbers.

Guide for the Instructor

This book is designed to be used as a text for a one-semester or full-year course in undergraduate number theory or for an independent study or reading course. It contains approximately two semesters' worth of material, so the instructor of a one-semester course will have some flexibility in the choice of topics. The first 11 chapters are basic, and probably most instructors will want to continue through the RSA cryptosystem in Chapter 18, since in my experience this is one of the students' favorite topics.

There are now many ways to proceed. Here are a few possibilities that seem to fit comfortably into one semester, but feel free to slice-and-dice the later chapters to fit your own tastes.

Chapters 20–32. Primitive roots, quadratic reciprocity, sums of squares, Pell's equation, and Diophantine approximation. (Add Chapters 39 and 40 on continued fractions if time permits.)

Chapters 28–32 & 43–48. Fermat's equation for exponent 4, Pell's equation, Diophantine approximation, elliptic curves, and Fermat's Last Theorem.

Chapters 29–37 & 39–40. Pell's equation, Diophantine approximation, Gaussian integers, transcendental numbers, binomial coefficients, linear recurrences, and continued fractions.

Chapters 19–25 & 36–38. Primality testing, primitive roots, quadratic reciprocity, binomial coefficients, linear recurrences, big-Oh notation. (This syllabus is designed in particular for students planning further work in computer science or cryptography.)

In any case, a good final project is to have the students read a few of the omitted chapters and do the exercises.

Most of the nonnumerical nonprogramming exercises in this book are designed to foster discussion and experimentation. They do not necessarily have "correct" or "complete" answers. Many students will find this extremely disconcerting at first, so it must be stressed repeatedly. You can make your students feel more at ease by prefacing such questions with the phrase "Tell me as much as you can about ...." Tell your students that accumulating data and solving special cases are not merely acceptable, but encouraged. On the other hand, tell them that there is no such thing as a complete solution, since the solution of a good problem always raises additional questions. So if they can fully answer the specific question given in the text, their next task is to look for generalizations and for limitations on the validity of their solution.

Aside from a few clearly marked exercises, calculus is required only in two late chapters (Big-Oh notation in Chapter 38 and Generating Functions in Chapter 41). If the class has not taken calculus, these chapters may be omitted with no harm to the flow of the material.

Number theory is not easy, so there's no point in trying to convince the students that it is. Instead, this book will show your students that they are capable of mastering a difficult subject and experiencing the intense satisfaction of intellectual discovery. Your reward as the instructor is to bask in the glow of their endeavors.

Computers, Number Theory, and This Book

At this point I would like to say a few words about the use of computers in conjunction with this book. I neither expect nor desire that the reader make use of a high-level computer package such as Maple, Mathematica, PARI, or Derive, and most exercises (except as otherwised indicated) can be done with a simple pocket calculator. To take a concrete example, studying greatest common divisors (Chapter 5) by typing `GCD[M,N]` into a computer is akin to studying electronics by turning on a television set. Admittedly, computers allow one to do examples with large numbers, and you will find such computer-generated examples scattered through the text, but our ultimate goal is always to understand concepts and relationships. So if I were forced to make a firm ruling, yea or nay, regarding computers, I would undoubtedly forbid their use.

However, just as with any good rule, certain exceptions will be admitted. First, one of the best ways to understand a subject is to explain it to someone else; so if you know a little bit of how to write computer programs, you will find it extremely enlightening to explain to a computer how to perform the algorithms described in this book. In other words, don't rely on a canned computer package; do the programming yourself. Good candidates for such treatment are the Euclidean algorithm (Chapters 5–6) the RSA cryptosystem (Chapters 16–18), quadratic reciprocity (Chapter 25), writing numbers as sums of two squares (Chapters 26–27), primality testing (Chapter 19), and generating rational points on elliptic curves (Chapter 43).

The second exception to the "no computer rule" is generation of data. Discovery in number theory is usually based on experimentation, which may involve examining reams of data to try to distinguish underlying patterns. Computers are well suited to generating such data and also sometimes to assist in searching for patterns, and I have no objection to their being used for these purposes.

I have included a number of computer exercises and computer projects to encourage you to use computers properly as tools to help understand and investigate the theory of numbers. Some of these exercises can be implemented on a small computer (or even a programmable calculator), while others require more sophisticated machines and/or programming languages. Exercises and projects requiring a computer are marked by the symbol 💻.

For many of the projects I have not given a precise formulation, since part of the project is to decide exactly what the user should input and exactly what form the output should take. Note that a good computer program must include all the following features:

- Clearly written documentation explaining what the program does, how to use it, what quantities it takes as input, and what quantities it returns as output.
- Extensive internal comments explaining how the program works.
- Complete error handling with informative error messages. For example, if $a = b = 0$, then the $\gcd(a, b)$ routine should return the error message "`gcd(0,0) is undefined`" instead of going into an infinite loop or returning a "division by zero" error.

As you write your own programs, try to make them user friendly and as versatile as possible, since ultimately you will want to link the pieces together to form your own package of number theoretic routines.

The moral is that computers are useful as a tool for experimentation and that you can learn a lot by teaching a computer how to perform number theoretic calculations, but when you are first learning a subject, prepackaged computer programs merely provide a crutch that prevent you from learning to walk on your own.

Chapter 1

What Is Number Theory?

Number theory is the study of the set of positive whole numbers

$$1, 2, 3, 4, 5, 6, 7, \ldots,$$

which are often called the set of *natural numbers*. We will especially want to study the *relationships* between different sorts of numbers. Since ancient times, people have separated the natural numbers into a variety of different types. Here are some familiar and not-so-familiar examples:

odd	$1, 3, 5, 7, 9, 11, \ldots$
even	$2, 4, 6, 8, 10, \ldots$
square	$1, 4, 9, 16, 25, 36, \ldots$
cube	$1, 8, 27, 64, 125, \ldots$
prime	$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$
composite	$4, 6, 8, 9, 10, 12, 14, 15, 16, \ldots$
1 (modulo 4)	$1, 5, 9, 13, 17, 21, 25, \ldots$
3 (modulo 4)	$3, 7, 11, 15, 19, 23, 27, \ldots$
triangular	$1, 3, 6, 10, 15, 21, \ldots$
perfect	$6, 28, 496, \ldots$
Fibonacci	$1, 1, 2, 3, 5, 8, 13, 21, \ldots$

Many of these types of numbers are undoubtedly already known to you. Others, such as the "modulo 4" numbers, may not be familiar. A number is said to be congruent to 1 (modulo 4) if it leaves a remainder of 1 when divided by 4, and similarly for the 3 (modulo 4) numbers. A number is called triangular if that number of pebbles can be arranged in a triangle, with one pebble at the top, two pebbles in the next row, and so on. The Fibonacci numbers are created by starting with 1 and 1. Then, to get the next number in the list, just add the previous two. Finally, a number is perfect if the sum of all its divisors, other than itself, adds back up to the original number. Thus, the numbers dividing 6 are 1, 2, and 3, and $1 + 2 + 3 = 6$. Similarly, the divisors of 28 are 1, 2, 4, 7, and 14, and

$$1 + 2 + 4 + 7 + 14 = 28.$$

We will encounter all these types of numbers, and many others, in our excursion through the Theory of Numbers.

Some Typical Number Theoretic Questions

The main goal of number theory is to discover interesting and unexpected relationships between different sorts of numbers and to prove that these relationships are true. In this section we will describe a few typical number theoretic problems, some of which we will eventually solve, some of which have known solutions too difficult for us to include, and some of which remain unsolved to this day.

Sums of Squares I. Can the sum of two squares be a square? The answer is clearly "YES"; for example $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$. These are examples of *Pythagorean triples*. We will describe all Pythagorean triples in Chapter 2.

Sums of Higher Powers. Can the sum of two cubes be a cube? Can the sum of two fourth powers be a fourth power? In general, can the sum of two n^{th} powers be an n^{th} power? The answer is "NO." This famous problem, called *Fermat's Last Theorem*, was first posed by Pierre de Fermat in the seventeenth century, but was not completely solved until 1994 by Andrew Wiles. Wiles's proof uses sophisticated mathematical techniques that we will not be able to describe in detail, but in Chapter 28 we will prove that no fourth power is a sum of two fourth powers, and in Chapter 48 we will sketch some of the ideas that go into Wiles's proof.

Infinitude of Primes. A *prime number* is a number p whose only factors are 1 and p.

- Are there infinitely many prime numbers?
- Are there infinitely many primes that are 1 modulo 4 numbers?
- Are there infinitely many primes that are 3 modulo 4 numbers?

The answer to all these questions is "YES." We will prove these facts in Chapters 12 and 24 and also discuss a much more general result proved by Lejeune Dirichlet in 1837.

Sums of Squares II. Which numbers are sums of two squares? It often turns out that questions of this sort are easier to answer first for primes, so we ask which (odd) prime numbers are a sum of two squares. For example,

$$\begin{array}{rrrr} 3 = \text{NO}, & 5 = 1^2 + 2^2, & 7 = \text{NO}, & 11 = \text{NO}, \\ 13 = 2^2 + 3^2, & 17 = 1^2 + 4^2, & 19 = \text{NO}, & 23 = \text{NO}, \\ 29 = 2^2 + 5^2, & 31 = \text{NO}, & 37 = 1^2 + 6^2, & \ldots \end{array}$$

Do you see a pattern? Possibly not, since this is only a short list, but a longer list leads to the conjecture that p is a sum of two squares if it is congruent to 1 (modulo 4). In other words, p is a sum of two squares if it leaves a remainder of 1 when divided by 4, and it is not a sum of two squares if it leaves a remainder of 3. We will prove that this is true in Chapter 26.

Number Shapes. The square numbers are the numbers 1, 4, 9, 16, ... that can be arranged in the shape of a square. The triangular numbers are the numbers 1, 3, 6, 10, ... that can be arranged in the shape of a triangle. The first few triangular and square numbers are illustrated in Figure 1.1.

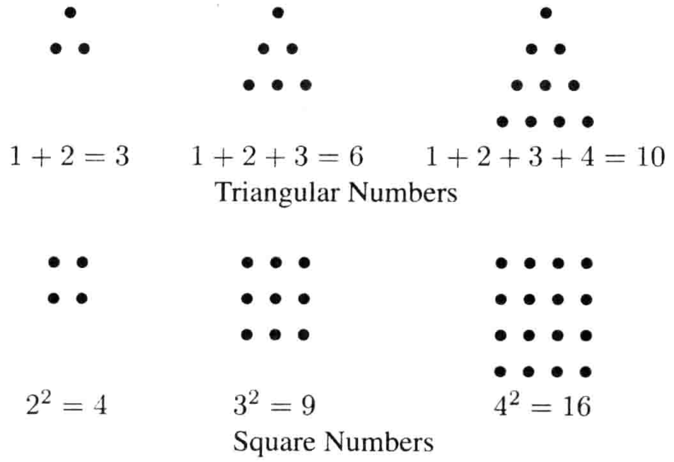


Figure 1.1: Numbers that form interesting shapes

A natural question to ask is whether there are any triangular numbers that are also square numbers (other than 1). The answer is "YES," the smallest example being

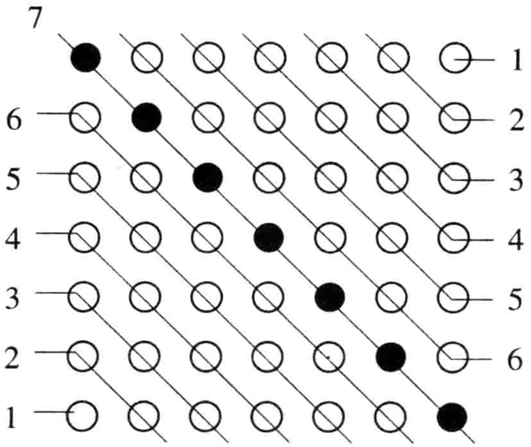
$$36 = 6^2 = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8.$$

So we might ask whether there are more examples and, if so, are there infinitely many? To search for examples, the following formula is helpful:

$$1 + 2 + 3 + \cdots + (n-1) + n = \frac{n(n+1)}{2}.$$

> There is an amusing anecdote associated with this formula. One day when the young Carl Friedrich Gauss (1777–1855) was in grade school, his teacher became so incensed with the class that he set them the task of adding up all the numbers from 1 to 100. As Gauss's classmates dutifully began to add, Gauss walked up to the teacher and presented the answer, 5050. The story goes that the teacher was neither impressed nor amused, but there's no record of what the next make-work assignment was!

There is an easy geometric way to verify Gauss's formula, which may be the way he discovered it himself. The idea is to take two triangles consisting of $1 + 2 + \cdots + n$ pebbles and fit them together with one additional diagonal of $n + 1$ pebbles. Figure 1.2 illustrates this idea for $n = 6$.



$$(1+2+3+4+5+6) + 7 + (6+5+4+3+2+1) = 7^2$$

Figure 1.2: The sum of the first n integers

In the figure, we have marked the extra $n + 1 = 7$ pebbles on the diagonal with black dots. The resulting square has sides consisting of $n + 1$ pebbles, so in mathematical terms we obtain the formula

$$\begin{array}{ccccc} 2(1+2+3+\cdots+n) & + & (n+1) & = & (n+1)^2, \\ \text{two triangles} & + & \text{diagonal} & = & \text{square.} \end{array}$$