What Is Number Theory?

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 we will prove that no fourth power is a sum of two fourth powers, and 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."

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,

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

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.

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.

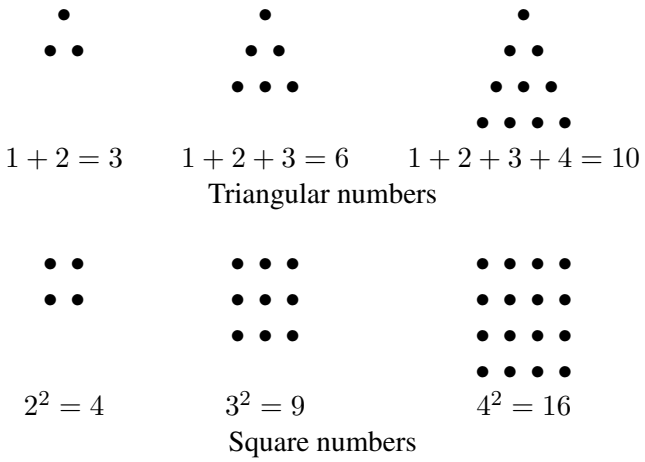


Figure 1: Numbers That Form Interesting Shapes

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

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

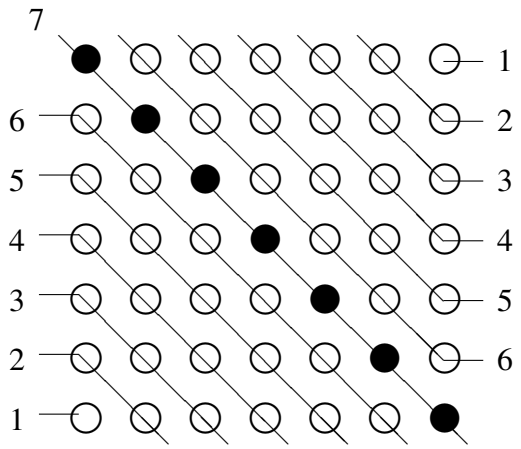
So we might ask whether there are more examples and, if so, are there in-

finitely 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 2 illustrates this idea for $n = 6$.



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

Figure 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

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

Now we can subtract $n+1$ from each side and divide by 2 to get Gauss's formula.

Twin Primes. In the list of primes it is sometimes true that consecutive odd numbers are both prime. We have boxed these *twin primes* in the following list of primes less than 100:

$$\boxed{3},\boxed{5},\boxed{7},\quad \boxed{11},\boxed{13},\quad \boxed{17},\boxed{19},\quad 23,\quad \boxed{29},\boxed{31},\quad 37$$
$$\boxed{41},\boxed{43},\quad 47, 53,\quad \boxed{59},\boxed{61},\quad 67,\quad \boxed{71},\boxed{73},\quad 79, 83, 89, 97.$$

Are there infinitely many twin primes? That is, are there infinitely many prime numbers p such that $p+2$ is also a prime? At present, no one knows the answer to this question.

Primes of the Form N^2+1. If we list the numbers of the form N^2+1 taking $N = 1, 2, 3, \ldots$, we find that some of them are prime. Of course, if N is odd, then N^2+1 is even, so it won't be prime unless $N = 1$. So it's really only interesting to take even values of N. We've highlighted the primes in the following list:

$$2^2+1 = \mathbf{5} \qquad 4^2+1 = \mathbf{17} \qquad 6^2+1 = \mathbf{37} \qquad 8^2+1 = 65 = 5\cdot 13$$
$$10^2+1 = \mathbf{101} \qquad 12^2+1 = 145 = 5\cdot 29 \qquad 14^2+1 = \mathbf{197}$$
$$16^2+1 = \mathbf{257} \qquad 18^2+1 = 325 = 5^2\cdot 13 \qquad 20^2+1 = \mathbf{401}.$$

It looks like there are quite a few prime values, but if you take larger values of N you will find that they become much rarer. So we ask whether there are infinitely many primes of the form N^2+1. Again, no one presently knows the answer to this question.

We have now seen some of the types of questions that are studied in the Theory of Numbers. How does one attempt to answer these questions? The answer is that Number Theory is partly experimental and partly theoretical. The experimental part normally comes first; it leads to questions and suggests ways to answer them. The theoretical part follows; in this part one tries to devise an argument that gives a conclusive answer to the questions. In summary, here are the steps to follow:

1. Accumulate data, usually numerical, but sometimes more abstract in nature.
2. Examine the data and try to find patterns and relationships.
3. Formulate conjectures (i.e., guesses) that explain the patterns and relationships. These are frequently given by formulas.

4. Test your conjectures by collecting additional data and checking whether the new information fits your conjectures.
5. Devise an argument (i.e., a proof) that your conjectures are correct.

All five steps are important in number theory and in mathematics. More generally, the scientific method always involves at least the first four steps. Be wary of any purported "scientist" who claims to have "proved" something using only the first three. Given any collection of data, it's generally not too difficult to devise numerous explanations. The true test of a scientific theory is its ability to predict the outcome of experiments that have not yet taken place. In other words, a scientific theory only becomes plausible when it has been tested against new data. This is true of all real science. In mathematics one requires the further step of a proof, that is, a logical sequence of assertions, starting from known facts and ending at the desired statement.

Exercises

1. The first two numbers that are both squares and triangles are 1 and 36. Find the next one and, if possible, the one after that. Can you figure out an efficient way to find triangular–square numbers? Do you think that there are infinitely many?

2. Try adding up the first few odd numbers and see if the numbers you get satisfy some sort of pattern. Once you find the pattern, express it as a formula. Give a geometric verification that your formula is correct.

3. The consecutive odd numbers 3, 5, and 7 are all primes. Are there infinitely many such "prime triplets"? That is, are there infinitely many prime numbers p such that $p+2$ and $p+4$ are also primes?

4. It is generally believed that infinitely many primes have the form N^2+1, although no one knows for sure.

(a) Do you think that there are infinitely many primes of the form N^2-1?
(b) Do you think that there are infinitely many primes of the form N^2-2?
(c) How about of the form N^2-3? How about N^2-4?
(d) Which values of a do you think give infinitely many primes of the form N^2-a?

5. The following two lines indicate another way to derive the formula for the sum of the first n integers by rearranging the terms in the sum. Fill in the details.

$$\begin{aligned} 1+2+3+\cdots+n &= (1+n)+(2+(n-1))+(3+(n-2))+\cdots \\ &= (1+n)+(1+n)+(1+n)+\cdots . \end{aligned}$$

How many copies of $n+1$ are in there in the second line? You may need to consider the cases of odd n and even n separately. If that's not clear, first try writing it out explicitly for $n=6$ and $n=7$.

6. For each of the following statements, fill in the blank with an easy-to-check criterion:

(a) M is a triangular number if and only if _____ is an odd square.

(b) N is an odd square if and only if _____ is a triangular number.

(c) Prove that your criteria in (a) and (b) are correct.