PART I

The Riemann Hypothesis

1 Thoughts About Numbers: Ancient, Medieval, and Modern

If we are to believe the ancient Greek philosopher Aristotle, the early Pythagoreans thought that the principles governing Number are "the principles of all things," the concept of Number being more basic than *earth, air, fire, or water*, which were according to ancient tradition the four building blocks of matter. To think about Number is to get close to the architecture of "what is."

So, how far along are we in our thoughts about numbers?

Figure 1.1. René Descartes (1596–1650) © RMN-Grand Palais / Art Resource, NY

The French philosopher and mathematician René Descartes, almost four centuries ago, expressed the hope that there soon would be "almost nothing more to discover in geometry." Contemporary physicists dream of a final

Figure 1.2. Jean de Bosschere, "Don Quixote and his Dulcinea del Toboso," from The History of Don Quixote De La Mancha, by Miguel De Cervantes. Trans. Thomas Shelton. Constable and Company, New York, 1922

theory.[1] But despite its venerability and its great power and beauty, the pure mathematics of numbers may still be in the infancy of its development, with depths to be explored as endless as the human soul, and *never* a final theory.

Numbers are obstreperous things. Don Quixote encountered this when he requested that the "bachelor" compose a poem to his lady Dulcinea del Toboso, the first letters of each line spelling out her name. The "bachelor" found[2]

> "a great difficulty in their composition because the number of letters in her name was 17, and if he made four Castilian stanzas of four octosyllabic lines each, there would be one letter too many, and if he made the stanzas of five octosyllabic lines each, the ones called *décimas* or *redondillas,* there would be three letters too few…"

"It must fit in, however you do it," pleaded Quixote, not willing to grant the imperviousness of the number 17 to division.

Seventeen is indeed a prime number: there is no way of factoring it as the product of smaller numbers, and this accounts – people tell us – for its occurrence in some phenomena of nature, as when the seventeen-year cicadas all emerged to celebrate a "reunion" of some sort in our fields and valleys.

Prime numbers, despite their *primary* position in our modern understanding of numbers, were not specifically doted over in the ancient literature before Euclid, at least not in the literature that has been preserved. Primes are mentioned as a class of numbers in the writings of Philolaus (a predecessor of Plato);

[1] See Weinberg's book *Dreams of a Final Theory: The Search for the Fundamental Laws of Nature*, by Steven Weinberg (New York: Pantheon Books, 1992).
[2] See Chapter IV of the Second Part of the *Ingenious Gentleman Don Quixote of La Mancha.*

Figure 1.3. Cicadas emerge every 17 years. Photo by Bob Peterson

they are not mentioned specifically in the Platonic dialogues, which is surprising given the intense interest Plato had in mathematical developments; and they make an occasional appearance in the writings of Aristotle, which is not surprising, given Aristotle's emphasis on the distinction between the *composite* and the *incomposite*. "The incomposite is prior to the composite," writes Aristotle in Book 13 of the Metaphysics.

Prime numbers do occur, in earnest, in Euclid's *Elements*!

There is an extraordinary wealth of established truths about whole numbers; these truths provoke sheer awe for the beautiful complexity of prime numbers. But each of the important new discoveries we make gives rise to a further richness of questions, educated guesses, heuristics, expectations, and unsolved problems.

2 What are Prime Numbers?

Primes as atoms. To begin from the beginning, think of the operation of multiplication as a bond that ties numbers together: the equation $2 \times 3 = 6$ invites us to imagine the number 6 as (a molecule, if you wish) built out of its smaller constituents 2 and 3. Reversing the procedure, if we start with a whole number, say 6 again, we may try to factor it (that is, express it as a product of smaller whole numbers) and, of course, we would eventually, if not immediately, come up with $6 = 2 \times 3$ and discover that 2 and 3 factor no further; the numbers 2 and 3, then, are the indecomposable entities (atoms, if you wish) that comprise our number.

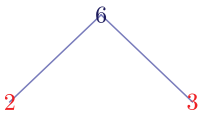

Figure 2.1. The number $6 = 2 \times 3$

By definition, a **prime number** (colloquially, *a prime*) is a whole number, bigger than 1, that cannot be factored into a product of two smaller whole numbers. So, 2 and 3 are the first two prime numbers. The next number along the line, 4, is not prime, for $4 = 2 \times 2$; the number after that, 5, is. Primes are, multiplicatively speaking, the building blocks from which all numbers can be made. A fundamental theorem of arithmetic tells us that any number (bigger than 1) can be factored as a product of primes, and the factorization is *unique* except for rearranging the order of the primes.

For example, if you try to factor 12 as a product of two smaller numbers – ignoring the order of the factors – there are two ways to begin to do this:

$$12 = 2 \times 6 \qquad \text{and} \qquad 12 = 3 \times 4$$

But neither of these ways is a full factorization of 12, for both 6 and 4 are not prime, so can be themselves factored, and in each case after changing the ordering of the factors we arrive at:

$$12 = 2 \times 2 \times 3.$$

If you try to factor the number 300, there are many ways to begin:

$$300 = 30 \times 10 \qquad \text{or} \qquad 300 = 6 \times 50$$

and there are various other starting possibilities. But if you continue the factorization ("climbing down" any one of the possible "factoring trees") to the bottom, where every factor is a prime number as in Figure 2.2, you always end up with the same collection of prime numbers[1]:

$$300 = 2^2 \times 3 \times 5^2.$$

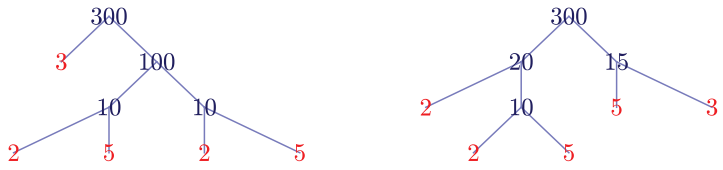

Figure 2.2. Factor trees that illustrate the factorization of 300 as a product of primes.

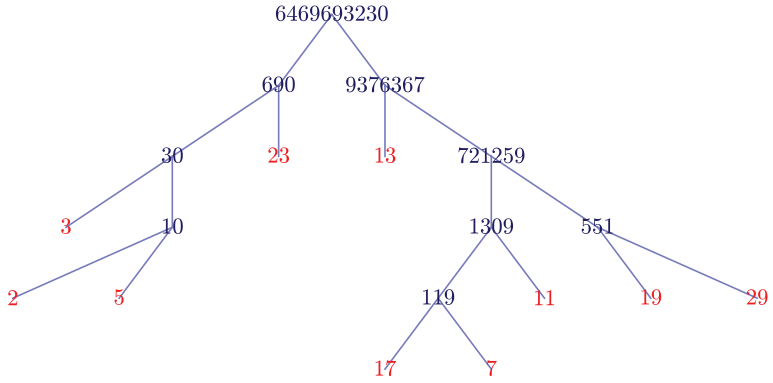

Figure 2.3. Factorization tree for the product of the primes up to 29.

The Riemann Hypothesis probes the question: how intimately can we know prime numbers, those *atoms* of multiplication? Prime numbers are an

[1] See Section 1.1 of Stein's *Elementary Number Theory: Primes, Congruences, and Secrets* (2008) at `http://wstein.org/ent/` for a proof of the "fundamental theorem of arithmetic", which asserts that every positive whole number factors uniquely as a product of primes.

important part of our daily lives. For example, often when we visit a website and purchase something online, prime numbers having hundreds of decimal digits are used to keep our bank transactions private. This ubiquitous use to which giant primes are put depends upon a very simple principle: it is much easier to multiply numbers together than to factor them. If you had to factor, say, the number 391 you might scratch your head for a few minutes before discovering that 391 is 17×23. But if you had to multiply 17 by 23 you would do it straightaway. Offer two primes, say, P and Q each with a few hundred digits, to your computing machine and ask it to multiply them together: you will get their product $N = P \times Q$ with its hundreds of digits in about a microsecond. But present that number N to any current desktop computer, and ask it to factor N, and the computer will (almost certainly) fail to do the task. See [1] and [2].

The safety of much encryption depends upon this "guaranteed" failure![2]

If we were latter-day number-phenomenologists we might revel in the discovery and proof that

$$p = 2^{43,112,609} - 1 = 3164702693\ldots\ldots\text{(millions of digits)}\ldots\ldots 6697152511$$

is a prime number, this number having 12,978,189 digits! This prime, which was discovered on August 23, 2008 by the GIMPS project,[3] is the first prime ever found with more than ten million digits, though it is not the largest prime currently known.

Now $2^{43,112,609} - 1$ is quite a hefty number! Suppose someone came up to you saying "surely $p = 2^{43,112,609} - 1$ is the largest prime number!" (which it is not). How might you convince that person that he or she is wrong without explicitly exhibiting a larger prime? [3]

Here is a neat – and, we hope, convincing – strategy to show there are prime numbers larger than $p = 2^{43,112,609} - 1$. Imagine forming the following humongous number: let M be the product of all prime numbers up to and including $p = 2^{43,11,2609} - 1$. Now go one further than M by taking the next number $N = M + 1$.

OK, even though this number N is wildly large, it is either a prime number itself – which would mean that there would indeed be a prime number larger than $p = 2^{43,112,609} - 1$, namely N; or in any event it is surely divisible by some prime number, call it P.

Here, now, is a way of seeing that this P is bigger than p: Since every prime number smaller than or equal to p divides M, these prime numbers cannot divide $N = M + 1$ (since they divide M evenly, if you tried to divide $N = M + 1$ by any of them you would get a remainder of 1). So, since P does divide N it must not be any of the smaller prime numbers: P is therefore a prime number bigger than $p = 2^{43,112,609} - 1$.

[2] Nobody has ever published a *proof* that there is no fast way to factor integers. This is an article of "faith" among some cryptographers.

[3] The GIMPS project website is `http://www.mersenne.org/`.

This strategy, by the way, is not very new: it is, in fact, well over two thousand years old, since it already occurred in Euclid's *Elements*. The Greeks did know that there are infinitely many prime numbers and they showed it via the same method as we showed that our $p = 2^{43,112,609} - 1$ is not the largest prime number.

Here is the argument again, given very succinctly: Given primes $p_1, \ldots, p_m$, let $n = p_1 p_2 \cdots p_m + 1$. Then n is divisible by some prime not equal to any p_i, so there are more than m primes.

You can think of this strategy as a simple game that you can play. Start with the bag of prime numbers that contains just the two primes 2 and 3. Now each "move" of the game consists of multiplying together all the primes you have in your bag to get a number M, then adding 1 to M to get the larger number $N = M + 1$, then factoring N into prime number factors, and then including all those new prime numbers in your bag. Euclid's proof gives us that we will – with each move of this game – be finding more prime numbers: the contents of the bag will increase. After, say, a million moves our bag will be guaranteed to contain more than a million prime numbers.

For example, starting the game with your bag containing only one prime number 2, here is how your bag grows with successive moves of the game:

{2}
{2, 3}
{2, 3, 7}
{2, 3, 7, 43}
{2, 3, 7, 43, 13, 139}
{2, 3, 7, 43, 13, 139, 3263443}
{2, 3, 7, 43, 13, 139, 3263443, 547, 607, 1033, 31051}
{2, 3, 7, 43, 13, 139, 3263443, 547, 607, 1033, 31051, 29881, 67003, 9119521, 6212157481}
etc.[4]

Though there are infinitely many primes, explicitly finding large primes is a major challenge. In the 1990s, the Electronic Frontier Foundation `http://www.eff.org/awards/coop` offered a $100,000 cash reward to the first group to find a prime with at least 10,000,000 decimal digits (the group that found the record prime p above won this prize[5]), and offers another $150,000 cash prize to the first group to find a prime with at least 100,000,000 decimal digits.

The number $p = 2^{43,112,609} - 1$ was for a time the largest prime known, where by "know" we mean that we know it so explicitly that we can *compute* things

[4] The sequence of prime numbers we find by this procedure is discussed in more detail with references in the Online Encyclopedia of Integer Sequences `http://oeis.org/A126263`.

[5] See `http://www.eff.org/press/archives/2009/10/14-0`. Also the 46th Mersenne prime was declared by *Time Magazine* to be one of the top 50 best "inventions" of 2008: `http://www.time.com/time/specials/packages/article/0,28804,1852747_1854195_1854157,00.html`.

about it. For example, the last two digits of p are both 1 and the sum of the digits of p is 58,416,637. Of course p is not the largest prime number since there are infinitely many primes, e.g., the next prime q after p is a prime. But there is no known way to efficiently compute anything interesting about q. For example, what is the last digit of q in its decimal expansion?