

Number Theory: From Greek to Modern Times

Justin Lai and Pete Cartwright

History of Mathematics

5/5/05

Number theory, the study of the integers and the properties of the integers, is one of the older branches of mathematics, with origins reaching back as far as the ancient Greeks and continuing into modern times. The ancient Greeks explored topics like divisibility, perfect and amiable numbers, and the identification and properties of prime numbers. In many cases, the Greeks tended to treat numbers with a near-mystical reverence, and attributed a great deal of importance and meaning to their findings. After the passing of the Greek era of mathematics, the popularity of number theory faded and nearly disappeared, until a resurgence in the 18th century, led by brilliant mind of Fermat. Fermat was the main architect for advancement of number theory, proving several theorems and at the same time leaving the subject open to scrutiny for further investigation by other great mathematicians such as Euler and Gauss. Although the subject was still considered one of the "purest" and least practical areas of math, number theory eventually found its way into modern, practical applications with its integration into cryptography.

There were many Greek mathematicians that dealt with number theory, but the work of Euclid stands out over the rest. Three of the ten books of his major work, *Elements*, are devoted to number theory. He did a great deal of work in the field, and introduced many important ideas. One such important idea that is still in use today is a brilliant method for finding the greatest common divisor (or GCD) of two numbers, appropriately called the Euclidean algorithm. It relies on the poorly named Division Algorithm (actually not an algorithm at all), which states that given any two integers n , m , with $n > m$, there exist integers q , r such that $n = q(m) + r$, with $m \geq r \geq 0$. The Euclidean algorithm then goes as follows (using q_i and r_i to represent the i^{th} quotient and remainder, respectively): Begin with $n = q_1(m) + r_1$. If $r_1 \neq 0$, then take $m = q_2(r_1) + r_2$. If $r_2 \neq 0$, then take $r_1 = q_3(r_2) + r_3$. Continue like so, until $r_n = 0$. Then r_{n-1} is the GCD of n and m . For example, let $m = 2235$ and $n = 8769$. Then, following the algorithm, we have:

$$\begin{aligned} 8769 &= 3(2235) + 2064 & (q_1 = 3, r_1 = 2064) \\ 2235 &= 1(2064) + 171 & (q_2 = 1, r_2 = 171) \\ 2064 &= 12(171) + 12 & (q_3 = 12, r_3 = 12) \\ 171 &= 14(12) + 3 & (q_4 = 14, r_4 = 3) \\ 12 &= 4(3) + 0 & (q_5 = 4, r_5 = 0) \end{aligned}$$

Since $r_5 = 0$, we know $r_4 = 3$ is the GCD of 2235 and 8769. This algorithm is useful in proving numbers composite (not prime), since if it shares any non-trivial (not one or itself) divisor with another number, it is clearly not prime.

Another highly influential Greek that dealt with number theory was Diophantus. He wrote a book, *Arithmetica*, that, though very different from Euclid's *Elements*, has played a major role in the developing history of number theory. His book was a collection of problems that have been rephrased in modern terms as equations in which only integer solutions are allowed (Kleiner). Catalan's famous conjecture that 8 and 9 are the only consecutive powers (2^3 and 3^2 , respectively) other than 0 and 1 is a Diophantine equation. The conjecture is saying that $3^2 - 2^3 = 1$ is the only solution to the equation $x^a - y^b = \pm 1$ (Weisstein). Diophantus was a major influence on the work of Fermat, and

many of his theorems, including his famous “Last Theorem” were written as comments in the margins of his personal copy of *Arithmetica*. Fermat's son published a copy of *Arithmetica* with his father's notes included after his death.

Many of the developments in ancient Greek number theory may seem more like interesting quirks than useful facts, but the Greeks of the time ascribed a great deal of importance to them. One such development was the concept of perfect numbers. A positive integer n is a perfect number if it is equal to the sum of all of its proper divisors (all positive factors of n , excluding n). 6, for example, is a perfect number, since its proper divisors are 1, 2, and 3, and $1+2+3=6$. The Greek mathematician Nicomachus, who was the first person to write a text that dealt with arithmetic separately from geometry, had very strong feelings about the inherent moral rightness of perfect numbers. He says in his book *Introduction to Arithmetic*,

“In the case of the too much, is produced excess, superfluity, exaggerations and abuse; in the case of too little, is produced wanting, defaults, privations and insufficiencies. And in the case of those that are found between the too much and the too little, that is in equality, is produced virtue, just measure, propriety, beauty and things of that sort - of which the most exemplary form is that type of number which is called perfect.”

He goes on to compare superabundant numbers (numbers that are smaller than the sum of their proper divisors) and deficient numbers (numbers that are larger than the sum of their proper divisors) to animals with too many or too few body parts. (O'Connor). From a modern viewpoint, it seems fairly strange that Nicomachus felt this strongly about perfect numbers, because when he lived, only four (6, 28, 496, and 8128) were known to exist.

Despite their great deal of attention given to types of integers that Peter Barlow called “merely curious, without being useful”, there was also a great deal of important work done on the concept of primes, a genuinely useful area of number theory. The Greeks developed a great deal of information about primes. They knew the theorem now called the Fundamental Theorem of Arithmetic, that for any positive integer n , there is a unique set of primes $\{p_1, p_2, \dots, p_t\}$ such that $n = p_1 p_2 \dots p_t$. Euclid himself proved in *Elements* that there are an infinite number of primes, with a remarkable proof that goes as follows: Take a finite sequence of consecutive primes $2, 3, \dots, p$. Then let $N = (2 \cdot 3 \cdot 5 \cdot \dots \cdot p) + 1$. So this N is either a new prime larger than any in the sequence or a composite number with a prime factor greater than p . To show this, assume that N is a composite number and has no prime factors greater than p . Then one of its prime factors must be one of the primes in the sequence $2, 3, \dots, p$. So then this prime divides the product $2 \cdot 3 \cdot 5 \cdot \dots \cdot p$, and N . Since it divides both N and $2 \cdot 3 \cdot 5 \cdot \dots \cdot p$, it also divides their difference, $N - 2 \cdot 3 \cdot 5 \cdot \dots \cdot p = 1$. But this contradicts the fact that the prime factor of N was in the sequence of primes. Thus, either N is a prime larger than any in the sequence or has a prime factor larger than any in the sequence. Either way, Euclid proved that there is a prime larger than those in any consecutive sequence of primes, so there must be an infinite amount. ([Weisstein](#)) The infiniteness of primes has proven to be an invaluable

tool in cryptography. The ability to utilize arbitrarily large primes is what forms the backbone of nearly all modern encryption standards, including the encryption protecting online transactions and banking.

After the Greeks, the Western world saw a steep decline in the study of number theory. Very little work was done on the subject until Fermat picked it back up many centuries later. However, some very important results were emerging in the Eastern World, including the Chinese Remainder Theorem. The idea behind this theorem is exhibited this a problem by Sun Tsu Suan-Ching in the 4th century CE : “There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?” (Bogomolny). This problem is generalized as a system of congruences to x modulo different numbers : $x \equiv k_1 \pmod{n_1}$, $x \equiv k_2 \pmod{n_2}$, ..., $x \equiv k_s \pmod{n_s}$. The theorem states there there is then a unique solution $x \pmod{n_1 * n_2 * ... * n_s}$. Reportedly, this theorem was used by Chinese generals to count large armies quickly without having to count each individual soldier. They would order the army to line up in rows of certain length and count the “leftover” ones, then have them line up in rows of a different length, and then repeat. This would give them the system of congruences they needed to solve for the size of the army. In modern times, this theorem is utilized to set up systems of secret-sharing, where the “key” to a secret is spread among a certain number of people, and it cannot be found without the participation of some amount k of them. After this development, there is not much to consider until the rise of Fermat's studies. It would take a millennium for any more advancement to take place in number theory until Fermat re-energized the study by picking up Diophantus's *Arithmetica*.

Pierre de Fermat and his contributions to Number Theory

Pierre de Fermat is widely considered to be the father of number theory. He was born the son of a wealthy leather merchant and he was the second consul of Beaumont-de-Lomagne in August 17th 1601. In the second half of the 1620's Fermat went to the University of Orléans where he studied and received his degree in civil law. Although Fermat was a lawyer by profession, he quickly attained the reputation as one of the leading mathematicians in the world. However, a lot of his work was not published due to the fact that Fermat never really wanted to put his work into a rigorous, polished form(O'Connor). Nevertheless, Fermat had a passion for number theory. His interest in number theory came about in the 1630's when Bachet translated the work of the Greek mathematician Diophantus, *Arithmetica* from Latin. In addition to *Arithmetica* was Euclid's *Elements*, which was another available source for Fermat to investigate his interest. While Euclid's *Elements* provided a foundation for Fermat's work in number theory, particularly the concepts of divisibility, prime and composite numbers, and the greatest common divisor, it was Diophantus' *Arithmetica* that would provide inspiration and spur a lot of Fermat's work. In fact, Pierre de Fermat would jot down notes in the margins of his personal copy of *Arithmetica*, writing down only enough to convince himself of the solution (Rees). His most famous "note in the margin" was written in 1637:

"It is impossible for a cube to be written as the sum of two cubes , or a fourth power to be written as the sum of two fourth powers, or, in general,

for any number which is a power greater than the second to be written as a sum of two like powers. I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain." (Weisstein)

This problem would come to be known as Fermat's Last Theorem. Fermat himself never told anyone about his proof and it is doubtful that he ever rigorously proved it. Nevertheless, Fermat's son Samuel published these notes in 1670 in the publication *Diophantus' Arithmetica Containing Observations by P. de Fermat*, five years after his father's death.

Although Fermat is most well known for his self-titled "Last Theorem", it would be his "Little Theorem" that would further fuel the evolution of number theory. The statement first appeared in a letter dated October 18th, 1640 that Fermat wrote to Frenicle de Bessy. Fermat's Little Theorem states "given any prime p and any geometric progression $1, a, a^2, \dots, a^{p-1}$ must divide some number $a^n - 1$ for which n divides $p-1$; if then N is any multiple of the smallest n for which this is so, p also divides $a^N - 1$ " (Kleiner). In other words, if p is prime and a is a positive integer such that p does not divide a , then $a^{p-1} \equiv 1 \pmod{p}$. Fermat is believed to have arrived at this result through his study of the perfect numbers: numbers that are the sum of all their positive divisors. Fermat's Little Theorem would eventually be proven by Leibniz and afterwards by Euler who further generalized the result. This theorem would prove useful in primality testing: determining whether or not a particular number is prime or not. Although not a foolproof method, the theorem greatly assisted the quest to find prime numbers, one of the major goals of number theory. In fact, Fermat himself was interested in the primality of the integers of the form $2^n - 1$ (the Mersenne numbers) and of the form $2^{2^n} + 1$ (the Fermat numbers). In the same letter sent to Frenicle, Fermat developed the method now known as "Fermat's factorization method," which is based on the observation that an odd number n can be factored if and only if it is the difference of two squares. The method of finding factorizations of n involves looking for solutions of $n = x^2 - y^2$ by searching for perfect squares of the form $x^2 - n$ (Kleiner). As ingenious as it may be, Fermat factorization can be woefully inefficient and it may be necessary to check as many as $(n+1)/2 - \sqrt{n}$ integers to determine whether they are perfect squares. In addition, it works best when it is used to factor integers having two factors of similar size. As a result, Fermat factorization is rarely used to factor large integers, although its overall idea is the basis for more powerful factorization algorithms used for computer calculations (Rosen).

Fermat pursued other avenues in number theory as well, most of which came from studying Diophantus' *Arithmetica*. And though he did not like to publish his results, Fermat became one of the greatest pioneers of number theory and built the foundation for the area of mathematics that Gauss would call the "Queen of Mathematics." Fermat tried his best to spurn interest amongst contemporary mathematicians of the time. However, those attempts were ultimately in vain. In a letter to Huygens, Fermat wrote:

"There in summary is an account of my thoughts on the subject of numbers. I wrote it only because I fear I shall lack the leisure to extend and to set down in detail all these demonstrations and methods. In any case, this indication will serve learned men in finding for themselves what I have not extended, particularly if MM. de Carcavi

and Frenicle share with them some proofs by infinite descent that I sent them on the subject of several negative propositions. And perhaps posterity will thank me for having shown it that the ancients did not know everything, and this relation will pass into the mind of those who come after me as a “passing of the torch to the next generation,” as the great Chancellor of England says, following the sentiment and the device of whom I will add, “Many will pass by and knowledge will increase. (Laubenbacher)”

Fermat was unsuccessful in trying to convince other mathematicians to carry his torch. This could be attributed to many things, such as his secrecy in his proofs, his falling out with Descartes, amongst other things. As a result, number theory would remain relatively untouched until Euler continued the quest that Fermat started a century later.)

Euler, Legendre, Gauss, and Quadratic Reciprocity

Leonhard Euler made many contributions in many areas of mathematics. Number theory was no exception. Initially, Euler studied number theory as a diversion from the more mainstream mathematics. However, he gained more interest in the area when Christian Goldbach introduced Euler to the works of Fermat in 1729. From there, a large part of Euler's work in number theory concentrated on rigorously proving the assertions of Fermat from a century earlier, among them Fermat's Last Theorem. He would go on to provide the proof for Fermat's Last Theorem for the case $n = 3$. In addition, there was the question of whether or not an integer n was a perfect square modulo a prime p . Euler found the answer to this question in the mid-1700s numerically; but was not able to prove it (Laubenbacher). However, this would be (was) the beginning of the development of the Law of Quadratic Reciprocity, a fundamental property of the prime numbers.

Adrien-Marie Legendre studied number theory extensively after Euler's death. Legendre published *Essay on the Theory of Numbers* in 1798, beginning a comprehensive research program in number theory. He first began by reproducing Euler's proofs for Fermat's Last Theorem for $n = 3$ and $n = 4$. He also proved the case for $n = 5$ afterwards in 1825. In addition, Legendre reformulated the law of quadratic reciprocity proposed by Euler in 1785. Legendre went on to publish several proposed proofs of this theorem, but each of his proofs contained a serious flaw. A young Carl Friedrich Gauss became the first mathematician to give a correct proof of the Law of Quadratic Reciprocity in 1796 at the youthful age of 18 (Laubenbacher).

Gauss published his results in 1801 in *Disquisitiones Arithmeticae* which laid the groundwork for the foundations of modern number theory. In addition to the Law of Quadratic Reciprocity, a fundamental result with prime numbers, Gauss also provided the first a clear presentation of modular arithmetic. Although Gauss was the first to formulate a proof of quadratic reciprocity, he was interested in finding an approach to proving this theorem that could be generalized into higher powers. For example, when given a prime p and an integer a not divisible by p , the congruences $x^3 = a \pmod{p}$ and $x^4 = a \pmod{p}$ are solvable. He continued to search for proofs, formulating at least six different ones during his lifetime. Gauss finally succeeded in generalizing this result to

higher powers. Finding proofs carried on beyond Gauss, and by 1963 no less than 192 different proofs of Quadratic Reciprocity were in existence (Rosen).

The Law of Quadratic Reciprocity is stated as follows: Let p and q be odd primes. Then $\boxed{\times} \left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$, where $\left(\frac{q}{p}\right)$ is a Legendre symbol that indicates whether q is a quadratic residue mod p . This proves to be important in primality testing as it tells us whether or not $x^2 \equiv q \pmod{p}$, which by the definition of congruence means p divides $x^2 - q$ (Rosen). Furthermore, quadratic reciprocity is used in the definitions of the Legendre and Jacobi symbol and can be used to formulate Euler pseudoprimes.

Gauss also held views on Fermat's Last Theorem. In a letter to his colleague W. Olbers on March 21st, 1816:

"I do admit that the Fermat Theorem as an isolated result is of little interest to me, since it is easy to postulate a lot of such theorems, which one can neither prove nor refute. Nonetheless, it has caused me to return to some old ideas for a *great* extension of higher arithmetic. Of course, this theory is one of those things where one cannot presuppose to what extent one will succeed in reaching goals looming in the far distance. A lucky star must also preside, and my situation as well as much detracting business do not allow me to indulge in such meditations as during the lucky years 1796–1798, when I formed the main parts of my *Disquisitiones Arithmeticae*. Alas, I am convinced, that if *luck* contributes more than I am allowed to hope for, and I succeed in some of the main steps in that theory, then the Fermat theorem will appear in it as one of the least interesting corollaries. (Laubenbacher)"

Although Gauss never returned to number theory after *Disquisitiones Arithmeticae*, he laid the groundwork for a new approach in trying to solve Fermat's Last Theorem in the general case rather than one exponent at a time. In fact, the French mathematician Sophie Germain perceived a way of getting a general proof of the theorem using Gauss's presentation of congruence. Although she was unsuccessful in her endeavors, her approach was replicated and pursued by researchers up till even the 1980s (Laubenbacher).

Euler and Fermat Pseudoprimes and Primality Testing

A pseudoprime is a number that is a probable prime (an integer that shares a property common to all prime numbers) which is not actually prime (Wikipedia). Although these numbers aren't actually prime, pseudoprimes are rare enough to have important applications such as probabilistic primality testing and public-key cryptography, particularly if the user is willing to tolerate a minute chance that the number isn't actually prime. Pseudoprimes come in several classes, the most important of which being the Fermat and Euler pseudoprimes. A Fermat pseudoprime is a number of the form $a^{n-1} \equiv 1 \pmod{n}$. An Euler pseudoprime is a composite number of the form $2^{\left(\frac{n-1}{2}\right)} \equiv \pm 1 \pmod{n}$ (Rosen). The properties of these classes can be used to help determine whether or not a given number is actually prime.

Probabilistic primality tests are preferred method for testing the primality of an integer. The goal of these types of tests is to determine whether or not a number of prime with a high probability. The tests generally begin with the picking of a random number a and the given number n . With those two numbers, you check equality based on a particular test. If the equality fails to hold true, then the number n is a composite number and the number a is a witness to its compositeness. This process repeats for several iterations: if it continues to hold true, then the number n is “probably prime” (Wikipedia). Examples of probabilistic primality tests include the aforementioned Fermat primality test and the Miller-Rabin primality test.

Michael Rabin published the Miller-Rabin test in 1976, building upon a result given by Gary Miller a year before regarding strong pseudoprimes. Gary Miller devised a test for primality that goes as follows: Let n be a positive integer with $n-1 = 2^s t$ where s is nonnegative and t is an odd positive integer. We say that n passes Miller’s test for base b if either $b^t \equiv 1 \pmod{n}$ or $b^{2^j t} \equiv -1 \pmod{n}$ for some j with $0 \leq j \leq s-1$. The Miller-Rabin primality test involves applying Miller’s test to k positive integers less than the target number n that you want to test for primality. If n is composite, the probability that

n passes all k tests is less than $\frac{1}{4^k}$ (Rosen). This test is a very quick way of testing a number has a good chance of being prime; the fastest deterministic primality tests run much slower, on the order of $O(n^6)$.

A more modern primality test is the Quadratic Sieve, developed in the late 1980's and early 1990's. The procedure involves quadratic residues, and the sieving (sifting) procedure begins with a number n you are trying to factor and picking a value r such that $r = \lfloor \sqrt{n} \rfloor + k$, where k is an integer. We then try to look for factors of p such that $n \equiv r^2 \pmod{p}$. The set of primes p for which this holds true is called the *factor base*. Next, the equation $x^2 \equiv n \pmod{p}$ must be solved for every p in the *factor base*. A sieve is applied to find values of $f(r) = r^2 - n$ which can be factored completely using only the factor base. This is followed by Gaussian elimination as indicated in Dixon's factorization method to find a product of $f(r)$, yielding a perfect square. (Weisstein). The entire run time of the algorithm requires $e^{\sqrt{\ln n \ln \ln n}}$ steps, which is considerably faster than other deterministic methods despite its exponential nature.

The Distribution of Primes and the Prime Number Theorem

Euclid had long proved the infinitude of the prime numbers. However, the question of how many primes are less than a particular number remained unanswered. In 1798, Legendre used tables of primes up to 400031, computed by Vega, and noted that the number of primes not exceeding x , $\pi(x)$, could be estimated by the function

$\frac{x}{\log x}$. Gauss would conjecture that $\pi(x)$ increases at the same rate as the function $\frac{x}{\log x}$. Unfortunately, Legendre and Gauss were both not able to prove this result for large values of x . In fact, it took several decades, until 1850 when the Russian

mathematician Chebyshev showed that the ratio of $\pi(x)$ and $\frac{x}{\log x}$ approaches the limit value of 1 as x increases. Formally, the prime number theorem states that the ratio of $\pi(x)$ and $\frac{x}{\log x}$ approaches the limit value of 1 as x increases without bound. The theorem was officially proven in 1896 by the French mathematician Jacques Hadamard and Charles-Jean-Gustave de la Vallée-Poussin using results from complex analysis. The distribution of primes yielded by the prime number theorem is one of the most highly regarded theorems in number theory, as well as all of mathematics (Rosen).

Applications of Number Theory

Number theory is often considered a very pure branch of mathematics. Because it is so pure, it is often seen as less useful as other branches of mathematics. However, as the world approaches a more globalized scheme with many transactions across a network medium, the need for information security has become increasingly more apparent. Modern cryptography applies a lot of number theory in order to accomplish its results: in particular, congruence and large prime numbers are needed. One such scheme involving congruence and large prime numbers is the RSA (Rivest Shamir Adelman) cryptography scheme.

The RSA Cryptography method is based on the problem of factoring large numbers into prime factors. We begin with a number n , which is the product of two enormous primes p and q . Given a message M and a random integer e , the sender of the message sends $M^e \pmod n$ to the receiver. The exponent e and the number n are called the public key of the receiver. The receiver has a private key, d , which they can use to quickly compute the inverse operation of M^e in order to extract the actual message (Rivest).

Because the security of this algorithm depends completely on the secrecy of the two primes and the difficulty of factoring products of large primes, there is a constant search for larger primes. The world's largest known prime at this moment is $2^{25964951} - 1$, the 42nd known Mersenne prime, and being able to choose from many such large primes is why the RSA algorithm remains a very useful algorithm. The tests used to determine primality might be probabilistic such as Miller-Rabin or deterministic such as the Quadratic sieve. However, both techniques are employed in order to search for large primes. While these tests are moderately quick, there is a need for development of faster prime-testing methods.

WORKS CITED

- Bogomolny, Alexander. "The Chinese Remainder Theorem." 2005
<<http://www.cut-the-knot.org/blue/chinese.shtml>>
- Kleiner, Israel. "Fermat: The Founder of Modern Number Theory." February 2005.
Mathematics Magazine. <http://www.rednova.com/news/display/?id=129877>
- Laubenbacher, Reinhard, and David Pengelley. "Mathematical Expeditions.
Chronicles by the Explorers." Springer: 1998.
<http://www.math.nmsu.edu/~history/book/numbertheory.pdf>
- O'Connor, J J and Robertson, E F. "Diophantus" February 1999
<<http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Diophantus.html>>
- O'Connor, J J and E F Robertson. "Fermat." December 1996. School of Mathematics
and Statistics University of St Andrews, Scotland. 5-1-05.
<http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Fermat.html>
- O'Connor, J J and Robertson, E F. "Nicomachus of Gerasa" School of Mathematics and
Statistics University of St Andrews, Scotland. April 1999
<<http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Nicomachus.html>>
- O'Connor, J J and Robertson, E F. "Perfect numbers". School of Mathematics and
Statistics University of St Andrews, Scotland. December 2001.
<http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Perfect_numbers.html>
- Rees, Sara. "Fermat's Last Theorem." <http://www.bath.ac.uk/~ma1sr/Introduction.html>
- Rivest, R.L. A. Shamir. L Adleman. "A Method for Obtaining Digital Signatures and
Public Key Cryptosystems." Association for Computing Machinery.
<http://delivery.acm.org/10.1145/360000/359342/p120rivest.pdf?key1=359342&key2=7347179011&coll=GUIDE&dl=ACM&CFID=39714862&CFTOKEN=29484238>
- Rosen, Kenneth. "Elementary Number Theory and Its Applications." New York:
Addison Wesley Longman, Inc. 2000
- Weisstein, Eric W.. "Fermat's Last Theorem." From MathWorld--A Wolfram Web
Resource. <http://mathworld.wolfram.com/FermatsLastTheorem.html>

Weisstein, Eric W. "Euclid's Theorems." From *MathWorld*--A Wolfram Web Resource.
<http://mathworld.wolfram.com/EuclidsTheorems.html>

Weisstein, Eric W.. "Quadratic Sieve." From *MathWorld*--A Wolfram Web Resource.
<http://mathworld.wolfram.com/QuadraticSieve.html>

"Primality Test." Wikipedia, the Free Encyclopedia. April 30 2005.

"Pseudoprime." Wikipedia, the Free Encyclopedia. March 2 2005.