2 Primes Numbers

Definition 2.1 *A number is prime is it is greater than 1, and its only divisors are itself and 1. A number is called composite if it is greater than 1 and is the product of two numbers greater than 1.*

Thus, the positive numbers are divided into three mutually exclusive classes. The prime numbers, the composite numbers, and the unit 1.

We can show that a number is composite numbers by finding a non-trivial factorization.[8] Thus, 21 is composite because $21 = 3 \times 7$. The letter p is usually used to denote a prime number.

The first fifteen prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41$$

These are found by a process of elimination. Starting with 2, 3, 4, 5, 6, 7, etc., we eliminate the composite numbers 4, 6, 8, 9, and so on. There is a systematic way of finding a table of all primes up to a fixed number. The method is called a sieve method and is called the Sieve of Eratosthenes[9]. We first illustrate in a simple example by finding all primes from 2 through 25. We start by listing the candidates:

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25$$

The first number 2 is a prime, but all multiples of 2 after that are not. Underline these multiples. They are eliminated as composite numbers. The resulting list is as follows:

$$2, 3, \underline{4}, 5, \underline{6}, 7, \underline{8}, 9, \underline{10}, 11, \underline{12}, 13, \underline{14}, 15, \underline{16}, 17, \underline{18}, 19, \underline{20}, 21, \underline{22}, 23, \underline{24}, 25$$

The next number not eliminated is 3, the next prime. Now eliminate all multiples of 3 after it, which have not yet been eliminated. Again, we are underlining the known composite

[8] That is, a factorization where both factors are greater than 1.

[9] After Eratosthenes of Cyrene (appr. 275-195 B.C.), a famous Greek scholar, once director of the Library in Alexandria, and the first to estimate the diameter of the earth.

numbers. We do this by multiplying by 3 (eliminating 9), and 3 again (except that this is too large and outside of our table), then by 5, eliminating 15, (and by 5 again, except that this is too large), then by 7 eliminating 21 and so on. This gives the following list:

$$2, 3, \underline{4}, 5, \underline{6}, 7, \underline{8}, \underline{9}, \underline{10}, 11, \underline{12}, 13, \underline{14}, \underline{15}, \underline{16}, 17, \underline{18}, 19, \underline{20}, \underline{21}, \underline{22}, 23, \underline{24}, 25$$

Since 5 is the next number not eliminated, it is the next prime, and we eliminate all multiples of 5 not yet eliminated. Thus 25 is eliminated. The final list is therefore

$$2, 3, \underline{4}, 5, \underline{6}, 7, \underline{8}, \underline{9}, \underline{10}, 11, \underline{12}, 13, \underline{14}, \underline{15}, \underline{16}, 17, \underline{18}, 19, \underline{20}, \underline{21}, \underline{22}, 23, \underline{24}, \underline{25}$$

No more eliminations are now needed, since the next prime is 7 and the first multiple of 7 not yet eliminated is 49 – way outside the range of the table. Thus what has not yet been eliminated are primes and by a process of elimination, we have found the all primes less than or equal to 25. The list is

$$2, 3, 5, 7, 11, 13, 17, 19, 23$$

This computation can easily be done on a computer and this is essentially the way a table of primes is created. The prime module in the laboratory computes prime numbers essentially using this method. The following table illustrates the sieve method for the numbers from 2 to 200. The underlined numbers are composite. Once all multiples of 7 were eliminated, the process stopped.

		2	3	$\underline{4}$	5	$\underline{6}$	7	$\underline{8}$	$\underline{9}$
$\underline{10}$	11	$\underline{12}$	13	$\underline{14}$	$\underline{15}$	$\underline{16}$	17	$\underline{18}$	19
$\underline{20}$	$\underline{21}$	$\underline{22}$	23	$\underline{24}$	$\underline{25}$	$\underline{26}$	$\underline{27}$	$\underline{28}$	29
$\underline{30}$	31	$\underline{32}$	$\underline{33}$	$\underline{34}$	$\underline{35}$	$\underline{36}$	37	$\underline{38}$	$\underline{39}$
$\underline{40}$	41	$\underline{42}$	43	$\underline{44}$	$\underline{45}$	$\underline{46}$	47	$\underline{48}$	$\underline{49}$
$\underline{50}$	$\underline{51}$	$\underline{52}$	53	$\underline{54}$	$\underline{55}$	$\underline{56}$	$\underline{57}$	$\underline{58}$	59
$\underline{60}$	61	$\underline{62}$	$\underline{63}$	$\underline{64}$	$\underline{65}$	$\underline{66}$	67	$\underline{68}$	$\underline{69}$
$\underline{70}$	71	$\underline{72}$	73	$\underline{74}$	$\underline{75}$	$\underline{76}$	$\underline{77}$	$\underline{78}$	79
$\underline{80}$	$\underline{81}$	$\underline{82}$	83	$\underline{84}$	$\underline{85}$	$\underline{86}$	$\underline{87}$	$\underline{88}$	89
$\underline{90}$	$\underline{91}$	$\underline{92}$	$\underline{93}$	$\underline{94}$	$\underline{95}$	$\underline{96}$	97	$\underline{98}$	$\underline{99}$
$\underline{100}$	101	$\underline{102}$	103	$\underline{104}$	$\underline{105}$	$\underline{106}$	107	$\underline{108}$	109
$\underline{110}$	$\underline{111}$	$\underline{112}$	113	$\underline{114}$	$\underline{115}$	$\underline{116}$	$\underline{117}$	$\underline{118}$	$\underline{119}$
$\underline{120}$	$\underline{121}$	$\underline{122}$	$\underline{123}$	$\underline{124}$	$\underline{125}$	$\underline{126}$	127	$\underline{128}$	$\underline{129}$
$\underline{130}$	131	$\underline{132}$	$\underline{133}$	$\underline{134}$	$\underline{135}$	$\underline{136}$	137	$\underline{138}$	139
$\underline{140}$	$\underline{141}$	$\underline{142}$	$\underline{143}$	$\underline{144}$	$\underline{145}$	$\underline{146}$	$\underline{147}$	$\underline{148}$	149
$\underline{150}$	151	$\underline{152}$	$\underline{153}$	$\underline{154}$	$\underline{155}$	$\underline{156}$	157	$\underline{158}$	$\underline{159}$
$\underline{160}$	$\underline{161}$	$\underline{162}$	163	$\underline{164}$	$\underline{165}$	$\underline{166}$	167	$\underline{168}$	$\underline{169}$
$\underline{170}$	$\underline{171}$	$\underline{172}$	173	$\underline{174}$	$\underline{175}$	$\underline{176}$	$\underline{177}$	$\underline{178}$	179
$\underline{180}$	181	$\underline{182}$	$\underline{183}$	$\underline{184}$	$\underline{185}$	$\underline{186}$	$\underline{187}$	$\underline{188}$	$\underline{189}$
$\underline{190}$	191	$\underline{192}$	193	$\underline{194}$	$\underline{195}$	$\underline{196}$	197	$\underline{198}$	199

The Sieve of Eratosthenes

It is customary to call the n-th prime p_n, so $p_1 = 2$, $p_2 = 3$, …, $p_{46} = 199$. Based on the above table, it is easy to make a table of all the primes less than 200.

n	p_n	n	p_n	n	p_n	n	p_n
1	2	13	41	25	97	37	157
2	3	14	43	26	101	38	163
3	5	15	47	27	103	39	167
4	7	16	53	28	107	40	173
5	11	17	59	29	109	41	179
6	13	18	61	30	113	42	181
7	17	19	67	31	127	43	191
8	19	20	71	32	131	44	193
9	23	21	73	33	137	45	197
10	29	22	79	34	139	46	199
11	31	23	83	35	149		
12	37	24	89	36	151		

The Primes Under 200

We shall return to this table later, in order to study some if its properties. For the present, we can use many of general division properties and apply them to primes. We shall use the following fact about primes:

> Let p be a prime number, and let a be any integer. Then either $p|a$ or p and a are relatively prime.

This is so because any common divisor of p and a must be a divisor of p, namely 1 or p. These two choices show that either $p|a$ or $\gcd(p, a) = 1$.

As a consequence of Theorem 1.10 and the above remark, we have

Theorem 2.2 *If p is a prime, and $p|ab$, then either $p|a$ or $p|b$. More generally, if a prime divides a product then it must divide one of the factors.*

A very famous consequence is this famous theorem of Pythagoras.

Theorem 2.3 *$\sqrt{2}$ is irrational.*

We appear to have departed from the integers in the statement of the result. But this result can be stated in terms of integers. A number is rational if it is the ratio of two integers. Otherwise, it is irrational. Thus, this theorem says that $\sqrt{2} \neq a/b$ or $2 \neq a^2/b^2$, or finally that it is impossible to find numbers a and b such that

$$a^2 = 2b^2$$

This is an example of a quadratic Diophantine equation. We now show that there is no solution, other than $a = b = 0$. This we prove by contradiction. We assume that a and b are relatively prime. (If they are not, divide this equation by d^2, where $d = \gcd(a, b)$.) Then since $2|2b^2$ it follows that $2|a^2$ or $2|a \cdot a$. Since 2 is a prime number, it follows from Theorem 2.2 that $2|b$. Thus 2 is a divisor of both a and b, contradicting our assumption that a and b are relatively prime.

It seems clear that any integer greater than 1 is a prime number or a product of primes.[10] Our experience with numbers is fairly limited, so why do we believe this? (For example, have you ever worked with a thousand digit number?) One idea for a proof is as follows. If a number a is a prime, there is nothing more to prove. Otherwise, it can be factored into two factors each smaller than a. Now work with these factors. If they are primes, we have

[10] We will say that a prime is a product of one prime, namely itself, so we can simply say that any integer greater than 1 is a product of primes.

factored a into two factors. Otherwise, factor the factors, and continue "indefinitely." For example, to factor 490 into primes, we write

$$490 = 10 \cdot 49 = 2 \cdot 5 \cdot 7 \cdot 7$$

Thus we have the following.

Theorem 2.4 *Every number greater than 1 is a product of primes.*

Although it seems clear that this is true, a *proof* is a little tricky. We shall prove it by *the method of contradiction.* If we assume that there is some number which cannot be decomposed into a finite product of primes, there will be a least such number. Call it A. A is not a prime, so it can be non-trivially factored: $A = bc$, with $1 < b, c < A$. Since b and c are smaller than A, and A was chosen as the least number which cannot be factored into primes, it follows that b and c are each a product of primes. So therefore $A = bc$ is, and this is the contradiction.

The proof is quite subtle. It used the principle that if there is any positive integer with some property, there is a least one. This gets to the heart of what integers are, and we will often use this principle.

Not only can a number be factored into primes, except for the order of the factors, there is only one way to do this. For example, we know that a number like 60 can be factored in many ways. Thus, $60 = 6 \cdot 10 = 5 \cdot 12$. But if we go further and break these into prime factors we find

$$60 = 6 \cdot 10 = 2 \cdot 3 \cdot 2 \cdot 5 = 2^2 \cdot 3 \cdot 5$$

Similarly, the alternate factorization gives

$$60 = 5 \cdot 12 = 5 \cdot 4 \cdot 3 = 5 \cdot 2^2 \cdot 3 = 2^2 \cdot 3 \cdot 5$$

the same factorization into primes. (We usually, write the primes in increasing order, so we can see that the factorizations are the same except for the order of the factors. Let us prove this result.

Theorem 2.5 (The Unique Factorization Theorem.) *Any integer greater than 1 has exactly one factorization into prime factors, not counting the order of the factors.*

The proof is again a proof by contradiction, and uses the same technique as in the proof of Theorem 2.4. Certainly the result is true for the first few numbers 2, 3, 4, 5, 6. Now assume that there is some number A which has two different factorizations into primes, and let A be the least such number. Let

$$A = p_1 p_2 \ldots = q_1 q_2 \ldots$$

be the factorizations into primes. This first equation shows that $p_1|A$. Thus $p_1|q_1q_2\ldots$. Since p_1 divides the product of the $q's$, it follows by Theorem 2.2 that p_1 divides one of the q's. Since the q's are primes, it follows that one of the q's is equal to p_1. Rearrange the q factors so that the first one is in fact p_1. Then we have

$$A = p_1p_2 \ldots = p_1q_2 \ldots$$

Therefore

$$A/p_1 = p_2p_3 \ldots = q_2q_3 \ldots$$

But since $A/p_1 < A$, it follows from the way A was chosen that A/p_1 has a unique factorization into primes. Therefore the rest of the q's are simply a rearrangement of the p's and this proves the theorem.

Theorem 2.5 is important enough to be called the *Fundamental Theorem of Arithmetic.*

If a number n is written as a product of primes, we can collect like primes and write the number as a product of prime powers. For example,

$$288 = 2 \cdot 144 = 2 \cdot 12^2 = 2 \cdot (2^2 \cdot 3)^2 = 2^5 3^2$$

In the same way, any integer n can be written in a unique way as a product $p_1^{a_1}p_2^{a_2}\ldots$, where the primes $p_1 < p_2 < \ldots$. If this factorization is available, we have a quick way of deciding where two integers are relatively prime, and in general, of finding the gcd of these numbers. For example, consider the two numbers (factored)

$$m = 2^3 5^2 11^2 \text{ and } n = 3^1 5^1 7^2 11^1$$

It is clear from these factorizations that these numbers are not relatively prime, because they have a common divisor $55 = 5 \cdot 11$, and in fact this is the least common divisor. Note that we have found that $\gcd(24200, 47685) = 55$ by observation. Divisibility is easily determined once the prime power factorization is determined. Thus, $d|n$ is and only if any prime power appearing in the factorization of d also appears in the factorization of n with a power not less than the power in d. For example, $2^7 3^5 11^3 | 2^8 3^5 11^7$.

We say that a number n is a *perfect square* provided $n = a^2$ for some integer a. Thus, the first six positive perfect squares are 1, 4, 9, 16, 25, and 36.

Theorem 2.6 *A number n is a perfect square if and only if the highest power of any prime which divides n is an even number.*[11]

[11] "If and only if" is common mathematical usage. This is actually two statements. First that if the number is a perfect square, the highest power of any prime dividing it must be even, and second, that if the highest power of any prime dividing the number is even, then the number must be a perfect square

For example, 45 is not a perfect square, since $45 = 3^2 5^1$ and the exponent of 5 is 1, and not even. But $144 = 2^4 3^2$ is a perfect square since the exponents 4 and 2 are even.

The proof uses unique factorization. First suppose that $n = m^2$ is a perfect square. If we factor m into primes with $m = p_1^a p_2^b \ldots$ where $p_1,\ p_2,\ \ldots$ are the different primes dividing m, then

$$n = m^2 = p_1^{2a} p_2^{2b} \ldots$$

so the powers in the prime factorization are all even. Conversely, if the powers in the prime factorization of n are all even, then

$$n = p_1^{2a} p_2^{2b} \ldots$$

then we can choose $m = p_1^a p_2^b \ldots$ and clearly we have $n = m^2$.

Note that perfect squares can easily be factored into numbers that are not perfect squares: For example, $16 = 2 \cdot 8$, $36 = 2 \cdot 18$. In each of these factorizations, the factors are not relatively prime. It turns out that if a perfect square is factored into the product of two relatively prime numbers, each of the factors is a perfect square. For example, $36 = 4 \cdot 9$. We prove this theorem.

Theorem 2.7 *If $n^2 = ab$, where a and b are relatively prime, then a and b are perfect squares.*

The proof follows easily from Theorem 2.6. Since a and b are relatively prime, they have no prime factor in common. Thus they use different primes in their unique factorization:

$$a = p_1^a p_2^b \ldots;\ b = q_1^c q_2^d \ldots$$

Since $n^2 = ab$, and the primes are all different, we have

$$n^2 = p_1^a p_2^b \ldots q_1^c q_2^d \ldots$$

Since n^2 is a perfect square, all the prime exponents are even, using Theorem 2.6. By this theorem, it follows that a and b are also perfect squares. This is the result.

The Pythogorean Diophantine Equation $a^2 + b^2 = c^2$.

The Pythagorean Theorem relates the sides a and b of a right triangle with its hypotenuse c by the equation $a^2+b^2 = c^2$. It is probably one of the most well known results of mathematics. Most of us are familiar with the 3–4–5 right triangle. Here $3^2+4^2 = 5^2$. Another less familiar solution of this equation is (5,12,13) since $5^2 + 12^2 = 25 + 144 = 169 = 13^2$.In this section we find all (integer) solutions to this equation.

We first consider the case that $\gcd(a, b) = 1$. As we shall see, this case quickly yield the general case. In this case, $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$. For if p were a prime divisor of bot a and c, it would divide b^2 and hence b, contradiction $\gcd(a, b) = 1$.

In this case, we claim that one of the numbers a, b must be odd, and the other even. It is clear that they both can't be even, since $\gcd(a, b) = 1$. If they were both odd, we shall obtain a contradiction. We first note that the square of an odd number leaves a remainder 1 when divided by 4. To see this, note that if $a = 2n+1$, then $a^2 = (2n+1)^2 = 4n^2+4n+1 = 4n(n+1)+1$, so its remainder when divided by 4 is 1. Further, since $c^2 = a^2 + b^2$, c^2 must be even, and so c must be even too. (If it were odd, so would its square.) Thus, $c = 2m$ and so $c^2 = 4m^2$. Thus if both a and b were odd, we would have

$$a^2 + b^2 = 4q_1 + 1 + 4q_2 + 1 = 4(q_1 + q_2) + 2 = c^2 = 4m^2$$

Dividing by 2, this gives $2(q_1 + q_2) + 1 = 2m^2$. This is a contradiction, since the left hand side is odd and the right hand side is even. This shows that one of a, b is even and the other if odd. This makes c odd too, since $a^2 + b^2 = c^2$ is odd. For simplicity, let's suppose that a is even and b is odd. Solving for a^2, we get

$$a^2 = c^2 - b^2 = (c - b)(c + b) \ (b, c \text{ odd, } a \text{ even})$$

Dividing by 4, this gives

$$\left(\frac{a}{2}\right)^2 = c^2 - b^2 = \left(\frac{c-b}{2}\right)\left(\frac{c+b}{2}\right)$$

Now we claim that $\left(\frac{c-b}{2}\right)$ and $\left(\frac{c+b}{2}\right)$ are relatively prime. For if d were a common divisor it would divide their sum c and the difference b. Thus we must have $d = 1$ since b and c are relatively prime. Therefore by Theorem 2.7, we must have

$$\left(\frac{c-b}{2}\right) = s^2, \ \left(\frac{c+b}{2}\right) = r^2$$

for relatively prime r and s. We're almost there. Add and subtract these equations to get

$$c = r^2 + s^2, \ b = r^2 - s^2 \text{ where } \gcd(r, s) = 1$$

Since $a^2 = c^2 - b^2$, we get

$$a^2 = (r^2 + s^2)^2 - (r^2 - s^2)^2 = r^4 + 2r^2s^2 + s^4 - (r^4 - r^2s^2 + s^4) = 4r^2s^2$$

and so $a = 2rs$. What we have found is that if a and b are relatively prime, with a even, we have

$$\begin{aligned} a &= 2rs \\ b &= r^2 - s^2 \\ c &= r^2 + s^2 \end{aligned}$$

Here we must have r and s relatively prime, with $r > s$. Since both b and c are odd, we must have one of r and s even, and one odd. For example, take $r = 2$ and $s = 1$ and we get the 3-4-5 right triangle. Take $r = 3$ and $s = 2$ to get the 5-12-13 right triangle. By experimenting in this way, so long as $r > s$, $\gcd(r, s) = 1$ and r and s of different parity,[12] we can generate as many solutions of the Pythagorean equation as we want.

What if a and b are not relatively prime. In this case, we take $d = \gcd(a, b)$ and write $a = da'$ and $b = db'$ where a' and b' are relatively prime. Then

$$c^2 = a^2 + b^2 = d^2(a'^2 + b'^2)$$

This implies that $d^2|c^2$ and so $d|c$. (This will be proved in the Exercises.) Thus $c = dc'$ and from $a^2 + b^2 = c^2$, wse divide by d^2 to get $a'^2 + b'^2 = c'^2$ where a' and b' are reltively prime. We now use the above analysis to find a', b', c' and so the general solution in this case is simply as above, with a constant d thrown in:

$$\begin{aligned} a &= 2drs \\ b &= d(r^2 - s^2) \\ c &= d(r^2 + s^2) \end{aligned}$$

This complete the analysis of the Pythagorean equation.

If we inspect the short table of primes on page 15, we notice a certain irregularity in the distributions of primes. First, there are a few gaps where no primes appear. For example, here are 13 consecutive composite numbers between the 30th and 31st prime (113 and 127). Similarly there are 9 consecutive composites between the 34th and 35th prime. On the other hand, there are various instances where there is only one composite number between consecutive primes. (These are the so-called twin primes.) Some examples are (17,19),(71,73), (191,193). Of course in the grand order of all numbers, this table is almost negligible. Yet we can ask several questions:

1. Are there infinitely many primes?
2. If so, are there arbitrarily large gaps between consecutive primes? For example, are there consecutive primes with 1,000 or more composite numbers between them?
3. Are there infinitely many twin primes?
4. How many primes are there between 1 and n?
5. Is there a formula for the n-th prime?

[12] This means that of the pair r, s, one is odd and one is even

These questions and many more have been considered and worked on by mathematicians for centuries. We can answer item 1 with a proof given over 2000 years ago by the Greek mathematician Euclid.[13]

Theorem 2.8 *There are infinitely many primes.*

The proof is by contradiction. Assuming the list of primes if finite, we may write all the primes in a list

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \ldots,\ p_n$$

Now consider the number $N = p_1 p_2 \ldots p_n + 1$. By its form, N leaves a remainder 1 when divided by any of the primes. For example, when divided by p_1, its quotient is $p_2 p_3 \ldots p_n$ and its remainder is 1. But N has a prime divisor p, and p is not in the alleged complete list of primes. This is a contradiction, proving the result.

We can see how this proof works by giving a few examples. For example, if we supposed that 2 and 3 were the only primes (admittedly we know better), we take $2 \cdot 3 + 1 = 7$ to find a number which has a prime divisor other than 2 or 3. Similarly, if we take 2, 3, 5 as the primes, then $2 \cdot 3 \cdot 5 + 1 = 31$ has a prime divisor other than 2, 3, or 5. (Note: we do not expect this constructed number to be prime. For example, if we start with the primes 3 and 5, we find $3 \cdot 5 + 1 = 16$ which has a prime divisor (2) other than 3 or 5.)

Since here are infinitely many primes, we might ask: What is the largest known prime? The answer is (at the moment that this is being written) $2^{13466917} - 1$. This is a number with over four million digits. By searching the internet, it is easy to find many results such as these, as well as a list of unsolved problems relating to prime numbers. By the time you read this, a larger prime might have been discovered.

We shall leave item 2 to the exercises, with a hint. The result is true.

As noted in the introduction, nobody has proved or disproved item 3. This is a classical unsolved problem in mathematics with a great pedigree. If you answered this question with a proof, you would be able to get yourself a professorship in the university of your choice and you would be world famous (at least among mathematicians). Most mathematicians strongly believe that there are infinitely many twin primes. This is an example that refutes a common misunderstanding that the advent of computers makes mathematics obsolete. You can't check this on the computer because there are infinitely many checks to be made, and no computer can do infinitely many checks. But for as far out as mathematicians have searched, twin primes have been found. Interestingly, if you searched for twin primes, you

[13] Euclid (appr. 365–300 B.C.) was most famous for this book *Elements*, a collection of mathematical results, mostly on geometry, with proofs. This result, with the following proof, is in this text. We have already mentioned the Euclidean Algorithm, which also came from this book.

will find that they are relatively abundant, so abundant it seems naturally to take this result for granted. You will have lab experiments on this.

The answers to the last two items depends on the meaning of the question. If you want a simple formula the answer is no. The number of primes between 1 and n is called $\pi(n)$, so that for example, $\pi(200) = 46$. A very famous theorem of number theory, called *the prime number theorem* states that $\pi(n)$ has order of magnitude $n/\ln n$. Here, $\ln n$ is the natural logarithm of n. A more accurate estimate turns out to be

$$\pi(n) \approx \frac{n}{\ln n - 1}$$

For example, this estimate gives $\pi(200) \approx 200/(\ln 200 - 1) = 46.53$, a very impressive calculation, since we have seen that the actual value is 46. Similarly $\pi(1,000,000) = 78,498$ while $\dfrac{1,000,000}{\ln 1,000,000 - 1} = 78,030.4$ a percentage error less than 0.6%.

The prime number theorem is an extremely deep result, and was first proved towards the end of the 19th century. The fact that the study of ordinary numbers lead to a result involving natural logarithms gives ample evidence that when it comes to "ordinary numbers," there's more to them than meets the eye.

Exercises on Primes.

1. Using the table of primes on page 15 find all twin prime pairs $(p, p+2)$ with $p+2$ under 200. How many such pairs did you find? How many with $p+2$ under 100? How many with $p+2$ between 100 and 200?

2. Show that the product of two consecutive numbers is even.

3. Show that the product of three consecutive numbers is divisible by 6.

4. What can you say about the product of four consecutive numbers?

5. Show that if a number n is composite, it is divisible by a prime less than or equal to $\sqrt{n}$.

6. Using the table of primes on page 15 and the above result, factor the following numbers. If any are primes, state so.
(a) 119 (b) 221 (c) 223 (d) 299 (e) 629

7. Show that $\sqrt{5}$ is irrational.

8. Show that $\sqrt{35}$ is irrational.

9. It was stated on page that if $d^2|n^2$ then $d|n$. Prove this. Hint: Use unique factorization.

10. Show that the square of an odd number has the form $8n+1$, and the square of an even number has the form $8n$ or $8n+4$

11. Using the above result show that any number of the form $8n+7$ is not the sum of three squares.

12. Show that there there 1,000 consecutive numbers none of which is prime. Hint: Let $N = 1,001!$.[14] Then consider the numbers $N+2, N+3, N+4, \ldots, N+1,001$. This method generalizes to show that there are arbitrarily large gaps of only composite numbers.

[14] This is the factorial notation: $1,001! = 2 \cdot 3 \cdot 4 \cdots 1,001$.