Prime Numbers

August 27, 2006

1 The Fundamental Theorem of Arithmetic

Definition 1 A prime number is an integer greater than 1 whose only positive divisors are itself and 1. Any positive integer greater than 1 that is not prime is said to be composite. The integer 1 is the only positive integer that is considered to be neither prime nor composite.

Since the set of positive divisors of 2 is $D(2) = \{1, 2\}$, we see that 2 is a prime number. The set of positive divisors of 3 is $D(3) = \{1, 3\}$, so 3 is also a prime number. The set of positive divisors of 4 is $D(4) = \{1, 2, 4\}$, so 4 is not a prime number (meaning that 4 is a composite number). It is easy to see that the prime numbers that lie between 1 and 20 are 2, 3, 5, 7, 11, 13, 17, and 19. It is also easy to see that 2 is the only even prime number because every even number greater than 2 is divisible by 2.

There is a nice way to identify all of the prime numbers that lie between 1 and some given positive integer $n$. It is called the Sieve of Eratosthenes. This method will be discussed in class where we will use the following list of all integers between 1 and 50 to find all prime numbers that lie between 1 and 50.

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>31</td>
<td>32</td>
<td>33</td>
<td>34</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>38</td>
<td>39</td>
<td>40</td>
</tr>
<tr>
<td>41</td>
<td>42</td>
<td>43</td>
<td>44</td>
<td>45</td>
<td>46</td>
<td>47</td>
<td>48</td>
<td>49</td>
<td>50</td>
</tr>
</tbody>
</table>
1.1 Homework

Use the Sieve of Eratosthenes to find all prime numbers that lie between 1 and 200.

2 Factorization of Integers Into Prime Factors

If $p$ is a prime number, then the set of positive divisors of $p$ is $D(p) = \{1, p\}$. If $a$ is any other integer such that $p$ does not divide $a$, then $p \notin D(a)$. It then follows that $\gcd(p,a) = 1$ because, in fact, $D(p) \cap D(a) = \{1\}$. This fact leads to the following lemma which is similar to Euclid’s Lemma.

Lemma 2 Suppose that $p$ is a prime number and suppose that $a$ and $b$ are integers such that $ab$ is divisible by $p$. Then either $a$ or $b$ is divisible by $p$.

Proof. Suppose that $p$ is prime and that $a$ and $b$ are integers such that $ab$ is divisible by $p$. If $a$ is not divisible by $p$, then $\gcd(p,a) = 1$. Then, by Euclid’s Lemma (page 18 of the textbook), we conclude that $b$ is divisible by $p$.

The following lemma is a more general version of the previous lemma. The proof of this lemma uses the previous lemma and also uses the Principle of Induction.

Lemma 3 Suppose that $p$ is a prime number and suppose that $a_1, a_2, \ldots, a_n$ are integers such that the product $a_1a_2\cdots a_n$ is divisible by $p$. Then at least one of the integers $a_1, a_2, \ldots, a_n$ must be divisible by $p$.

Proof. The statement that we want to prove is true for all integers $n \geq 2$ is

$P(n):$ If $p$ is prime and $a_1, a_2, \ldots, a_n$ are integers such the product $a_1a_2\cdots a_n$ is divisible by $p$, then at least one of the integers $a_1, a_2, \ldots, a_n$ must be divisible by $p$.

By the previous lemma, we already know that the statement $P(2)$ is true: If $p$ is prime and we have two integers $a_1$ and $a_2$ such that the product $a_1a_2$ is divisible by $p$, then either $a_1$ or $a_2$ must be divisible by $p$.

We must now show (since we are going to use the Principle of Induction) that the truth of the statement $P(n)$ implies the truth of the statement $P(n+1)$.
Supposing that the statement $P(n)$ is true, let $a_1, a_2, \ldots, a_n, a_{n+1}$ be integers such the product $a_1a_2 \cdots a_n a_{n+1}$ is divisible by $p$. Then since $a_1a_2 \cdots a_n a_{n+1} = (a_1a_2 \cdots a_n) a_{n+1}$, we know (since statement $P(2)$ is true) that either $a_1a_2 \cdots a_n$ or $a_{n+1}$ must be divisible by $p$. If $a_{n+1}$ is divisible by $p$, then statement $P(n+1)$ is true. If $a_1a_2 \cdots a_n$ is divisible by $p$ then (since statement $P(n)$ is assumed to be true) at least of the integers $a_1, a_2, \ldots, a_n$ must be divisible by $p$, meaning that statement $P(n+1)$ is true.

We have now proved that statement $P(2)$ is true and that the truth of statement $P(n)$ implies the truth of statement $P(n+1)$. By the Principle of Induction, the statement $P(n)$ must be true for all $n \geq 2$. ■

The proof of the following theorem, which is called the Fundamental Theorem of Arithmetic, uses the Generalized Principle of Induction.

**Theorem 4 (Fundamental Theorem of Arithmetic)** Let $a$ be any integer greater than 1. Then there is a unique set of prime numbers $p_1 < p_2 < \ldots < p_n$ and a unique set of exponents (all positive integers) $k_1, k_2, \ldots, k_n$ such that

\[ a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}. \]

The Fundamental Theorem of Arithmetic states that every integer $n > 1$ can be written as a product of prime numbers and that this can be done in only one way. Here is an example: The number 8,500 can be written as

\[ 8,500 = 2^2 \cdot 5^3 \cdot 17. \]

This has the form $p_1^{k_1} p_2^{k_2} p_3^{k_3}$ where $p_1 = 2$, $p_2 = 5$, $p_3 = 17$, $k_1 = 2$, $k_2 = 3$, and $k_3 = 1$. There is no other way to express 8,500 in terms of prime factors.

We will now state a corollary to the above theorem concerning rational numbers. First we define what a rational number is.

**Definition 5** A rational number is any number that can be written in the form $m/n$ where $m$ and $n$ are integers.

Note that there are infinitely many ways to express any given rational number. For example

\[ \frac{24}{32} = \frac{3}{4}. \]

The following corollary to Theorem 4 states that there is only one way to express a rational number in the form $m/n$ where $m$ and $n$ are relatively prime.
Corollary 6  Every positive rational number, \( a \), can be expressed uniquely as 
\[ a = \frac{m}{n} \]
where \( m \) and \( n \) are relatively prime positive integers.

Proof. First we will prove that every positive rational number, \( a \), can be written in the form 
\[ a = \frac{m}{n} \]
where \( m \) and \( n \) are relatively prime: Since \( a \) is assumed to be a positive rational number, we know that there are positive integers \( b \) and \( c \) such that 
\[ a = \frac{b}{c} \]
. By the Fundamental Theorem of Arithmetic, we know that there is a unique set of prime numbers \( p_1 < p_2 < \ldots < p_s \) and a unique set of exponents (all positive integers) \( k_1, k_2, \ldots, k_s \) such that 
\[ b = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s} \]
and we also know that there is a unique set of prime numbers \( q_1 < q_2 < \ldots < q_t \) and a unique set of exponents (all positive integers) \( r_1, r_2, \ldots, r_t \) such that 
\[ c = q_1^{r_1} q_2^{r_2} \ldots q_t^{r_t} \]. Thus
\[ a = \frac{p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}}{q_1^{r_1} q_2^{r_2} \ldots q_t^{r_t}}. \]

If any of the prime factors in the numerator are equal to any of the prime factors in the denominator of the above expression on the right, then we may cancel them and we will arrive at
\[ \frac{p_1^{f_1} p_2^{f_2} \ldots p_s^{f_s}}{q_1^{g_1} q_2^{g_2} \ldots q_t^{g_t}} \]
where \( f_i \leq k_i \) for all \( i = 1 \ldots s \) and \( g_i \leq r_i \) for all \( i = 1 \ldots t \) and it is possible that some of the exponents \( f_i \) and \( g_i \) are equal to 0 (meaning that \( p_i^{f_i} \) or \( q_i^{g_i} \) are 1). Assuming that all possible cancellations have been performed, it must be true that
\[ \gcd(p_1^{f_1} p_2^{f_2} \ldots p_s^{f_s}, q_1^{g_1} q_2^{g_2} \ldots q_t^{g_t}) = 1. \]

We have thus shown that \( a = \frac{m}{n} \) where \( m \) and \( n \) are relatively prime.

Now we show that there is only one way to write \( a = \frac{m}{n} \) where \( m \) and \( n \) are relatively prime positive integers: To do this, we suppose that
\[ a = \frac{m}{n} = \frac{y}{z} \]
where \( \gcd(m, n) = 1 \) and \( \gcd(y, z) = 1 \). Then since \( mz = ny \) and hence \( ny \) is divisible by \( m \), we see (by Euclid’s Lemma) that \( m \) divides \( y \) and that \( y \) divides \( m \). The fact that \( m \) divides \( y \) tells (and that \( m \) and \( y \) are both positive integers) tell us that \( m \leq y \). Likewise, the fact that \( y \) divides \( m \) tells us that \( y \leq m \). We conclude that \( y = m \). By the same type of reasoning we can conclude that \( z = n \). This shows that there is only one way to write \( a = \frac{m}{n} \) where \( m \) and \( n \) are relatively prime. ■
3 Distribution of the Prime Numbers

A major area of research in mathematics is the question of the distribution of the prime numbers. For each integer \( n \geq 1 \), we can define an integer \( \pi(n) \) as follows

\[ \pi(n) = \text{the number of prime numbers that are less than or equal to } n. \]

Thus, for example, since the prime numbers between 1 and 20 are 2, 3, 5, 7, 11, 13, 17, and 19, we see that

\[
\begin{align*}
\pi(1) &= 0 & \pi(11) &= 5 \\
\pi(2) &= 1 & \pi(12) &= 5 \\
\pi(3) &= 2 & \pi(13) &= 6 \\
\pi(4) &= 2 & \pi(14) &= 6 \\
\pi(5) &= 3 & \pi(15) &= 6 \\
\pi(6) &= 3 & \pi(16) &= 6 \\
\pi(7) &= 4 & \pi(17) &= 7 \\
\pi(8) &= 4 & \pi(18) &= 7 \\
\pi(9) &= 4 & \pi(19) &= 8 \\
\pi(10) &= 4 & \pi(20) &= 8
\end{align*}
\]

A basic problem in number theory is to understand the behavior of the function \( \pi \) and hence to gain an understanding of exactly how many prime numbers there are between 1 and \( n \) for any given positive integer \( n \). Many famous mathematicians have worked on this problem for centuries and some progress has been made. One major piece of progress was made in 1896 when the French mathematician Jacques Hadamard proved the Prime Number Theorem which states (roughly, in a sense to be discussed) that \( \pi(n) \approx n / \ln(n) \) when \( n \) is a large number. More specifically, the Prime Number Theorem states that

\[
\lim_{n \to \infty} \left( \pi(n) \cdot \frac{\ln(n)}{n} \right) = 1.
\]

This means that the ratio of \( \pi(n) \) to \( n / \ln(n) \) gets closer and closer to 1 as \( n \) becomes larger and larger.

Another way to look at the Prime Number Theorem is in terms of the density of prime numbers between 1 and \( n \). This is the quantity \( \pi(n) / n \).
Figure 1: Jacques Hadamard, 1865–1963
Since
\[
\frac{\pi(n)}{n} - \frac{1}{\ln(n)} = \frac{\pi(n) \cdot \ln(n)}{n} \cdot \frac{1}{\ln(n)} \cdot \left(1 - \frac{n}{\pi(n) \cdot \ln(n)}\right)
\]
and since
\[
\lim_{n \to \infty} \frac{\pi(n) \cdot \ln(n)}{n} = 1
\]
\[
\lim_{n \to \infty} \frac{1}{\ln(n)} = 0
\]
\[
\lim_{n \to \infty} \left(1 - \frac{n}{\pi(n) \cdot \ln(n)}\right) = 1 - 1 = 0
\]
we see that
\[
\lim_{n \to \infty} \left(\frac{\pi(n)}{n} - \frac{1}{\ln(n)}\right) = 1 \cdot 0 \cdot 0 = 0.
\]
This tells us that if \(n\) is very large, then the density, \(\pi(n)/n\), of prime numbers between 1 and \(n\) should be approximately equal to \(1/\ln(n)\).

To illustrate the Prime Number Theorem, suppose we take \(n = 7,920\). Then
\[
\frac{1}{\ln(n)} = \frac{1}{\ln(7920)} \approx 0.11139.
\]
Also it is known (thanks to number theorists and computers) that the exact number of prime numbers between 1 and 7,920 is
\[
\pi(n) = \pi(7,920) = 1,000.
\]
Thus
\[
\frac{\pi(7920)}{7920} \approx \frac{1000}{7920} \approx 0.12626.
\]
Thus the actual density of prime numbers between 1 and 7,920 is about 12.63%; whereas the Prime Number Theorem estimates the density to be about 11.14% (an underestimate).

For \(n = 15,485,863\), we have
\[
\frac{1}{\ln(n)} = \frac{1}{\ln(15485863)} \approx 0.0604,
\]
and the exact number of prime numbers between 1 and 15,485,863 is 1,000,000. Therefore
\[
\frac{\pi(15,485,863)}{15,485,863} \approx \frac{1000000}{15485863} \approx 0.0646.
\]
In this case, the Prime Number Theorem predicts a density of about 6.04% and the actual density is about 6.46%.

For $n = 32,452,843$, we have

$$\frac{1}{\ln(n)} = \frac{1}{\ln(32452843)} \approx 0.0578$$

and

$$\pi(n) = \pi(32,452,843) = 2,000,000.$$ 

Thus

$$\frac{\pi(32,452,843)}{32,452,843} \approx \frac{2000000}{32452843} \approx 0.0616.$$ 

Notice that the Prime Number Theorem estimate for $n = 32,452,843$ is actually not as good as the estimate for $n = 15,485,863$. Nonetheless, we know that as $n \to \infty$, the value of $\pi(n)/n$ approaches 0 at the “same rate” that $1/\ln(n)$ approaches 0. We are guaranteed by the Prime Number Theorem that we can make the value of

$$\left| \frac{\pi(n)}{n} - \frac{1}{\ln(n)} \right|$$

be as small as we like by taking the value of $n$ to be large enough.

Although we cannot go any further into the problem of the distribution of prime numbers in this Abstract Algebra course, we can at least use the tools that we have developed to prove the following theorem.

**Theorem 7** There is no largest prime number.

**Proof.** Suppose that there is a largest prime number. Then we could write out a complete list of the prime numbers $2 < 3 < 5 < \ldots < P$ where $P$ is the largest prime number. Now we consider the number

$$Q = 2 \cdot 3 \cdot 5 \cdots P + 1.$$ 

(Thus $Q$ is the product of all of the prime numbers in our list plus 1). Since $Q$ is obviously larger than $P$, then we know that $Q$ cannot be a prime number. This means that $Q$ must be a composite number and hence (by the Fundamental Theorem of Arithmetic) must be divisible by one of the prime
numbers in our list. Call this number $p$. Since $p$ divides $Q$ and $p$ also divides $2 \cdot 3 \cdot 5 \cdot \ldots \cdot P$, and since

$$1 = Q - 2 \cdot 3 \cdot 5 \cdot \ldots \cdot P,$$

we conclude that $p$ divides 1. But this is not possible, since no prime number divides 1.

By assuming that there is a largest prime number $(P)$, we have arrived at a contradiction. We conclude that there is no largest prime number. ■

4 Homework

In Section 1.4 (page 31), do Problems 1–6.