

Primes

Definition: A **prime number** is an integer greater than 1 which is divisible only by 1 and itself, and by no other positive integer. A **composite number** is an integer greater than 1 which is not prime.

A composite number n has a positive divisor other than 1 and itself. This factor must be less than n and greater than 1.

The first few prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 and 37.

The first few composite numbers are 4, 6, 8, 9, 10, 12, 14, 15, 16, 18 and 20.

The integers $4 = 2 \cdot 2$, $12 = 2 \cdot 2 \cdot 3$ and $63 = 3 \cdot 3 \cdot 7$ are all composite because they each have divisors other than 1 and themselves.

THEOREM: Let a , b and c be positive integers. If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

Proof: Since a and b are relatively prime, there are integers x and y so that $ax + by = \gcd(a, b) = 1$. Multiply by c to get $axc + bcy = c$. Clearly $a|axc$. Also, $a|bcy$ by the hypothesis. Therefore, a divides $axc + bcy = c$.

THEOREM: If a prime p divides a product $a_1a_2\cdots a_k$ of positive integers, then it divides at least one of them.

Proof: We use mathematical induction on the number n of factors. If $n = 1$, there is nothing to prove. Assume the statement is true for n factors. Suppose the prime p divides a product of $n + 1$ positive integers $a_1a_2\cdots a_na_{n+1}$. If $p|a_1$, we are done. Otherwise, p is relatively prime to a_1 because p has only the divisors 1 and p , and p doesn't divide a_1 , so $\gcd(p, a_1) = 1$. By the previous theorem, p divides the product $a_2a_3\cdots a_na_{n+1}$ of n factors, and so p must divide one of these n numbers by the induction hypothesis.

The Fundamental Theorem of Arithmetic:

Every integer greater than 1 can be written as a product of primes, perhaps with just one prime, and this product is unique if the primes are written in nondecreasing order.

Suppose the positive integer n is factored into the product of primes, and the primes are in nondecreasing order. The fundamental theorem of arithmetic says that this representation is unique. If we collect repeated prime factors and write them as the power p^e of a prime, we have the following **standard representation**:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = \prod_{i=1}^k p_i^{e_i},$$

where p_1, p_2, \dots, p_k are the primes that actually divide n and $e_i \geq 1$ is the number of factors of p_i dividing n . We make the convention that $n = 1$ has this representation with the empty product.

Definition: For positive real numbers x , let $\pi(x)$ be the number of prime numbers less than or equal to x .

For example, $\pi(1) = 0$, $\pi(10) = 4$ and $\pi(100) = 25$. To use some ciphers, we will have to choose some large primes, say, 100-digit primes. The growth rate of $\pi(x)$ has a strong effect on the difficulty of finding a large prime. Fortunately for cryptography, $\pi(x)$ grows nearly as rapidly as x .

The Prime Number Theorem:

The ratio of $\pi(x)$ to $x/\ln x$ tends to 1 as x goes to infinity. In symbols,

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1.$$

Identifying and Finding Primes

Now that we know there are plenty of large primes, how do we distinguish them from composite numbers? The next theorem tells how to tell in $O(\sqrt{n})$ steps whether n is prime or composite.

THEOREM: If the integer $n > 1$ is composite, then n has a prime divisor $p \leq \sqrt{n}$. In other words, if the integer $n > 1$ has no prime divisor $p \leq \sqrt{n}$, then n is prime.

Proof: Suppose n is composite. Then we can write $n = ab$, where a and b are integers greater than 1. Swap a and b , if necessary, to make $1 < a \leq b < n$. Then $a \leq \sqrt{n}$, for if $a > \sqrt{n}$, then $b \geq a > \sqrt{n}$ and $n = ab > \sqrt{n}\sqrt{n} = n$, which is impossible. By the fundamental theorem of arithmetic a must have a prime divisor $p \leq a \leq \sqrt{n}$. Then p divides n .

The theorem suggests a simple algorithm for testing a small number for primality and for factoring it if it is composite.

[Factoring and Prime Testing by Trial Division]

Input: A positive integer n to factor or to test for primeness.

Output: Whether n is prime, or one or more prime factors of n .

```
 $m = n$   
 $p = 2$   
while ( $p \leq \sqrt{m}$ ) {  
    if ( $m \bmod p = 0$ ) {  
        Print " $n$  is composite with factor  $p$ "  
         $m = m/p$   
    }  
    else {  $p = p + 1$  }  
}  
if ( $m = n$ ) { Print " $n$  is prime" }  
else if ( $m > 1$ )  
{ Print "The last prime factor of  $n$  is  $m$ " }
```