CISC-102
Winter 2016
Lecture 10

Prime Numbers

Definition: A positive integer p > 1 is called a ***prime number*** if its only divisors are 1, -1, and p, -p.

The first 10 prime numbers are:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

Definition: If an integer c > 2 is not prime, then it is ***composite***. Every composite number c can be written as a product of two integers a,b such that a,b $\notin$ {1,-1, c, -c}.

Theorem: Every integer $n > 1$ is either prime or can be written as a product of primes.

For example:

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

17 is prime.

$90 = 2 \times 5 \times 3 \times 3$.

$143 = 11 \times 13$.

$147 = 3 \times 7 \times 7$.

$330 = 2 \times 5 \times 3 \times 11$.

Note: If factors are repeated we can use exponents.

$48 = 2^4 \times 3$.

Theorem: Every integer $n > 1$ is either prime or can be written as a product of primes.

Proof:

(1) Suppose there is an integer k > 1 that is the largest integer that is the product of primes. This then implies that the integer k+1 is not prime or a product of primes.

(2) If k+1 is not prime it must be composite and:

$k+1 = ab,\ a,b \in \mathbb{Z},\ a,b \notin \{1,-1, k+1, -(k+1)\}$.

(3) Observe that $|a| <$ k+1 and $|b| <$ k+1, because a | k+1 and b | k+1. We assume that k+1 is the smallest positive integer that is not prime or the product of primes, therefore |a| and |b| are prime or a product of primes.

(4) Since k+1 is a product of a and b it follows that it too is a product of primes.

(5) Thus we have contradicted the assumption that there is a largest integer that is the product of primes, and we can therefore conclude that every integer n > 1 is either prime or written as a product of primes. □

Mathematical Induction (2nd form)

Let P(n) be a proposition defined on a subset of the Natural numbers (b, b+1, b+2, ...) such that:

i) P(b) is true
(Base)
ii) Assume P(j) is true for all j, $b \leq j \leq k$.
(Induction Hypothesis)
iii) Use Induction Hypothesis to show that P(k+1) is true.
(Induction Step)
NOTE: Go back to all of the proofs using mathematical induction that we have seen so far and replace the assumption:

(1) Assume P(k) is true for $k \geq b$. (*b is the base case*)

with the following assumption:

(2) Assume P(j) is true for all j, $b \leq j \leq k$.

and the rest of the proof can remain as is.

Assumption (2) above is stronger than assumption (1). Sometimes this form of induction is called *strong induction. NOTE: A stronger assumption it makes it easier to prove the result.*

Let P(n) be the proposition:

$\sum_{i=1}^{n} 2^i = 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 2$

Theorem: P(n) is true for all $n \in \mathbb{N}$.

Proof:

Base: P(1) is $2 = 2^2 - 2$ which is clearly true.

Induction Hypothesis: P(j) is true for j, $1 \leq j \leq k$.

Induction Step:

$$\sum_{i=1}^{k+1} 2^i = 2^{k+1} - 2 + 2^{k+1}$$ (because P(k) is true)

$$= 2(2^{k+1}) - 2$$

$$= 2^{k+2} - 2 \qquad \square$$

Theorem: Every integer $n > 1$ is either prime or can be written as a product of primes.

Proof: (Mathematical Induction of the 2[nd] form) Let P(n) be the proposition that all natural numbers $n \geq 2$ are either prime or the product of primes.

Base: n = 2, P(2) is true because 2 is prime.
Induction Hypothesis:
(1) Assume that P(j) is true, for all j, $2 \leq j \leq k$.
Induction Step: Consider the integer k+1.

(2) Observe that if k+1 is prime P(k+1) is true, so consider the case where k+1 is composite. That is: k+1 = ab, $a,b \in \mathbb{Z}$, $a,b \notin \{1,-1, k+1, -(k+1)\}$.
(3) Therefore, $|a| <$ k+1 and $|b| <$ k+1.
So |a| and |b| are prime or a product of primes.
(4) Since k+1 is a product of a and b it follows that it too is a product of primes.
(5) Therefore, by the 2nd form of mathematical induction we can conclude that P(n) is true for all $n \geq 2$. □

Well-Ordering Principle

In our initial proof that shows that integers greater than 2 are either prime or a product of primes we assumed that if that wasn't true for all integers greater than 2, then there was a smallest integer where the proposition is false. (we called that integer k.) This statement may appear to be obvious, but there is a mathematical property of the positive integers at play that makes this true.

Theorem: Well Ordering Principle: Let S be a non-empty subset of the positive integers. Then S contains a least element, that is, S contains an element $a \leq s$ for all $s \in S$.

- Observe that S could be an infinite set.
- Well ordering does NOT apply to subsets of $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$. It is a special property of the positive integers.

NOTE: The Well Ordering Principle can be used to prove both forms of the Principle of Mathematical Induction.

In essence the statement “use the proposition P(k) to show that P(k+1) is true” uses an underlying assumption:

> “Should there be a value of n where the proposition is false then there must be a smallest value of n where the proposition is false”

In all of our induction proofs so far the value k+1 plays the role of that smallest value of n where the proposition may be false. For all other values j, $b \le j \le k$, we can assume that P(j) is true. In the induction step we show that P(k+1) is also true, in essence showing that there is no smallest value of n where the proposition is false. And by well ordering this implies that the result is true for all values of n.

Theorem: There exists a prime greater than n for all positive integers n. (We could also say that there are infinitely many primes.)

Proof: Consider $y = n!$ and $x = n! + 1$. Let p be a prime divisor of x, such that $p \leq n$. This implies that p is also a divisor of y, because n! is the product of all natural numbers from 1 to n. So we have $p \mid x$ and $p \mid y$. According to one of the divisibility theorems we have $p \mid x - y$. But $x - y = 1$ and the only divisor of 1 is -1, or 1, both not prime. So there are no prime divisors of x less than n. And since every integer is either prime or a product if primes, we either have $x > n$ is prime, or there exists a prime p, $p > n$ in the prime factorization of x. □

Theorem: There is no largest prime.

(Proof by contradiction.)

Suppose there is a largest prime. So we can write down all of the finitely many primes as: $\{p_1, p_2, \ldots, p_\omega\}$.

Now let $n = p_1 \times p_2 \times \cdots \times p_\omega + 1$.

Observe that n must be larger the p_ω the largest prime. Therefore n is composite and is a product of primes. Let p_k denote a prime factor of n. Thus we have

$p_k \mid n$

And since $p_k \in \{p_1, p_2, \ldots, p_\omega\}$ we also have

$p_k \mid (n\text{-}1)$

We know that $p_k \mid n$ and $p_k \mid (n\text{-}1)$ implies that $p_k \mid$ n - (n-1) or $p_k \mid 1$. But no integer divides 1 except 1, and 1 is not prime, so $p_k \mid 1$ is impossible, and raises a mathematical contradiction. This implies that our assumption that p_ω is the largest prime is false, and so we conclude that there is no largest prime. □