CS1231 Part 4 - Number Theory

Based on lectures by Terence Sim and Aaron Tan
Notes taken by Andrew Tan
AY18/19 Semester 1

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

1 Mathematical Induction

The Principle of Mathematical Induction is an inference rule concerning a predicate $P(n)$:

Base case:	$P(0)$
Inductive step:	$\forall k \in \mathbb{N}, P(k) \rightarrow P(k+1)$
Conclusion:	$\bullet \forall n \in \mathbb{N}, P(n)$

The steps for using mathematical induction are outlined as such:

1. Identify the predicate $P(n)$. The predicate is a statement that evaluates to true or false. Usually, $n \in \mathbb{N}$, and in any case, we need to qualify the domain of n by saying "For all $n \in \mathbb{N}$" or the respective domain.
2. Prove the **Base case**, P(0). Note that there can be more than one base case, and it need not start at P(0).
3. Prove the **Inductive step**, which is an implication statement involving universal quantification. The usual rules for proving such statements apply here, and should have the following steps:

   For any $k \in \mathbb{N}$:

   3.1 Assume $P(k)$ is true [Denoted as the *Inductive hypothesis*]
   3.2 Consider P(k+1), and break it down into a smaller problem of size k.
   3.3 Apply the inductive hypothesis on the size-k problem.
   3.4 Proceed to show that P(k+1) is true.
4. Write the **Conclusion** (Given that the base case $P(0)$ is true, it follows that $P(1)$ is true and so on.)

1.1 Strong induction

The only difference between Strong Induction and Regular Induction lies only in the Inductive hypothesis.
In Strong Induction, we assume $P(k), P(k-1), P(k-2), \ldots, P(a)$ are *all* true.
Essentially, we're making a stronger assumption about the values of n which make $P(n)$ true, from this stronger assumption, we proceed as before to show that $P(k+1)$ is true.

2 Prime numbers

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n.
An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with

$1 < r < n$ and $1 < s < n$.

Symbolically,

n is prime $\iff$ $\forall$ positive integers r and s, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$

n is composite $\iff$ $\exists$ positive integers r and s such that $n = rs$ and $1 < r < n$ and $1 < s < n$

Clearly, every integer $n > 1$ is either prime or composite.

2.1 The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states that every positive integer greater than 1 can be *uniquely* factorized into a product of prime numbers.

More formally, given any integer $n > 1$, there exists a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$ and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k},$$

and any other expression for n as a product of primes is identical to this except, perhaps, for the order in which the factors are written.

2.2 Primality test

There are multiple tests to see if an integer n is prime.

The most straightforward method is Trial Division, by testing if n is divisible by all integers k between 2 and $\sqrt{n}$.

The Sieve of Eratosthenes is a list of primes that is generated simply by starting with a list C of all integers greater than 1 and $p = 2$, and crossing out all multiples of p, and repeating with the next uncrossed number in C.

The Miller-Rabin primality test is another primality test which determines whether a given number is prime. It relies on a set of equalities that hold true for prime values. However, it is probabalistic, and composites may be passed off as a prime.

2.3 Open questions

There are several open questions concerning prime numbers, and listed below are a few of interest:

Goldbach's Conjecture: Every even integer greater than 2 can be written as a sum of two primes.
Twin Primes Conjecture: There are infinitely many primes p such that $p + 2$ is also a prime.

A Prime properties

A.1 Theorems

Theorem 4.2.3: If p is a prime and $x_1, x_2, \ldots, x_n$ are any integers such that: $p \mid x_1 x_2 \ldots x_n$, then $p \mid x_i$ for some x_i $(1 \le i \le n)$.

Theorem 4.3.5 (Epp): Fundamental Theorem of Arithmetic: Given any integer $n > 1$, there exists a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$ and positive integers $e_1, e_2, \ldots, e_k$ such that $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$, and any other expression for n as a product of primes is identical to this except, perhaps, for the order in which the factors are written.

Theorem 4.7.3 (Epp): The set of primes is infinite.

Prime Number Theorem: The number of primes less than or equal to an integer x is approximately $x/\log(x)$.

A.2 Propositions

Proposition 4.2.2: For any two primes p and p', if $p \mid p'$ then $p = p'$.

Proposition 4.7.3 (Epp): For any $a \in \mathbb{Z}$ and any prime p, if $p \mid a$ then $p \nmid a$ then $p \mid (a+1)$.