MATH145 Readings

Johnson Ng

May 31, 2017

Introduction

Below is an introduction written by the author of the referred notes, Kenneth R. Davidson.

As a student entering university to study mathematics, you probably have encountered prime bumbers. Chances are great that you believe that every integer factors uniquely into a product of primes but have not seen a proof. This important fact, known as the Fundamental Theorem of Algebra, is of crucial importance in the theory of numbers. It is not easy to prove. More importantly, it is not *intuitively obvious*. Indeed, its significance is only realized with very large numbers beyond our real experience. The crucial fact that enables us to prove this with relative ease is the Euclidean Algorithm for finding greatest common divisors. The first two chapters deal with these basic properties of the integers and modular arithmetic.

It is worth noting that there are number systems not very much different from the intergers in which this unique factorization into primes fails. Far from being a disaster, this is an opportunity to investigate why this phenomena occurs. It shows us which properties of the integers themsevles are crucial to make the theory work. That is why we make a foray into quadratic number domains in chapter 3. Naturally, we merely touch the surface here as this theory lies in a rather deep connection between algebra and number theory.

A nice application of modular arithmetic is the Rivest-Shamir-Adelman (RSA) public key cryptography scheme. This code allows the author to publish the method of *encoding* a message in a public place, while keeping the method of *decoding* the message secret. This is a rather different idea of coding, as for all previously known codes, the method of decoding merely reversed the endoing method. The secret here is that it is very easy (with a computer) to find large primes (say 100-200 digits) but very difficult to factor the product of two large primes. If you believe that checking whether a number is prime involes trial division by all numbers up to the square root, it might be hard to imagine why determining if a number if prime should be any easier than finding factors. So we delve more deeply into methods used to determine whether a number is prime or composite. It quickly becomes clear that simple tests can determine beyond any doubt that a number is

composite without giving any information at all about the factors.

In chapter 5, we introduce the complex numbers. There is a tacit assumption that the student is already reasionably familiar with the real numbers from studying calculus. However, a section is devoted to a brief discussion of how the real numbers are developed. No attempt is made to separate algebra from analysis. Indeed, all of mathematics is integrated and it is foolish to pretend that there are natural walls. In particular, we prove the Fundamental Theorem of Algebra that every complex polynomial factors into a product of linear terms. In spite of its name, this is a theorem of analysis because it relies on the (topological) completeness of the complex numbers. The proof we give is one of the simplest, and relies on the Extreme Value Theorem. We also develop the complex exponential function. This again is really a theorem of analysis. But it is included because it plays such an important role in other applications of the compelx numbers.

In chapter 6, we show that the same theory applies to the algebra of polynomials. In particular, there is a Euclidean Algorithm and unique factorization into irreducible polynomials. We exanime various tests for irreducibility, and study connections with irrationality of the roots. Then we do a few special topics about real and complex polynomials such as Sturm's Theorem for counting real roots, and the formula for solving cubics. Then in chapter 7, we study finite fields in some detail. This is just doing modular arithmetic modulo an irreducible polynomial instead of modulo a prime integer. Many of the results for $\mathbb{Z}_p$ carry over to finite fields with the same ideas. A rather beautiful application of these ideas is an algorithm for factoring polynomials over the rationals. This algorithm is based on a method for factoring polynomial of degree d mod p is much easeier than factoring a d digit base p number.

Contents

List of Definitions

List of Theorems

Chapter 1

The Integers

1.1 Basic Properties

The following list of properties is what a student taught in the 'modern' style would come up with when talking about properties of integers.

1. The **integers** consist of a set $\mathbb{Z}$ together with two binary operations **addition** $(+)$ and **multiplication** $(\cdot)$
2. (**commutativity of addition**) $\forall a, b \in \mathbb{Z} \quad a + b = b + a$
3. (**associativity of addition**) $\forall a, b, c \in \mathbb{Z} \quad (a + b) + c = a + (b + c)$
4. (**additive identity**) $\exists 0 \in \mathbb{Z} \ \forall a \in \mathbb{Z} \quad a + 0 = a = 0 + a$
5. (**additive inverse**) $\forall a \in \mathbb{Z} \ \exists (-a) \in \mathbb{Z} \quad a + (-a) = 0$
6. (**commutativity of multiplication**) $\forall a, b \in \mathbb{Z} \quad a \cdot b = b \cdot a$
7. (**associativity of multiplication**) $\forall a, b, c \in \mathbb{Z} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
8. (**multiplicative identity**) $\exists 1 \in \mathbb{Z} \ \forall a \in \mathbb{Z} \quad a \cdot 1 = a = 1 \cdot a$
9. (**distributive law**) $\forall a, b, c \in \mathbb{Z} \ (a + b) \cdot c = a \cdot c + b \cdot c$

But this does not fully distinguish integers from many other sets, for example:

1. The real numbers $\mathbb{R}$
2. The set $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$