MATH342 Review Notes

By Jack 'jryzkns' Zhou

1 The division Algorithm

If $a, b \in \mathbb{Z}$ with $b > 0$, then $\exists!(q, r) \in \mathbb{Z}^1$ s.t.

$$a = bq + r; \quad 0 \leq r < b$$

2 Divisibility and Primes

If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say that a *divides* b if $\exists c \in \mathbb{Z}$ s.t. $b = ac$. We write this relationship as $a \mid b$. If a *does not divide* b, we write $a \nmid b$.
Below are some properties of divisibility, using $a, b, c \in \mathbb{Z}$ and $m, n \in \mathbb{Z}$:

- $a \mid b \wedge b \mid c \to a|c$
- $c \mid a \wedge c \mid b \to c|(ma + nb)$

An integer n is said to have *odd* parity when $n \nmid 2$, and otherwise *even* parity when $n \mid 2$. Often times an odd number can be written in the form $n = 2k + 1$ for some integer k, and $n = 2k$ for even numbers.
A *prime* is an integer greater than 1 thatis divisible by no positive integers other than 1 and itself. Otherwise, a number is said to be a *composite*. Note that by this definition. The number 2 is a prime. Often times there will be indications to exclude 2 from primes by specifying odd primes.
Here are some facts about prime numbers, where $n \in \mathbb{Z}$:

- when $n > 1$, $p \mid n$ for some prime $p \leq n$
- There are infinitely many primes
- If n is composite, then $p \mid n$ for some prime $p \leq \sqrt{n}$

The function $\pi(x)$ where x is a positive real number denotes the number of primes not exceeding x.

Dirichlet's Theorem in Arithmetic Progressons

Suppose that $a, b \in \mathbb{N}$ where $(a, b) = 1$. Then the arithmetic progression $an + b, n \in \mathbb{N}$ contains infinitely many primes.

3 Greatest Common Divisors

The *greatest common divisor* (GCD) of $a, b \in \mathbb{Z}$ is the largest divisor d such that $d \mid a$ and $d \mid b$. The GCD of a and b are often written as $\gcd(a, b)$ or (a, b).
One way to describe the GCD is that a positive integer d is a GCD iff:

- $d \mid a$ and $d \mid b$
- if $c \in \mathbb{Z}$ s.t. $c \mid a$ and $c \mid b$, then $c \mid d$

[1] The symbol $\exists!$ indicates that the existence is unique

Some facts about GCD's:

- Two integers $a, b \in \mathbb{Z}$ are said to be *relatively prime* if $(a, b) = 1$
- Suppose $d = (a, b)$, then $(\frac{a}{d}, \frac{b}{d}) = 1$
- A fraction $\frac{p}{q}$ is in lowest terms when $(p, q) = 1$
- The notion of GCD's applies to multiple values too, suppose $a_1, a_2, \cdots, a_n \in \mathbb{Z}$, then

  $$(a_1, a_2, \cdots, a_n) = (a_1, a_2, \cdots, (a_{n-1}, a_n))$$

  Note that simply with the above definition, $(a_1, a_2, \cdots, a_n) = 1$ means that these numbers are *mutually relatively prime*. A stronger statement is *pairwise relatively prime*, where for any pair of the numbers a_i and a_j with $i \neq j$, $(a_i, a_j) = 1$.

Bezout's Theorem

If $a, b \in \mathbb{Z}$, then $\exists m, n \in \mathbb{Z}$ s.t.

$$ma + nb = (a, b)$$

Where m, n are denoted the bezout coefficients to a, b. Furthermore, $(a, b) = 1 \Leftrightarrow ma + nb = 1$.
The set of linear combinations of a, b is the set of integer multiples of (a, b).

Euclidean Algorithm (+Backtracking)

The Euclidean Algorithm computes (a, b). It proceeds by heavily using a property of GCD's:
Let $b, q, r \in \mathbb{Z}$,

$$(bq + r, b) = (b, r)$$

Suppose $a = bq + r$ (by the division algorithm), we have $(a, b) = (b, r)$. As $0 \leq r < b$, the RHS will always be in lower terms: each time we apply this property, we will get smaller computations to carry out until a base case of $(b, 0)$ is reached, in which case $(b, 0) = b$.
Once the series of division algorithms are applied, the results can be used in reverse with substitution to find the bezout coefficients.
As a side note, suppose we have f_{n+1}, f_{n+2} be successive terms of the Fibonacci Sequence with $n > 1$, then the Euclidean algorithm takes exactly n divisions to show that $(f_{n+1}, f_{n+2}) = 1$.

4 Continued Fraction Expansions

Given the sequence $a_0, a_1, a_2, \cdots$ (may be infinite), a continued fraction is a fraction of the following form

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}$$

A fraction of this form can also be written as $[a_0, a_1, a_2, \cdots]$. If the sequence is infinite and has repeating elements, we denote one instance of the repeating values with a line drawn over it.
The numbers $a_1, a_2, \cdots, a_n$ are called *partial quotients* of the continued fraction, and if all a_i's are integers, the continued fraction is said to be a *simple* continued fraction. We are only concerned with *simple* continued fractions and unless otherwise stated, all continued fractions under discussion are simple.

Finite Continued Fractions

For a rational number that can be expressed as $\frac{p}{q}$, where $p, q \in \mathbb{Z}$ and $p > q$. Its continued fraction expansion is finite. The way to generate the expansion is to consider the division algorithms applies when computing (p, q). For each row, it will be of the form $a = q \cdot b + r$. We apply the following transformation:

$$a = bq + r \Rightarrow \frac{a}{b} = q + \frac{1}{\frac{b}{r}}$$

The $\frac{b}{r}$ term will correspond to the LHS on the next row, recall that the next row would be computing b divided by r, and thus a substitution can be made. We can continuously apply these substitutions until a continued fraction is formed.

Infinite Continued Fractions

For an irrational number n, its continued fraction expansion is computed in the following manner:

$$\begin{aligned} &\alpha_0 = n \\ a_i = [\alpha_i] \quad &\alpha_{i+1} = (\alpha_i - a_i)^{-1} \end{aligned}$$

It's good to note that a_i is the integral component to α_i, and that $\alpha_i - a_i$ is the fractional component to α_i.

Convergents

Given a continued fraction

$$C = [a_0; a_1, a_2, \cdots, a_n]$$

and $C_k = [a_0; a_1, a_2, \cdots, a_k]$ with $0 < k \leq n$, C_k is called the kth convergent of C. Given C, we can compute all of the convergents of C as follows:

$$\begin{array}{lll} p_0 = a_0 & q_0 = 1 & \\ p_1 = a_0 a_1 + 1 & q_1 = a_1 & C_1 = \dfrac{p_1}{q_1} \\ p_k = a_k p_{k-1} + p_{k-2} & q_k = a_k q_{k-1} + q_{k-2} & C_k = \dfrac{p_k}{q_k} \end{array}$$