Notes on notation

sets are denoted with { ... }

$\mathbb{Z}$ set of all integers {..., -2, -1, 0, 1, 2, ...}

$\mathbb{N}$ set of all natural numbers {0, 1, 2, ...}

\{x} means x is not in the set ie. {1, 2, ...} can be denoted as $\mathbb{N}\backslash\{0\}$

$\in$ - element in set

$\exists$ - there exists

$\forall$ - for all

Recurrence Relations

Given a kth order recurrence of the form $a_n = x_1 a_{n-1} + x_2 a_{n-2} + ... + x_k a_{n-k}$, the closed form is $a_n = C_1 r_1^n + C_2 r_2^n + ... + C_k r_k^n$ where $r_1, r_2, ..., r_k$ are solutions to $r^k - x_1 r^{k-1} - x_2 r^{k-2} - ... - x_k = 0$.

For example fibonacci numbers, $F_n = F_{n-1} + F_{n-2}$, have the characteristic polynomial equation, $r^2 - r - 1 = 0$ and the solutions to the equation are $r = \frac{1+\sqrt{5}}{2}$ and $r = \frac{1-\sqrt{5}}{2}$.

Theorems

Addition, multiplication and subtraction are closed $\forall x$; $x \in \mathbb{Z}$.

THM: The Division Algorithm

For $\frac{a}{b}$ where $a \in \mathbb{Z}$ and $b \in \mathbb{N}\backslash\{0\}$, there is some quotient $q \in \mathbb{N}$ and remainder $0 \leq r < b$ such that,

$$a = bq + r$$

b is said to divide a if $r = 0$. We denote this as $b|a$. If b does not divide a we say $b \nmid a$.

THM: Integer Combination “I.C Theorem”

If $d|a$ and $d|b$ then $d|(ax + by)$ for $x, y \in \mathbb{Z}$.

Greatest Common Divisor: We denote gcd(x,y) simply as (x,y)

Notes to self: if in doubt, (x,y) = 1 (ie. 1 is best guess when you are too lazy too compute gcd). Also, (x,0) = x.

THM: Benzout’s theorem:

For $a, b \in \mathbb{Z}$, (a,b) is the smallest positive integer of the form $ax + by$ where $x, y \in \mathbb{Z}$.