An integer $p > 1$ is called a **prime number** if 1 and p are the only positive divisors of p. An integer $n > 1$ is called a **composite number** if n is not a prime number.

Lemma: Any integer $n > 1$ has a prime factor.

Proof by strong induction: Let $P(n)$ be the proposition that $n > 1$ has a prime factor. $n_0 = 2$

Basis of induction: $P(2)$ is true. 2 is a prime factor of 2. so 2 has a prime factor. So $P(2)$ is true.

Inductive step: Suppose that $P(i)$ is true for $2 < i \leq k$. Show that $P(k+1)$ follows.

Consider $k+1 > 2$. If $k+1$ itself is a prime, then we are done because $k+1$ is a product of one prime. (so $k+1$ is a prime factor of $k+1$.)

Suppose $k+1$ is a composite number. Then $k+1 = ab$ for some positive integers $a \geq 2$ and $b \geq 2$.

⋮

$k+1 = a \cdot b \quad (a, b \geq 2)$

Then $a < k+1$ and $b < k+1$.
Then by the induction hypothesis a has a prime factor, say c.
So $k+1 = a \cdot b$ (where c is a prime factor of a).
then c is a prime factor of $k+1$, and we are done.

Repeated application of this procedure yields the following result:

Fundamental Theorem of Arithmetic: Any integer greater than 1 can be expressed as a product of one or more prime numbers.

Example: Prove that for any integer $n \geq 1$, if $x_1, x_2, \ldots, x_n$ are n numbers, then no matter how the parentheses are inserted into their product, the number of multiplications used to compute the product is $n - 1$.

left as an exercise

Example: Suppose that $h_0, h_1, h_2, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3,$$

$$h_k = h_{k-1} + h_{k-2} + h_{k-3}$$

for all integers $k \geq 3$.

$\underset{}{h_3} = \underset{3}{h_2} + \underset{2}{h_1} + \underset{1}{h_0}$

$k=3 \quad h_3 = 6$

$h_4 = h_3 + h_2 + h_1 = 11$

$(k=4) \quad 6 \quad 3 \quad 2$

Prove that $h_n \leq 3^n$ for all integers $n \geq 0$.

$P(n): \quad h_n \leq 3^n, \; n \geq 0$

where $h_0 = 1, \; h_1 = 2$ and $h_2 = 3$

BI: $\quad h_0 = 1 \leq 3^0$ ✓ $\qquad h_2 = 3 \leq 3^2$ ✓

$\qquad h_1 = 2 \leq 3^1$ ✓ $\qquad h_3 = 6 \leq 3^3$ ✓

IS: Suppose that $P(n)$ is true for $0 \leq n \leq k$.

So we supposed that $h_n \leq 3^n$ for $0 \leq n \leq k$.

We want to show that $P(k+1)$ is true, so we want to show that $h_{k+1} \leq 3^{k+1}$.

Consider h_{k+1}. We can write $h_{k+1} = h_k + h_{k-1} + h_{k-2}$ (by the given formula for ~~h_k~~ the sequence h_k.)

By IS $\quad h_k \leq 3^k, \; h_{k-1} \leq 3^{k-1}$ and $h_{k-2} \leq 3^{k-2}$.

So $\quad h_{k+1} = h_k + h_{k-1} + h_{k-2} \leq 3^k + \underset{<3^k}{3^{k-1}} + \underset{<3^k}{3^{k-2}}$

$h_{k+1} \leq 3^k + 3^k + 3^k = 3 \cdot 3^k = 3^{k+1}$

So, $P(k+1)$ is true, which finishes the proof.

Recurrence Relations

We have already seen some recursive relations in this course.

In this section we aim to focus on some special types of recursive relations that we can manipulate algebraically.

A **recurrence relation** is an equation (usually accompanied by some **initial conditions**) that expresses a sequence according to a rule that gives the next term as a function of the previous term(s).

Example: The very famous Fibonacci sequence can be expressed as a recurrence relation $F_n = F_{n-1} + F_{n-2}$ ($n \geq 3$) with the initial conditions $F_1 = 1$ and $F_2 = 2$.

[Space for random blabber about the Fibonacci sequence :)]

$F_1 = 1$ $\quad F_2 = 2$ $\quad F_n = F_{n-1} + F_{n-2}$

$F_3 = F_2 + F_1 = 2+1 = 3$

$F_4 = F_3 + F_2 = 3+2 = 5$

$F_5 = F_4 + F_3 = 5+3 = 8$

1, 2, 3, 5, 8, 13, 21, . . .

Example: (Towers of Hanoi) (maybe inspired by Buddhist temples in Hanoi like this one here)

$n = 3$

– There are n discs, all of different sizes, with holes at their centres (like ~~gramophone records~~ ... ~~CD's?~~ DVD's!).

– There are three vertical poles onto which the discs can slide.

– At the beginning all discs are on the same pole, in order of size with the largest at the bottom, forming a tower.

Goal :

Aim: move one disc at a time (from one pole to another) to eventually arrange the discs in the same order on one of the other poles.

Rule: You are not allowed to put a disc on top of a smaller disc at any step of the game.

Let h_n be the smallest number of moves needed to move n discs.

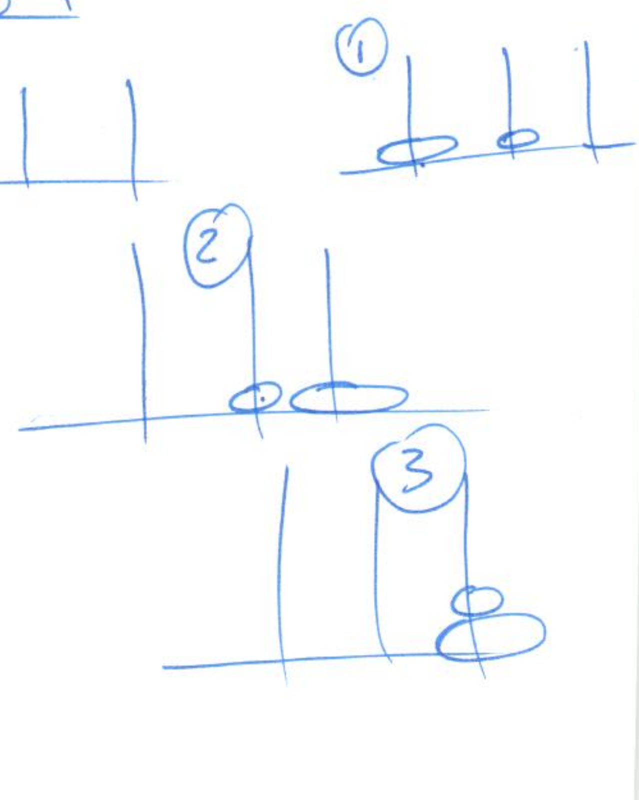
$h_1 = 1$ ✓

$n = 1$

$h_2 = 3$ ✓

$n = 2$

$h_3 = ?$ 7

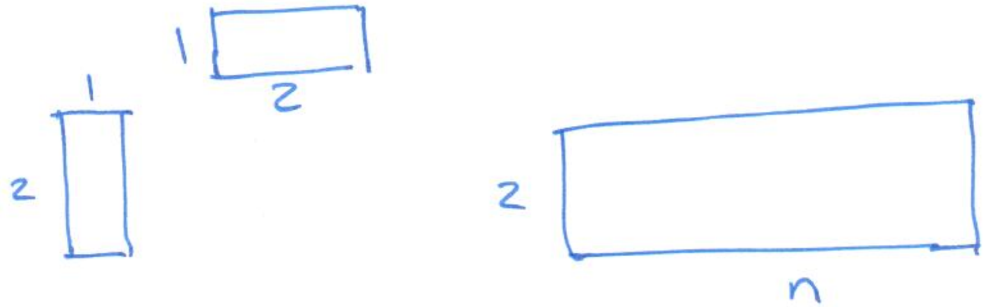


Actually, we can show that $h_n = \dots$

$h_4 = 15$

$h_n = h_{n-1} + 1 + h_{n-1}$

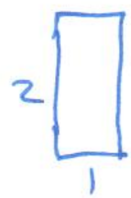
$h_n = 2h_{n-1} + 1$



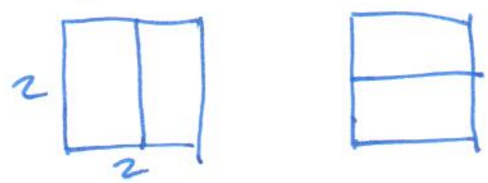
Example: (Paving a Path) A path is 2 meters wide and n meters long. You want to pave it using stones of size 1 meter $\times$ 2 meters. In how many ways can you do this?

Let p_n be the numbers of pavings of the $2 \times n$ path.

$p_1 = 1$

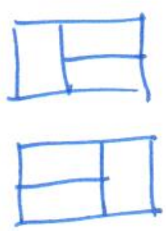


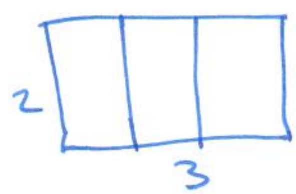
$p_2 = 2$



$p_3 = ?$

3



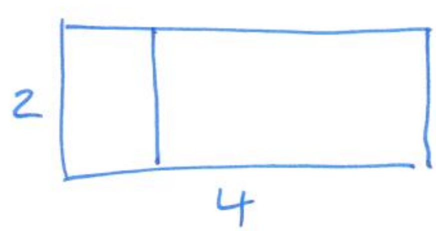


$p_n = p_{n-1} + p_{n-2}$

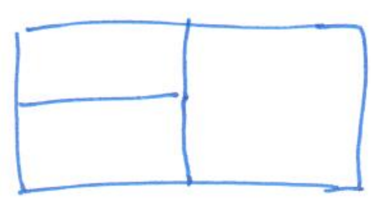
$p_3 = p_2 + p_1$

Find a recurrence relation for p_n. (Hint: We are looking for a **second order recurrence relation**, i.e p_n is given as a function of the previous two terms p_{n-1} and p_{n-2}.)

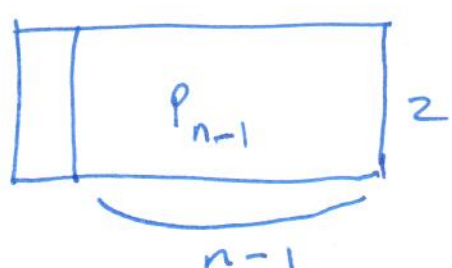
p_4



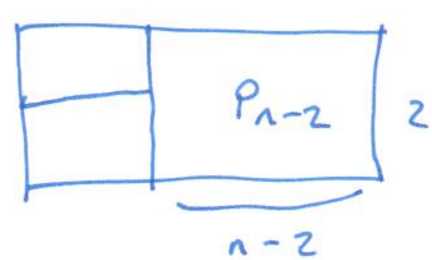
or



p_n



or



So $p_n = p_{n-1} + p_{n-2}$

Solving Recurrence Relations

We want to find an explicit formula to a given recurrence relation rather than having to calculate each term of the sequence one by one.

Defn: A **linear homogeneous recurrence relation of degree** k **with constant coefficients** is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}, \quad (\ddagger)$$

where $c_1, c_2, \ldots, c_k \in \mathbb{R}$ and $c_k \neq 0$.

"Linear" means that $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$ appear in separate terms and to the first power.

"Homogeneous" means that there is no constant term.

"Degree k" denotes that the expression for a_n depends on the previous k terms $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$ (some of these terms may not appear, but a_{n-k} has to).

Such a recurrence relation is completely (and uniquely) determined by the values of the k initial conditions $a_1 = t_1, a_2 = t_2, \ldots, a_k = t_k$.

Examples:

$$a_n = 7a_{n-1} + 8a_{n-2} - 3a_{n-4} + 2a_{n-5}$$

recurrence relation of degree 5