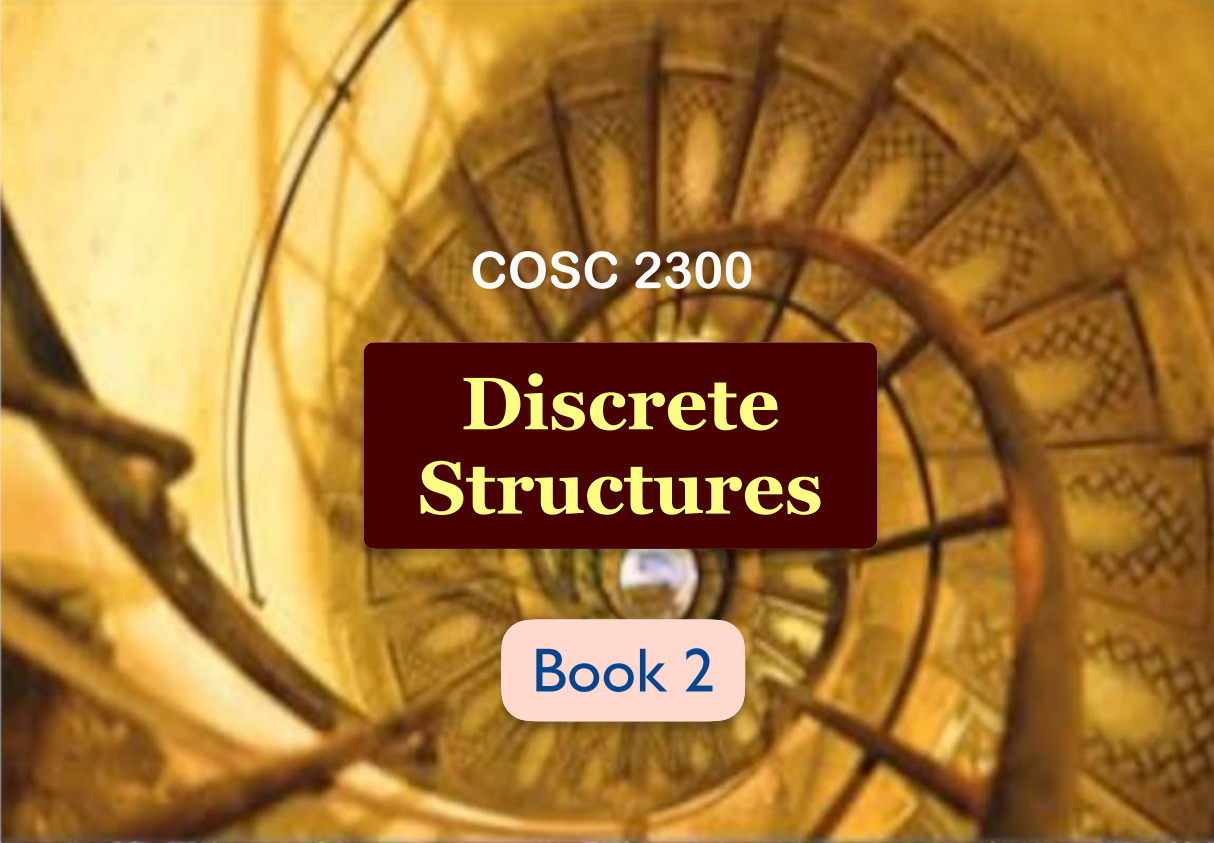

COSC 2300
Discrete Structures
Book 2

If $x, y \in \mathbb{R}$, then the average or mean or arithmetic mean of x and y is $\frac{x+y}{2}$.
Assuming $x, y > 0$, their geometric mean is $\sqrt{xy}$.
eg. the arithmetic mean of 3 and 5 is $\frac{3+5}{2} = 4$; the geometric mean of 3 and 5 is $\sqrt{3 \cdot 5} = \sqrt{15} \approx 3.872983$...

Theorem If $x, y > 0$ then $\underbrace{\sqrt{xy}}_{\text{geometric mean}} \leq \underbrace{\frac{x+y}{2}}_{\text{arithmetic mean}}$. Moreover, equality holds iff $x = y$.

Proof Since $(x-y)^2 \geq 0$ we have $x^2 - 2xy + y^2 \geq 0$ so $x^2 + 2xy + y^2 \geq 4xy$ i.e. $(x+y)^2 \geq 4xy$
So $x + y \geq \sqrt{4xy} = 2\sqrt{xy}$. Finally, $\frac{x+y}{2} \geq \sqrt{xy}$. $\square$

This is a direct proof... but where did the idea come from?

$$\frac{x+y}{2} \geq \sqrt{xy}$$
$$\Leftrightarrow x + y \geq 2\sqrt{xy}$$
$$\Leftrightarrow (x+y)^2 \geq 4xy$$
$$\Leftrightarrow x^2 + 2xy + y^2 \geq 4xy$$
$$\Leftrightarrow x^2 - 2xy + y^2 \geq 0$$
$$\Leftrightarrow (x-y)^2 \geq 0$$

Does the equation $x^2+y^2=22$ have any integer solution(s)? Justify your answer.

Answer: No. Any integer solution (x,y) can be taken from $x,y \in \{0,1,2,3,4\}$ without loss of generality. We consider the value of x^2+y^2 for each (x,y) pair in this set:

$$x^2+y^2 \in \{0,1,2,4,5,8,9,10,13,16,17,18,20,25,32\}$$

so $x^2+y^2 \neq 22$.

We used case analysis.

Scratch:

+	0	1	4	9	16
0	0	1	4	9	16
1	1	2	5	10	17
4	4	5	8	13	20
9	9	10	13	18	25
16	16	17	20	25	32

Does the equation $x^2-y^2=22$ have any integer solution(s)? Justify your answer.

Answer: No. We are asking for integer solutions of $(x+y)(x-y)=22$. Note that $x+y$ and $x-y$ have the same parity (they are both even or both odd since $(x-y)+2y=x+y$.) If $x+y$ and $x-y$ are both odd, then $x^2-y^2=(x+y)(x-y)$ is odd; but if $x+y$ and $x-y$ are both even, then $(x+y)(x-y)$ is a multiple of 4. However, 22 is neither odd nor a multiple of 4.

Diophantine equations: polynomial equations in several variables for which integer (or rational) solutions are required.

There is no algorithm for answering such problems in general.

If α, β are real irrational, can $\alpha+\beta$ be rational? Justify your answer.

Yes, for example $\underbrace{\pi}_{\text{irrational}} + \underbrace{(4-\pi)}_{\text{irrational}} = 4 \in \mathbb{Q}$.

If you don't know that π is irrational then use this example: $\underbrace{\sqrt{2}}_{\text{irrational}} + \underbrace{(4-\sqrt{2})}_{\text{irrational}} = 4 \in \mathbb{Q}$

If α, β are real irrational, can $\alpha\beta$ be rational? Justify your answer.
Yes; for example $\sqrt{2}\cdot\sqrt{2} = 2$.

If α, β are real irrational, can α^β be rational? Justify your answer.

If $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ then we're done. Otherwise $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ and then $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$. This proves that such α, β exist.

Scratch:
Try $\sqrt{2}^{\sqrt{2}}$.

This is a nonconstructive proof of existence of such α, β.

Theorem There exist irrational numbers in $\mathbb{R}$.

Proof Clearly $\mathbb{Q} \subseteq \mathbb{R}$ so $|\mathbb{Q}| \leq |\mathbb{R}|$. If $\mathbb{Q} = \mathbb{R}$ then $|\mathbb{Q}| = |\mathbb{R}|$, contrary to Cantor's theorem that $|\mathbb{Q}| < |\mathbb{R}|$ ($\mathbb{Q}$ is countable but $\mathbb{R}$ is not). $\square$

Proof that e, π are irrational: I have proofs on my website ericmoorhouse.org/handouts)
Actually π and e are transcendental. (stronger than irrational).

e^π is irrational. π^e? Nobody knowns.
$e+\pi$, $e\pi$? We know that at least one of $e+\pi$ and $e\pi$ is irrational. This is known because:

$$(x-e)(x-\pi) = x^2 - (e+\pi)x + e\pi$$

e and π are transcendental: not roots of any polynomial in x with rational coefficients.
Algebraic numbers: roots of polynomials with rational coeffients.
$\frac{3}{5}$ is a root of $x - \frac{3}{5}$ so $\frac{3}{5}$ is algebraic.
$\sqrt{2}$ — — — $x^2 - 2$ … $\sqrt{2}$ is algebraic

there are only countably many algebraic numbers.
Transcendental numbers exist by the same argument as above using cardinality.
1844 Liouville found a transcendental number.

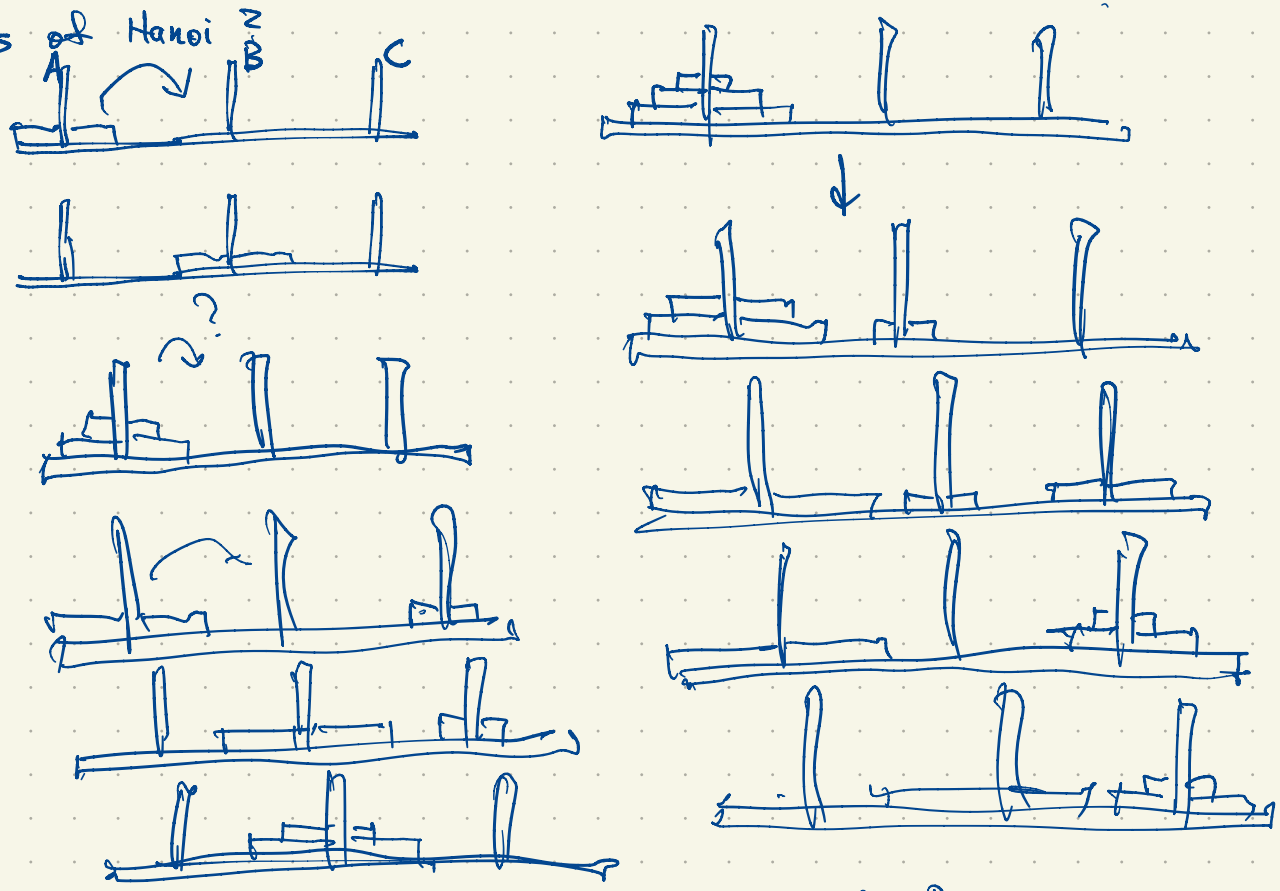
"Is $x^2 \geq 0$ for any real x?" "Any" and "every" are often interchangeable. Not always.

For every $x \in \mathbb{R}$, $x^2 \geq 0$. } Universal quantifier
For any $x \in \mathbb{R}$, $x^2 \geq 0$. }

For some $x \in \mathbb{R}$, $x^2 = 0$. } Existential quantifier

Is any real number transcendental? Yes, for example e and π.
Is every real number transcendental? No, for example $\frac{3}{5}$, $\sqrt{2}$ are algebraic.

Towers of Hanoi



Mathematical Induction and Recursion

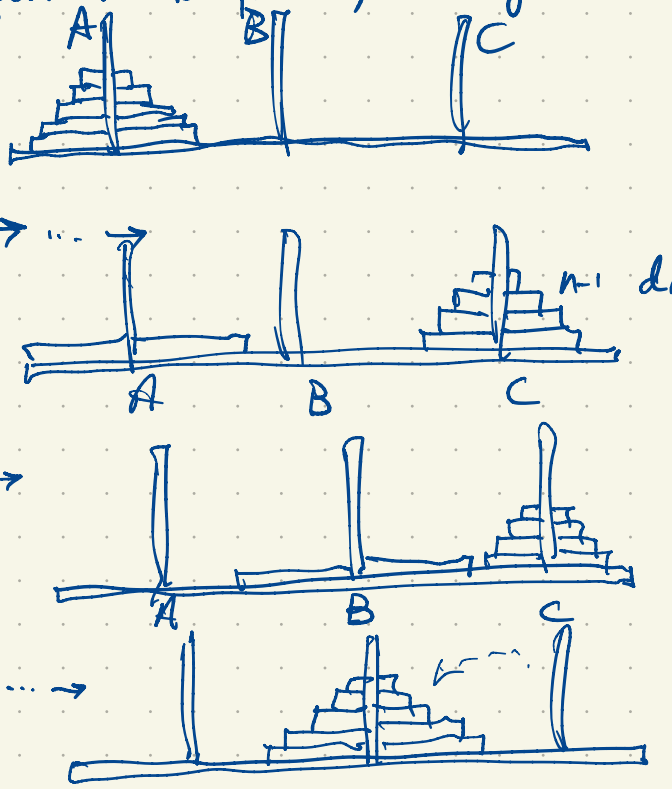
There is an inductive proof that there exists an (recursive) algorithm to move a tower of n disks from one stack to another. Beyond this, we can prove (also by induction) a formula for the number of steps it takes.

Theorem The Towers of Hanoi puzzle has a solution for any number of disks.

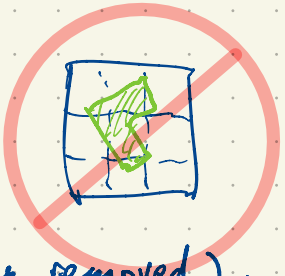
Proof (Initial case) For one disk, simply move the disk from post A to post B.

(General case with $n \geq 2$ disks) Using the previous strategy, we can move the top $n-1$ disks from post A to post C, leaving the largest disk on post A. Then move the largest disk from post A to post B. Then move the smallest $n-1$ disks from post C to post B, again using the strategy for $n-1$ disks. At this point all disks are stacked on post B in the correct order.

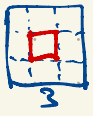
The result of the theorem follows for every $n \geq 1$. □



This is an example of a proof by induction.
See the handout on the course website.



Another example: a tiling problem using  (2 × 2 square with a 1×1 corner removed).
I'll call this shape an L-tile.

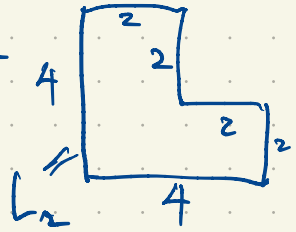


The 3×3 square cannot be tiled using (three) L-tiles.

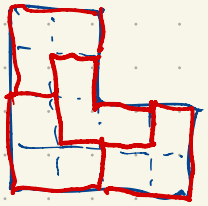
Proof In any tiling of the 3×3 square, we consider how the middle 1×1 square is covered. If this is covered by the middle of an L-tile  then the remaining corner is disconnected from the rest and so it cannot complete to a tiling of the entire 3×3 square. Otherwise, the middle 1×1 square is covered by an "end" of some L-tile (and without loss of generality the tile is oriented as shown).

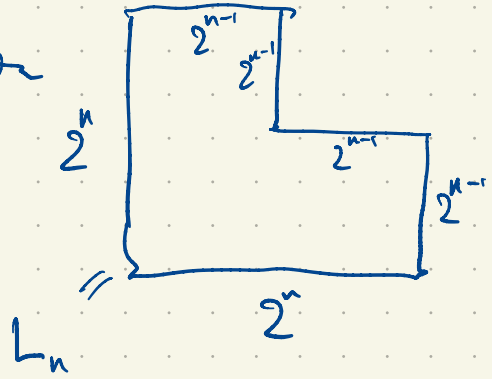


But this leaves another 1×1 square (as shown) that cannot be covered by any L-tile. This proves (by contradiction) that the 3×3 square cannot be tiled using L-tiles. □

The region 

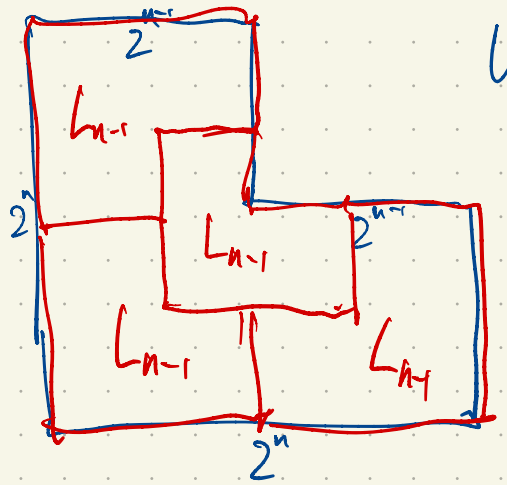
can be tiled using L-tiles, $L = 2\,L_1 = L_1$



Theorem The region 

can be tiled using L-tiles, for every $n \geq 1$.

Proof We prove the result by induction. For $n=1$, the result is trivial: a single L-tile tiles L_1. Now if $n \geq 2$ then we divide L_n into four copies of L_{n-1} as shown:

$L_n =$ 

Use the previous step (called the inductive hypothesis) to tile each of the four L_{n-1}-regions using L-tiles; so the entire L_n-region can be tiled using L-tiles.

□

Formalizing the concept of proof by induction:

Our goal is to prove $(\forall n \geq 1)(P(n))$ i.e. we want to prove

$P(1), P(2), P(3), P(4), \ldots$

This can be accomplished by proving

- $P(1)$ (the initial case); and
- $(\forall n \geq 1)(P(n) \to P(n+1))$.

the inductive step: $P(n)$ is the (inductive) hypothesis of this conditional statement.

Recall: Bitstrings (words of 0's and 1's)

'', '0', '1', '00', '01', '10', '11', ...

There are 2^n bitstrings of length n.

Let a_n be the number of bitstrings of length n having no two consecutive 1's (strings having no substring '11', i.e. 11-free strings)

n	strings	a_n
0	''	1
1	0, 1	2
2	00, 01, 10	3
3	000, 100, 010, 001, 101	5
4	0000, 1000, 0100, 0010, 0001, 1010, 1001, 0101	8
5		13
⋮		⋮

Theorem The sequence $a_0, a_1, a_2, a_3, \ldots$ is defined recursively by

$$a_n = \begin{cases} 1, & \text{if } n = 0; \\ 2, & \text{if } n = 1; \\ a_{n-1} + a_{n-2}, & \text{if } n \geq 2. \end{cases}$$

This is a recursive formula for a_n.

The formula $a_n = a_{n-1} + a_{n-2}$ is called a recurrence relation

Let a_n be the number of 11-free bitstrings of length n.

Theorem $a_n = \begin{cases} 1, & \text{if } n=0; \\ 2, & \text{if } n=1; \\ a_{n-1}+a_{n-2}, & \text{if } n \geq 2. \end{cases}$

Proof This is clear for $n \in \{0,1\}$. So we may assume $n \geq 2$. Every string of length $n \geq 2$ ends in 0 or 01 and so it has the form w0 (concatenation of strings) where w is a 11-free bitstring of length $n-1$; or w01 where w is a 11-free bitstring of length $n-2$. So the total number of 11-free bitstrings of length $n \geq 2$ is

$a_n = a_{n-1} + a_{n-2}$. □

Note: This is a direct proof using cases and subcases.

Compare a_n with the Fibonacci sequence 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ... defined (recursively) by $F_n = \begin{cases} 0, & \text{if } n=0; \\ 1, & \text{if } n=1; \\ F_{n-1}+F_{n-2}, & \text{if } n \geq 2. \end{cases}$

F_n satisfies the same recurrence relation (recurrence formula) as the previous sequence but with different initial terms (starting terms).

Clearly $a_n = F_{n+2}$ for all $n \geq 0$. (although this fact can also be formulated as a proof by induction as follows).

Theorem $a_n = F_{n+2}$ for all $n \geq 2$.

Proof For $n=0,1$ this is clear ($a_0 = 1 = F_2$ and $a_1 = 2 = F_3$). Now assuming $n \geq 2$,

$a_n = a_{n-1} + a_{n-2} = F_{n+1} + F_n = F_{n+2}$. □

by the inductive hypothesis

A stronger form of induction (called strong induction or complete induction) may be useful. This works as follows. We want to prove $(\forall n \geq 1)(P(n))$ i.e. prove $P(1), P(2), P(3), P(4), \cdots$

To do this,

- first prove $P(1)$.
- Then prove $(\forall n)((P(1) \wedge P(2) \wedge \cdots \wedge P(n)) \longrightarrow P(n+1))$.

Test Thurs Oct 29

T	R	
20	22	Oct
27	29	
3	5	Nov
10	12	

We really used this form of induction in our previous example of proof.

Prime numbers 2, 3, 5, 7, 11, 13, 17, ...
A positive integer $p \geq 2$ is prime if p cannot be factored as $p = ab$ for any positive integers $a, b < p$
i.e. $(\forall a \geq 2)(\forall b \geq 2)(p \neq ab)$

Every positive integer has a prime factorization:

Theorem If $n \geq 2$ then $n = p_1 p_2 \cdots p_k$ for some $k \geq 1$ and some primes $p_1, \cdots, p_k$.

Remark This is the "easy" part of the Fundamental Theorem of Arithmetic which says that every $n \geq 2$ has an essentially unique prime factorization.

Proof Let $n \geq 2$. If n is prime then we're done. Otherwise $n = ab$ for some positive integers a, b satisfying $a, b \in \{2, 3, \cdots, n-1\}$. By the inductive hypothesis, $a = p_1 p_2 \cdots p_k$ and $b = q_1 q_2 \cdots q_l$ for some $k, l \geq 1$ and primes $p_1, \cdots, p_k, q_1, \cdots, q_l$. Then $n = ab = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_l$ is a product of primes. The conclusion follows by induction. □

An integer of the form $2k$ is even; and an integer of the form $2k+1$ is odd. Here $k \in \mathbb{Z}$.

Theorem Every integer is either even or odd.

Proof 0 is even by definition since $0 = 2 \cdot 0$. Let $n \geq 1$. (Here all variables are integers.) By induction, $n-1$ is either even or odd. If $n-1 = 2k$ then $n = 2k+1$ is odd; whereas if $n-1 = 2k+1$ then $n = 2(k+1)$ is even. By induction

i.e. by the inductive hypothesis

the conclusion holds for all non-negative integers.

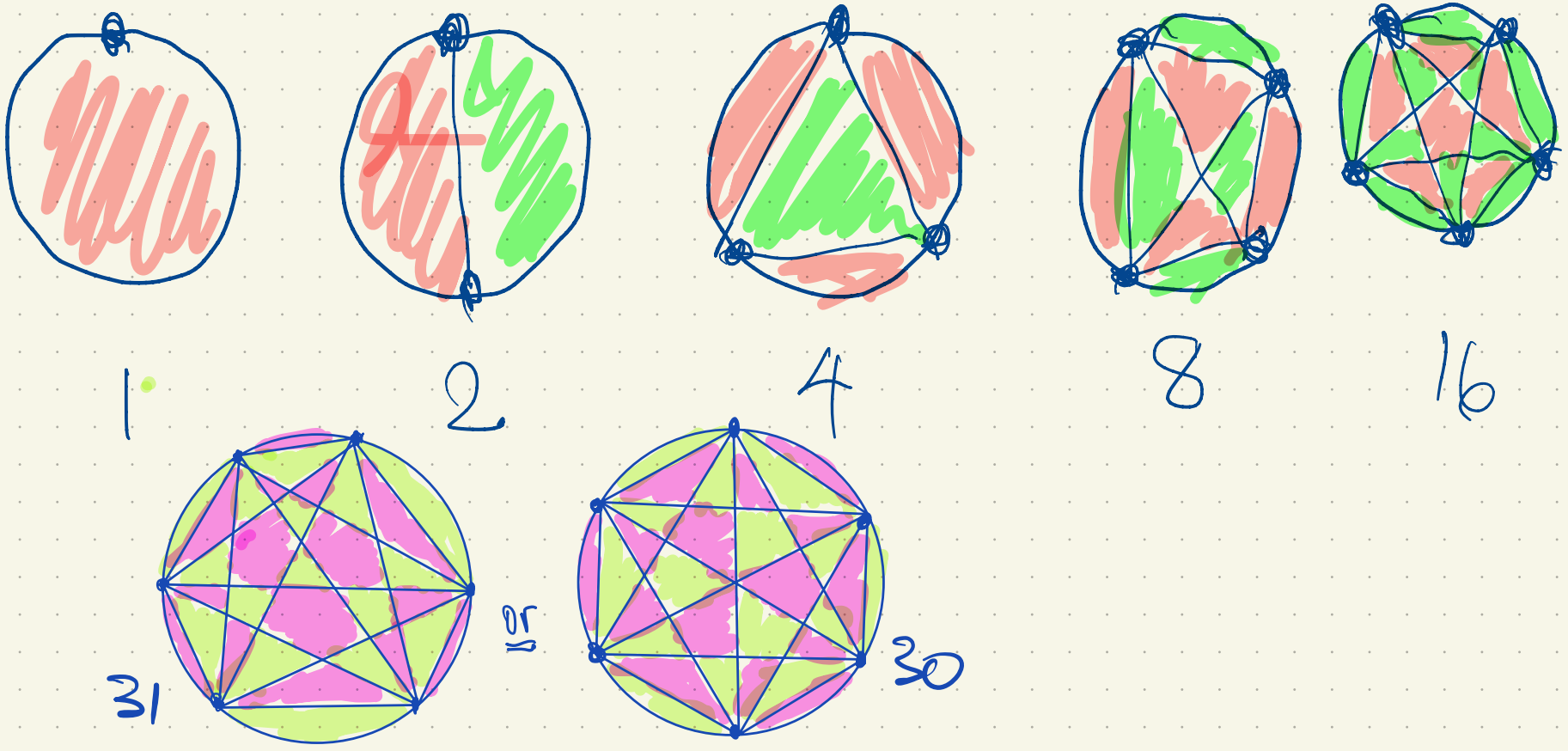
For negative integers: if $n<0$ then $\underbrace{-n}_{|n|} > 0$ so $\underbrace{-n}_{|n|} = 2k$ or $2k+1$ for some $k \in \mathbb{Z}$

so $n = 2(-k)$ or $2(-k-1)+1$ is even or odd. $\square$

In fact the previous 'or' can be made exclusive.

Theorem Every integer is even or odd, but never both.

Proof Let $n \in \mathbb{Z}$. We have shown that n is even or odd. If n is both even and odd then $n = 2k = 2l+1$ for some $k, l \in \mathbb{Z}$ so $\underbrace{2(k-l)}_{\text{integer}} = 1$. This has no solution in $\mathbb{Z}$. $\square$



Fibonacci sequence $F_n = \begin{cases} 0, & \text{if } n=0; \\ 1, & \text{if } n=1; \\ F_{n-1}+F_{n-2}, & \text{if } n \geq 2. \end{cases}$

n	F_n	F_n^2	$F_{n-1}F_{n+1}$
0	0	0	
1	1	1	0
2	1	1	2
3	2	4	3
4	3	9	10
5	5	25	24
6	8	64	65
7	13	169	168
8	21	441	
	⋮	⋮	

Theorem For $n \geq 1$, $F_n^2 - F_{n-1}F_{n+1} = (-1)^{n+1}$

Proof the relation holds for $n=1$ (the initial case). Assuming $F_n^2 - F_{n-1}F_{n+1} = (-1)^{n+1}$ for some $n \geq 1$,

$$\begin{aligned} F_{n+1}^2 - F_n F_{n+2} &= F_{n+1}^2 - F_n(F_{n+1}+F_n) \\ &= (F_{n+1}-F_n)F_{n+1} - F_n^2 \\ &= F_{n-1}F_{n+1} - F_n^2 \\ &= -(F_n^2 - F_{n-1}F_{n+1}) \\ &= -(-1)^{n+1} = (-1)^n \\ &= (-1)^{n+2} \end{aligned}$$

So the theorem holds by induction.

In addition to the recursive formula for F_n, there is a direct (closed) formula using $\tau = \frac{1+\sqrt{5}}{2} \approx 1.618$, $\bar{\tau} = \frac{1-\sqrt{5}}{2} \approx -0.618$

$\tau + \bar{\tau} = 1$, $\tau - \bar{\tau} = \sqrt{5}$

$\tau = \frac{1+\sqrt{5}}{2}$

$\tau^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+5+2\sqrt{5}}{4} = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2}$

$\tau^3 = \left(\frac{3+\sqrt{5}}{2}\right)\left(\frac{1+\sqrt{5}}{2}\right) = \frac{3+5+4\sqrt{5}}{4} = \frac{4+2\sqrt{5}}{2}$

$\tau^4 = \left(\frac{4+2\sqrt{5}}{2}\right)\left(\frac{1+\sqrt{5}}{2}\right) = \frac{4+10+6\sqrt{5}}{4} = \frac{7+3\sqrt{5}}{2}$

$\tau^n = \left(\frac{L_n + F_n\sqrt{5}}{2}\right)$

$\tau^0 = 1 = \frac{2+0\sqrt{5}}{2}$

n	f_n	L_n
0	0	2
1	1	1
2	1	3
3	2	4
4	3	7
5	5	...
6	...	

f_n and L_n have the same recurrence formula

$F_{n+1} = F_n + F_{n-1}$

$L_{n+1} = L_n + L_{n-1}$

$\tau = \frac{1+\sqrt{5}}{2}$

$\bar{\tau} = \frac{1-\sqrt{5}}{2}$

$\tau^n = \frac{L_n + F_n\sqrt{5}}{2}$

$\bar{\tau}^n = \frac{L_n - F_n\sqrt{5}}{2}$

$\tau^n - \bar{\tau}^n = F_n\sqrt{5}$

$F_n = \frac{\tau^n - \bar{\tau}^n}{\sqrt{5}}$ closed formula for F_n.

Both formulas for F_n (recursive and closed) are useful. The recursive formula is easy to implement using a recursive subroutine:

```
Fib := procedure (n)
    if n < 2 then return n;
    return Fib(n-1) + Fib(n-2);
    end;
```

The closed formula has the advantage of providing an understanding of the rate of growth of the sequence (i.e. exponential).

$$F_n = \frac{\tau^n}{\sqrt{5}} - \frac{\bar{\tau}^n}{\sqrt{5}}$$

$$\bar{\tau} = \frac{1-\sqrt{5}}{2} \approx -0.618, \quad |\bar{\tau}| < 1$$

$$\bar{\tau}^n \to 0 \text{ as } n \to \infty$$

$$\left|\frac{\bar{\tau}^n}{\sqrt{5}}\right| < \frac{1}{2}$$

$$F_n = \frac{\tau^n}{\sqrt{5}} \text{ rounded to the nearest integer}$$

n	n^2	2^n
0	0	1
1	1	2
2	4	4
3	9	8
4	16	16
5	25	32
6	36	64
7	49	128
8	64	256

Theorem For all $n \geq 5$, $2^n > n^2$.

We can prove this by induction starting at $n=5$ as our initial case.

Theorem $x^2 - 3y^2 = 4k+3$ has no solution in integers x, y, k.

The simple proof of this relies on x being of the form $4m$ or $4m+1$; Similarly for $-3y^2$

The proof the Theorem does not lend itself to induction.

Theorem For all $n \geq 1$, $1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^n} < 2$.

Proof For $n=0$, the relation holds since $1 < 2$.

Now assuming the relation holds for some $n \geq 0$, i.e.

$$1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} < 2,$$

we must prove $1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} + \frac{1}{2^{n+1}} < 2$.

But if we add $\frac{1}{2^{n+1}}$ to both sides of our inductive hypothesis we obtain $1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} + \frac{1}{2^{n+1}} < 2 + \frac{1}{2^{n+1}}$. which fails to prove the conclusion

By the inductive hypothesis we obtain

$$1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} < 2$$

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^{n+1}} < 1$$

and so

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^{n+1}} < 1 + 1 = 2$$

as required.

The result follows by induction.

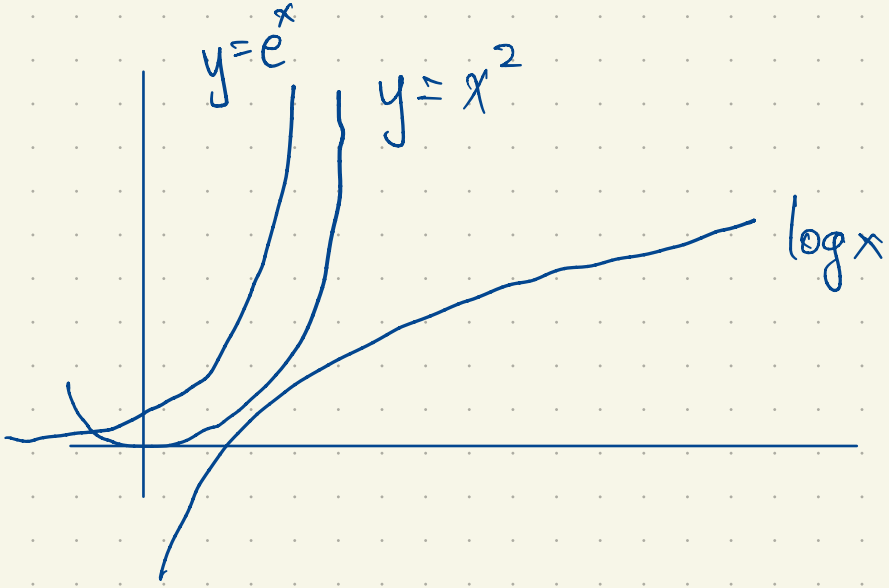
Growth of functions using O-notation: $O, o, \Omega, \sim, \Theta$

$\log x \to \infty$ as $x \to \infty$

$x^k \to \infty$ as $x \to \infty$ for $(k > 0)$

$a^x \to \infty$ as $x \to \infty$ (for $a > 1$)

$\lim_{x \to \infty} a^x = \infty$

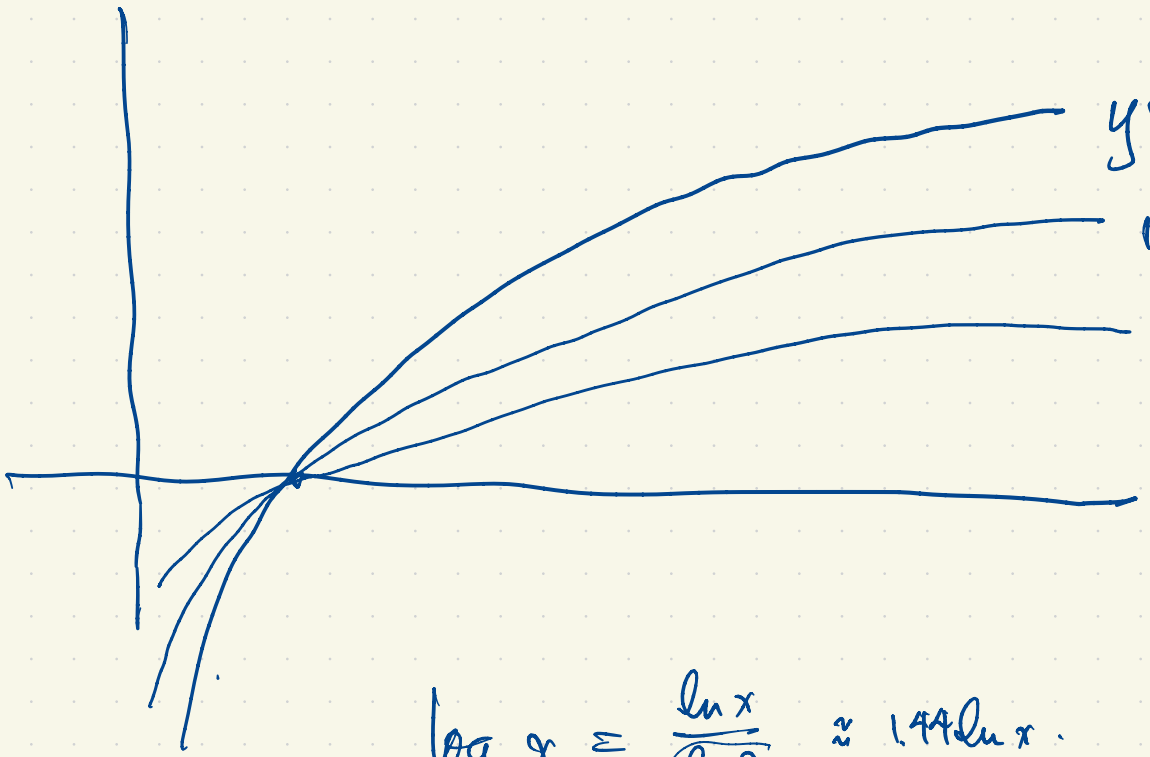


$f(x) \to \infty$ as $x \to \infty$ means:

For all $M > 0$ there exists $a \in \mathbb{R}$ such that for all $x > a$, $f(x) > M$.

$$(\forall M > 0)(\exists a \in \mathbb{R})(\forall x > a)\ (f(x) > M).$$

$\lim_{x \to \infty} f(x) = \infty$ say the same thing.



$$\log_2 x = \frac{\ln x}{\ln 2} \approx 1.44 \ln x.$$

$\ln 2 \approx 0.69$

$$\log_a x = \frac{\ln x}{\ln a}$$

$\ln a$ ← constant

For a positive integer N, the number of decimal digits is in the interval $[\log_{10} N + 1, \log_{10} N + 2)$

Number of decimal digits $= O(\log_{10} N)$

The binary representation of N is about 3.3 times as long ie. $\log_2 N$. ie. $O(\log_2 N) = O(\log_{10} N)$

At this rough scale, we disregard constant factors.

Consider behavior of functions $f(x)$, $g(x)$ as $x \to \infty$. We write

$f(x) = O(g(x))$ if $|f(x)| \leq C|g(x)|$ for all sufficiently large x, where C is some constant

i.e. $(\exists C>0)(\exists a>0)(\forall x>a)(|f(x)| \leq C|g(x)|)$.

Eg. $x^3 + 5x^2 + 100x + 37 = O(x^3)$ as $x \to \infty$

For x sufficiently large, $x^3 + 5x^2 + 100x + 37 \leq 2x^3$.

For us, this is typically understood.

$$\lim_{x\to\infty} \frac{x^3 + 5x^2 + 100x + 37}{x^3} = 1$$

$$\lim_{x\to\infty} \left(1 + \frac{5}{x} + \frac{100}{x^2} + \frac{37}{x^2}\right) = 1 + 0 + 0 + 0 = 1.$$

For x sufficiently large, $\frac{x^3 + 5x^2 + 100x + 37}{x^3} < 2$.

Similarly, $x^3 + 5x^2 + 100x + 37 = O(x^7)$ although this estimate is not as good as $O(x^3)$.

However, $x^3 + 5x^2 + 100x + 37 = O(x^2)$ is false.

Be careful: $O(x^3)$ is not the same as $O(x^7)$ so we cannot strictly read these as equations.

$O(g(x))$ gives upper bounds for rates of growth.
$\Omega(g(x))$ gives lower bounds for - - - - -

$$x^3 + 5x^2 + 100x + 17 = \Omega(x^2)$$

meaning: $|x^3 + 5x^2 + 100x + 17| \geq C|x^2|$ for sufficiently large x
(C is some constant)

$f(x) = \Omega(g(x))$ as $x \to \infty$ means: $(\exists a > 0)(\exists C > 0)(\forall x > a)(|f(x)| \geq C|g(x)|)$

Θ or Θ $\quad$ E

↑ upper case theta
(not lower case θ)

$f(x) = \Theta(g(x))$ as $x \to \infty$ means: $f(x) = O(g(x))$ and $f(x) = \Omega(g(x))$

eg. $x^3 + 5x^2 + 100x + 17 = \Theta(x^3)$

Large integer multiplication
N is a large n-digit number in decimal or binary