GABRIEL MOISE

DISCRETE MATHEMATICS
MT 2018
PROBLEM SHEET 5
Chapters 8 (Orders) and Vacation Revision

5.1. $A = \mathcal{P}(\{1,2,3,4,5,6\})$ with the order $\subseteq$.

(i) Let's suppose that there exists a chain $\{B_1, B_2, \dots, B_m\}$ with $m \geq 8$ ($B_1, B_2, \dots, B_m \in A$).
Let b_i be the number of elements from B_i, where $i \in \{1,2,\dots,m\}$.

Now, if we have $B_i \subseteq B_j \Rightarrow b_i \leq b_j$ (comes from the definition of $\subseteq$).

Also, as all the elements from $\{B_1, B_2, \dots, B_m\}$ are different (as they form a set), we cannot have both $B_i \subseteq B_j$ and $B_j \subseteq B_i$ for $i \neq j$.

Let B_i and $B_j \in \{B_1, B_2, \dots, B_m\}$. Let's suppose that $b_i = b_j$. As we stated that $\{B_1, B_2, \dots, B_m\}$ is a chain, then we have $B_i \subseteq B_j$ or $B_j \subseteq B_i$ (but not both, as we stated above). Let's suppose that $B_j \nsubseteq B_i$, therefore there exists an $x \in B_j$, which $\notin B_i$. From the fact that $B_i \subseteq B_j$, we can say that $b_i \leq b_j$ (we are working on finite sets), but because there are some elements in B_j, which are not in B_i, we conclude that $b_i < b_j$ (so we reach a contradiction).

Therefore, all b_i are different. As all $B_i \in \mathcal{P}(\{1,2,3,4,5,6\}) \Rightarrow b_i \in \{0,1,2,3,4,5,6\}$. However, we have only 7 values that b_i can take and $m \geq 8$, therefore two cardinalities must be equal (at least), and this gets us to the final contradiction.

Therefore, $m \leq 7$.

(ii) We take $m = 7$. As we proved at (i) all cardinalities must be distinct, so the chain must contain: the empty set ($\emptyset$), a set with 1 element, a set with 2 elements, ..., a set with 6 elements ($\{1,2,3,4,5,6\}$).

Let $B_1 = \emptyset$, $B_2 = \{a\}$, $B_3 = \{b,c\}$, $B_4 = \{d,e,f\}$, $B_5 = \{g,h,i,j\}$, $B_6 = \{k,l,m,n,o\}$, $B_7 = \{1,2,3,4,5,6\}$.
As $B_1 \subseteq B_2 \subseteq B_3 \subseteq B_4 \subseteq B_5 \subseteq B_6 \subseteq B_7$ (from the chain property), we can replace the letters:
$B_1 = \emptyset$, $B_2 = \{a\}$, $B_3 = \{a,c\}$, $B_4 = \{a,c,f\}$, $B_5 = \{a,c,f,j\}$, $B_6 = \{a,c,f,j,o\}$, $B_7 = \{1,2,3,4,5,6\}$, where all different letters correspond to different digits from $\{1,2,3,4,5,6\}$.

For a we have 6 choices, for c we have 5 ... for o we have 2 $\Rightarrow$ by the product law we get $6! = 720$ chains with exactly 7 elements.

(iii) Any antichain has the property that no two pairs of elements are comparable. Let M be the antichain we are looking for: $|M| = 20$ and if $A, B \in M$ then $A \nsubseteq B$ and $B \nsubseteq A$. As we proved at (i), if $|A| = |B|$, then $A \subseteq B$ or $B \subseteq A$ only if $A = B$. If not, then they are not comparable. As there are $\binom{6}{3} = 20$ distinct subsets of $\{1,2,3,4,5,6\}$ with exactly 3 elements, we deduce that M contains all of them and nothing else, and is the largest antichain of A.

$\boxed{5.2}$

(i) $S = \{A \mid A$ is a finite set of real numbers$\}$.

$A \preceq B$ if $\max A \leq \max B$

Reflexivity: As $\max A \leq \max A \Rightarrow A \preceq A \Rightarrow \preceq$ is reflexive

Transitivity: Let $a = \max A$
$b = \max B$
$c = \max C$

transitivity of "$\leq$"

From $\left.\begin{array}{l} A \preceq B \Rightarrow a \leq b \\ B \preceq C \Rightarrow b \leq c \end{array}\right| \Rightarrow a \leq c \Rightarrow \max A \leq \max C \Rightarrow A \preceq C \Rightarrow \preceq$ is transitive

Antisymmetry: For $A = \{1, 2\}$, $B = \{0, 2\}$ $A, B \in S$ we have $\max A = \max B = 2 \Rightarrow$

$\left.\begin{array}{l} \Rightarrow \max A \leq \max B \Rightarrow A \preceq B \\ \max B \leq \max A \Rightarrow B \preceq A \\ \text{But, } A \neq B \end{array}\right| \Rightarrow \preceq$ is not antisymmetric.

Therefore, $\preceq$ is a preorder on S.

(ii) $S = \{$all sequences of natural numbers$\}$

$(x_n) \preceq (y_n)$ if $x_i \leq y_i$ for all $i \in \mathbb{N}$

Reflexivity: $(x_n) \preceq (x_n)$ as for all $i \in \mathbb{N}$ we have $x_i \leq x_i \Rightarrow \preceq$ is reflexive

transitivity of "$\leq$"

Transitivity: $\left.\begin{array}{l} (x_n) \preceq (y_n) \Rightarrow (\forall)\, i \in \mathbb{N}\ x_i \leq y_i \\ (y_n) \preceq (z_n) \Rightarrow (\forall)\, i \in \mathbb{N}\ y_i \leq z_i \end{array}\right| \Rightarrow (\forall)\, i \in \mathbb{N}\ x_i \leq z_i \Rightarrow (x_n) \preceq (z_n) \Rightarrow$

$\Rightarrow \preceq$ is transitive

antisymmetry of "$\leq$"

Antisymmetry: We consider $\left.\begin{array}{l} (x_n) \preceq (y_n) \Rightarrow (\forall)\, i \in \mathbb{N}\ x_i \leq y_i \\ (y_n) \preceq (x_n) \Rightarrow (\forall)\, i \in \mathbb{N}\ y_i \leq x_i \end{array}\right| \Rightarrow (\forall)\, i \in \mathbb{N}\ x_i = y_i \Rightarrow (x_n) = (y_n) \Rightarrow$

$\Rightarrow \preceq$ is antisymmetric

Total relation: We consider (x_n) given by: $x_1 = 1$, $x_2 = 2$, $x_i = 7$, $i \geq 3$, $(x_n) \in S$
(y_n) given by: $y_1 = 0$, $y_2 = 3$, $y_i = 7$, $i \geq 3$, $(y_n) \in S$

We don't have $\left.\begin{array}{l} (x_n) \preceq (y_n) \text{ as } x_1 \not\leq y_1 \\ (y_n) \preceq (x_n) \text{ as } y_2 \not\leq x_2 \end{array}\right| \Rightarrow \preceq$ is not a total relation.

Therefore, $\preceq$ is a partial order on S.

For a pair of elements from S, let's say (x_n) and (y_n), the lub is (z_n), where $z_i = \max\{x_i, y_i\}$, $i \geq 1$. It is obvious to prove that $(x_n) \preceq (z_n)$ and $(y_n) \preceq (z_n)$.

Now, if we suppose that there exists $(t_n) \in S$, with $(t_n) \not\succeq (z_n)$ and $(x_n) \preceq (t_n)$, $(y_n) \preceq (t_n)$ we get that $t_i \not\geq \max\{x_i, y_i\}$ for some $i \in \mathbb{N}$ (from $(t_n) \not\succeq (z_n)$) $\Rightarrow t_i > \max\{x_i, y_i\} \Rightarrow t_i > x_i \Rightarrow$ $(x_n) \not\preceq (t_n)$ (so we reach a contradiction).

Therefore, (z_n) is the lub of (x_n) and (y_n) (each element z_i of (z_n) is the maximum of x_i and y_i $\Rightarrow$ easily computable).

(iii) $S = \{1, 2, 3, \dots, 20\}$, the "divides" order "$|$".

<u>Reflexivity</u>: As $x | x$ $(\forall)$ $x \in S$, $|$ is reflexive. $(x = 1 \cdot x)$

<u>Transitivity</u>: If $a, b, c \in S$ with $a | b$ and $b | c \Rightarrow b = ak$, $c = bp \Rightarrow c = a(kp)$, $k \in \mathbb{N}$, $p \in \mathbb{N} \Rightarrow$ $\Rightarrow kp \in \mathbb{N} \Rightarrow a | c \Rightarrow$ $|$ is transitive.

<u>Antisymmetry</u>: If $a, b \in S$ with $\left.\begin{array}{l} a | b \Rightarrow b = ka \\ b | a \Rightarrow a = pb \end{array}\right| \Rightarrow a = pka \Rightarrow \left.\begin{array}{l} kp = 1 \\ k, p \in \mathbb{N} \end{array}\right| \Rightarrow k = p = 1 \Rightarrow a = b \Rightarrow$

$\Rightarrow$ $|$ is antisymmetric

<u>Total relation</u>: We have $7, 11 \in S$ with $7 \nmid 11$ and $11 \nmid 7 \Rightarrow$ $|$ is <u>not</u> a total relation.

Therefore, $|$ is a <u>partial order</u> on S.

If we take for example 7 and 11, then no element x from S satisfies $7 | x$ and $11 | x$ as that would mean that $77 | x$ (as 7 and 11 are coprime) $\Rightarrow x \geq 77$, but $x \in S \Rightarrow x \leq 20$, which is impossible. So, the pair $(7, 11) \in S \times S$ has no least upper bound, so not all pair of elements from $S \times S$ have a least upper bound.

(iv) $S = (0, \infty)$, $x \preceq y$ if $\frac{1}{x} \leq \frac{1}{y}$

As $\frac{1}{x} \leq \frac{1}{y} \Leftrightarrow x \geq y$, we deduce that $\preceq$ is in fact $\geq$.

<u>Reflexivity</u>: $x \geq x$, $(\forall)$ $x \in S \Rightarrow$ $\geq$ is reflexive

<u>Transitivity</u>: If $x \geq y$ and $y \geq z \Rightarrow x \geq z$, which is obviously true $\Rightarrow$ $\geq$ is transitive.

<u>Antisymmetry</u>: If $x \geq y$ and $y \geq x \Rightarrow x = y$, true $\Rightarrow$ $\geq$ is antisymmetric

<u>Total relation</u>: Let's take $x, y \in S$. We can say that $x = y + p$, where $p \in \mathbb{R}$. If $p \geq 0 \Rightarrow$ $\Rightarrow x \geq y$. If $p < 0 \Rightarrow y = x - p$, with $(-p) > 0 \Rightarrow y \geq x \Rightarrow$ $\geq$ is a total relation.

Therefore, $\geq$, which is also $\preceq$, is a <u>linear order</u> on S.

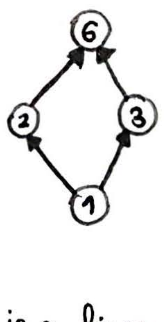
$\preceq$ linear order $\Rightarrow$ $\preceq$ partial order, too.

For $x, y \in S$ we take $z = \min\{x, y\}$. As $x \geq z$ and $y \geq z$, z is an upper bound for $(x, y) \in S \times S$. By considering z' with $z \neq z'$ (or $z < z'$) with $x \geq z'$ and $y \geq z'$, we get that $\min\{x, y\} \geq z'$, or $z \geq z'$ (which contradicts the fact that $z < z'$).

Therefore, $z = \min\{x, y\}$ is the lub of the pair $(x, y) \in S \times S$, which is also easily computable.

$\boxed{5.3}$ Let $A = \{1, 2, 3, 6\}$ be ordered by $|$.

The Hasse diagram looks like:



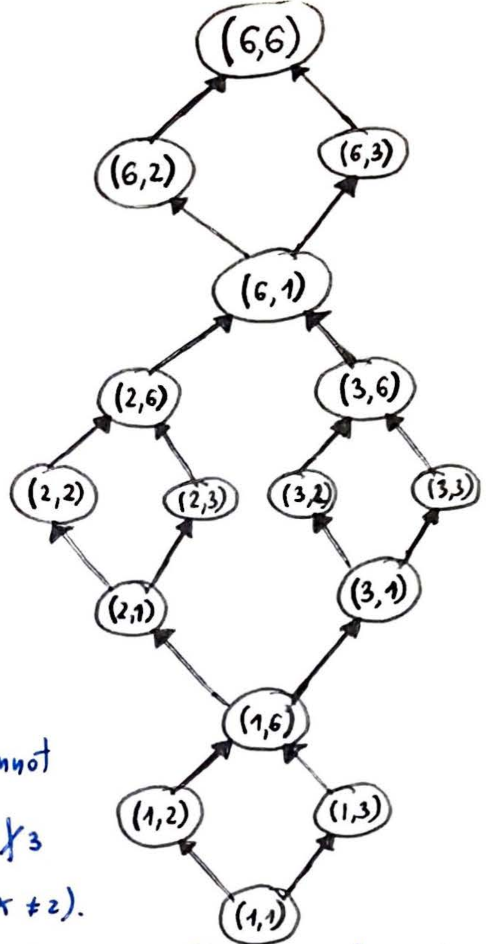
The lexicographic order, $|_L$ is defined by

$(x, y) \ |_L \ (x', y') \Leftrightarrow x | x'$ or $(x = x'$ and $y | y')$

with $(x, y), (x', y') \in A \times A$.

(and $x' \nmid x$, or, as $|$ is a linear order for A, $x \neq x'$)

The Hasse diagram of $|_L$ is:



We want to determine the glb of the following pairs:

(i) $(1,2)$ and $(1,3)$

$(x,y) \,|_L\, (1,2)$ and $(x,y) \,|_L\, (1,3) \Rightarrow \underline{x=1}$ and $y \mid 2$ and $y \mid 3 \Rightarrow y \mid \gcd(2,3)=1 \Rightarrow \underline{y=1}$.

As there is no greater lower bound than $(1,1)$ for $(1,2)$ and $(1,3)$, then $(1,1)$ is their glb.

(ii) $(2,3)$ and $(3,2)$.

$(x,y) \,|_L\, (2,3)$ and $(x,y) \,|_L\, (3,2)$. if $x=6 \Rightarrow$ $\Rightarrow x \nmid 2$, $x \neq 2$ and $x \nmid 3$, $x \neq 3$, so (x,y) cannot be a lower bound. if $x=2 \Rightarrow (x,y) \not|_L (3,2)$ (as $x \nmid 3$ and $x \neq 3$). if $x=3 \Rightarrow (x,y) \not|_L (2,3)$ (as $x \nmid 2$ and $x \neq 2$).

Therefore $x=1$. The greatest (x,y) with $x=1$ is when $y=6$. All other lower bounds have $x=1$, and as $(1,y) \,|_L\, (1,6)$ $(\forall)\, y \in A$, then $(1,6)$ is the glb (we can always observe that in the Hasse diagram, by going in the opposite direction from the 2 pairs until we find a common vertice).

(iii) $(6,2)$ and $(3,3)$

As $(3,3) \,|_L\, (6,2)$, we can easily conclude that $(3,3)$ is the glb of the pair. (a different lower bound would require $(x,y) \,|_L\, (3,3)$, so it cannot be "greater" than $(3,3)$, by definition).

$\boxed{5.4}$ Let $A, B \subseteq \mathbb{R}$ be nonempty and suppose that lub A and lub B exist. We want to prove that

$$\text{lub}\,\{a+b \mid a \in A \text{ and } b \in B\} = \text{lub}\,A + \text{lub}\,B.$$

We begin by noticing that $\leq$ is a linear order on $\mathbb{R}$. Therefore, we can use the definition of lub for linear ordered relations:

$\alpha = \text{lub}\,A \Rightarrow$ (i) $(\forall)\, x \in A$, $x \leq \alpha$ and (ii) $(\forall)\, y \in \mathbb{R}$, if $y < \alpha$ then $(\exists)\, x \in A$ with $y < x$.

$\beta = \text{lub}\,B \Rightarrow$ (i) $(\forall)\, x \in B$, $x \leq \beta$ and (ii) $(\forall)\, y \in \mathbb{R}$, if $y < \beta$ then $(\exists)\, x \in B$ with $y < x$.

Now, we will prove that lub $\{a+b \mid a \in A$ and $b \in B\} = \alpha + \beta$. (we'll say $C = \{a+b \mid a \in A, b \in B\}$)

(i) Let $k \in C \Rightarrow k = a+b$, $a \in A$, $b \in B$.
$\alpha = \text{lub}\,A \Rightarrow a \leq \alpha$
$\beta = \text{lub}\,B \Rightarrow b \leq \beta$
$\Rightarrow a+b \leq \alpha+\beta \Rightarrow k \leq \alpha+\beta$, $(\forall)\, k \in C$.

(ii) Let $y \in \mathbb{R}$, such that $y < \alpha + \beta$.

As $\alpha = \text{lub } A \Rightarrow \alpha = \max A$
$\beta = \text{lub } B \Rightarrow \beta = \max B$ $\Rightarrow \alpha + \beta \in C$ (as $\max A \in A$ and $\max B \in B$).

So, for all $y \in \mathbb{R}$, if $y < \alpha + \beta$, then we found $x = \alpha + \beta \in C$ such that $y < x$.

Therefore, $\alpha + \beta = \text{lub } C$.

REVISION QUESTIONS

$\boxed{5.5}$ We want to prove that

S and T are disjoint $\Leftrightarrow (S \setminus T) \cup (T \setminus S) = S \cup T$ (or $S \oplus T = S \cup T$)

S and T are disjoint $\Leftrightarrow$ (definition of disjoint sets)

$\Leftrightarrow S \cap T = \emptyset \Leftrightarrow$ (Cancellation laws)

$\Leftrightarrow (S \cup T) \setminus (S \cap T) = S \cup T \Leftrightarrow$ (Right-distributivity laws)

$\Leftrightarrow (S \setminus (S \cap T)) \cup (T \setminus (S \cap T)) = S \cup T \Leftrightarrow$ (De Morgan's laws)

$\Leftrightarrow ((S \setminus S) \cup (S \setminus T)) \cup ((T \setminus S) \cup (T \setminus T)) = S \cup T \Leftrightarrow$ (Cancellation laws)

$\Leftrightarrow (\emptyset \cup (S \setminus T)) \cup ((T \setminus S) \cup \emptyset) = S \cup T \Leftrightarrow$ (One law)

$\Leftrightarrow (S \setminus T) \cup (T \setminus S) = S \cup T$. (or $S \oplus T = S \cup T$)

$\boxed{5.6}$ $m, n \in \mathbb{N}_+$

The numbers with exactly m digits are between 10^{m-1} and $10^m - 1$. The first number in that range which is divisible by n is $n \cdot \left\lceil \frac{10^{m-1}}{n} \right\rceil$ (as $n \cdot \left\lceil \frac{10^{m-1}}{n} \right\rceil \geq \cancel{n} \cdot \frac{10^{m-1}}{\cancel{n}} = 10^{m-1}$ and $n \cdot \left(\left\lceil \frac{10^{m-1}}{n} \right\rceil - 1 \right) = n \cdot \left\lceil \frac{10^{m-1}}{n} \right\rceil - n < n \cdot \left(\frac{10^{m-1}}{n} + 1 \right) - n = 10^{m-1}$) and the last number is $n \cdot \left\lfloor \frac{10^m - 1}{n} \right\rfloor$ (as $n \cdot \left\lfloor \frac{10^m - 1}{n} \right\rfloor \leq n \cdot \frac{10^m - 1}{n} = 10^m - 1$ and $n \cdot \left(\left\lfloor \frac{10^m - 1}{n} \right\rfloor + 1 \right) = n \cdot \left\lfloor \frac{10^m - 1}{n} \right\rfloor + n >$
$> n \cdot \left(\frac{10^m - 1}{n} - 1 \right) + n = n \cdot \frac{10^m - 1}{n} = 10^m - 1$).

Therefore, the formula for how many m-digit positive integers are divisible by n is

$$\left\lfloor \frac{10^m - 1}{n} \right\rfloor - \left\lceil \frac{10^{m-1}}{n} \right\rceil + 1.$$

How many 4-digit positive integers are divisible by 6 and 15? We'll choose $m = 4$ and $n = 30$, as for a number to be divisible by 6 and 15, it must be divisible by 30. From our formula, we get

$$\left\lfloor \frac{9999}{30} \right\rfloor - \left\lceil \frac{1000}{30} \right\rceil + 1 = 333 - 34 + 1 = 300$$

Let $nmb(m, n)$ = the number of m-digit positive integers which are divisible by n.

We proved that $nmb(m, n) = \left\lfloor \frac{10^m - 1}{n} \right\rfloor - \left\lceil \frac{10^{m-1}}{n} \right\rceil + 1$.

The number of 4-digit positive integers, which are divisible by 6 or by 15 is equal to:

$nmb(4,6) + nmb(4,15) - nmb(4,30)$.

$nmb(4,6) = \left\lfloor \frac{9999}{6} \right\rfloor - \left\lceil \frac{1000}{6} \right\rceil + 1 = 1666 - 167 + 1 = 1500$

$nmb(4,15) = \left\lfloor \frac{9999}{15} \right\rfloor - \left\lceil \frac{1000}{15} \right\rceil + 1 = 666 - 67 + 1 = 600$

$nmb(4,30) = 300$

So, the answer we want is $1500 + 600 - 300 = 1800$.

We next want to calculate

$nmb(4,6) + nmb(4,15) + nmb(4,10) - nmb(4,30) - nmb(4,30) - nmb(4,30) + nmb(4,30)$

$nmb(4,10) = \left\lfloor \frac{9999}{10} \right\rfloor - \left\lceil \frac{1000}{10} \right\rceil + 1 = 999 - 100 + 1 = 900$.

The answer is $1500 + 600 + 900 - 300 - 300 - 300 + 300 = 2400$.

$\boxed{5.7}$ Let $f: \mathbb{Z} \to \mathbb{Z}$, $f(n) = a_0 + a_1 n + a_2 n^2 + \dots + a_k n^k$, $a_0, a_1, \dots, a_k \in \mathbb{Z}$

(i) For any $m, n \in \mathbb{Z}$ we have

$f(n) - f(m) = (a_0 + a_1 n + a_2 n^2 + \dots + a_k n^k) - (a_0 + a_1 m + a_2 m^2 + \dots + a_k m^k) =$

$= (a_0 - a_0) + a_1 (n - m) + a_2 (n^2 - m^2) + \dots + a_k (n^k - m^k) = \sum_{i=1}^{k} a_i (n^i - m^i) =$

$= \sum_{i=1}^{k} \left(a_i (n-m) \sum_{j=0}^{i-1} n^j \cdot m^{i-j-1} \right) = (n-m) \cdot t$, where $t = \sum_{i=1}^{k} \left(a_i \sum_{j=0}^{i-1} n^j \cdot m^{i-j-1} \right) \in \mathbb{Z} \Rightarrow$

$\Rightarrow (n-m) \mid f(n) - f(m)$ for any distinct integers m and n (we consider them distinct so as not to have $0 \mid f(n) - f(m)$, as we do not work with division by 0).

(ii) We'll prove that if $f(0) = f(3) = 0$, then $1 \notin \mathrm{Im}(f)$.

Let's suppose that $1 \in \mathrm{Im}(f) \Rightarrow (\exists)\, n \in \mathbb{Z}$ such that $f(n) = 1$.

$\left.\begin{array}{l} f(0) = 0 \\ f(n) = 1 \end{array}\right| \overset{(i)}{\Rightarrow} n - 0 \mid f(n) - f(0) \Rightarrow n \mid 1 \Rightarrow n \in \{-1, 1\}$

$\left.\begin{array}{l} f(3) = 0 \\ f(n) = 1 \end{array}\right| \overset{(i)}{\Rightarrow} n - 3 \mid f(n) - f(3) \Rightarrow n - 3 \mid 1 \Rightarrow n \in \{2, 4\}$

$\Rightarrow$ Contradiction (n does not exist).

Therefore, we conclude that $1 \notin \mathrm{Im}(f)$.

$\boxed{5.8}$ The sequence of Catalan numbers (C_m) is defined by the recurrence:

$$C_0 = 1, \quad C_{m+1} = \frac{2(2m+1)}{m+2} C_m \;, \quad m \geq 0$$

(i) $C_1 = \frac{2(2\cdot 0+1)}{0+2} C_0 = \frac{2\cdot 1}{2} \cdot 1 = 1$

$C_2 = \frac{2\cdot(2\cdot 1+1)}{1+2} C_1 = 2$

$C_3 = \frac{2\cdot(2\cdot 2+1)}{2+2} C_2 = 5$

$C_4 = \frac{2\cdot(2\cdot 3+1)}{3+2} C_3 = 14$

(ii) We will prove by induction on n that $C_m = \frac{1}{n+1}\binom{2n}{n}$, $m \geq 0$.

Base case: $S(0)$: $C_0 = \frac{1}{0+1}\cdot\binom{0}{0}$

$1 = 1$ true

Inductive step

iH: We know that $S(k)$: $C_k = \frac{1}{k+1}\binom{2k}{k}$ is true and we'll prove

$S(k+1)$: $C_{k+1} = \frac{1}{k+2}\binom{2k+2}{k+1}$

$$C_{k+1} \overset{\text{recurrence relation}}{=} \frac{2(2k+1)}{k+2}\cdot C_k \overset{\text{iH}}{=} \frac{2(2k+1)}{k+2}\cdot\frac{1}{k+1}\binom{2k}{k} = \frac{2(2k+1)}{(k+1)(k+2)}\cdot\frac{(2k)!}{k!\cdot k!} = \frac{2}{k+2}\cdot\frac{(2k+1)!}{k!\cdot(k+1)!} =$$

$$= \frac{2k+2}{2k+2}\cdot\frac{2}{k+2}\cdot\frac{(2k+1)!}{k!\cdot(k+1)!} = \frac{1}{(k+1)(k+2)}\cdot\frac{(2k+2)!}{k!\cdot(k+1)!} = \frac{1}{k+2}\cdot\frac{(2k+2)!}{(k+1)!(k+1)!} = \frac{1}{k+2}\binom{2k+2}{k+1} \Rightarrow$$

$\Rightarrow S(k+1)$ is true.

Therefore, we proved that $C_m = \frac{1}{n+1}\binom{2n}{m}$, for all $m \in \mathbb{N}$.

(iii) Let p be a prime number such that $p \mid C_m$.

Let's suppose that $p > 2m$ (if $p = 2n$ prime $\Rightarrow n = 1 \Rightarrow 2 \mid C_1 = 1$, which is false)

$p \mid C_m \overset{(ii)}{\Rightarrow} p \mid \frac{1}{n+1}\cdot\binom{2m}{m} \Rightarrow p \mid \frac{(2n)!}{n!\,(n+1)!} = \frac{(n+2)\cdot(n+3)\cdot\ldots\cdot(2n)}{1\cdot 2\cdot\ldots\cdot n}$

As p is prime $\Rightarrow p \mid k \Leftrightarrow k = tp$, where $t \in \mathbb{Z} \overset{p \text{ is prime}}{\Rightarrow} p \nmid n+2,\; p \nmid n+3, \ldots\; p \nmid 2n$, as $p > 2m \Rightarrow p \nmid (n+2)\cdot(n+3)\cdot\ldots\cdot(2n) \Rightarrow p \nmid \frac{(n+2)\cdot(n+3)\cdot\ldots\cdot(2n)}{n!} = C_m$ (which leads to a contradiction).

Therefore, $p < 2n$.

(iv) We'll prove by induction on n that $C_n > 2n-1$, for $n \geq 4$

Base case: $S(4)$: $C_4 > 2\cdot 4-1$

$14 > 7$ true

Inductive step

iH: We know that $S(k)$ is true $\Rightarrow C_k > 2k-1$ and we'll prove $S(k+1)$:

$C_{k+1} > 2k+1 \Leftrightarrow$ (we use the recurrence relation)

$\Leftrightarrow \frac{2(2k+1)}{k+2} C_k > 2k+1 \quad \Big| : (2k+1) \neq 0 \quad \Leftrightarrow$

$\Leftrightarrow \frac{2}{k+2} C_k > 1 \quad \Leftrightarrow$

$\Leftrightarrow \quad C_k > \frac{k+2}{2}$ (we use the iH)

$C_k > 2k-1 > \frac{k+2}{2}$

$\downarrow$

$4k-2 > k+2$

$4k > k+4$

$k > \frac{4}{3}$, true $\Rightarrow C_k > \frac{k+2}{2}$ is true $\Rightarrow C_{k+1} > 2k+1 \Rightarrow S(k+1)$ is true $\Rightarrow$

$\Rightarrow C_n > 2n-1$, for all $n \geq 4$.

(v) Let's suppose that $(\exists) n \in \mathbb{N}$, $n \geq 4$ such that C_n is prime.

$C_n \mid C_n$, C_n is prime $\overset{(iii)}{\Rightarrow} C_n < 2n$

$n \geq 4 \overset{(iv)}{\Rightarrow} C_n > 2n-1$

$\Rightarrow$ Contradiction $\Rightarrow$

$\Rightarrow$ For all $n \geq 4$, C_n is not prime.

$C_0 = C_1 = 1$ are not prime

$C_2 = 2$, which is prime

$C_3 = 5$, which is prime

$\Rightarrow C_2$ and C_3 are the only prime Catalan numbers.

(vi) We'll first write the statement, which is known as true:

(*) There exist nonzero constants b and c such that

$$b n^{n+\frac{1}{2}} e^{-n} \leq n! \leq c n^{n+\frac{1}{2}} e^{-n}, \text{ for all } n \in \mathbb{N}_+$$

We'll prove that $C_n = O\left(4^n n^{-\frac{3}{2}}\right)$

We have $C_n = O(4^n n^{-\frac{3}{2}})$ if there exist $a \in \mathbb{R}$ and $N \in \mathbb{Z}$ with

$$|C_n| \leq a \left| 4^n n^{-\frac{3}{2}} \right| \text{, for all } n \geq N$$

As we work only with positive numbers here, we'll rewrite that as

$$C_n \leq a\, 4^n n^{-\frac{3}{2}} \text{, for all } n \geq N.$$

From (ii), we know that $C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{1}{n+1} \cdot \frac{(2n)!}{n! \cdot n!}$

From (*), we have

$(\exists)$ c such that $(2n)! \leq c(2n)^{2n+\frac{1}{2}} \cdot e^{-2n}$

$(\exists)$ b such that $n! \geq b\, n^{n+\frac{1}{2}} \cdot e^{-n}$ $\Rightarrow$

$$\Rightarrow C_n = \frac{1}{n+1} \cdot \frac{(2n)!}{(n!)^2} \leq \frac{1}{n+1} \cdot \frac{c(2n)^{2n+\frac{1}{2}} \cdot e^{-2n}}{(b n^{n+\frac{1}{2}} \cdot e^{-n})^2} = \frac{1}{n+1} \cdot \frac{c \cdot 2^{2n+\frac{1}{2}} \cdot n^{2n+\frac{1}{2}} \cdot \cancel{e^{-2n}}}{b^2 \cdot n^{2n+1} \cdot \cancel{e^{-2n}}} =$$

$$= \frac{1}{n+1} \cdot \frac{c}{b^2} \cdot \frac{4^n \sqrt{2}}{\sqrt{n}}$$

We want to find $a \in \mathbb{R}$ and $N \in \mathbb{Z}$ such that $C_n \leq a\, 4^n n^{-\frac{3}{2}}$, $(\forall)\, n \geq N$, or

$$\frac{c}{b^2} \cdot \frac{\cancel{4^n}\sqrt{2}}{(n+1)\cancel{\sqrt{n}}} \leq \frac{a \cdot \cancel{4^n}}{n\cancel{\sqrt{n}}}$$

$$\frac{c}{b^2} \cdot \frac{\sqrt{2}}{n+1} \leq \frac{a}{n}$$

if we choose a to be $\frac{2c}{b^2}$, where we already know that b and c always exist for any $n \in \mathbb{N}$, then:

$$\cancel{\frac{c}{b^2}} \cdot \frac{\sqrt{2}}{n+1} \leq \cancel{\frac{c}{b^2}} \cdot \frac{2}{n}$$

$$\frac{\sqrt{2}}{n+1} \leq \frac{2}{n}$$

$$n\sqrt{2} \leq 2(n+1) \quad \Big|^2$$

$$\cancel{2n^2} \leq \cancel{2n^2} + 4n + 2$$

$$0 \leq 4n+2$$

$$-\frac{1}{2} \leq n \text{, true for all } n \geq 0.$$

Therefore, if we choose $a = \frac{2c}{b^2}$, where c and b satisfy

$$(2n)! \leq c \cdot (2n)^{2n+\frac{1}{2}} \cdot e^{-2n} \text{ and } b\, n^{n+\frac{1}{2}} \cdot e^{-n} \leq n!$$

and $N = 0$, we obtained that

$$|C_n| \leq a \cdot \left| 4^n \cdot n^{-\frac{3}{2}} \right| \text{, for all } n \geq N \Rightarrow$$

$$\Rightarrow C_n = O(4^n \cdot n^{-\frac{3}{2}}).$$