1 [6 p]

Given $A = \{a \in \mathbb{N}^+ : a \leq 6\}$, with $\mathbb{N}^+$ as always the natural numbers starting at 1, let us define the following sets (with $a|b$ iff $\exists k(k \in \mathbb{N}^+ \wedge ka = b)$):

$$B = \left\{\frac{a}{b} : a, b \in A\right\}$$
$$C = \left\{\frac{a}{b} : a, b \in A \wedge b|a\right\}$$
$$D = \left\{\frac{a}{b} : a, b \in A \wedge a|b\right\}$$

Give the number of elements in these sets as follows:

1. [2 p] $\#(B) =$ 23
2. [2 p] $\#(C) =$ 6
3. [2 p] $\#(D) =$ 6

Note that the question is about the *cardinality* of sets, so the answers are numbers.

2 [7 p]

Given $A = \{a, b, c, d, e, f\}$, what is

1. [1 p] $\#(\{s \in \mathcal{P}(A) : \#(s) = 0\}) = 1$
2. [1 p] $\#(\{s \in \mathcal{P}(A) : \#(s) = 1\}) = 6$
3. [1 p] $\#(\{s \in \mathcal{P}(A) : \#(s) = 2\}) = 15$
4. [1 p] $\#(\{s \in \mathcal{P}(A) : \#(s) = 3\}) = 20$
5. [1 p] $\#(\{s \in \mathcal{P}(A) : \#(s) = 4\}) = 15$
6. [1 p] $\#(\{s \in \mathcal{P}(A) : \#(s) = 5\}) = 6$
7. [1 p] $\#(\{s \in \mathcal{P}(A) : \#(s) = 6\}) = 1$

3 [8 p]

With $A = \{n \in \mathbb{N}^+ : n \leq 20\}$ and $R = \{(a, b) \in A^2 : a|b\}$ compute the following images of R:

1. [2 p] $R(6) = \{6, 12, 18\}$
2. [2 p] $R(7) = \{7, 14\}$
3. [2 p] $R(2) = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$
4. [2 p] $R(\{2, 5\}) = \{2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18, 20\}$

4 [19 p]

With $A = \{2, 3, 4, 5, 6, 7\}$, $R = \{(a, b) \in A^2 : a > b\}$, and $S = \{(a, b) \in A^2 : a|b\}$. We are looking at the composition $S \circ R$ in this task.

1. [3 p] $\#(S \circ R) = 21$
2. [3 p] $S \circ R(2) = \emptyset$
3. [3 p] $S \circ R(3) = \{2, 4, 6\}$
4. [3 p] $S \circ R(4) = \{2, 3, 4, 6\}$
5. [3 p] $S \circ R(7) = \{2, 3, 4, 5, 6\}$
6. [4 p] $S \circ R$ is ... (circle those that apply)

reflexive symmetric transitive antisymmetric

Many solutions to 2-5 produced sets of tuples, rather than numbers. If you produced one of those, you might want to review the definition of an *image* of a relation.

I marked those answers by making a deduction in the first (otherwise correct) answer, and marking the others by only regarding the right side of the tuples listed.

5 [12 p]

Assume you have an injection $j : A \hookrightarrow B$ and a surjection $s : B \twoheadrightarrow C$.

1. [1 p] Is their composition $s \circ j$ always injective?

   YES NO

2. [5 p] If yes, prove that it is. If no, show a counterexample. (A counterexample involves making the three sets A, B, and C concrete, giving two functions for j and s with the required properties, and showing how their composition is not injective.)

   A = {a, b}, B = {c, d}, C = {e}

   j = {(a, c), (b, d)}, s = {(c, e), (d, e)}

   s*j = {(a, e), (b, e)}

3. [1 p] Is their composition $s \circ j$ always surjective?

   YES NO

4. [5 p] If yes, prove that it is. If no, show a counterexample. (A counterexample involves making the three sets A, B, and C concrete, giving two functions for j and s with the required properties, and showing how their composition is not surjective.)

   A = {a}, B = {c, d}, C = {e, f}

   j = {(a, c)}, s = {(c, e), (d, f)}

   s*j = {(a, e)}

Some counterexamples that people constructed involved s and j that were not, in fact, *functions.* Some folks tried to prove that the composition was injective or surjective, and, obviously, failed, since it isn't.

A lesson here could be that if you are trying to prove something and find you can't, do consider the possibility that what you are trying to show just isn't so. Not always (see 8.4/5), but sometimes.

6 [11 p]

Consider the lower-case alphabet $A = \{"a", ..., "z"\}$ and the set
$C = A \cup \{"(", ")", "\neg", " \vee ", " \wedge "\}$ of characters.
We define a small language $\mathcal{L} \subseteq C^*$ of propositional formulae over the set of variable names $V = A^* \setminus \{\varepsilon\}$, and the following set of rules $R = \{R_1, R_2, R_3\}$ with

$$R_1 = \{(s, "\neg" s) : s \in C^*\}$$
$$R_2 = \{(s_1, s_2, "(" s_1 " \vee " s_2 ")") : s_1, s_2 \in C^*\}$$
$$R_3 = \{(s_1, s_2, "(" s_1 " \wedge " s_2 ")") : s_1, s_2 \in C^*\}$$

such that $\mathcal{L} = R[V]$.

1. [1 p] Show that $\mathcal{L} \subset C^*$ by giving a string $s \in C^*$ such that $s \notin \mathcal{L}$:

   $s = ($

   Hint: Make sure the strings are in $C^* \setminus \mathcal{L}$!

2. [3 p] Give three strings $s_1, s_2, s_3 \in C^* \setminus \mathcal{L}$ such that $(s_1, s_2, s_3) \in R_3$:

   $s_1 =)$
   $s_2 = ($
   $s_3 = () \wedge ()$ Note that $(s_1, s_2, s_3) \in R_3$ -- many solutions missed that point.

3. [7 p] Assume a function $E : V \longrightarrow \{0, 1\}$ that assigns every variable name a value in $\{0, 1\}$. Using **structural recursion**, define an evaluation function $\text{eval}_E : \mathcal{L} \longrightarrow \{0, 1\}$ that interprets the formulae in $\mathcal{L}$ in a way consistent with the usual interpretation of the symbols $\neg$, $\vee$, and $\wedge$ in propositional logic. **Use arithmetic operators (+, -, *, min, max) to compute with the values 0 and 1.**

$$\text{eval}_E : s \mapsto \begin{cases} E(s) & \text{for } s \in V \\ 1 - eval_E(s') & \text{for } s = \neg s' \\ max(eval_E(s_1), eval_E(s_2)) & \text{for } s = (s_1 \vee s_2) \\ min(eval_E(s_1), eval_E(s_2)) & \text{for } s = (s_1 \wedge s_2) \end{cases}$$

In many solutions the eval function could produce values outside of {0, 1} --- for example, if the second clause is simply -eval(s'), it may result in -1, and if the third is eval(s1) + eval(s2), you may get 2 etc.

7 [12 p]

Suppose we have a set A that is **totally ordered** by a relation $<$ on A. A function $f : A \longrightarrow A$ is called *strictly monotonic* iff for any $a, b \in A$ it is the case that $a < b \rightarrow f(a) < f(b)$.

1. [1 p] If a function f is strictly monotonic, does that imply it is **injective**? (circle answer)

   YES NO

2. [5 p] If yes, prove it. If no, provide a counterexample.
   (If you use a counterexample, you may use any totally ordered set that you find convenient, such as the natural/integer/rational/real numbers under the usual arithmetic order.)

   It is to show that $x \neq y$ implies $f(x) \neq f(y)$
   Since $x \neq y$, and A is totally ordered, then either $x < y$ or $y < x$.
   If the former, then $f(x) < f(y)$ and therefore $f(x) \neq f(y)$.
   If the latter, correspondingly.

   Some observed that x<y implies x!=y, which is correct, but in itself not helpful, because you need to show that x!=y implies f(x)!=f(y), so x!=y is the starting point of the proof. To get from there to x<y (or y<x), you need to invoke the *total* order property of <.
   One solution actually interpreted < as non-strict, and thus concluded that a "strictly monotonic" function in the above definition would not be injective. That conclusion is correct, and since I did not explicitly say that < is supposed to be strict, I gave it full marks. (Even if the term "strictly monotonic" and the use of the symbol < might have suggested the intent, the ambiguity ultimately was mine.)

3. [1 p] If a function f is strictly monotonic, does that imply it is **surjective**? (circle answer)

   YES NO

4. [5 p] If yes, prove it. If no, provide a counterexample.
   (If you use a counterexample, you may use any totally ordered set that you find convenient, such as the natural/integer/rational/real numbers under the usual arithmetic order.)

   $f : \mathbb{R} \longrightarrow \mathbb{R}$
   $x \mapsto 2^x$

   f is strictly monotonic, but not surjective.

8 [21 p]

Let us use $\mathbb{P}$ as the name for the set of all prime numbers, that is positive integers greater than 1 that are only divisible by 1 and themselves, so $\mathbb{P} = \{2, 3, 5, 7, 11, 13, ...\}$. You can use $\mathbb{P}$ in answering the following questions, and also the "divides" relation, defined as $a|b$ iff $\exists k(k \in \mathbb{N}^+ \wedge ka = b)$.

1. [3 p] Give a definition of the set F_n of all prime factors of a positive natural number $n \in \mathbb{N}^+$, i.e. all prime numbers that are divisors of n.

   $F_n = \{p \in \mathbb{P} : p|n\}$

2. [6 p] The number *n primorial* is the product of all prime numbers less than or equal to n, i.e. $\prod\{p \in \mathbb{P} : p \leq n\}$. Let us call the function that computes n primorial P, so for example, $P(3) = 2 \cdot 3 = 6$, $P(4) = 2 \cdot 3 = 6$, $P(5) = 2 \cdot 3 \cdot 5 = 30$, $P(6) = 2 \cdot 3 \cdot 5 = 30$, $P(7) = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ and so forth. The first primorial number is defined to be $P(1) = 1$.
   Using **simple recursion**, give a definition of the function $P : \mathbb{N}^+ \longrightarrow \mathbb{N}^+$ computing n primorial for any $n \in \mathbb{N}^+$, as follows:

$$P : n \mapsto \begin{cases} 1 & \text{for } n = 1 \\ P(n-1) & \text{for } n > 1, n \notin \mathbb{P} \\ nP(n-1) & \text{for } n > 1, n \in \mathbb{P} \end{cases}$$

3. [2 p] Is the function $P : \mathbb{N}^+ \longrightarrow \mathbb{N}^+$... (circle the answer)

   (a) injective? YES (NO)

   (b) surjective? YES (NO)

4. [4 p] Using **simple recursion**, define an **injective function** $Q : \mathbb{N}^+ \hookrightarrow \mathbb{P}$.
Use the fact that for any $k \in \mathbb{N}^+$, the number $P(k) + 1$ is a prime number (a so-called *primorial prime*).
Hint: It's NOT as simple as mapping n to $P(n) + 1$. (Make sure you understand why that is)
The reason is that P is not injective, e.g. P(3) = P(4).

$$Q : n \mapsto \begin{cases} P(1) + 1 & \text{for } n = 1 \\ P(Q(n-1)) + 1 & \text{for } n > 1 \end{cases}$$

Many people answered P(n^2) + 1. (Of course that does not result in a recursive definition, but let's forget about this for a moment.) This is based on the realization that just P(n)+1 is not injective because not every n is a new prime, and so in a lot of cases P(n)+1 = P(n+1)+1, making Q not injective. This gave rise to the suspicion/hope that between any n^2 and the next (n+1)^2 there will be at least one prime so that the next Q(n+1) is different from Q(n), making Q injective.

Interestingly, that suspicion has a name, it's called *Legendre's conjecture*, and while it has been around for over a hundred years and is almost certainly true, it hasn't been proven yet. I gave full marks for that answer even if it does not use simple recursion, because it does ("almost certainly") produce an injective Q. However, actually *proving* it injective would involve proving Legendre's conjecture, which, sadly, none of the solutions did (you would have heard about it in the news otherwise).

5. [6 p] Prove that Q above is injective.
You may use the fact that $n \leq P(n)$ for all $n \in \mathbb{N}^+$ without needing to prove it.
Hint: Answering this might become easier if you use a result from a previous task.

Using the result from 7, it is sufficient to show that Q is strictly monotonic, i.e.
$a < b \rightarrow Q(a) < Q(b)$, or alternatively $Q(a) < Q(a + k)$ for $k \geq 1$.

For $k = 1$ we have $Q(a + 1) \overset{(1)}{=} P(Q(a)) + 1 > P(Q(a)) \overset{(2)}{\geq} Q(a)$.

Assuming that $Q(a) < Q(a + k)$, we need to show that $Q(a) < Q(a + k + 1)$.

$Q(a + k + 1) \overset{(1)}{=} P(Q(a + k)) + 1 > P(Q(a + k)) \overset{(2)}{\geq} Q(a + k) \overset{(3)}{>} Q(a)$. QED

(1) definition of Q(n) for n>1 (a+1 and a+k+1 are both >1, because a and k are > 0)
(2) using $n \leq P(n)$
(3) induction hypothesis

Most solutions skipped the induction, and contended themselves with showing that for any n, Q(n) < Q(n+1), waving in the general direction of the transitivity of < to imply monotonicity. I let that one slide and gave it full marks.

9 [7 p]

Let $A = \{a, b, c\}$ and $X = \{x, y\}$, and correspondingly A^* and X^* be the sets of finite sequences in A and X, respectively.

Using recursion over the structure of the sequence, define two **injections** $f : X^* \hookrightarrow A^*$ and $g : A^* \hookrightarrow X^*$, as follows. In both definitions, the first case deals with the empty sequence, the other cases "peel off" the first element in the sequence and the rest of the sequence is called s'.

$$f : s \mapsto \begin{cases} \varepsilon & \text{for } s = \varepsilon \\ af(s') & \text{for } s = xs', s' \in X^* \\ bf(s') & \text{for } s = ys', s' \in X^* \end{cases}$$

$$g : s \mapsto \begin{cases} \varepsilon & \text{for } s = \varepsilon \\ xxg(s') & \text{for } s = as', s' \in A^* \\ xyg(s') & \text{for } s = bs', s' \in A^* \\ yyg(s') & \text{for } s = cs', s' \in A^* \end{cases}$$

There are, of course, many ways of answering here. The important point is that the resulting f and g be injective, and also (which many answers got wrong) that they map to A* and X*, respectively.

10 [4 p]

1. [2 p] Is the composition $f \circ g$ of the two functions defined in the previous task... (circle all that apply)

   injective surjective

2. [2 p] Is the composition $g \circ f$ of the two functions defined in the previous task... (circle all that apply)

   injective surjective

11 [9 p]

Identify free and bound occurrences of variables in the following formula. Put a dot **above** a free variable occurrence, and **below** a bound one.
Note that variable symbols immediately following quantifiers do not count as "occurrences".

free

$$Py \vee \exists z(Qxzy) \rightarrow \forall y(Rxy \leftrightarrow \exists y(Py \rightarrow \forall x(Rzx)))$$

bound

12 [15 p]

Find a DNF for each of the following formulae

1. [5 p] $\neg((r \vee q) \leftrightarrow (q \vee p))$

   $(\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r)$

2. [5 p] $\neg((p \rightarrow q) \vee (q \rightarrow r) \vee (r \rightarrow p))$

   none

3. [5 p] $(p \rightarrow q) \wedge (q \rightarrow r) \wedge (r \rightarrow p)$

   $(p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$

   Quite a few solutions produced formulae that were not, in fact, in DNF.