Exercises 5 — induction and recursion

1.

Show by simple induction that for every positive integer n, $5^n - 1$ is divisible by 4.
(SLAM Exercise 4.1)

Basis, n = 1:

$5^1 - 1 = 4$, which is divisible by 4.

Induction step from n to n+1:

Assuming that $5^n - 1$ is divisible by 4, i.e. there is an integer k such that $4k = 5^n - 1$, we need to show that so is $5^{n+1} - 1$, i.e. for some integer k' we have $4k' = 5^{n+1} - 1$.

$5^{n+1} - 1 = 5 \cdot 5^n - 1 = 5 \cdot 5^n - 5 + 5 - 1 = 5(5^n - 1) + 4 = 5(4k) + 4 = 20k + 4 = 4(5k + 1)$
So $k' = 5k + 1$ exists and is an integer. QED

2.

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. 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:

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

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

   (a) injective? YES NO

   (b) surjective? YES NO

3. 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).

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

   One common answer here is 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, so far nobody did (you might have heard about it in the news otherwise).

4. 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.

   Showing the Q is injective, we need to show that for all $a, b \in \mathbb{N}^+$ we have $a \neq b \Rightarrow Q(a) \neq Q(b)$. Now if $a \neq b$ we can assume without loss of generality that $a < b$. We will show that this implies that $Q(a) < Q(b)$, as this implies that $Q(a) \neq Q(b)$. In other words we will show that Q is *strictly monotonic*.
   So now we need to show that $a < b \rightarrow Q(a) < Q(b)$, or alternatively $Q(a) < Q(a + k)$ for $k \geq 1$.

   For $k = 1$ we have $Q(a + 1) = P(Q(a)) + 1 > P(Q(a)) \geq Q(a)$. (because of (1) and (2))

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

$Q(a) < Q(a+k) < Q(a+k+1)$ (using the induction hypothesis and the base case)

(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.

Recall that $\{0,1\}^*$ is the set of all finite sequences of 0s and 1s. Define an **injective** function $f : \{0,1\}^* \hookrightarrow \mathbb{N}$.

Keep in mind that sequences of 0s and 1s may start and end with any number of 0s, so interpreting the string simply as a binary number is not going to result in an injective function, because 00100100 and 100100 would be mapped to the same natural number.

Use recursion over the structure of the sequence, as follows. The first case deals with the empty sequence, the other two cases "peel off" the first element in the sequence and the rest of the sequence is called s'.

$$f : s \mapsto \begin{cases} 1 & \text{for } s = \varepsilon \\ 2f(s') & \text{for } s = 0s', s' \in \{0,1\}^* \\ 2f(s') + 1 & \text{for } s = 1s', s' \in \{0,1\}^* \end{cases}$$

4.

As above, $\{0,1\}^*$ is the set of all finite sequences of 0s and 1s. Define an **injective** function $g : \mathbb{N} \hookrightarrow \{0,1\}^*$.

Use recursion over $\mathbb{N}$, as follows. The first case deals with 0, the other with positive numbers, where you can use the values for smaller numbers.

$$g : n \mapsto \begin{cases} \varepsilon & \text{for } n = 0 \\ 0g(n-1) & \text{for } n > 0 \end{cases}$$

5.

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 that they map to A* and X*, respectively.

6.

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

   $s = ($

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

   $s_1 =)$
   $s_2 = ($
   $s_3 = () \wedge ()$

3. 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 $\neg$ (not), $\vee$ (or), and $\wedge$ (and) in propositional logic. **Use arithmetic operators (+, -, *, min, max) to compute with the values 0 and 1.**

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

7.

Suppose we have a set of five characters $C = \{"a", "b", "(", ")", ","\}$, the set $S = \{"a", "b"\}$ consisting only of the letters a and b, and a relation $R = \{(s_1, s_2, "("s_1", "s_2")") : s_1, s_2 \in C^*\}$.

As you can see, R is a 3-place relation. Let us define a function $F : \mathcal{P}(C^*) \longrightarrow \mathcal{P}(C^*)$ such that

$$F : X \mapsto R(X \times X)$$

In other words, $F(X) = \{y : x_1, x_2 \in X, (x_1, x_2, y) \in R\}$.

Now let $F^n(X)$ be the set that results from applying F to some set $X \subseteq C^*$ n times in a row, with $F^0(X) = X$, $F^1(X) = F(X)$, $F^2 = F(F(X))$ and so forth, so that $F^{n+1}(X) = F(F^n(X))$.

1. Give an element in $F^0(S)$: a

2. Give an element in $F^1(S)$: (a,b)

3. Give an element in $F^2(S)$: ((a,b),(b,a))

4. Suppose $U = \bigcup_{n \in \mathbb{N}} F^n(S)$.

   Give an element in $R[S] \setminus U$, or write "none" if no such element exists: (a,(a,b))

8.

Suppose we have a set A partially ordered by a strict order $<$. What would you need to show in order to demonstrate that $(A, <)$ is **not** well-founded? (in English/Swedish)

An infinite descending chain in A. [or]
A non-empty subset of A without a minimal element.

9.

1. Is the set $\mathcal{P}(\mathbb{Q})$ under strict set inclusion $\subset$ well-founded? (circle answer)

   YES NO

2. Prove it or provide a counterexample.

   $S = \left\{ \left[0, \frac{1}{n}\right] : n \in \mathbb{N}^+ \right\}$

   S has no minimal element, since for any $\left[0, \frac{1}{n+1}\right] \subset \left[0, \frac{1}{n}\right]$ for any $n \in \mathbb{N}$.

3. Is the set $\mathcal{P}(\mathbb{N})$ under strict set inclusion $\subset$ well-founded? (circle answer)

   YES NO

4. Prove it or provide a counterexample.

   $S = \{\{i : i \in \mathbb{N}^+, i > n\} : n \in \mathbb{N}^+\}$
   S has no minimal element, since $\{i : i \in \mathbb{N}^+, i > n+1\} \subset \{i : i \in \mathbb{N}^+, i > n\}$ for every $n \in \mathbb{N}$.

   It's also possible to make a more "abstract" argument here that reuses the result from the previous task. Since $\mathbb{N} \sim \mathbb{Q}$, there is a bijection $b : \mathbb{Q} \longleftrightarrow \mathbb{N}$. Then the set $S' = \{b(s) : s \in S\}$ has no minimal element under set inclusion, because S has no minimal element and $s \subset s' \Leftrightarrow b(s) \subset b(s')$.

10.

Let the set $\mathbb{S}$ be the set of all finite strings consisting of lower-case characters from a to z, including the empty string "". So, for example, "abc", "string", and "ordered" are all members of $\mathbb{S}$.
The *length* of a string is the number of characters in it. We shall use $\text{len}(s)$ for the number of characters in s. Note that $\text{len}(\text{""}) = 0$.

Let < be the **strict prefix order** on $\mathbb{S}$. This means that for any two strings s and t, we have $s < t$ if and only if s is a proper prefix of t, i.e. t starts with s and then contains at least one more character. For example, $\text{"}abc\text{"} < \text{"}abcd\text{"}$ and $\text{""} < \text{"}xyz\text{"}$, but $\text{"}abc\text{"} \not< \text{"}abc\text{"}$, $\text{"}ab\text{"} \not< \text{"}xyz\text{"}$ and of course $\text{"}xyz\text{"} \not< \text{""}$.

Note that for any two strings s and t, it is always the case that $s < t \Rightarrow \text{len}(s) < \text{len}(t)$.

1. $(\mathbb{S}, <)$ is partially / totally ordered (circle the one that applies).

   (For the purposes of this question, "partially" should be understood as the opposite of "totally", rather than as its generalization.)

2. Is $(\mathbb{S}, <)$ well-founded? (circle answer)

   YES NO