Question 1. [9 MARKS]

Consider the following recursive definition of a set S of strings.
Notice that each string contains only the characters "a" and/or "b".
We use the Python syntax $s + t$ to mean the concatenation of strings s and t.

1. "a" $\in S$.
2. If $s \in S$ and $t \in S$, then "b" $+ s + t \in S$ and $s + t +$ "b" $\in S$.

Part (a) [1 MARK]

Write 4 examples of strings in S.

$a, baa, bbaaa, baabaab$

Part (b) [8 MARKS]

For each string s, let $P(s)$ be defined as: s has more "a"s than "b"s.
Use structural induction on the definition of S to prove: $\forall s \in S, P(s)$.
Clearly indicate where you use your Induction Hypothesis.

Let u be an arbitrary element of S. Assume $P(u')$ holds for every $u' \in S$ that is structurally smaller than u (i.e. u' can be generated with fewer applications of the rules defining S than can u.)

Case 1: $u \in S$ by rule 1. So $u =$ "a", which has one more "a" than "b".

Case 2: $u \in S$ by rule 2.

Case 2.a) $u =$ "b" $+ s + t$ for some $s, t \in S$. By the IH on s and t (since they are structurally smaller than u), s and t each have at least one more "a" than "b"s. So $s + t$ has at least two more "a"s than "b"s. So "b" $+ s + t = u$ has at least one more "a" than "b"s.

Case 2.b) $u = s + t +$ "b" for some $s, t \in S$. Same reasoning as in Case 2.a.

Question 2. [13 marks]

```
# PREcondition: m and n are positive natural numbers.
def f(m, n):
  r = m
  s = n
  while r != s:
    if r < s:
      s = s - r
    else:
      r = r - s
  return r
```

Let r_i, s_i be the values of r and s just before the i-th iteration of the loop, where $r_0 = m, s_0 = n$ are the initial values. The sequences are finite iff the loop terminates after some $t \geq 0$ loop iterations, and in that case we define the final, t-th elements of the sequences to be the values of r and s just after the last iteration.

Part (a) [1 mark]

Fill in the following table, showing the sequence of values for r and s when f(30, 42) is executed:

loop iteration number	r_i	s_i
(before loop) 0	30	42
1	30	12
2	18	12
3	6	12
4	6	6

Part (b) [1 mark]

List all positive natural numbers c such that both of 30 and 42 are multiples of c:

1, 2, 3, 6

Part (c) [1 mark]

State a variant (measure) for the loop: a combination of the values of the variables, that is always a natural number and that decreases at each iteration of the loop.

$i \mapsto \max(r_i, s_i)$ (or written $\max(r, s)$).
$i \mapsto r_i + s_i$ and $i \mapsto r_i \cdot s_i$ also work.

Part (d) [1 MARK]

Assuming r and s are always positive, prove your variant is a decreasing sequence.

In every loop iteration when the loop condition is true, the quantity $k := \max(r, s) - \min(r, s)$ is positive, and k is subtracted from the larger of r or s, which makes the max of r and s strictly smaller. Thus, if $i + 1 \leq t$, then $\max(r_{i+1}, s_{i+1}) < \max(r_i, s_i)$.

Part (e) [1 MARK]

Consider this POSTcondition: $f(m, n)$ returns a number r, such that if both of m and n are multiples of a positive natural number c, then r is a multiple of that number c. Equivalently:

$$\forall \text{ positive } c \in \mathbb{N}, [(m \text{ is a multiple of } c \text{ and } n \text{ is a multiple of } c) \implies (r \text{ is a multiple of } c)]$$

What does this POSTcondition say for $f(30, 42)$? Fill in the blanks:

Since 30 and 42 are both multiples of 1, 2, 3, and 6,
$f(30, 42)$ returns a number r that is a multiple of 1, 2, 3, and 6.

Part (f) [2 MARKS]

State an invariant that would prove the POSTcondition from part (e):

$$\forall \text{ positive } c \in \mathbb{N}, [(m \text{ and } n \text{ are multiples of } c) \implies (r_i \text{ and } s_i \text{ are multiples of } c)]$$

That is, a loop iteration does not result in r and s losing any common divisors (to see that this statement is equivalent, recall that r and s are initially m and n).

Part (g) [4 MARKS]

Prove your invariant is true.

This is by simple induction on i. You did not need to say so to get full points.

The invariant is true for $i = 0$, since then it just says the triviality: For all c, if m and n are multiples of c then m and n are multiples of c.

Let $i < t$ be arbitrary and assume the invariant (IH) is true for i. We will show it is true for $i + 1$. Let c be an arbitrary positive natural number such that m and n are multiples of c. The invariant for i says that r_i and s_i are multiples of c. Let a_r and a_s be such that $ca_r = r_i$ and $ca_s = s_i$. It remains to show that r_{i+1} and s_{i+1} are multiples of c. Since $i < t$, have $r_i \neq s_i$.

Case $r_i < s_i$.
Then $r_{i+1} = r_i$ so r_{i+1} is a multiple of c.
And $s_{i+1} = s_i - r_i = ca_s - ca_r = c(a_s - a_r)$. Note that $a_s > a_r$ since $s_i > r_i$. Thus s_{i+1} is also a multiple of c.

Case $s_i < r_i$ is symmetric:
Then $s_{i+1} = s_i$ so s_{i+1} is a multiple of c.
And $r_{i+1} = r_i - s_i = ca_r - ca_s = c(a_r - a_s)$. Note that $a_r > a_s$ since $r_i > s_i$. Thus r_{i+1} is also a multiple of c.

Part (h) [1 MARK]

Consider this second POSTcondition: $f(m,n)$ returns a number r, such that if r is a multiple of a positive natural number c, then both of m and n are multiples of that number c. Equivalently:

$$\forall \text{ positive } c \in \mathbb{N}, [(r \text{ is a multiple of } c) \implies (m \text{ is a multiple of } c \text{ and } n \text{ is a multiple of } c)]$$

State an invariant that would prove this POSTcondition, assuming the loop terminates:

$$\forall \text{ positive } c \in \mathbb{N}, [(r_i \text{ and } s_i \text{ are multiples of } c) \implies (m \text{ and } n \text{ are multiples of } c)]$$

That is, a loop iteration does not result in r and s gaining any common divisors (to see that this statement is equivalent, recall that r and s are initially m and n).

Combined with the previous invariant, this means that the set of common divisors of r and s stays the same throughout execution of the loop.

Part (i) [1 MARK]

Prove your invariant is true.

This is by simple induction on i. You did not need to say so to get full points.

The invariant is true for $i = 0$, since then it just says the triviality: For all c, if m and n are multiples of c then m and n are multiples of c.

Let $i < t$ be arbitrary and assume the invariant (IH) is true for i. We will show it is true for $i+1$. Let c be an arbitrary positive natural number such that r_{i+1} and s_{i+1} are multiples of c. It suffices to show that r_i and s_i are multiples of c as well, since then the invariant for i implies that m and n are multiples of c.

Let a_r and a_s be such that $ca_r = r_{i+1}$ and $ca_s = s_{i+1}$.

Case $r_{i+1} < s_{i+1}$.
Then $r_{i+1} = r_i$ so r_i is a multiple of c.
And $s_{i+1} = s_i - r_i$, so

$$\begin{aligned} s_i &= s_{i+1} + r_i \\ &= s_{i+1} + r_{i+1} \quad \text{since } r_i = r_{i+1} \\ &= ca_s + ca_r \\ &= c(a_s + a_r) \end{aligned}$$

So s_i is a multiple of c.

Case $r_{i+1} > s_{i+1}$ is symmetric:
Then $s_{i+1} = s_i$ so s_i is a multiple of c.
And $r_{i+1} = r_i - s_i$, so

$$\begin{aligned} r_i &= r_{i+1} + s_i \\ &= r_{i+1} + s_{i+1} \quad \text{since } s_i = s_{i+1} \\ &= ca_r + ca_s \\ &= c(a_r + a_s) \end{aligned}$$

So r_i is a multiple of c.