Prove: $\forall n \geq 0(P(n))$

1. (Base) $P(0)$ Start state is $(0, 0)$, 0 is a multiple of 3.
2. (Inductive step) $\forall n \geq 0(P(n) \Rightarrow P(n+1))$
   1. Fix $n \geq 0$.
   2. Assume $P(n)$: after n steps, both jars have multiples of 3.
   3. $P(n+1)$: after $n+1$ steps, both jars have multiples of 3. ???
   4. QED Implication, UG
3. QED Induction

3. $P(n+1)$, that is, after $n+1$ steps, both jars have multiples of 3.
    1. Fix $q_0, q_1, \ldots, q_{n+1}$, an execution with $n+1$ steps.
    2. In q_n, both jars have multiples of 3. Inductive hypothesis.
    3. In q_{n+1}, both jars have multiples of 3.
        1. If the last move is to fill the little jar, then ...
        2. If the last move is to fill the big jar, then...
        3. If the last move is to empty the little jar...
        4. If the last move is to empty the big jar...
        5. Pour from little to big...
        6. Pour from big to little...
        7. QED Cases
    4. QED UG

Prove: $\forall n \geq 0(P(n))$

1. (Base) $P(0)$ — Start state is $(0,0)$, $0 + 2 \times 0$ is a multiple of 7.
2. (Inductive step) $\forall n \geq 0(P(n) \Rightarrow P(n+1))$
   1. Fix $n \geq 0$.
   2. Assume $P(n)$, that is, after n steps, $x + 2y$ is a multiple of 7.
   3. $P(n+1)$, that is, after $n+1$ steps, $x + 2y$ is a multiple of 7.
      1. Fix $q_0, q_1, \ldots, q_{n+1}$, an execution with $n+1$ steps.
      2. In q_n, $x + 2y$ is a multiple of 7. — Inductive hypothesis.
      3. In q_{n+1}, $x + 2y$ is a multiple of 7.
         1. If the last move is $(+2, -1)$ then in q_{n+1}, $x + 2y$ is a multiple of 7.
         2. If the last move is $(-2, +1)$ then in q_{n+1}, $x + 2y$ is a multiple of 7.
         3. If the last move is $(+1, +3)$ then in q_{n+1}, $x + 2y$ is a multiple of 7.
         4. If the last move is $(-1, -3)$ then in q_{n+1}, $x + 2y$ is a multiple of 7.
         5. QED — Cases
   4. QED — Implication, UG
3. QED — Induction

1. If last move is $(+2, -1)$ then in q_{n+1}, $x + 2y$ is a multiple of 7.
   1. Assume the last move is $(+2, -1)$.
   2. Let x and y denote the values in state q_n,
      x' and y' the values in state q_{n+1}.
   3. $x' = x + 2$, $y' = y - 1$. Definition of the move
   4. $x + 2y \cong 0 mod 7$ Inductive hypothesis
   5. $x' + 2y' = (x + 2) + 2(y - 1) = x + 2y \cong 0 mod 7$
      Algebra
   6. In q_{n+1}, $x + 2y$ is a multiple of 7.
   7. QED Implication

3. If last move is $(+1, +3)$ then in q_{n+1}, $x + 2y$ is a multiple of 7.
   1. Assume the last move is $(+1, +3)$.
   2. Let x and y denote the values in state q_n,
      x' and y' the values in state q_{n+1}.
   3. $x' = x + 1$, $y' = y + 3$. Definition of the move
   4. $x + 2y \cong 0 mod 7$ Inductive hypothesis
   5. $x' + 2y' = (x + 1) + 2(y + 3) = x + 2y + 7 \cong 0 mod 7$
      Algebra
   6. In q_{n+1}, $x + 2y$ is a multiple of 7.
   7. QED Implication

3. $P(n+1)$, that is, after $n+1$ steps, $GCD(x,y) = GCD(a,b)$.
    1. Fix $q_0, q_1, \ldots, q_{n+1}$, an execution with $n+1$ steps.
    2. In q_n, $GCD(x,y) = GCD(a,b)$. Inductive hypothesis.
    3. In q_{n+1}, $GCD(x,y) = GCD(a,b)$.
        1. If $x > y$ in q_n then in q_{n+1}, $GCD(x,y) = GCD(a,b)$.
            1. Assume $x > y$ in q_n.
            2. Let x and y denote the values in state q_n, x' and y' the values in state q_{n+1}.
            3. $x' = x - y$, $y' = y$ Definition of the step
            4. $GCD(x,y) = GCD(a,b)$. Inductive hypothesis
            5. $GCD(x',y') = GCD(x-y,y)$ Plug in
            6. $GCD(x-y,y) = GCD(x,y)$ Number theory fact
            7. $GCD(x',y') = GCD(a,b)$ Algebra
            8. In q_{n+1}, $GCD(x,y) = GCD(a,b)$
            9. QED Implication
        2. If $x < y$ in q_n then in q_{n+1}, $GCD(x,y) = GCD(a,b)$. Analogous to prev. case
        3. QED Cases

Prove: Any live execution of GCD contains some state in which $x = y$.

1. Assume not, that is, $\exists$ a live execution in which we never have $x = y$.
2. Fix $q_0, q_1, q_2, \ldots$, a live execution in which we never have $x = y$.
   EI
3. $q_0, q_1, q_2, \ldots$ is either finite with $x = y$ in the final state, or is infinite.
   Definition of "live execution"
4. $q_0, q_1, q_2, \ldots$ is infinite — By 3 and the fact that we don't have $x = y$.
5. $\exists$ a smallest value of $x + y$ that occurs in the states of the execution
   Well-ordering
6. Fix q_k to be a state in which this smallest value is reached.
   EI
7. The value of $x + y$ in q_{k+1} is smaller than the value of $x + y$ in q_k.
   By the way the steps are defined
8. q_k does not have the smallest value of $x + y$ in the execution.
   By 7
9. QED — Contradiction, 6 and 8.

Prove: In any live execution, there exists some state in which all
the nodes are colored.

1. Fix $q_0, q_1, q_2, \ldots$, a live execution.
2. $q_0, q_1, q_2, \ldots$ is either finite with no step enabled in the final state, or is infinite.
   Definition of "live execution".
3. $q_0, q_1, q_2, \ldots$ isn't infinite — Number of uncolored nodes decreases at every step, can't go below 0.
4. $q_0, q_1, q_2, \ldots$ is finite with no step enabled in the final state.
   By 2. and 3.
5. All nodes are colored in the final state.
   1. If not all nodes are colored in the final state, then some step is enabled.
      Any uncolored node can be colored;
      there are enough colors.
   2. QED — Contradiction (5.1. and 4.)
6. QED — EG, UG