Let $a$ and $b$ be positive integers. Let $x$, $u$, and $v$ be integer variables. Let

$$P = u \geq 0 \land v \geq 0 \land x = ux - vx \Rightarrow x' = 0$$

(a) Prove

$$P \iff \text{if } x > 0 \text{ then } x := x - a. \ u := u - 1. \ P \quad \text{else if } x < 0 \text{ then } x := x + b. \ v := v - 1. \ P \quad \text{else ok if}$$

§ Using refinement by cases, I must prove three things:

1. Prove

$$P \iff x > 0 \land (x := x - a. \ u := u - 1. \ P)$$

$$P \iff x < 0 \land (x := x + b. \ v := v - 1. \ P)$$

$$P \iff x = 0 \land \text{ok}$$

Let's start with the first.

$$(P \iff x > 0 \land (x := x - a. \ u := u - 1. \ P)) \text{ replace } P \text{ twice, use substitution law twice}$$

$$= (u \geq 0 \land v \geq 0 \land x = ux - vx \Rightarrow x' = 0)$$

$$= x > 0 \land (u - 1 \geq 0 \land v \geq 0 \land x - a = (u - 1)x - (v - 1)x \Rightarrow x' = 0))$$

simplify, portation

$$= u \geq 0 \land v \geq 0 \land x = ux - vx \land x > 0 \land (u > 0 \land v \geq 0 \land x = ux - vx \Rightarrow x' = 0) \Rightarrow x' = 0$$

context

$$= u \geq 0 \land v \geq 0 \land x = uxa - vxb \land x > 0 \land (u > 0 \land \neg x \Rightarrow x' = 0) \Rightarrow x' = 0$$

identity, context

$$= u \geq 0 \land v \geq 0 \land x = uxa - vxb \land x > 0 \land (u > 0 \land v \geq 0 \land x = uxa - vxb \Rightarrow x' = 0) \Rightarrow x' = 0$$

indirect proof

$$= u \geq 0 \land v \geq 0 \land x = uxa - vxb \land x > 0 \land u \geq 0 \Rightarrow x' = 0$$

$$= u \geq 0 \land v \geq 0 \land x = uxa - vxb \land x > 0 \land x = uxa - vxb \Rightarrow x' = 0$$

note that $b > 0$

$$= u \geq 0 \land v \geq 0 \land 0 < x = -vxb < 0 \Rightarrow x' = 0$$

transitivity, $\neg(0 < 0)$

$$= \text{base law}$$

$$= T$$

The second one is similar to the first.

$$(P \iff x < 0 \land (x := x + b. \ v := v - 1. \ P)) \text{ replace } P \text{ twice, use substitution law twice}$$

$$= (u \geq 0 \land v \geq 0 \land x = ux - vx \Rightarrow x' = 0)$$

$$= x < 0 \land (u \geq 0 \land v \geq 0 \land x + b = uxa - (v - 1)x \Rightarrow x' = 0))$$

simplify, portation

$$= u \geq 0 \land v \geq 0 \land x = uxa - vxb \land x < 0 \land (u \geq 0 \land v \geq 0 \land x = uxa - vxb \Rightarrow x' = 0) \Rightarrow x' = 0$$

Now we are going to have to use discharge. Two of the three conjuncts to be discharged, $u \geq 0$ and $x = uxa - vxb$, have conjuncts to discharge them, leaving

$$= u \geq 0 \land v \geq 0 \land x = uxa - vxb \land x < 0 \Rightarrow v > 0$$

$$= u \geq 0 \land uxa < vxb \Rightarrow v > 0$$

note that $a > 0$

$$= 0 < vxb \Rightarrow v > 0$$

note that $b > 0$

$$= T$$

The last one is easiest.

$$(P \iff x = 0 \land \text{ok}) \text{ replace } P \text{ and ok}$$

$$= (u \geq 0 \land v \geq 0 \land x = uxa - vxb \Rightarrow x' = 0)$$

$$= x = 0 \land x' = x \land u' = u \land v' = v \land u \geq 0 \land v \geq 0 \land x = uxa - vxb \Rightarrow x' = 0$$

context

$$= x = 0 \land x' = 0 \land u' = u \land v' = v \land u \geq 0 \land v \geq 0 \land x = uxa - vxb \Rightarrow x' = 0$$

specialization

$$= T$$

(b) Find an upper bound for the execution time of the program in part (a).

§ The exact execution time is

$$T = t' = t + u - u' - v'$$

Adding recursive time, we prove

$$T \iff \text{if } x > 0 \text{ then } x := x - a. \ u := u - 1. \ t := t + 1. \ T$$

$$\quad \text{else if } x < 0 \text{ then } x := x + b. \ v := v - 1. \ t := t + 1. \ T$$

$$\quad \text{else ok if}$$

by cases. First

$$T \iff x > 0 \land (x := x - a. \ u := u - 1. \ t := t + 1. \ T)$$

by three substitutions and specialization. Second
by three substitutions and specialization. Finally

\[ T \iff x < 0 \land (x := x + b, v := v - 1, t := t + 1). \]

by specialization. But this execution time involves the final state, so it's no use as a predictor. So I now prove

\[ U = t' \leq t + u + v \]

by cases. First

\[ U \iff x > 0 \land (x := x - a, u := u - 1, t := t + 1). \]

by three substitutions and specialization. Second

\[ U \iff x < 0 \land (x := x + b, v := v - 1, t := t + 1). \]

by three substitutions and specialization. Finally

\[ U \iff x = 0 \land ok \]

by specialization.