\[ a, d \text{ compute } g, r \text{ s.t. } a = gd + r \text{ and } 0 \leq r < d \]

\[ \text{precondition: } a \geq 0, \ d > 0 \]

\[ \text{postcondition} \]

\[ g = 0 \]

\[ k \rightarrow g \text{ while } (r \geq d) \]

\[ r = r - d \]

\[ g = g + 1 \]

invARIANT: always true at some point in code (usually after 11th iteration of loop)

\[ I(n) = \text{"if } n \text{ is } r \geq 0 \text{ and } r = a \mod d \text{"} \]

**Complete statements of the loop**

\[ g = r \geq d \]

"guard"

something that

must be \( true \) for

loop to execute
1) \( I(0) \) is true when loop starts (at \( \theta \))

2) \( \forall k \in \mathbb{N} \rightarrow I(k) \rightarrow I(k+1) \) (loop preserves invariant)

3) \( G \) eventually becomes \( F \) (loop terminates)

4) \( I(N) \land G \rightarrow \text{postconditions} \) (code does what it says it will do)

**Basis:** \( I(0) \) is \( g = 0 \land r \geq 0 \land r = a \), which is true

- \( g = 0 \) by prev. assign.
- \( r = a \) by prev. assign.
- \( r \geq 0 \) true \( r = a \geq 0 \) by precondition

**Inductive step:** Suppose \( k \geq 0 \) and \( I(k) \) and \( G \) are true

\( g_{\text{old}} = \text{value after } k \text{th iteration of loop} \) \( g_{\text{old}} = k \land g_{\text{new}} \geq 0 \land r_{\text{old}} = a - k \cdot d \)

\( r_{\text{new}} = \text{value after } (k+1) \text{ iteration} \)

\[ [\text{want } g_{\text{new}} = k + 1 \land g_{\text{new}} \geq 0 \land r_{\text{new}} = a - (k+1) \cdot d] \]

By assignment in loop \( r_{\text{new}} = r_{\text{old}} - d \)
by assignment \( z \) in loop \( g_{new} = g_{old}+1 \)

by substitution, \( g_{new} = a - kd - d = a - (k+1)d \)
\[ g_{new} = k+1 \]
\[ g_{new} = \textcircled{1} - d \geq d - d = 0 \]

Eventual Falsity of Guard: \( g_{new} < g_{old} \), so \( r \) gets smaller and smaller, eventually must be \( < d \) (well ordering—
there must be a smallest value of \( r \))

by \( r \) is always \( \geq 0 \); if smallest value is \( \geq d \) then loop iterates again, making
an even smaller value \( \Rightarrow \Rightarrow \)

Postconditions: Suppose \( N \) is s.t. \( I(N) \) and \[ \text{want } a = \text{den}\r
D < cd \]
\[ I(N) = \text{"} r = a - Nd \wedge r < d \wedge b = N \text{"} \]

Then \( a = Nd + r = g_{old} + r \)
\[ G = r \geq a \]
\[ \sim G = r < a \]

Sets (Ch. 5)

\[ A = \{ x \in D \mid P(x) \} \] means \( x \in A \iff x \in D \land P(x) \)
\[ A = \{ x \in \mathbb{Z}^+ \mid x < 4 \} = \{ 1, 2, 3 \} \]
\[ B = \{ x \in \mathbb{Z} \mid x^2 < 10 \} = \{ -3, -2, -1, 0, 1, 2, 3 \} \]

\( A \subseteq B \) means \( \forall x, x \in A \rightarrow x \in B \)

"A is a subset of B"

proper subset = subset but not equal

\( A = B \) means \( \forall x, x \in A \iff x \in B \)

\[ \forall x, x \in A \rightarrow x \in B \land x \in B \rightarrow x \in A \]
\[ A \subseteq B \land B \subseteq A \]

\[ A \subseteq B \land B \subseteq A \]
\[ A \cup B = \{ x \mid x \in A \lor x \in B \} \]

"union of A, B"

\[ A \cap B = \{ x \mid x \in A \land x \in B \} \]

"intersection of A, B"

\[ B - A = \{ x \mid x \in B \land x \notin A \} \]

"set difference"

\[ A^c = \{ x \in U \mid x \notin A \} \]

universe

\[ \emptyset = \{ \} = \{ x \mid x \notin x \} \]

x \in \emptyset is always false

"empty set"