Computing GCD's: The Euclidean Algorithm

Lemma: for \( b \neq 0 \)
\[ \gcd(a, b) = \gcd(b, \text{rem}(a, b)) \]

Proof: \( a = qb + r \)
so \( a, b \) and \( b, r \) have the same divisors

Example: \( a = 899, b = 493 \)
\[ \begin{align*}
\text{GCD}(899, 493) &= \\
\text{GCD}(493, 406) &= \\
\text{GCD}(406, 87) &= \\
\text{GCD}(87, 58) &= \\
\text{GCD}(58, 29) &= \\
\text{GCD}(29, 0) &= 29
\end{align*} \]
Euclidean Algorithm
as a State Machine:
States ::= \( \mathbb{N} \times \mathbb{N} \)
start ::= \( (a,b) \)
state transitions defined by \((x,y) \rightarrow (y, \text{rem}(x,y))\)
for \( y \neq 0 \)

GCD correctness
By Lemma, \( \gcd(x,y) \) is constant.
so preserved invariant is
\[ P((x,y)) ::= [\gcd(a,b) = \gcd(x,y)] \]
\( P(\text{start}) \) is trivially true:
\[ [\gcd(a,b) = \gcd(a,b)] \]

GCD partial correctness
at termination
\[ x = \gcd(a,b) \]
Proof: at termination, \( y = 0 \), so
\[ x = \gcd(x,0) = \gcd(x,y) = \gcd(a,b) \]
preserved invariant

GCD Termination
\( y \) halves or smaller at every other step, so
reaches minimum in \( \leq 2 \log_2 b \) transitions