Computing GCD's
The Euclidean Algorithm

Proof: $a = qb + r$
any divisor of 2 of these terms must divide all 3.

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

Example: $a = 899, b = 493$
$\gcd(899, 493) = \gcd(493, 406) = \gcd(406, 87) = \gcd(87, 29) = 29$
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 $y \neq 0$

By Lemma, $\gcd(x,y)$ is constant.
so preserved invariant is
$P((x,y)) ::= [\gcd(a,b) = \gcd(x,y)]$

P(start) is trivially true:
$[\gcd(a,b) = \gcd(a,b)]$

GCD partial correctness
at termination (if any)
$x = \gcd(a,b)$

Proof: at termination, $y = 0$, so
$x = \gcd(x,0) = \gcd(x,y) = \gcd(a,b)$
preserved invariant

GCD Termination
At each transition, $x$ is replaced by $y$. 
GCD Termination

At each transition, $x$ is replaced by $y$. If $y \leq x/2$, then $x$ gets halved at this step.

GCD Termination

At each transition, $x$ is replaced by $y$. If $y \leq x/2$, then $x$ gets halved at this step. If $y > x/2$, then $\text{rem}(x,y) = x - y < x/2$, so $y$ gets halved when it is replaced by $\text{rem}(x,y)$ after the next step.

GCD Termination

$y$ halves or smaller at every other step, so reaches minimum in $\leq 2 \log_2 b$ steps.