while $b > 0$
  \begin{align*}
    r &= a \mod b \\
    a &= b \\
    b &= r
  \end{align*}

Claim: $b$ gets shorter by at least 1 bit every 2 iterations.
\[ \text{Time } O(n) \text{ (length of bin bits)} \]

Case 1:
\[ r \leq b/2 \]

Case 2:
\[ r > b/2 \]

in next iteration, $g = 1$
\[ \text{new } r = b - \text{odd } r \leq \frac{b}{2} \]
Theorem \ \forall a, b \geq 0 \ \exists ! t \in \mathbb{Z} \ \text{ s.t. } \ a \cdot t + b = \gcd(a, b)

Proof by example

\begin{align*}
  440 &= 300 \cdot 1 + 140 \\
  300 &= 140 \cdot 2 + 20 \\
  140 &= 9 \cdot 20 + 0
\end{align*}

\begin{align*}
  140 &= 440 - 3 \cdot 140 \\
  20 &= 300 - 2 \cdot 140 \\
  &= 300 - 2(440 - 2 \cdot 140) \\
  &= 5 \cdot 300 - 2 \cdot 440
\end{align*}

\begin{align*}
  6.6 - 1.35 &= 1 \\
  \gcd(6.6, 3.5) &= 1
\end{align*}

if \ a | b \ and \ a \n | \ b \ ? \ n | a | c

\begin{align*}
  2.3 | 4.9 \\
  6 | 4.7
\end{align*}
**Theorem**

If \( a \mid b \cdot c \) and \( \gcd(a, b) = 1 \) then \( a \mid c \).

**Proof**

\[ \exists t, s \quad a + t \cdot b = 1 \]

\[ \therefore a \cdot a + t \cdot b = a \cdot c + t \cdot c \]

\[ a \mid a \cdot c \]

\[ a \mid a \cdot c \quad \therefore a \mid t \cdot b \cdot c \]

\[ \therefore a \mid (a \cdot c + t \cdot b \cdot c) \]

\[ a \mid c \]
if prime \( p \mid \prod_{i=2}^{n} g_i \)

Then \( \exists j \) s.t. \( p \mid g_j \)

\( p \) is by and so \( n \)

if \( p \mid g_i \), done

if not \( \gcd(p, g_i) = 1 \)

by previous theorem \( p \mid \prod_{i=2}^{n} g_i \)

by and \( p \mid g_j \) for some \( j \).

uniqueness of prime factorization

Suppose not. Let \( n \) be smallest exception

\[ p_1 \cdot p_2 \cdots p_n = n = g_1 \cdot g_2 \cdots g_k \]

\[ p_1 = g_j \] for some \( j \)

\[ p_2 \cdot p_3 \cdots p_n = \frac{n}{p_1} = g_1 \cdot g_{j+1} \cdots g_k \]

contradicting minimality of \( n \).