Procedure. (iterated division?)

$P_0 = P$, $q_0 = q$, where $P, q \in \mathbb{Z}$, $P \geq q > 0$

$$\begin{cases} P_{n+1} = q_n & n \geq 0 \\ 0 \leq q_{n+1} < q_n, \quad P_n = q_n \cdot k_n + q_{n+1}, & k_n \in \mathbb{Z}. \end{cases}$$

(Stops when q_n becomes 0.)

Note that $0 \leq q_{n+1} < q_n$. So q_n becomes 0 in at most q steps. So $\exists\, 0 \leq l < q$, s.t., $q_l \neq 0$, $q_{l+1} = 0$.

And $\text{g.c.d.}(P, q) = q_l$.

Proof. (A) If $P = q$, then the procedure stops in 1 step, and $l = 0$, $q_l = q_0 = q$. Clearly, $q_0 = q = \text{g.c.d.}(P, q)$.

(B) Next, prove the case when $P > q > 0$ (*).

Induct on P. By (*), P is at least 2.

(i) If $P = 2$, then $q = 1$. The procedure stops in 1 step, $l = 0$, and $q_l = 1 = \text{g.c.d.}(2, 1)$.

(ii) Assume that the procedure gives the g.c.d. for $P \leq m$.

Consider the pair $(m+1, q)$, where $m+1 > q > 0$.

Let $P_0 = q$, and q_0 satisfy $0 \leq q_0 < q (= P_0)$, and $m+1 = q \cdot k_0 + q_0$, for some $k \in \mathbb{Z}$.

Then $m \geq P_0 > q_0 \geq 0$. If $q_0 = 0$, then the procedure stops in 1 step, gives $q = \text{g.c.d}(m+1, q)$.

If $q_0 > 0$, then $m \geq P_0 > q_0 > 0$. By induction hypothesis, we know $\exists\, l < q_0$, s.t., $q_l = \text{g.c.d}(P_0, q_0)$, $q_{l+1} = 0$.

We claim that $q_l = \text{g.c.d.}(m+1, q)$.

Since $q_l \mid P_0, q_0$, we have $q_l \mid k_0 \cdot P_0 + q_0 = m+1$, and $q = P_0$.

$\Rightarrow q_l$ is a common divisor of $m+1$ and q.

If $d \mid m+1, q$, then $d \mid q_0 = (m+1) - k_0 \cdot q$, $P_0 = q$. $\Rightarrow d \leq q_l$

$\Rightarrow q_l$ is the greatest common divisor of $m+1$ & q, i.e., $q_l = \text{g.c.d}(m+1, q)$ #.