Theorem: (termination) The Euclidean Algorithm, applied to integers m and n, terminates in $\gcd(m,n)$.

proof: Let $m = q_{-1}$ and $n = q_0$.

In general, we have

$$\boxed{n_{k-2} = q_k n_{k-1} + n_k}.$$

The process terminates with n_ℓ where

$$n_{\ell-1} = q_{\ell+1} n_\ell.$$

Rewrite the equation as

$$r_k = r_{k-2} - q_k r_{k-1}$$

Observe that, with

$$Q_k = \begin{bmatrix} 0 & 1 \\ 1 & -q_k \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 \\ 1 & -q_k \end{bmatrix} \begin{bmatrix} r_{k-2} \\ r_{k-1} \end{bmatrix}$$

$$= \begin{bmatrix} r_{k-1} \\ r_{k-2} - q_k r_{k-1} \end{bmatrix} = \begin{bmatrix} r_{k-1} \\ r_k \end{bmatrix}$$

Note that $\det(Q_k) = -1$,

so Q_k is invertible, with

inverse $\begin{bmatrix} q_k & 1 \\ 1 & 0 \end{bmatrix}$.

Starting with

$$\begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} n_{-1} \\ n_0 \end{bmatrix},$$

$$Q_1 \begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} n_0 \\ n_1 \end{bmatrix}$$

$$Q_2 \begin{bmatrix} n_0 \\ n_1 \end{bmatrix} = \begin{bmatrix} n_1 \\ n_2 \end{bmatrix}, \text{ so}$$

$$Q_2 Q_1 \begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} n_1 \\ n_2 \end{bmatrix}.$$

After $l+1$ steps, we get

$$Q_{l+1} Q_l \cdots Q_2 Q_1 \begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} n_l \\ 0 \end{bmatrix}.$$

Each Q_k for $1 \le k \le l+1$ has integer entries, so any product of Q_k's has integer entries.

In particular, if

$$Q = Q_{l+1} Q_l \cdots Q_2 Q_1,$$

then Q has integer entries,

$$Q = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ with } a, b, c, d \in \mathbb{Z}.$$

$$\underbrace{Q \begin{bmatrix} m \\ n \end{bmatrix}} = \begin{bmatrix} n_\ell \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} n_\ell \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} am + bn \\ cm + dn \end{bmatrix} = \begin{bmatrix} n_\ell \\ 0 \end{bmatrix},$$

So $n_\ell = am + bn \in I(m,n)$.

But since Q_k is invertible with determinant -1 for all $1 \le k \le \ell+1$,

$$\det(Q) = \det(Q_{\ell+1} Q_\ell \cdots Q_2 Q_1)$$

$$= \det(Q_{\ell+1}) \det(Q_\ell) \cdots \det(Q_2) \det(Q_1)$$

$$= (-1)^{\ell+1}.$$

Therefore, Q is invertible, and the inverse is

$$Q^{-1} = (-1)^{\ell+1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Since

$$Q \begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} n_e \\ 0 \end{bmatrix},$$

applying Q^{-1} on the left gives

$$\begin{bmatrix} m \\ n \end{bmatrix} = Q^{-1} \begin{bmatrix} n_e \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} m \\ n \end{bmatrix} = (-1)^{d+1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} n_e \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} m \\ n \end{bmatrix} = (-1)^{d+1} \begin{bmatrix} dn_e \\ -cn_e \end{bmatrix}$$

Since m and n are nonzero integers, $d \neq 0$ and $c \neq 0$.

Therefore,

$$m = (-1)^{\ell+1} d n_\ell$$

$$n = (-1)^{\ell+1} (-c n_\ell),$$

which implies

$$n_\ell \mid m \quad \text{and} \quad n_\ell \mid n.$$

So we have: $n_\ell \mid m$, $n_\ell \mid n$

and $n_\ell \in I(m,n)$.

By a previous lemma,

$$n_\ell = \gcd(m,n). \qquad \square$$

Corollary: Let $m, n \in \mathbb{Z}$, $m \neq 0 \neq n$ and let $d = \gcd(m, n)$. Then

1) d is the least element in $\mathbb{N} \cap I(m, n)$

2) $I(m,n) = d\mathbb{Z}$
$= \{dk \mid k \in \mathbb{Z}\}$.

proof: 1) We already know that $d \in I(m,n)$. Since $d \mid m$ and $d \mid n$, we know d divides every element of $I(m,n)$.

This implies that if $a \in \mathbb{N} \cap I(m,n)$, then $d \mid a \Rightarrow d \leq a$, so d is the least element of $I(m,n)$.

2) By 1), we know that if $a \in I(m,n)$, then $d \mid a$, so $I(m,n) \subseteq d\mathbb{Z}$.

But since $d \in I(m,n)$, we can write

$$d = tm + bn \text{ for } t, b \in \mathbb{Z},$$

and so if $k \in \mathbb{Z}$,

$$dk = (kt)m + (kb)n \in I(m,n).$$

$\square$

Definition: (relatively prime) Let $m, n \in \mathbb{Z}$, $m \neq 0 \neq n$. We say m and n are **relatively prime** if $\gcd(m,n) = 1$.

Corollary: If $m, n \in \mathbb{Z}$, $m \neq 0 \neq n$. Then m and n are relatively prime if and only if $\exists\, a, b \in \mathbb{Z}$

$$\boxed{1 = am + bn}$$

Proof: $\Rightarrow$ Suppose m and n are relatively prime. Then

$$1 = \gcd(m,n) \in I(m,n),$$

so $\exists\, a, b \in \mathbb{Z}$ with

$$1 = am + bn.$$

$\Leftarrow$ Suppose $\exists\ a, b \in \mathbb{Z}$,

$$1 = am + bn.$$

Then $1 \in I(m,n)$.

But $d = \gcd(m,n)$, we know that d is the least element in $\mathbb{N} \cap I(m,n)$, which implies $d = 1$.

$\square$

Example 1: Are 60997 and 51343 relatively prime? Write their gcd as a linear combination of integers.

Solution: Start the Euclidean Algorithm!

$m = 60997, \quad n = 51343$

$Q_1 = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}$ $\quad 60997 = 1 \cdot 51343 + 9654$

$Q_2 = \begin{bmatrix} 0 & 1 \\ 1 & -5 \end{bmatrix}$ $\quad 51343 = 5 \cdot 9654 + 3073$

$Q_3 = \begin{bmatrix} 0 & 1 \\ 1 & -3 \end{bmatrix}$ $\quad 9654 = 3 \cdot 3073 + 435$

$Q_4 = \begin{bmatrix} 0 & 1 \\ 1 & -7 \end{bmatrix}$ $\quad 3073 = 7 \cdot 435 + 28$

$Q_5 = \begin{bmatrix} 0 & 1 \\ 1 & -15 \end{bmatrix}$ $\quad 435 = 15 \cdot 28 + 15$

$Q_6 = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}$ $\quad 28 = 1 \cdot 15 + 13$

$Q_7 = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}$ $\quad 15 = 13 \cdot 1 + 2$

$Q_8 = \begin{bmatrix} 0 & 1 \\ 1 & -6 \end{bmatrix}$ $\quad 13 = 2 \cdot 6 + 1$

$\quad 2 = 2 \cdot 1$

$Q_9 = \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix}$ relatively prime!

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = Q \cdot \begin{bmatrix} 60997 \\ 51343 \end{bmatrix}$$

$$Q = \begin{bmatrix} -23842 & 28325 \\ 51343 & -60997 \end{bmatrix}$$