L9: Euclidean algorithm

<u>Interlude</u> : <u>Euclidean algorithm</u>

<u>Def</u> We say m is a divisor of n if $\exists k \in \mathbb{Z}$ s.t. $n = km$
and write $m | n$ in that case.

<u>Ex</u>
- $1 | n \quad \forall n$
- $d | m$ and $d | n \Rightarrow d | m \pm n$ [Pf: $\begin{matrix} m = k_1 d \\ n = k_2 d \end{matrix} \Rightarrow m \pm n = (k_1 \pm k_2) d$]
- $n | 0 \quad \forall n$
- $d | n \Rightarrow |d| \leq |n|$ if $n \neq 0$
- $n | n \quad \forall n$

<u>Def</u> For $m, n \in \mathbb{Z}$ we define the greatest common divisor
$$gcd(m,n) := (m,n) := \max\{ d \in \mathbb{Z}^{>0} \mid d | m \text{ and } d | n \}$$
we set $(0,0) = 0$

<u>Lemma</u>
i) $(m,n) = (n,m)$

ii) $(m,n) = (m+n, n) = (m-n, n)$

iii) $(m,n) = (r,n)$ whenever $r \equiv m \mod n$
In particular, we can choose $0 \leq r < |n|$ if $n \neq 0$.

iv) $(m,0) = |m|$

<u>Pf</u> i) ✓

ii) We have seen $d | m$ and $d | n \Rightarrow d | m+n$ and $d | n$
$$\Rightarrow \quad (m,n) \leq (m+n, n)$$
Same argument $(m,n) \leq (m-n, n)$
and thus $(m,n) \leq (m+n, n) \leq (m,n)$

iii) repeatedly apply ii)

iv) ✓

Thm (Euclidean algorithm)
Let $m, n \in \mathbb{Z}$. Then $\exists\, a, b \in \mathbb{Z}$ s.t.
$$(m,n) = am + bn.$$

Example $(30, 21)$

$$
\begin{aligned}
(30,21) &= (9,21) \\
&= (9,3) \\
&= (0,3)
\end{aligned}
\qquad
\begin{aligned}
&= -2\cdot(30-21)+21 = 3\cdot 21 - 2\cdot 30 \\
&= 0 + 1\cdot(21-2\cdot 9) = -2\cdot 9 + 21 \\
&= 0 + 1\cdot 3 \\
&= 3
\end{aligned}
$$

Pf Using i) we can assume that $m \geq n$.
Repeatedly apply iii) and i) to get
$$(m,n) = (n, r_1) = (r_1, r_2) = \dots$$
where $0 \leq r_{i+1} < |r_i|$ and hence has to end with
$$(r_\ell, r_{\ell+1}) = (r_\ell, 0) = r_\ell \qquad (= (m,n))$$
We have $r_{i+1} + k_{i+1} r_i = r_{i-1}$ $\quad k_{i+1} \in \mathbb{Z}$
i.e.
$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -k_{i+1} \end{pmatrix}}_{A_i} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}$$

Thus
$$\begin{pmatrix} r_\ell \\ 0 \end{pmatrix} = \underbrace{A_\ell \cdot A_{\ell-1} \cdot \ldots \cdot A_1 \cdot A_0}_{\text{matrix with coefficients in } \mathbb{Z}.} \begin{pmatrix} m \\ n \end{pmatrix}$$
$$= \begin{pmatrix} a & b \\ * & * \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$$