Hermite Normal Form

Spring, 2019

$$36x_1 + 30x_2 + 21x_3 = 10$$

- ▶ If and only if gcd(36, 30, 21) is a divisor of 10!
- ▶ gcd(36, 30, 21) ... by Euclid's algorithm (≈ 300 BC)
- ▶ ... by computing the **Hermite normal form** of [36, 30, 21]:

$$36, 30, \mathbf{21}] \\ \rightarrow [15, \mathbf{9}, 21] \rightarrow [21, 15, \mathbf{9}] \\ \rightarrow [\mathbf{3}, 6, 9] \rightarrow [9, 6, \mathbf{3}] \\ \rightarrow [0, 0, 3] \rightarrow [3, 0, 0]$$

$$36x_1 + 30x_2 + 21x_3 = 10$$

- ▶ If and only if gcd(36, 30, 21) is a divisor of 10!
- ▶ gcd(36, 30, 21) ... by Euclid's algorithm (≈ 300 BC)
- ▶ ... by computing the **Hermite normal form** of [36, 30, 21]:

 $[36, 30, \mathbf{21}] \\ \rightarrow [15, \mathbf{9}, 21] \rightarrow [21, 15, \mathbf{9}] \\ \rightarrow [\mathbf{3}, 6, 9] \rightarrow [9, 6, \mathbf{3}]$

$$36x_1 + 30x_2 + 21x_3 = 10$$

- ▶ If and only if gcd(36, 30, 21) is a divisor of 10!
- ▶ gcd(36, 30, 21) ... by Euclid's algorithm (≈ 300 BC)
- \blacktriangleright ... by computing the **Hermite normal form** of [36, 30, 21]:

$$[36, 30, \mathbf{21}] \\ \rightarrow [15, \mathbf{9}, 21] \rightarrow [21, 15, \mathbf{9}] \\ \rightarrow [\mathbf{3}, 6, 9] \rightarrow [9, 6, \mathbf{3}] \\ \rightarrow [0, 0, 3] \rightarrow [3, 0, 0]$$

$$36x_1 + 30x_2 + 21x_3 = 10$$

- ▶ If and only if gcd(36, 30, 21) is a divisor of 10!
- ▶ gcd(36, 30, 21) ... by Euclid's algorithm (≈ 300 BC)
- \blacktriangleright ... by computing the **Hermite normal form** of [36, 30, 21]:

$$\begin{array}{c} [36,30,\mathbf{21}] \\ \rightarrow [15,\mathbf{9},21] \rightarrow [21,15,\mathbf{9}] \\ \rightarrow [\mathbf{3},6,9] \rightarrow [9,6,\mathbf{3}] \\ \rightarrow [0,0,3] \rightarrow [3,0,0] \end{array}$$

$$36x_1 + 30x_2 + 21x_3 = 10$$

- ▶ If and only if gcd(36, 30, 21) is a divisor of 10!
- ▶ gcd(36, 30, 21) ... by Euclid's algorithm (≈ 300 BC)
- ▶ ... by computing the **Hermite normal form** of [36, 30, 21]:

•

$$[36, 30, \mathbf{21}] \\ \rightarrow [15, \mathbf{9}, 21] \rightarrow [21, 15, \mathbf{9}] \\ \rightarrow [\mathbf{3}, 6, 9] \rightarrow [9, 6, \mathbf{3}] \\ \rightarrow [0, 0, 3] \rightarrow [3, 0, 0]$$

$$36x_1 + 30x_2 + 21x_3 = 10$$

- ▶ If and only if gcd(36, 30, 21) is a divisor of 10!
- ▶ gcd(36, 30, 21) ... by Euclid's algorithm (≈ 300 BC)
- ▶ ... by computing the **Hermite normal form** of [36, 30, 21]:

•

$$[36, 30, \mathbf{21}] \\ \rightarrow [15, \mathbf{9}, 21] \rightarrow [21, 15, \mathbf{9}] \\ \rightarrow [\mathbf{3}, 6, 9] \rightarrow [9, 6, \mathbf{3}] \\ \rightarrow [0, 0, 3] \rightarrow [3, 0, 0]$$

$$\begin{bmatrix} 15 & -6 & 9 & 6 \\ -1 & 0 & -7 & 10 \\ 4 & -1 & 2 & 8 \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 15 \\ 3 \\ 7 \end{pmatrix}$$

Row 1: switch the sign ... and sort ...

$$\begin{bmatrix} 15 & \mathbf{-6} & 9 & 6 \\ -1 & 0 & -7 & 10 \\ 4 & -1 & 2 & 8 \end{bmatrix} \rightarrow \begin{bmatrix} 15 & 6 & 9 & 6 \\ -1 & 0 & -7 & 10 \\ 4 & 1 & 2 & 8 \end{bmatrix} \rightarrow \begin{bmatrix} 15 & 9 & 6 & 6 \\ -1 & -7 & 0 & 10 \\ 4 & 2 & 1 & 8 \end{bmatrix}$$

Row 1: take away the smallest positive \dots and resort \dots

$$\begin{bmatrix} 15 & 9 & 6 & \mathbf{6} \\ -1 & -7 & 0 & 10 \\ 4 & 2 & 1 & 8 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 3 & 0 & \mathbf{6} \\ -21 & -17 & -10 & 10 \\ -12 & -6 & -7 & 8 \end{bmatrix} \rightarrow \begin{bmatrix} 6 & 3 & 3 & 0 \\ 10 & -21 & -17 & -10 \\ 8 & -12 & -6 & -7 \end{bmatrix}$$

Row 1: take away the smallest positive \dots and resort \dots

$$\begin{bmatrix} 6 & 3 & \mathbf{3} & 0 \\ 10 & -21 & -17 & -10 \\ 8 & -12 & -6 & -7 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 0 & \mathbf{3} & 0 \\ 44 & -4 & -17 & -10 \\ 20 & -6 & -6 & -7 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 \\ -17 & 44 & -4 & -10 \\ -6 & 20 & -6 & -7 \end{bmatrix}$$

Row 2: switch the sign ... and sort ...

$$\begin{bmatrix} 3 & 0 & 0 & 0 \\ -17 & 44 & -4 & -10 \\ -6 & 20 & -6 & -7 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 \\ -17 & 44 & 4 & 10 \\ -6 & 20 & 6 & 7 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 \\ -17 & 44 & 10 & 4 \\ -6 & 20 & 7 & 6 \end{bmatrix}$$

Row 2: take away the smallest positive \dots and resort \dots

$$\begin{bmatrix} 3 & 0 & 0 & 0 \\ -17 & 44 & 10 & 4 \\ -6 & 20 & 7 & 6 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 \\ -17 & 0 & 2 & 4 \\ -6 & -46 & -5 & 6 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 \\ -17 & 4 & 2 & 0 \\ -6 & 6 & -5 & -46 \end{bmatrix}$$

Row 2: take away the smallest positive \dots and resort \dots

$$\begin{bmatrix}
3 & 0 & 0 & 0 \\
-17 & 4 & 2 & 0 \\
-6 & 6 & -5 & -46
\end{bmatrix}
\rightarrow
\begin{bmatrix}
3 & 0 & 0 & 0 \\
-17 & 0 & 2 & 0 \\
-6 & 16 & -5 & -46
\end{bmatrix}
\rightarrow
\begin{bmatrix}
3 & 0 & 0 & 0 \\
-17 & 2 & 0 & 0 \\
-6 & -5 & 16 & -46
\end{bmatrix}$$

Row 3: switch the sign ... and sort ...

$$\begin{bmatrix}
3 & 0 & 0 & 0 & 0 \\
-17 & 2 & 0 & 0 & 0 \\
-6 & -5 & 16 & -46
\end{bmatrix}
\rightarrow
\begin{bmatrix}
3 & 0 & 0 & 0 & 0 \\
-17 & 2 & 0 & 0 & 0 \\
-6 & -5 & 16 & 46
\end{bmatrix}
\rightarrow
\begin{bmatrix}
3 & 0 & 0 & 0 & 0 \\
-17 & 2 & 0 & 0 & 0 \\
-6 & -5 & 16 & 46
\end{bmatrix}$$

Row 3: take away the smallest positive \dots and resort \dots

$$\begin{bmatrix}
3 & 0 & 0 & 0 & 0 \\
-17 & 2 & 0 & 0 & 0 \\
-6 & -5 & 46 & 16
\end{bmatrix}
\rightarrow
\begin{bmatrix}
3 & 0 & 0 & 0 & 0 \\
-17 & 2 & 0 & 0 & 0 \\
-6 & -5 & 14 & 16
\end{bmatrix}
\rightarrow
\begin{bmatrix}
3 & 0 & 0 & 0 & 0 \\
-17 & 2 & 0 & 0 & 0 \\
-6 & -5 & 16 & 14
\end{bmatrix}$$

Row 3: take away the smallest positive \dots and resort \dots

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ -17 & 2 & 0 & 0 & 0 \\ -6 & -5 & 16 & 14 & 14 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ -17 & 2 & 0 & 0 & 0 \\ -6 & -5 & 2 & 14 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ -17 & 2 & 0 & 0 & 0 \\ -6 & -5 & 14 & 2 & 0 \end{bmatrix}$$

Row 3: take away the smallest positive \dots and resort \dots

$$\begin{bmatrix}
3 & 0 & 0 & 0 & 0 \\
-17 & 2 & 0 & 0 & 0 \\
-6 & -5 & 14 & 2
\end{bmatrix}
\rightarrow
\begin{bmatrix}
3 & 0 & 0 & 0 & 0 \\
-17 & 2 & 0 & 0 & 0 \\
-6 & -5 & 0 & 2
\end{bmatrix}
\rightarrow
\begin{bmatrix}
3 & 0 & 0 & 0 & 0 \\
-17 & 2 & 0 & 0 & 0 \\
-6 & -5 & 2 & 0 & 0
\end{bmatrix}$$

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ -17 & \mathbf{2} & 0 & 0 & 0 \\ -6 & -5 & 2 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ -51 & -5 & \mathbf{2} & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 3 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 2 \end{bmatrix} \quad B \cdot y = \begin{pmatrix} 15 \\ 3 \\ 7 \end{pmatrix}$$

$$y_1 = 5$$

$$y_2 = -$$

$$y_3 = \frac{3}{2}$$

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ -17 & \mathbf{2} & 0 & 0 & 0 \\ -6 & -5 & 2 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ -51 & -5 & \mathbf{2} & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 3 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 2 \end{bmatrix} \quad B \cdot y = \begin{pmatrix} 15 \\ 3 \\ 7 \end{pmatrix}$$

$$y_1 = 5$$

$$y_2 = -1$$

$$y_3 = \frac{3}{2}$$

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ -17 & \mathbf{2} & 0 & 0 & 0 \\ -6 & -5 & 2 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ -51 & -5 & \mathbf{2} & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 \end{bmatrix}$$

•

$$B = \begin{bmatrix} 3 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 2 \end{bmatrix} \quad B \cdot y = \begin{pmatrix} 15 \\ 3 \\ 7 \end{pmatrix}$$

▶
$$y_1 = 5$$

$$y_2 = -1$$

$$y_3 = \frac{3}{2}$$

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ -17 & \mathbf{2} & 0 & 0 & 0 \\ -6 & -5 & 2 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ -51 & -5 & \mathbf{2} & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 \end{bmatrix}$$

•

$$B = \begin{bmatrix} 3 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 2 \end{bmatrix} \quad B \cdot y = \begin{pmatrix} 15 \\ 3 \\ 7 \end{pmatrix}$$

- $y_1 = 5$
- $y_2 = -1$
- $y_3 = \frac{3}{2}$
- ► The answer is **NO**

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ -17 & \mathbf{2} & 0 & 0 & 0 \\ -6 & -5 & 2 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ -51 & -5 & \mathbf{2} & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 3 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 2 \end{bmatrix} \quad B \cdot y = \begin{pmatrix} 15 \\ 3 \\ 7 \end{pmatrix}$$

$$y_1 = 5$$

$$y_2 = -1$$

$$y_3 = \frac{3}{2}$$

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ -17 & \mathbf{2} & 0 & 0 & 0 \\ -6 & -5 & 2 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ -51 & -5 & \mathbf{2} & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 \end{bmatrix}$$

•

$$B = \begin{bmatrix} 3 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 2 \end{bmatrix} \quad B \cdot y = \begin{pmatrix} 15 \\ 3 \\ 7 \end{pmatrix}$$

- $y_1 = 5$
- $y_2 = -1$
- $y_3 = \frac{3}{2}$
- ► The answer is **NO**!