ExtendedGCD

Notations

Traditional name

Extended greatest common divisor

Traditional notation

$\text{egcd}(n_1, n_2, \ldots, n_m)$

Mathematica StandardForm notation

`ExtendedGCD[n1, n2, .., nm]`

Primary definition

04.09.02.0001.02

$$\text{egcd}(n_1, n_2, \ldots, n_m) = \{\gcd(n_1, n_2, \ldots, n_m), \{r_1, r_2, \ldots, r_m\}\} /; \gcd(n_1, n_2, \ldots, n_m) = n_1 r_1 + n_2 r_2 + \ldots + n_m r_m \wedge \text{Re}(n_k) \in \mathbb{Z} \wedge \text{Im}(n_k) \in \mathbb{Z} \wedge \text{Re}(r_k) \in \mathbb{Z} \wedge \text{Im}(r_k) \in \mathbb{Z} \wedge 1 \leq k \leq m$$

$\text{egcd}(n_1, n_2, \ldots, n_m)$ is the extended greatest common divisor of the integers n_k. In particular, $\text{egcd}(m, n) = \{\gcd(m, n), \{r, s\}\} /; \gcd(m, n) = m r + n s \wedge \text{Re}(m) \in \mathbb{Z} \wedge \text{Im}(m) \wedge \text{Re}(n) \in \mathbb{Z} \wedge \text{Im}(n) \in \mathbb{Z} \wedge \text{Re}(r) \in \mathbb{Z} \wedge \text{Im}(r) \wedge \text{Re}(s) \in \mathbb{Z} \wedge \text{Im}(s) \in \mathbb{Z}$.

Examples: The extended greatest common divisor $\text{egcd}(21, 48)$ is $\{3, \{7, -3\}\}$ because the greatest common divisor $\gcd(21, 48) = 3$ and $21 \times 7 + 48(-3) = 3$. Similar other example is $\text{egcd}(15 - 9 i, 5 - 7 i) = \{1 + i, \{2 - 4 i, -7 + 6 i\}\} /; 1 + i = \gcd(15 - 9 i, 5 - 7 i) = (-7 + 6 i)(5 - 7 i) + (2 - 4 i)(15 - 9 i)$.

Specific values

Specialized values

04.09.03.0001.01

$$\text{egcd}(n) = \{|n|, \{\text{sgn}(n)\}\}$$

04.09.03.0004.01

$$\text{egcd}(0, n) = \{|n|, \{0, \text{sgn}(n)\}\}$$

04.09.03.0002.01

$$\text{egcd}(n, n) = \{|n|, \{0, \text{sgn}(n)\}\}$$

04.09.03.0003.01

$$\text{egcd}(n, -n) = \{|n|, \{0, -\text{sgn}(n)\}\}$$

04.09.03.0023.01

$\text{egcd}(n, n, n) = \{|n|, \{0, 0, \text{sgn}(n)\}\}$

04.09.03.0024.01

$\text{egcd}(n, n, n, n) = \{|n|, \{0, 0, 0, \text{sgn}(n)\}\}$

04.09.03.0025.01

$\text{egcd}(n_1, n_2, \ldots, n_p) = \{|n_1|, \{m_1, m_2, \ldots, m_{p-1}, \text{sgn}(n_1)\}\} /; n_1 = n_2 = \ldots = n_p \wedge m_1 = m_2 = \ldots = m_{p-1} = 0$

Values at fixed points

04.09.03.0005.01

$\text{egcd}(1, 1) = \{1, \{0, 1\}\}$

04.09.03.0006.01

$\text{egcd}(1, 2) = \{1, \{1, 0\}\}$

04.09.03.0007.01

$\text{egcd}(2, 2) = \{2, \{0, 1\}\}$

04.09.03.0008.01

$\text{egcd}(3, 2) = \{1, \{1, -1\}\}$

04.09.03.0009.01

$\text{egcd}(4, 2) = \{2, \{0, 1\}\}$

04.09.03.0010.01

$\text{egcd}(1, 3) = \{1, \{1, 0\}\}$

04.09.03.0011.01

$\text{egcd}(2, 3) = \{1, \{-1, 1\}\}$

04.09.03.0012.01

$\text{egcd}(3, 3) = \{3, \{0, 1\}\}$

04.09.03.0013.01

$\text{egcd}(4, 3) = \{1, \{1, -1\}\}$

04.09.03.0014.01

$\text{egcd}(5, 3) = \{1, \{-1, 2\}\}$

04.09.03.0015.01

$\text{egcd}(6, 3) = \{3, \{0, 1\}\}$

04.09.03.0016.01

$\text{egcd}(4, 6) = \{2, \{-1, 1\}\}$

04.09.03.0017.01

$\text{egcd}(36, 45) = \{9, \{-1, 1\}\}$

04.09.03.0018.01

$\text{egcd}(-36, 45) = \{9, \{1, 1\}\}$

04.09.03.0019.01

$\text{egcd}(36, -45) = \{9, \{-1, -1\}\}$

04.09.03.0020.01

$\text{egcd}(-36, -45) = \{9, \{1, -1\}\}$

04.09.03.0021.01

$\text{egcd}(-45, -36) = \{9, \{-1, 1\}\}$

04.09.03.0022.01

$\text{egcd}(12, 30) = \{6, \{-2, 1\}\}$

General characteristics

Domain and analyticity

egcd$(n_1, n_2, \ldots, n_m)$ is an vector-valued nonanalytical function defined over $\mathbb{Z}^m$.

04.09.04.0001.02

$(n_1 * n_2 * \ldots * n_m) \longrightarrow \text{egcd}(n_1, n_2, \ldots, n_m) :: \mathbb{Z}^m \longrightarrow \mathbb{Z} \otimes \mathbb{Z}^m$

Symmetries and periodicities

Permutation symmetry

No symmetry

Periodicity

No periodicity

Transformations

Transformations and argument simplifications

Argument involving basic arithmetic operations

04.09.16.0003.01

$\text{egcd}(m + k\, n, n)[\![2, 1]\!] = \text{egcd}(m, n)[\![2, 1]\!] \;/;\; k \in \mathbb{Z}$

Representations through equivalent functions

With related functions

04.09.27.0001.02

$\text{egcd}(m, n) = \{\gcd(m, n), \{r, s\}\} \;/;\; \gcd(m, n) = m\, r + n\, s \land \text{Re}(m) \in \mathbb{Z} \land \text{Im}(m) \in \mathbb{Z} \land \text{Re}(n) \in \mathbb{Z} \land \text{Im}(n) \in \mathbb{Z} \land \text{Re}(r) \in \mathbb{Z} \land \text{Im}(r) \in \mathbb{Z} \land \text{Re}(s) \in \mathbb{Z} \land \text{Im}(s) \in \mathbb{Z}$

04.09.27.0002.01

$\text{egcd}(n_1, n_2, \ldots, n_m) = \{\gcd(n_1, n_2, \ldots, n_m), \{r_1, r_2, \ldots, r_m\}\} \;/;\; \gcd(n_1, n_2, \ldots, n_m) = n_1\, r_1 + n_2\, r_2 + \ldots + n_m\, r_m \land \text{Re}(n_k) \in \mathbb{Z} \land \text{Im}(n_k) \in \mathbb{Z} \land \text{Re}(r_k) \in \mathbb{Z} \land \text{Im}(r_k) \in \mathbb{Z} \land 1 \leq k \leq m$

History

– Euclid

Copyright