Introductions to ExtendedGCD

Introduction to the GCD and LCM (greatest common divisor and least common multiple)

General

The legendary Greek mathematician Euclid (ca. 325–270 BC) suggested an algorithm for finding the greatest common divisor of two integers, which was later named the Euclidean algorithm. This algorithm, as well as computationally refined versions, are in widespread use today.

Definitions of GCD and LCM

The GCD and LCM group of functions includes the following three functions:

- the greatest common divisor (gcd): $\gcd(n_1, n_2, \ldots, n_m)$
- the least common multiple (lcm): $\operatorname{lcm}(n_1, n_2, \ldots, n_m)$
- the extended greatest common divisor (egcd): $\operatorname{egcd}(n_1, n_2, \ldots, n_m)$

These functions are defined in the following ways:

$$\gcd(n_1, n_2, \ldots, n_m) == p \,/;\, p \in \mathbb{Z} \bigwedge \frac{n_k}{p} \in \mathbb{Z} \bigwedge 1 \le k \le m \bigwedge \left(\neg \exists_q \, (q \in \mathbb{Z} \wedge q > p) \bigwedge \frac{n_k}{q} \in \mathbb{Z} \bigwedge 1 \le k \le m \right)$$

$$\gcd(n_1, n_2, \ldots, n_m) == p \,/;\, \operatorname{Re}(p) \in \mathbb{Z} \bigwedge \operatorname{Im}(p) \in \mathbb{Z} \bigwedge \operatorname{Re}\left(\frac{n_k}{p}\right) \in \mathbb{Z} \bigwedge \operatorname{Im}\left(\frac{n_k}{p}\right) \in \mathbb{Z} \bigwedge$$
$$1 \le k \le m \bigwedge \left(\neg \exists_q \, (|q| > |p| \wedge \operatorname{Re}(q) \in \mathbb{Z} \wedge \operatorname{Im}(q) \in \mathbb{Z}) \bigwedge \operatorname{Re}\left(\frac{n_k}{q}\right) \in \mathbb{Z} \bigwedge \operatorname{Im}\left(\frac{n_k}{q}\right) \in \mathbb{Z} \bigwedge 1 \le k \le m \right)$$

$$\operatorname{lcm}(n_1, n_2, \ldots, n_m) == p \,/;\, p \in \mathbb{N}^+ \bigwedge \frac{p}{n_k} \in \mathbb{Z} \bigwedge 1 \le k \le m \bigwedge \left(\neg \exists_q \, q < p \bigwedge p \in \mathbb{Z} \bigwedge \frac{q}{n_k} \in \mathbb{Z} \bigwedge 1 \le k \le m \right)$$

$$\operatorname{lcm}(n_1, n_2, \ldots, n_m) == p \,/;\, \operatorname{Re}(p) \in \mathbb{Z} \bigwedge \operatorname{Im}(p) \in \mathbb{Z} \bigwedge \operatorname{Re}\left(\frac{p}{n_k}\right) \in \mathbb{Z} \bigwedge \operatorname{Im}\left(\frac{p}{n_k}\right) \in \mathbb{Z} \bigwedge 1 \le k \le m \bigwedge$$
$$\left(\neg \exists_q \, (\operatorname{RAbs}(q) < |p| \wedge \operatorname{Re}(q) \in \mathbb{Z} \wedge \operatorname{Im}(q) \in \mathbb{Z}) \bigwedge \operatorname{Re}\left(\frac{q}{n_k}\right) \in \mathbb{Z} \bigwedge \operatorname{Im}\left(\frac{q}{n_k}\right) \in \mathbb{Z} \bigwedge 1 \le k \le m \right)$$

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

$\gcd(n_1, n_2, \ldots, n_m)$ is the greatest common divisor of the integers (or rational) n_k. It is the greatest integer factor common to all the n_k, $1 \le k \le m$.

$\operatorname{lcm}(n_1, n_2, \ldots, n_m)$ is the least common multiple of the integers (or rational) n_k. It is the minimal positive integer that divides all the n_k, $1 \le k \le m$.

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

Examples:

The greatest common divisor of 21 and 48, gcd(21, 48) is 3. Similar examples are gcd(27, 48, 36) == 3, gcd(27 + 3 i, 48 − 6 i) == 3 + 3 i, gcd($\frac{2}{3}$, $\frac{3}{4}$) == $\frac{1}{12}$.

The least common multiple of the three numbers 2, 4, and 5, lcm(2, 4, 5) is 20. Similar examples are lcm(27, 48, 36) == 432, lcm(27 + 3 i, 48 − 6 i) == 222 + 216 i, lcm($\frac{2}{3}$, $\frac{3}{4}$) == 6.

The extended greatest common divisor of 21 and 48 egcd (21, 48) is {3, {7, −3}} because the greatest common divisor gcd(21, 48) == 3 and 21 × 7 + 48 (−3) == 3. Similarly, 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)

Connections within the group of the GCD and LCM and with other function groups

Representations through equivalent functions

The functions gcd(n_1, n_2, …, n_m) and lcm(n_1, n_2, …, n_m) satisfy the following interrelations:

$$\gcd(n, m) == \frac{n\,m}{\operatorname{lcm}(n, m)} /; m \in \mathbb{N}^+ \bigwedge n \in \mathbb{N}^+$$

$$\gcd(n_1, n_2, \ldots, n_m) == \frac{\left(\prod_{k_1=1}^{m} n_{k_1}\right) \times \left(\prod_{k_1=1}^{m} \prod_{k_2=k_1+1}^{m} \prod_{k_3=k_2+1}^{m} \operatorname{lcm}\left(n_{k_1}, n_{k_2}, n_{k_3}\right)\right) \ldots}{\left(\prod_{k_1=1}^{m} \prod_{k_2=k_1+1}^{m} \operatorname{lcm}\left(n_{k_1}, n_{k_2}\right)\right) \times \left(\prod_{k_1=1}^{m} \prod_{k_2=k_1+1}^{m} \prod_{k_3=k_2+1}^{m} \prod_{k_4=k_3+1}^{m} \operatorname{lcm}\left(n_{k_1}, n_{k_2}, n_{k_3}, n_{k_4}\right)\right) \ldots}$$

$$\operatorname{lcm}(n, m) == \frac{n\,m}{\gcd(n, m)} /; m \in \mathbb{N}^+ \bigwedge n \in \mathbb{N}^+$$

lcm(n, m, k) gcd($n\,m$, $m\,k$, $k\,n$) == $n\,m\,k$ /; {n, m, k} ∈ ℤ

gcd(lcm(k, m), lcm(k, n), lcm(m, n)) == lcm(gcd(k, m), gcd(k, n), gcd(m, n)) /; {n, m, k} ∈ ℤ.

The best-known properties and formulas of the GCD and LCM

Specific values for specialized variables

The functions GCD and LCM gcd(n_1, n_2, …, n_m), egcd(n_1, n_2, …, n_m), and lcm(n_1, n_2, …, n_m) have the following values for specialized values:

gcd	**egcd**	**lcm**
$\gcd(n) == \lvert n\rvert$	$\text{egcd}(n) == \{\lvert n\rvert, \{\text{sgn}(n)\}\}$	$\text{lcm}(n) == \lvert n\rvert$
$\gcd(0, n) == n$	$\text{egcd}(0, n) == \{\lvert n\rvert, \{0, \text{sgn}(n)\}\}$	$\text{lcm}(0\, n) == 0$
$\gcd(n, n) == \lvert n\rvert$	$\text{egcd}(n, n) == \{\lvert n\rvert, \{0, \text{sgn}(n)\}\}$	$\text{lcm}(n, n) == \lvert n\rvert$
$\gcd(n, -n) == \lvert n\rvert$	$\text{egcd}(n, -n) == \{\lvert n\rvert, \{0, -\text{sgn}(n)\}\}$	$\text{lcm}(n, -n) == \lvert n\rvert$
$\gcd(n_1, n_1, \ldots, n_1) == \lvert n_1\rvert$	$\text{egcd}(n_1, n_2, \ldots, n_p) == \{\lvert n_1\rvert, \{m_1, m_2, \ldots, m_{p-1}, \text{sgn}(n_1)\}\}$ /; $n_1 == n_2 == \ldots == n_p \bigwedge m_1 == m_2 == \ldots == m_{p-1} == 0$	$\text{lcm}(n_1, n_1, \ldots, n_1) == \lvert n_1$
$\gcd(p_1, p_2) == 1$ /; $p_1 \neq p_2 \bigwedge p_1 \in \mathbb{P} \bigwedge p_2 \in \mathbb{P}$		$\text{lcm}(p_1, p_2) == p_1\, p_2$ /; $p_1 \neq p_2 \bigwedge p_1 \in \mathbb{P} \bigwedge p_2$
$\gcd(n, \text{lcm}(m, n)) == n$ /; $m \in \mathbb{N}^+ \bigwedge n \in \mathbb{N}^+$		$\text{lcm}(n, \gcd(m, n)) == n$ /;
$\gcd(n, \text{lcm}(p, q)) == \text{lcm}(\gcd(n, p), \gcd(n, q))$ /; $n \in \mathbb{N}^+ \bigwedge p \in \mathbb{N}^+ \bigwedge q \in \mathbb{N}^+$		$\text{lcm}(n, \gcd(p, q)) == \gcd($ $n \in \mathbb{N}^+ \bigwedge p \in \mathbb{N}^+ \bigwedge q$
$\gcd(\text{lcm}(n, p), \text{lcm}(n, q)) == \text{lcm}(n, \gcd(p, q))$ /; $n \in \mathbb{N}^+ \bigwedge p \in \mathbb{N}^+ \bigwedge q \in \mathbb{N}^+$		$\text{lcm}(\gcd(n, p), \gcd(n, q))$ $n \in \mathbb{N}^+ \bigwedge p \in \mathbb{N}^+ \bigwedge q \in$
$\gcd(\text{lcm}(k, m), \text{lcm}(k, n), \text{lcm}(m, n)) == \text{lcm}(\gcd(k, m), \gcd(k, n), \gcd(m, n))$ /; $k \in \mathbb{N}^+ \bigwedge m \in \mathbb{N}^+ \bigwedge n \in \mathbb{N}^+$		$\text{lcm}(\gcd(k, m), \gcd(k, n)$ $\gcd(\text{lcm}(k, m), \text{lcm}(k$ $k \in \mathbb{N}^+ \bigwedge m \in \mathbb{N}^+ \bigwedge n \in$

$\gcd(n \bmod m, m) == \gcd(n, m)$ /; $m \in \mathbb{N}^+$

$\gcd(2^m - 1, 2^n - 1) == 2^{\gcd(m,n)} - 1$ /; $m \in \mathbb{N}^+ \bigwedge n \in \mathbb{N}^+$

$\gcd(F_m, F_n) == F_{\gcd(m,n)}$ /; $m \in \mathbb{Z} \bigwedge n \in \mathbb{Z}$.

The first values of the greatest common divisor ($\gcd(m, n)$) of the integers m and n for $1 \le m \le 20$ and $1 \le n \le 20$ are described in the following table:

$m \setminus n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2
3	1	1	3	1	1	3	1	1	3	1	1	3	1	1	3	1	1	3	1	1
4	1	2	1	4	1	2	1	4	1	2	1	4	1	2	1	4	1	2	1	4
5	1	1	1	1	5	1	1	1	1	5	1	1	1	1	5	1	1	1	1	5
6	1	2	3	2	1	6	1	2	3	2	1	6	1	2	3	2	1	6	1	2
7	1	1	1	1	1	1	7	1	1	1	1	1	1	7	1	1	1	1	1	1
8	1	2	1	4	1	2	1	8	1	2	1	4	1	2	1	8	1	2	1	4
9	1	1	3	1	1	3	1	1	9	1	1	3	1	1	3	1	1	9	1	1
10	1	2	1	2	5	2	1	2	1	10	1	2	1	2	5	2	1	2	1	10
11	1	1	1	1	1	1	1	1	1	1	11	1	1	1	1	1	1	1	1	1
12	1	2	3	4	1	6	1	4	3	2	1	12	1	2	3	4	1	6	1	4
13	1	1	1	1	1	1	1	1	1	1	1	1	13	1	1	1	1	1	1	1
14	1	2	1	2	1	2	7	2	1	2	1	2	1	14	1	2	1	2	1	2
15	1	1	3	1	5	3	1	1	3	5	1	3	1	1	15	1	1	3	1	5
16	1	2	1	4	1	2	1	8	1	2	1	4	1	2	1	16	1	2	1	4
17	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	17	1	1	1
18	1	2	3	2	1	6	1	2	9	2	1	6	1	2	3	2	1	18	1	2
19	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	19	1
20	1	2	1	4	5	2	1	4	1	10	1	4	1	2	5	4	1	2	1	20

The first values of the extended greatest common divisor (egcd(m, n) of the integers m and n for $1 \le m \le 10$ and $1 \le n \le 10$ are described in the following table:

$m \setminus n$	1	2	3	4	5	6	7	8	9	1
1	{1, {0, 1}}	{1, {1, 0}}	{1, {1, 0}}	{1, {1, 0}}	{1, {1, 0}}	{1, {1, 0}}	{1, {1, 0}}	{1, {1, 0}}	{1, {1, 0}}	{
2	{1, {0, 1}}	{2, {0, 1}}	{1, {−1, 1}}	{2, {1, 0}}	{1, {−2, 1}}	{2, {1, 0}}	{1, {−3, 1}}	{2, {1, 0}}	{1, {−4, 1}}	{
3	{1, {0, 1}}	{1, {1, −1}}	{3, {0, 1}}	{1, {−1, 1}}	{1, {2, −1}}	{3, {1, 0}}	{1, {−2, 1}}	{1, {3, −1}}	{3, {1, 0}}	{
4	{1, {0, 1}}	{2, {0, 1}}	{1, {1, −1}}	{4, {0, 1}}	{1, {−1, 1}}	{2, {−1, 1}}	{1, {2, −1}}	{4, {1, 0}}	{1, {−2, 1}}	{
5	{1, {0, 1}}	{1, {1, −2}}	{1, {−1, 2}}	{1, {1, −1}}	{5, {0, 1}}	{1, {−1, 1}}	{1, {3, −2}}	{1, {−3, 2}}	{1, {2, −1}}	{
6	{1, {0, 1}}	{2, {0, 1}}	{3, {0, 1}}	{2, {1, −1}}	{1, {1, −1}}	{6, {0, 1}}	{1, {−1, 1}}	{2, {−1, 1}}	{3, {−1, 1}}	{
7	{1, {0, 1}}	{1, {1, −3}}	{1, {1, −2}}	{1, {−1, 2}}	{1, {−2, 3}}	{1, {1, −1}}	{7, {0, 1}}	{1, {−1, 1}}	{1, {4, −3}}	{
8	{1, {0, 1}}	{2, {0, 1}}	{1, {−1, 3}}	{4, {0, 1}}	{1, {2, −3}}	{2, {1, −1}}	{1, {1, −1}}	{8, {0, 1}}	{1, {−1, 1}}	{
9	{1, {0, 1}}	{1, {1, −4}}	{3, {0, 1}}	{1, {1, −2}}	{1, {−1, 2}}	{3, {1, −1}}	{1, {−3, 4}}	{1, {1, −1}}	{9, {0, 1}}	{
10	{1, {0, 1}}	{2, {0, 1}}	{1, {1, −3}}	{2, {1, −2}}	{5, {0, 1}}	{2, {−1, 2}}	{1, {−2, 3}}	{2, {1, −1}}	{1, {1, −1}}	{

The first values of the least common multiple (lcm (m, n)) of the integers m and n for $1 \le m \le 20$ and $1 \le n \le 20$ are described in the following table:

$m \setminus n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	2	2	6	4	10	6	14	8	18	10	22	12	26	14	30	16	34	18	38	20
3	3	6	3	12	15	6	21	24	9	30	33	12	39	42	15	48	51	18	57	60
4	4	4	12	4	20	12	28	8	36	20	44	12	52	28	60	16	68	36	76	20
5	5	10	15	20	5	30	35	40	45	10	55	60	65	70	15	80	85	90	95	20
6	6	6	6	12	30	6	42	24	18	30	66	12	78	42	30	48	102	18	114	60
7	7	14	21	28	35	42	7	56	63	70	77	84	91	14	105	112	119	126	133	140
8	8	8	24	8	40	24	56	8	72	40	88	24	104	56	120	16	136	72	152	40
9	9	18	9	36	45	18	63	72	9	90	99	36	117	126	45	144	153	18	171	180
10	10	10	30	20	10	30	70	40	90	10	110	60	130	70	30	80	170	90	190	20
11	11	22	33	44	55	66	77	88	99	110	11	132	143	154	165	176	187	198	209	220
12	12	12	12	12	60	12	84	24	36	60	132	12	156	84	60	48	204	36	228	60
13	13	26	39	52	65	78	91	104	117	130	143	156	13	182	195	208	221	234	247	260
14	14	14	42	28	70	42	14	56	126	70	154	84	182	14	210	112	238	126	266	140
15	15	30	15	60	15	30	105	120	45	30	165	60	195	210	15	240	255	90	285	60
16	16	16	48	16	80	48	112	16	144	80	176	48	208	112	240	16	272	144	304	80
17	17	34	51	68	85	102	119	136	153	170	187	204	221	238	255	272	17	306	323	340
18	18	18	18	36	90	18	126	72	18	90	198	36	234	126	90	144	306	18	342	180
19	19	38	57	76	95	114	133	152	171	190	209	228	247	266	285	304	323	342	19	380
20	20	20	60	20	20	60	140	40	180	20	220	60	260	140	60	80	340	180	380	20

Analyticity

The functions $\gcd(n_1, n_2, \ldots, n_m)$ and $\operatorname{lcm}(n_1, n_2, \ldots, n_m)$ are nonanalytical functions defined over $\mathbb{Z}^m$ with values in $\mathbb{Z}$.

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

Periodicity

All three functions $\gcd(n_1, n_2, \ldots, n_m)$, egcd$(n_1, n_2, \ldots, n_m)$, and $\operatorname{lcm}(n_1, n_2, \ldots, n_m)$ do not have periodicity.

Parity and symmetry

The functions $\gcd(n_1, n_2, \ldots, n_m)$ and $\operatorname{lcm}(n_1, n_2, \ldots, n_m)$ are even functions:

$$\gcd(-n_1, -n_2, \ldots, -n_m) == \gcd(n_1, n_2, \ldots, n_m)$$

$$\gcd(-n_1, n_2, \ldots, n_m) == \gcd(n_1, n_2, \ldots, n_m)$$

$$\operatorname{lcm}(-n_1, -n_2, \ldots, -n_m) == \operatorname{lcm}(n_1, n_2, \ldots, n_m)$$

$$\operatorname{lcm}(-n_1, n_2, \ldots, n_m) == \operatorname{lcm}(n_1, n_2, \ldots, n_m).$$

The functions $\gcd(n_1, n_2, \ldots, n_m)$ and $\operatorname{lcm}(n_1, n_2, \ldots, n_m)$ have permutation symmetry:

$$\gcd(m, n) == \gcd(n, m)$$

$$\gcd\left(n_1, n_2, \ldots, n_k, \ldots, n_j, \ldots, n_m\right) == \gcd\left(n_1, n_2, \ldots, n_j, \ldots, n_k, \ldots, n_m\right) /; n_k \neq n_j \wedge k \neq j$$

$$\operatorname{lcm}(m, n) == \operatorname{lcm}(n, m)$$

$$\text{lcm}\left(n_1, n_2, \ldots, n_k, \ldots, n_j, \ldots, n_m\right) == \text{lcm}\left(n_1, n_2, \ldots, n_j, \ldots, n_k, \ldots, n_m\right) /; n_k \neq n_j \bigwedge k \neq j.$$

Series representations

The function gcd(m, n) has the following sum representations:

$$\text{gcd}(m, n) == m + n - m\,n + 2\sum_{k=1}^{m-1}\left\lfloor \frac{k\,n}{m} \right\rfloor$$

$$\text{gcd}(m, n) == 1 - 2\left\lfloor \frac{m}{2} \right\rfloor\left\lfloor \frac{n}{2} \right\rfloor - \delta_{\frac{m}{2}-\left\lfloor \frac{m}{2} \right\rfloor}\,\delta_{\frac{n}{2}-\left\lfloor \frac{n}{2} \right\rfloor} + 2\sum_{k=1}^{\left\lfloor \frac{m}{2} \right\rfloor}\left\lfloor \frac{k\,n}{m} \right\rfloor + 2\sum_{k=1}^{\left\lfloor \frac{n}{2} \right\rfloor}\left\lfloor \frac{k\,m}{n} \right\rfloor,$$

where $\lfloor p \rfloor$ is the floor function and δ_q is the Kronecker delta function.

Product representations

The functions gcd(n_1, n_2) and lcm(n_1, n_2) have the following product representations:

$$\text{gcd}(n_1, n_2) == \prod_{j=1}^{j_k} p_{i,j}^{\min\left(\alpha_{1,j}, \alpha_{2,j}\right)} /;$$

$$n_1 \in \mathbb{N}^+ \bigwedge n_2 \in \mathbb{N}^+ \bigwedge \text{factors}(n_k) == \left\{\{p_{k,1}, \alpha_{k,1}\}, \ldots, \left\{p_{k,j_k}, \alpha_{k,j_k}\right\}\right\} \bigwedge p_{k,j} \in \mathbb{P} \bigwedge \alpha_{k,j} \in \mathbb{N}^+ \bigwedge 1 \leq k \leq 2$$

$$\text{lcm}(n_1, n_2) == \prod_{j=1}^{j_k} p_{i,j}^{\max\left(\alpha_{1,j}, \alpha_{2,j}\right)} /;$$

$$n_1 \in \mathbb{N}^+ \bigwedge n_2 \in \mathbb{N}^+ \bigwedge \text{factors}(n_k) == \left\{\{p_{k,1}, \alpha_{k,1}\}, \ldots, \left\{p_{k,j_k}, \alpha_{k,j_k}\right\}\right\} \bigwedge p_{k,j} \in \mathbb{P} \bigwedge \alpha_{k,j} \in \mathbb{N}^+ \bigwedge 1 \leq k \leq 2.$$

Generating functions

The function gcd(k, n) can be represented as the coefficients of the series expansion of corresponding generating functions, which includes a sum of the Euler totient function:

$$\sum_{k=1}^{\infty} \text{gcd}(k, n)\, x^k == \sum_{d|n} \phi(d)\, \frac{x^d}{1 - x^d}.$$

Transformations with multiple arguments

The GCD and LCM functions gcd(n_1, n_2, …, n_m), egcd(n_1, n_2, …, n_m), and lcm(n_1, n_2, …, n_m) satisfy special relations including multiple arguments, for example:

$$\text{gcd}(p\,n_1, p\,n_2, \ldots, p\,n_m) == p\,\text{gcd}(n_1, n_2, \ldots, n_m) /; p \in \mathbb{N}$$

$$\text{gcd}(m\,\mu, n\,\nu) == \text{gcd}(m, n)\,\text{gcd}(\mu, \nu)\,\text{gcd}\left(\frac{m}{\text{gcd}(m, n)}, \frac{\nu}{\text{gcd}(\mu, \nu)}\right)\text{gcd}\left(\frac{n}{\text{gcd}(m, n)}, \frac{\mu}{\text{gcd}(\mu, \nu)}\right) /;$$
$$m \in \mathbb{N}^+ \bigwedge n \in \mathbb{N}^+ \bigwedge \mu \in \mathbb{N}^+ \bigwedge \nu \in \mathbb{N}^+.$$

Identities

The GCD and LCM functions satisfy some parallel identities that can be presented in the forms shown in the following table:

gcd	**lcm**
gcd (gcd(m, n), p) == gcd (m, gcd(n, p))	lcm (lcm(m, n), p) == lcm (m, lcm(n, p))
gcd (n_1, gcd(n_2, n_3, …, n_m)) == gcd (n_1, n_2, n_3, …, n_m)	lcm (n_1, lcm(n_2, n_3, …, n_m)) == lcm (n_1, n_2, n_3, …, n_m)
gcd (m, n, p) == gcd (m, gcd(n, p))	lcm (m, n, p) == lcm (m, lcm(n, p))

Summation

There are many finite and infinite sums containing GCD and LCM functions, for example:

$$\sum_{k_1=1}^{n}\sum_{k_2=1}^{n}\cdots\sum_{k_m=1}^{n} F(\gcd(k_1, k_2, \ldots, k_m)) == \sum_{k=1}^{n} f(d)\left\lfloor\frac{n}{d}\right\rfloor^m /; F(n) == \sum_{d|n} f(d)$$

$$\sum_{n=1}^{\infty}\sum_{k=1}^{n}\frac{\delta_{1,\gcd(k,n)}}{k\,n\,(k+n)} == \frac{5}{4}$$

$$\sum_{n=1}^{\infty}\sum_{k=1}^{n}\frac{\delta_{1,\gcd(k,n)}}{n^2\,(k+n)} == \frac{3}{4}$$

$$\sum_{n=1}^{\infty}\sum_{k=1}^{n}\frac{\delta_{1,\gcd(k,n])}}{k\,n\,(k+n)^2} == \frac{3}{8}$$

$$\sum_{n=1}^{\infty}\sum_{k=1}^{n}\frac{\delta_{1,\gcd(k,n)}}{(k\,n\,(k+n))^2} == \frac{7}{24}$$

$$\sum_{b=1}^{\infty}\sum_{d=1}^{\infty}\frac{\delta_{1,\gcd(b,d)}}{(b\,d\,(b+d))^2} == \frac{1}{3}.$$

Limit operation

The following two related limits include the function gcd(n_1, n_2, …, n_m). The third limit includes lcm(n_1, n_2, …, n_m):

$$\lim_{n\to\infty}\frac{1}{n^2}\sum_{k=1}^{n}\sum_{l=1}^{n}\delta_{1,\gcd(k,l)} == \frac{6}{\pi^2}$$

$$\lim_{n\to\infty}\frac{1}{n^r}\sum_{k_1=1}^{n}\sum_{k_2=1}^{n}\cdots\sum_{k_r=1}^{n}\gcd(k_1, k_2, \ldots, k_r)^k == \frac{\zeta(r-k)}{\zeta(r)}$$

Inequalities

The functions gcd(n_1, n_2, …, n_m) and lcm(n_1, n_2, …, n_m) satisfy various inequalities, for example:

$$\gcd(n_1, n_2, \ldots, n_k)\,\mathrm{lcm}(n_1, n_2, \ldots, n_k)^{k-1} \le \prod_{j=1}^{k} n_j \le \gcd(n_1, n_2, \ldots, n_k)^{k-1}\,\mathrm{lcm}(n_1, n_2, \ldots, n_k) \text{ /;}$$

$$n_1 \in \mathbb{N}^+ \bigwedge n_2 \in \mathbb{N}^+ \bigwedge \ldots \bigwedge n_k \in \mathbb{N}^+ \bigwedge k \in \mathbb{N}^+$$

$$\mathrm{lcm}(1, 2, \ldots, n) \ge 2^{n-2} \text{ /; } n \in \mathbb{N}^+.$$

Applications of the GCD and LCM

The GCD and LCM functions have numerous applications throughout mathematics, number theory, symbolic algorithms, and linear Diophantine equations.

Copyright