3. Greatest Common Divisor - Least Common Multiple

Definition 3.1: The **greatest common divisor** of two natural numbers *a* and *b* is the largest natural number *c* which divides both *a* and *b*. We denote the greatest common divisor of *a* and *b* as $\gcd(a,b)$.

Example 3.2: Find $\gcd(24,90)$.

Solution: The natural numbers that divide 24 are 1, 2, 3, 4, 6, 12 and 24. The natural numbers that divide 90 are 1, 2, 3, 5, 6, 9, 10, 15, 18, 30 and 90. Therefore, $\gcd(24,90)=6$.

One way to compute the greatest common divisor of two natural numbers *a* and *b* is to write their prime factorizations. For example, in the case of the numbers 24 and 90 above, we have $24=(2)^3(3)$ and $90=(2)(3)^2(5)$. Notice that we can include all of the prime factors from both numbers by using an exponent of 0.

$$24=(2)^3(3)(5)^0$$

$$90=(2)(3)^2(5)$$

Now we take the smallest exponent that occurs for each prime factor and obtain

$$\begin{aligned}\gcd(24,90)&=(2)^{\min(3,1)}(3)^{\min(1,2)}(5)^{\min(0,1)}\\&=(2)^1(3)^1(5)^0\\&=(2)(3)\\&=6\end{aligned}$$

We generalize this idea in the theorem below.

Theorem 3.3: Let $a,b\in\mathbb{N}$ and suppose $p_1, p_2, ..., p_n$ are prime numbers so that

$$a=(p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$$

and

$$b=(p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$$

where the values $\alpha_1,\alpha_2,...,\alpha_n,\beta_1,\beta_2,...,\beta_n$ are either natural numbers or 0. Then

$$\gcd(a,b)=(p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}...(p_n)^{\min(\alpha_n,\beta_n)}$$

Proof: Let $c=\gcd(a,b)$. Since $p_1, p_2, ..., p_n$ are prime numbers, p_j divides both *a* and *b* implies that p_j divides *c*.

If $p_j^{\alpha_j}$ divides *a* and $p_j^{\beta_j}$ divides *b*, then the smaller of $p_j^{\alpha_j}$ and $p_j^{\beta_j}$ divides both *a* and *b*. (2^2 divides 12 and 2 divides 30 implies 2 divides $\gcd(12,30)=6$). So, $p_j^{\min(\alpha_j,\beta_j)}$ divides both *a* and *b*; and hence *c*. If p_j divides *a* but does not divide *b*, then p_j does not divide *c*. But when we say $p_j^{\min(\alpha_j,0)} = p_j^{0} = 1$ divides *c*, we mean that p_j does not divide *c*.

Hence, $\gcd(a,b) = (p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}\ldots(p_n)^{\min(\alpha_n,\beta_n)}$. ■

Example 3.4: Find the greatest common divisor of 1260 and 600.

Solution: The prime factorization of these numbers is given by

$$1260 = (2)^2(3)^2(5)(7)$$

and

$$600 = (2)^3(3)(5)^2$$

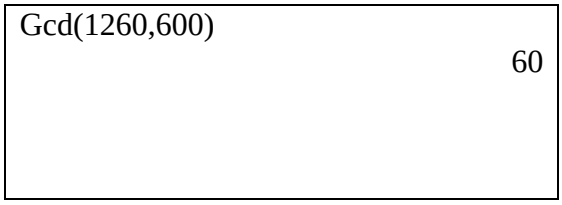
So the combined prime factors are 2, 3, 5 and 7. Notice that these are all factors of 1260. Also, 600 can be written using these prime factors as

$$600 = (2)^3(3)(5)^2(7)^0$$

Then Theorem 3.3 implies

$$\begin{aligned}\gcd(1260,600) &= (2)^{\min(2,3)}(3)^{\min(2,1)}(5)^{\min(2,1)}(7)^{\min(1,0)}\\ &= (2)^2(3)^1(5)^1(7)^0\\ &= 60\end{aligned}$$

Remark 3.5: The TI-83 function **gcd** can be used to find the greatest common divisor of two natural numbers. This function can be found by pressing **MATH**, selecting **NUM**, and then scrolling down to item 9. This will place **gcd(** on the calculator screen. Typing **1260,600)** and pressing **ENTER** results in the screen shot below.



How Do Calculators Compute The Greatest Common Divisor?

Calculators DO NOT use prime factorizations to compute the greatest common divisor of two natural numbers. Instead, they use a very efficient process called the Euclidean algorithm. We give this process after the definition and theorem below.

Definition 3.6: Let $a,b \in \mathbb{N}$. The **integer part** of a/b is the largest value c chosen from $\{0,1,2,3,...\}$ so that $c \le a/b$. We denote the **integer part** of a/b by **iPart(a/b)**.

Remark 3.7: **iPart** is a built-in function on the TI-83. You can access this function by pressing **MATH** and selecting **NUM**. The function **iPart** is item 3.

Theorem 3.8: Let $a,b \in \mathbb{N}$ with $a > b$, and suppose $c = \text{iPart}(a/b)$. Then

$$r = a - cb$$

and $0 \le r < b$.

Proof: $c = \text{iPart}(a/b)$ implies that $\frac{a}{b} = c + k$ where $0 \le k < 1$ (otherwise c will not be the largest integer which is less than or equal to a/b).

$$\frac{a}{b} = c + k \quad \Rightarrow \quad a = b(c+k) = bc + bk \quad \Rightarrow \quad a - bc = bk .$$

Since $0 \le k < 1$, we have; $0 \le bk < b$. Let $r = bk$. Then, $r = a - cb$ and $0 \le r < b$. ■

Remark 3.9: The value r in Theorem 3.8 is sometimes referred to as the **remainder** associated with the division a/b, and the integer part c of a/b is sometimes referred to as the **quotient** associated with the division a/b.

Example 3.10: The integer part of 2/3 is 0, the integer part of 9/4 is 2, and the integer part of 67/13 is 5. That is, iPart(2/3) = 0, iPart(9/4) = 2 and iPart(67/13) = 5. Theorem 14 can be realized with the equations

$$1 = 9 - (2)(4)$$

and

$$2 = 67 - (5)(13)$$

The **Euclidean algorithm** uses the Theorem 14 to find the greatest common divisor of two natural numbers. This algorithm was originally proposed in Euclid's *Elements* around 300 B.C. It is amazing that this process is still widely used in practice by high speed computing devices. The process is given below.

Euclidean algorithm

Let $a,b \in \mathbb{N}$ with $a > b$.

$r_1 = a - \text{ipart}(a/b)b$	Continue until the first time $r_i = 0$
$r_2 = b - \text{ipart}(b/r_1)r_1$	
$r_3 = r_1 - \text{ipart}(r_1/r_2)r_2$	If $i = 1$ then $\gcd(a,b) = 1$.
$r_4 = r_2 - \text{ipart}(r_2/r_3)r_3$	Otherwise, $\gcd(a,b) = r_{i-1}$.
$\vdots$	

Theorem 3.11: Let $a,b \in \mathbb{N}$ with $a > b$. The Euclidean algorithm computes $\gcd(a,b)$.

Proof: Let $a,b \in \mathbb{N}$ with $a > b$. We are looking for $\gcd(a,b)$. Suppose the remainder of the division of *a* by *b* is *c*. Then $a = qb + c$, where *q* is the quotient of the division. Any common divisor of *a* and *b* also divides *c* (since *c* can be written as $c = a - qb$); similarly any common divisor of *b* and *c* will also divide *a*. Thus, the greatest common divisor of *a* and *b* is the same as the greatest common divisor of *b* and *c*. Therefore, it is enough if we continue the process with numbers *b* and *c*. Since *c* is smaller in absolute value than *b*, we will reach $c = 0$ after finitely many steps. ■

Example 3.12: Use the Euclidean algorithm to compute $\gcd(1260,600)$.

Solution: You can verify that

$$r_1 = 1260 - \text{ipart}(1260/600)(600) = 1260 - (2)(600) = 60$$
$$r_2 = 600 - \text{ipart}(600/60)(60) = 600 - (10)(60) = 0$$

So, $\gcd(1260,600) = 60$.

Example 3.13: Use the Euclidean algorithm to compute $\gcd(860,1375)$.

Solution: The algorithm results in

$$r_1 = 1375 - (1)(860) = 515$$
$$r_2 = 860 - (1)(515) = 345$$
$$r_3 = 515 - (1)345 = 170$$
$$r_4 = 345 - (2)(170) = 5$$
$$r_5 = 170 - (34)(5) = 0$$

Consequently, $\gcd(860,1375) = 5$.

Example 3.14: Use the Euclidean algorithm to compute $\gcd(1326,741)$.

Solution: You can verify that

$$r_1 = 1326 - (1)(741) = 585$$
$$r_2 = 741 - (1)(585) = 156$$
$$r_3 = 585 - (3)(156) = 117$$
$$r_4 = 156 - (1)(117) = 39$$
$$r_5 = 117 - (3)(39) = 0$$

Consequently, $\gcd(1326, 741) = 39$.

A quantity which is closely related to the greatest common divisor is the least common multiple.

Definition 3.15: Let $a, b \in \mathbb{N}$. The **least common multiple** of *a* and *b* is the smallest natural number which is a multiple of both *a* and *b*. The least common multiple of *a* and *b* is denoted by $\text{lcm}(a,b)$.

Remark 3.16: $\text{lcm}(a,b) \le ab$ whenever $a, b \in \mathbb{N}$.

Since the $\text{lcm}(a,b)$ is the smallest number that is a multiple of both *a* and *b*, it is also the smallest number for which both *a* and *b* are divisors. As a result, all of the prime factors of *a* must divide $\text{lcm}(a,b)$, and all of the prime factors of *b* must divide $\text{lcm}(a,b)$. This leads to the following theorem.

Theorem 3.17: Let $a, b \in \mathbb{N}$, and suppose the prime factorizations of *a* and *b* are given by

$$a = (p_1)^{\alpha_1} (p_2)^{\alpha_2} \ldots (p_n)^{\alpha_n}$$

and

$$b = (p_1)^{\beta_1} (p_2)^{\beta_2} \ldots (p_n)^{\beta_n}$$

where the values $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n$ are either natural numbers or 0. Then

$$\text{lcm}(a,b) = (p_1)^{\max(\alpha_1,\beta_1)} (p_2)^{\max(\alpha_2,\beta_2)} \ldots (p_n)^{\max(\alpha_n,\beta_n)}$$

Proof: Let $c = \text{lcm}(a,b)$. If a and b are both multiples of p_j, then c is a multiple of p_j too. If a is a multiple of $p_j^{\alpha_j}$ and b is a multiple of $p_j^{\beta_j}$, then c is a multiple of the bigger of $p_j^{\alpha_j}$ and $p_j^{\beta_j}$ (since c is a multiple of both a and b).Hence, c is a multiple of $p_j^{\max(\alpha_j,\beta_j)}$. Note that, if a is not a multiple of p_j but b is; then c should be a multiple of p_j. Using $p_j^{\max(0,\beta_j)} = p_j^{\beta_j}$ solves this problem. Thus,

$$\text{lcm}(a,b) = (p_1)^{\max(\alpha_1,\beta_1)} (p_2)^{\max(\alpha_2,\beta_2)} \ldots (p_n)^{\max(\alpha_n,\beta_n)} \quad \blacksquare$$

Example 3.18: Use Theorem 17 to compute $\text{lcm}(24,15)$.

Solution: We can see that $24 = (2)^3 (3)$ and $15 = (3)(5)$. These can be written in common form as

$$24 = (2)^3 (3)(5)^0$$

and

$$15 = (2)^0 (3)(5)$$

As a result,

$$\begin{aligned} \text{lcm}(24,15) &= (2)^{\max(3,0)} (3)^{\max(1,1)} (5)^{\max(0,1)} \\ &= (2)^3 (3)^1 (5)^1 \\ &= 120 \end{aligned}$$

Example 3.19: We show the value of $\text{lcm}(a,b)$, $\gcd(a,b)$ and ab for several choices of $a,b \in \mathbb{N}$.

a, b	lcm(a,b)	gcd(a,b)	ab
16, 28	112	4	448
18, 24	72	6	432
14, 21	42	7	294
15, 24	120	3	360

Although it might not be readily apparent, the table above gives some insight to the relationship between $\text{lcm}(a,b)$, $\gcd(a,b)$ and ab. The table above has been reproduced below, along with an additional column containing the product of $\text{lcm}(a,b)$ and $\gcd(a,b)$.

a, b	lcm(a,b)	gcd(a,b)	ab	lcm(a,b)gcd(a,b)
16, 28	112	4	448	448
18, 24	72	6	432	432
14, 21	42	7	294	294
15, 24	120	3	360	360

For the choices of a and b above, it appears that

$$\text{lcm}(a,b)\gcd(a,b) = ab$$

This result is always true.

Theorem 3.20: Let $a,b \in \mathbb{N}$. Then $\text{lcm}(a,b)\gcd(a,b) = ab$.

Proof: Let $a = (p_1)^{\alpha_1} (p_2)^{\alpha_2} \ldots (p_n)^{\alpha_n}$ and $b = (p_1)^{\beta_1} (p_2)^{\beta_2} \ldots (p_n)^{\beta_n}$ where the values $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n$ are either natural numbers or 0. Then

$$\text{lcm}(a,b) = (p_1)^{\max(\alpha_1,\beta_1)} (p_2)^{\max(\alpha_2,\beta_2)} \ldots (p_n)^{\max(\alpha_n,\beta_n)}$$

and

$$\gcd(a,b)=(p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}\ldots(p_n)^{\min(\alpha_n,\beta_n)}.$$

$$\begin{aligned}\operatorname{lcm}(a,b)\gcd(a,b)&=\left[(p_1)^{\max(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)}\ldots(p_n)^{\max(\alpha_n,\beta_n)}\right]\left[(p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}\ldots(p_n)^{\min(\alpha_n,\beta_n)}\right]\\&=(p_1)^{\max(\alpha_1,\beta_1)+\min(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)+\min(\alpha_2,\beta_2)}\ldots(p_n)^{\max(\alpha_n,\beta_n)+\min(\alpha_n,\beta_n)}\end{aligned}$$

If $\max(\alpha_1,\beta_1)=\alpha_1$ then $\min(\alpha_1,\beta_1)=\beta_1$. And if $\min(\alpha_1,\beta_1)=\alpha_1$, then $\max(\alpha_1,\beta_1)=\beta_1$. Hence, in any case $\max(\alpha_1,\beta_1)+\min(\alpha_1,\beta_1)=\alpha_1+\beta_1$. So we have;

$$\begin{aligned}\operatorname{lcm}(a,b)\gcd(a,b)&=(p_1)^{\alpha_1+\beta_1}(p_2)^{\alpha_2+\beta_2}\ldots(p_n)^{\alpha_n+\beta_n}\\&=\left[(p_1)^{\alpha_1}(p_2)^{\alpha_2}\ldots(p_n)^{\alpha_n}\right]\left[(p_1)^{\beta_1}(p_2)^{\beta_2}\ldots(p_n)^{\beta_n}\right]\\&=ab\end{aligned}$$

■

Exercises

1. Use the prime factorizations of 860 and 1375 to compute $\gcd(860,1375)$.
2. Use the prime factorizations of 6300 and 1584 to compute $\gcd(6300,1584)$.
3. Use the prime factorizations of 1260 and 2640 to compute $\gcd(1260,2640)$.
4. Use the prime factorizations of 2373 and 1374 to compute $\gcd(2373,1374)$.
5. Use the division algorithm to compute $\gcd(6300,1584)$.
6. Use the division algorithm to compute $\gcd(1260,2640)$.
7. Use the division algorithm to compute $\gcd(2373,1374)$.
8. Use the prime factorizations of 75 and 124 to find $\operatorname{lcm}(75,124)$.
9. Use the prime factorizations of 236 and 125 to find $\operatorname{lcm}(236,125)$.
10. Use the prime factorizations of 84 and 118 to find $\operatorname{lcm}(84,118)$.
11. Suppose $ab=900$ and $\operatorname{lcm}(a,b)=300$. Give $\gcd(a,b)$.
12. Let $m,a,b\in\mathbb{N}$. Show that $\gcd(ma,mb)=m\gcd(a,b)$; i.e. the greatest common divisor satisfies a distributive property.
13. Let $a,b,c\in\mathbb{N}$. Show that $\gcd(\gcd(a,b),c)=\gcd(a,\gcd(b,c))$; i.e. the greatest common divisor satisfies an associative property.
14. Let $a\in\mathbb{N}$. Show that $\gcd(a,a)=a$; i.e. the greatest common divisor is idempotent.
15. Let $a,b\in\mathbb{N}$. Show that $\gcd(a,b)=\gcd(b,a)$; i.e. the greatest common divisor satisfies a commutative property.
16. Let $a,b\in\mathbb{N}$. Show that $\operatorname{lcm}(a,\gcd(a,b))=a$ and $\gcd(a,\operatorname{lcm}(a,b))=a$.
17. Let $a\in\mathbb{N}$. Show that $\operatorname{lcm}(a,a)=a$; i.e. the least common multiple is idempotent.
18. Let $a,b\in\mathbb{N}$. Show that $\operatorname{lcm}(a,b)=\operatorname{lcm}(b,a)$; i.e. the least common multiple satisfies a commutative property.

19. Let $a,b,c \in \mathbb{N}$. Show that $\text{lcm}\left(\text{lcm}(a,b),c\right) = \text{lcm}\left(a,\text{lcm}(b,c)\right)$; i.e. the least common multiple satisfies an associative property.
20. Let $m,a,b \in \mathbb{N}$. Show that $\text{lcm}\left(ma,mb\right) = m\text{lcm}\left(a,b\right)$; i.e. the least common multiple satisfies a distributive property.

Solutions:

1. $860 = 2^2 \cdot 5 \cdot 43$ and $1375 = 5^3 \cdot 11$. Therefore;

$$\begin{aligned}\gcd(860,1375) &= (2)^{\min(0,2)}(5)^{\min(1,3)}(11)^{\min(0,1)}(43)^{\min(0,1)} \\ &= (2)^0(5)(11)^0(43)^0 \\ &= 5\end{aligned}$$

2. $6300 = 2^2 \cdot 5^2 \cdot 7 \cdot 9$ and $1584 = 2^4 \cdot 9 \cdot 11$. Therefore;

$$\begin{aligned}\gcd(6300,1584) &= (2)^{\min(2,4)} \cdot (5)^{\min(0,2)} \cdot (7)^{\min(0,1)} \cdot (9) \cdot (11)^{\min(0,1)} \\ &= 2^2 \cdot 9 = 36\end{aligned}$$

3. $1260 = 2^2 \cdot 5 \cdot 7 \cdot 9$ and $2640 = 2^4 \cdot 3 \cdot 5 \cdot 11$. Therefore;

$$\begin{aligned}\gcd(1260,2640) &= (2)^{\min(2,4)}(3)^{\min(0,1)}(5)(7)^{\min(0,1)}(9)^{\min(0,1)}(11)^{\min(0,1)} \\ &= (2)^2(5) = 20\end{aligned}$$

4. $2373 = 3 \cdot 7 \cdot 113$ and $1374 = 2 \cdot 3 \cdot 229$. Therefore;

$$\gcd(2373,1374) = (2)^0(3)(7)^0(113)^0(229)^0 = 3.$$

5. $\gcd(6300,1584)$

$$\begin{aligned}r_1 &= 6300 - (3)(1584) = 1548 \\ r_2 &= 1584 - (1)(1548) = 36 \\ r_3 &= 1548 - (43)36 = 0\end{aligned}$$

Thus; $\gcd(6300,1584)=36$.

6.

$$r_1 = 2640-(2)(1260)=120$$
$$r_2 = 1260-(10)(120)=60$$
$$r_3 = 120-(2)60=0$$

Consequently, $\gcd(1260,2640)=60$.

7.

$$r_1 = 2373-(1)(1374)=999$$
$$r_2 = 1374-(1)(999)=375$$
$$r_3 = 999-(2)375=249$$
$$r_4 = 375-(1)(249)=126$$
$$r_5 = 249-(1)(126)=123$$
$$r_6 = 126-(1)(123)=3$$
$$r_7 = 123-(41)(3)=0$$

Hence, $\gcd(2373,1374)=3$.

8. $75=3\cdot 5^2$ and $124=2^2\cdot 31$.
Thus,

$$\begin{aligned}\operatorname{lcm}(75,124) &= (2)^{\max(2,0)}(3)^{\max(1,0)}(5)^{\max(2,0)}(31)^{\max(1,0)}\\ &= (2)^2(3)^1(5)^2(31)^1\\ &= 9300\end{aligned}$$

9. $236=2^2\cdot 59$ and $125=5^3$.
Hence,

$$\begin{aligned}\operatorname{lcm}(236,125) &= (2)^{\max(2,0)}(5)^{\max(3,0)}(59)^{\max(1,0)}\\ &= (2)^2(5)^3(59)^1\\ &= 29500\end{aligned}$$

10. $84=2^2\cdot 3\cdot 7$ and $118=2\cdot 59$.
Therefore,

$$\begin{aligned}\operatorname{lcm}(84,118) &= (2)^{\max(2,1)}(3)^{\max(1,0)}(7)^{\max(1,0)}(59)^{\max(1,0)} \\ &= (2)^2(3)^1(7)^1(59)^1 \\ &= 4956\end{aligned}$$

11. Suppose $ab = 900$ and $\operatorname{lcm}(a,b) = 300$. We know that $\operatorname{lcm}(a,b)\gcd(a,b) = ab$.

So, $\gcd(a,b) = \dfrac{ab}{\operatorname{lcm}(a,b)} = \dfrac{900}{300} = 3$. The greatest common divisor is:

$\gcd(a,b) = 3$.

12. Let $m, a, b \in \mathbb{N}$.

Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ and $b = (p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$, where the values $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n$ are either natural numbers or 0. Then

$\gcd(a,b) = (p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}...(p_n)^{\min(\alpha_n,\beta_n)}$

We have: $ma = (m)(p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ and $mb = (m)(p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$.

So, the greatest common divisor is:

$$\begin{aligned}\gcd(ma,mb) &= (m)^{\min(1,1)}(p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}...(p_n)^{\min(\alpha_n,\beta_n)} \\ &= m(p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}...(p_n)^{\min(\alpha_n,\beta_n)} \\ &= m\gcd(a,b)\end{aligned}$$

Hence, the greatest common divisor satisfies a distributive property.

13. Let $a, b, c \in \mathbb{N}$.

Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$, $b = (p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$ and $c = (p_1)^{\gamma_1}(p_2)^{\gamma_2}...(p_n)^{\gamma_n}$, where the values $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n, \gamma_1, \gamma_2, ..., \gamma_n$ are either natural numbers or 0. Then

$\gcd(a,b) = (p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}...(p_n)^{\min(\alpha_n,\beta_n)}$ and

$\gcd(b,c) = (p_1)^{\min(\beta_1,\gamma_1)}(p_2)^{\min(\beta_2,\gamma_2)}...(p_n)^{\min(\beta_n,\gamma_n)}$.

$\gcd(\gcd(a,b),c) = (p_1)^{\min(\min(\alpha_1,\beta_1),\gamma_1)}(p_2)^{\min(\min(\alpha_2,\beta_2),\gamma_2)}...(p_n)^{\min(\min(\alpha_n,\beta_n),\gamma_n)}$ and

$$\gcd\left(a,\gcd\left(b,c\right)\right)=\left(p_1\right)^{\min(\alpha_1,\min(\beta_1,\gamma_1))}\left(p_2\right)^{\min(\alpha_2,\min(\beta_2,\gamma_2))}...\left(p_n\right)^{\min(\alpha_n,\min(\beta_n,\gamma_n))}.$$

Here, it is important to observe that
$\min(\min(\alpha_n,\beta_n),\gamma_n)=\min(\alpha_n,\min(\beta_n,\gamma_n))=\min(\alpha_n,\beta_n,\gamma_n)$.
The reason behind this is; while comparing 3 natural numbers, you can start comparing from whichever you want. If you want to find the smallest of 5, 9 and 6, then arrange them in order; 5 < 6 < 9. The smallest is 5, this does not change. So, it is not important if you compare 5 & 9 first and then the result with 6; or if you compare 6 & 9 first and then the result with 5.

Therefore, $\gcd\left(\gcd(a,b),c\right)=\gcd\left(a,\gcd(b,c)\right)$; i.e. the greatest common divisor satisfies an associative property.

14. Let $a\in\mathbb{N}$. Show that $\gcd(a,a)=a$; i.e. the greatest common divisor is idempotent.
Suppose $p_1,p_2,...,p_n$ are prime numbers so that $a=\left(p_1\right)^{\alpha_1}\left(p_2\right)^{\alpha_2}...\left(p_n\right)^{\alpha_n}$ where the values $\alpha_1,\alpha_2,...,\alpha_n$ are either natural numbers or 0. Then $\gcd\left(a,a\right)=\left(p_1\right)^{\min(\alpha_1,\alpha_1)}\left(p_2\right)^{\min(\alpha_2,\alpha_2)}...\left(p_n\right)^{\min(\alpha_n,\alpha_n)}$ where, of course, $\min(\alpha_n,\alpha_n)=\alpha_n$. Hence,

$$\begin{aligned}\gcd\left(a,a\right)&=\left(p_1\right)^{\min(\alpha_1,\alpha_1)}\left(p_2\right)^{\min(\alpha_2,\alpha_2)}...\left(p_n\right)^{\min(\alpha_n,\alpha_n)}\\&=\left(p_1\right)^{\alpha_1}\left(p_2\right)^{\alpha_2}...\left(p_n\right)^{\alpha_n}=a\end{aligned}$$

It is easier to see this result if we restate the question as “what is the greatest number that divides both *a* and *a*?”. The answer is, of course, *a* itself.

15. Let $a,b\in\mathbb{N}$. Show that $\gcd(a,b)=\gcd\left(b,a\right)$; i.e. the greatest common divisor satisfies a commutative property.
Suppose $p_1,p_2,...,p_n$ are prime numbers so that $a=\left(p_1\right)^{\alpha_1}\left(p_2\right)^{\alpha_2}...\left(p_n\right)^{\alpha_n}$ and $b=\left(p_1\right)^{\beta_1}\left(p_2\right)^{\beta_2}...\left(p_n\right)^{\beta_n}$, where the values $\alpha_1,\alpha_2,...,\alpha_n,\beta_1,\beta_2,...,\beta_n$ are either natural numbers or 0. Then

$$\gcd\left(a,b\right)=\left(p_1\right)^{\min(\alpha_1,\beta_1)}\left(p_2\right)^{\min(\alpha_2,\beta_2)}...\left(p_n\right)^{\min(\alpha_n,\beta_n)}$$

and

$$\gcd\left(b,a\right)=\left(p_1\right)^{\min(\beta_1,\alpha_1)}\left(p_2\right)^{\min(\beta_2,\alpha_2)}...\left(p_n\right)^{\min(\beta_n,\alpha_n)}.$$

The conclusion follows from the observation that $\min(\alpha_n,\beta_n)=\min(\beta_n,\alpha_n)$.
Hence, $\gcd(a,b)=\gcd\left(b,a\right)$.

16. Let $a,b \in \mathbb{N}$.

Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ and $b = (p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$, where the values $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n$ are either natural numbers or 0. Then

$\text{lcm}(a,b) = (p_1)^{\max(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)}...(p_n)^{\max(\alpha_n,\beta_n)}$ and

$\gcd(a,b) = (p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}...(p_n)^{\min(\alpha_n,\beta_n)}$.

$$\text{lcm}(a,\gcd(a,b)) = (p_1)^{\max(\alpha_1,\min(\alpha_1,\beta_1))}(p_2)^{\max(\alpha_2,\min(\alpha_2,\beta_2))}...(p_n)^{\max(\alpha_n,\min(\alpha_n,\beta_n))}$$

Let's find $\max(\alpha_1, \min(\alpha_1, \beta_1))$. If $\alpha_1 < \beta_1$, then $\min(\alpha_1, \beta_1) = \alpha_1$ and $\max(\alpha_1, \min(\alpha_1, \beta_1)) = \max(\alpha_1, \alpha_1) = \alpha_1$. If $\beta_1 < \alpha_1$, then $\min(\alpha_1, \beta_1) = \beta_1$ and $\max(\alpha_1, \min(\alpha_1, \beta_1)) = \max(\alpha_1, \beta_1) = \alpha_1$. Similarly, for any *n*, $\max(\alpha_n, \min(\alpha_n, \beta_n)) = \alpha_n$. Therefore;

$$\begin{aligned}\text{lcm}(a,\gcd(a,b)) &= (p_1)^{\max(\alpha_1,\min(\alpha_1,\beta_1))}(p_2)^{\max(\alpha_2,\min(\alpha_2,\beta_2))}...(p_n)^{\max(\alpha_n,\min(\alpha_n,\beta_n))} \\ &= (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n} = a\end{aligned}$$

$$\gcd(a,\text{lcm}(a,b)) = (p_1)^{\min(\alpha_1,\max(\alpha_1,\beta_1))}(p_2)^{\min(\alpha_2,\max(\alpha_2,\beta_2))}...(p_n)^{\min(\alpha_n,\max(\alpha_n,\beta_n))}$$

With the reasoning we used above we can conclude that $\min(\alpha_n, \max(\alpha_n, \beta_n)) = \alpha_n$. Thus,

$$\begin{aligned}\gcd(a,\text{lcm}(a,b)) &= (p_1)^{\min(\alpha_1,\max(\alpha_1,\beta_1))}(p_2)^{\min(\alpha_2,\max(\alpha_2,\beta_2))}...(p_n)^{\min(\alpha_n,\max(\alpha_n,\beta_n))} \\ &= (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n} = a\end{aligned}$$

Hence, $\text{lcm}(a,\gcd(a,b)) = a$ and $\gcd(a,\text{lcm}(a,b)) = a$.

17. Let $a \in \mathbb{N}$. Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ where the values $\alpha_1, \alpha_2, ..., \alpha_n$ are either natural numbers or 0. Then

$$\begin{aligned}\text{lcm}(a,a) &= (p_1)^{\max(\alpha_1,\alpha_1)}(p_2)^{\max(\alpha_2,\alpha_2)}...(p_n)^{\max(\alpha_n,\alpha_n)} \\ &= (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n} = a\end{aligned}$$

Therefore, $\text{lcm}(a,a) = a$; i.e. the least common multiple is idempotent.

18. Let $a,b \in \mathbb{N}$. Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ and $b = (p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$, where the values $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n$ are either natural numbers or 0. Then $\text{lcm}(a,b) = (p_1)^{\max(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)}...(p_n)^{\max(\alpha_n,\beta_n)}$ and $\text{lcm}(b,a) = (p_1)^{\max(\beta_1,\alpha_1)}(p_2)^{\max(\beta_2,\alpha_2)}...(p_n)^{\max(\beta_n,\alpha_n)}$. Since $\max(\alpha_1,\beta_1) = \max(\beta_1,\alpha_1)$, we can conclude that $\text{lcm}(a,b) = \text{lcm}(b,a)$.

19. Let $a,b,c \in \mathbb{N}$. Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$, $b = (p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$ and $c = (p_1)^{\gamma_1}(p_2)^{\gamma_2}...(p_n)^{\gamma_n}$, where the values $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n, \gamma_1, \gamma_2, ..., \gamma_n$ are either natural numbers or 0. Then $\text{lcm}(a,b) = (p_1)^{\max(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)}...(p_n)^{\max(\alpha_n,\beta_n)}$ and $\text{lcm}(b,c) = (p_1)^{\max(\beta_1,\gamma_1)}(p_2)^{\max(\beta_2,\gamma_2)}...(p_n)^{\max(\beta_n,\gamma_n)}$.

$\text{lcm}(\text{lcm}(a,b),c) = (p_1)^{\max(\max(\alpha_1,\beta_1),\gamma_1)}(p_2)^{\max(\max(\alpha_2,\beta_2),\gamma_2)}...(p_n)^{\max(\max(\alpha_n,\beta_n),\gamma_n)}$ and

$\text{lcm}(a,\text{lcm}(b,c)) = (p_1)^{\max(\alpha_1,\max(\beta_1,\gamma_1))}(p_2)^{\max(\alpha_2,\max(\beta_2,\gamma_2))}...(p_n)^{\max(\alpha_n,\max(\beta_n,\gamma_n))}$.

As we have pointed out before, the order at which you start to compare natural numbers does not matter;

$$\max(\max(\alpha_n,\beta_n),\gamma_n) = \max(\alpha_n,\max(\beta_n,\gamma_n)) = \max(\alpha_n,\beta_n,\gamma_n).$$

Hence, $\text{lcm}(\text{lcm}(a,b),c) = \text{lcm}(a,\text{lcm}(b,c))$; i.e. the least common multiple satisfies an associative property.

20. Let $m,a,b \in \mathbb{N}$.

Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ and $b = (p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$, where the values $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n$ are either natural numbers or 0. Then $\text{lcm}(a,b) = (p_1)^{\max(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)}...(p_n)^{\max(\alpha_n,\beta_n)}$

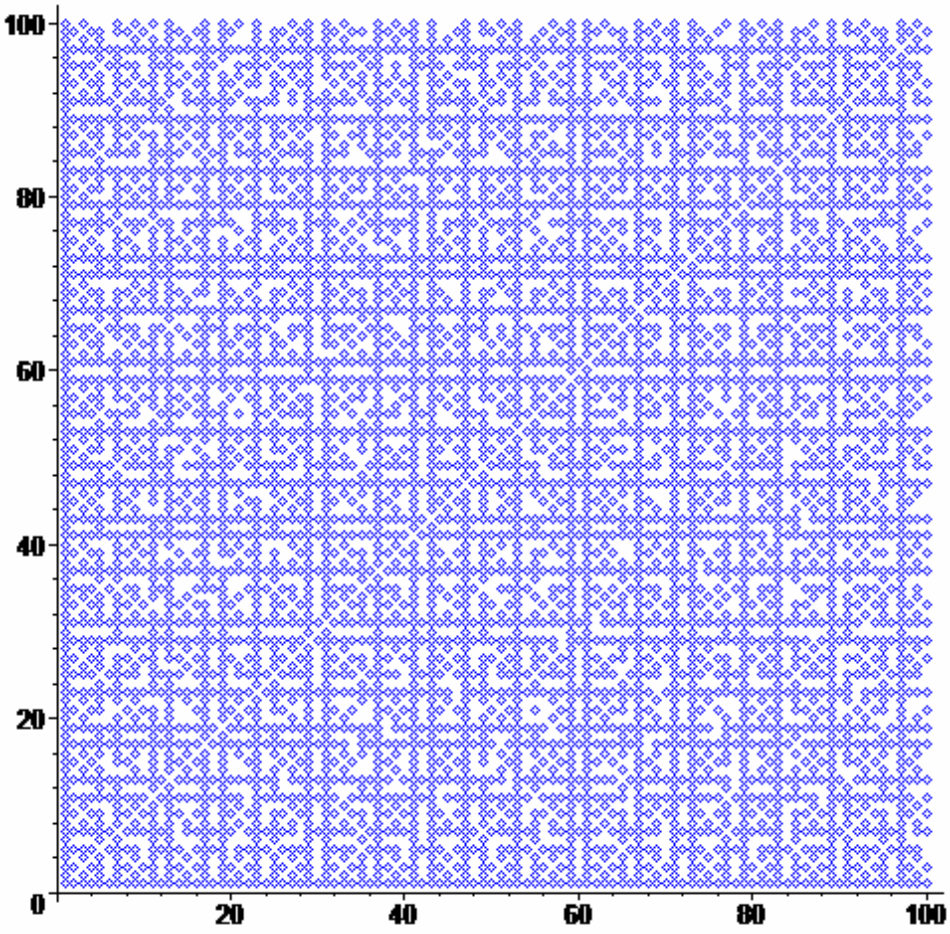
We have: $ma = (m)(p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ and $mb = (m)(p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$. So, the least common multiple is:

$$\begin{aligned}\operatorname{lcm}(ma, mb) &= (m)^{\max(1,1)}(p_1)^{\max(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)}...(p_n)^{\max(\alpha_n,\beta_n)} \\ &= m(p_1)^{\max(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)}...(p_n)^{\max(\alpha_n,\beta_n)} \\ &= m\operatorname{lcm}(a,b)\end{aligned}$$

Thus, $\operatorname{lcm}(ma, mb) = m\operatorname{lcm}(a,b)$; i.e. the least common multiple satisfies a distributive property.

Graphical Representation Of gcd(a,b) = 1

Numbers $a,b \in \mathbb{N}$ are said to be **relatively prime** if and only if $\gcd(a,b)=1$. It is possible to visualize all of the pairs (a,b) for which *a* and *b* are relatively prime by plotting the points (a,b) for *a* and *b* between 1 and 100. We give this plot below, and the pattern is very interesting! Surprisingly, there are more pairs in this range that are relatively prime than those that are not. In fact, of the 10,000 pairs (a,b) for *a* and *b* between 1 and 100, there are 6,087 pairs which are relatively prime.



(a,b) for which $\gcd(a,b)=1$ for $a,b \in \{1,...,100\}$