gcd, lcm & the Euclidean Algorithm

Table of contents

Greatest common divisor 1
Lowest common multiple 2
Computing both from the prime factorisation 2
The Euclidean algorithm 4
Proofs about gcd and lcm 5
Extended Euclidean algorithm (non-assessed) 6
Where this gets used 6
See also 6

Greatest common divisor

For integers a and b, not both zero, the **greatest common divisor** $\gcd(a, b)$ is the integer d for which:

- $d \mid a$ and $d \mid b$ — d is a divisor of both; and
- $\forall c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$ then $c \leq d$ — every other common divisor is smaller.

Order doesn't matter: $\gcd(a, b) = \gcd(b, a)$.

On the name. $\mathrm{hcf}(a, b)$ — *highest common factor* — names the same object; gcd is the name this course uses.

Negatives. The divisors of 15 are $1, 3, 5, 15, -1, -3, -5, -15$ — exactly the divisors of -15. Since an integer and its negation have the same divisors, $\gcd(-15, 36) = \gcd(15, 36)$, and in general

$$\gcd(a, b) = \gcd(|a|, |b|)$$

Note $\gcd(0, b) = b$ for every positive integer b — this is the base case the Euclidean algorithm terminates on.

Lowest common multiple

For **non-zero** integers a and b, the **lowest common multiple** $\text{lcm}(a, b)$ is the smallest integer n for which:

- $n > 0$; and
- $a \mid n$ and $b \mid n$ — n is a multiple of both.

Again $\text{lcm}(a, b) = \text{lcm}(b, a)$, and since the multiples of a are the multiples of $-a$ ($\ldots, -10, -5, 0, 5, 10, 15, \ldots$ for both 5 and -5),

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

Computing both from the prime factorisation

Using the standard factored form (see divisibility-and-factorisation[1]): take the **minimum** exponent of each prime for the gcd, the **maximum** for the lcm.

$$30 = 2 \cdot 3 \cdot 5 \qquad 72 = 2^3 \cdot 3^2$$

$$\gcd(30, 72) = 2 \cdot 3 = 6 \qquad \text{lcm}(30, 72) = 2^3 \cdot 3^2 \cdot 5 = 360$$

Lemma: if $a, b \in \mathbb{Z}^+$ then

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

Checking: $\gcd(30, 72) \cdot \text{lcm}(30, 72) = 6 \cdot 360 = 2160 = 30 \cdot 72$. Each prime's min and max exponents together account for both original exponents, which is why it works.

More generally, for non-zero integers a and b: $\gcd(a, b) \cdot \text{lcm}(a, b) = |ab|$.

Worked

- $\gcd(63, -105)$ and $\text{lcm}(63, -105)$: factor $63 = 3^2 \cdot 7$ and $-105 = -3 \cdot 5 \cdot 7$, then read off the common primes — gcd $= 3 \cdot 7 = 21$ and lcm $= 3^2 \cdot 5 \cdot 7 = 315$. (Keeping the minus sign out the front like this and replacing -105 by 105 first both work, since $\gcd(a, b) = \gcd(|a|, |b|)$.)
- For distinct primes p, q: $\gcd(p, q) = 1$ and $\text{lcm}(p, q) = pq$.
- $\text{lcm}(12, 18)$: $12 = 2^2 \cdot 3$, $18 = 2 \cdot 3^2$, so lcm $= 2^2 \cdot 3^2 = 36$.
- $\text{lcm}(2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2) = 2^3 \cdot 3^2 \cdot 5 = 360$.
- $\text{lcm}(2800, 6125)$: $2800 = 2^4 \cdot 5^2 \cdot 7$ and $6125 = 5^3 \cdot 7^2$, so lcm $= 2^4 \cdot 5^3 \cdot 7^2 = 98\,000$.

[1] courses/math1061/divisibility-and-factorisation.pdf

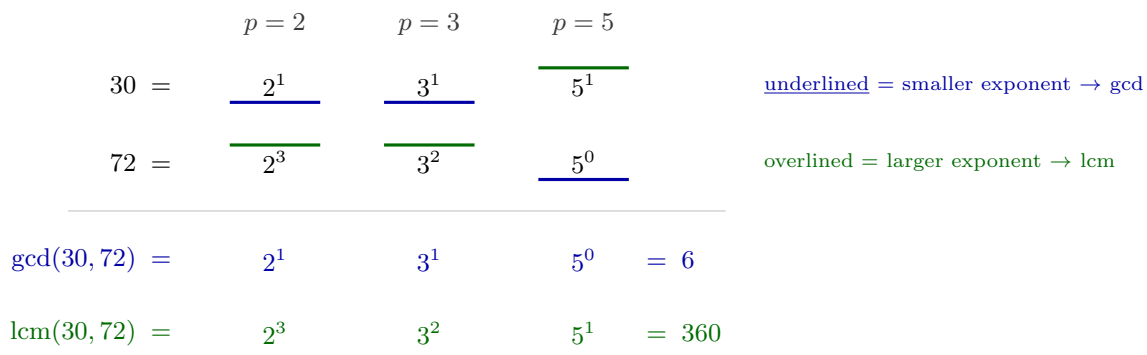

Figure 1: The min/max recipe laid out by prime column. In each column the blue underline marks the smaller exponent, which the gcd takes, and the green overline marks the larger, which the lcm takes. 72 has no factor of 5, so its entry in that column is 5^0. Setting it out this way also shows why the lemma $\gcd \cdot \operatorname{lcm} = ab$ holds: in each column the smaller and larger exponents together are exactly the two original exponents.

The Euclidean algorithm

Factorising large numbers is slow; the Euclidean algorithm finds $\gcd(a, b)$ for $a, b \in \mathbb{Z}^+$ without it. It rests on this fact:

> If $a, b \in \mathbb{Z}$ are not both zero and $q, r \in \mathbb{Z}$ satisfy $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

Why: suppose $c \mid a$ and $c \mid b$; then $c \mid (a - bq)$ and hence $c \mid r$. Conversely suppose $d \mid b$ and $d \mid r$; then $d \mid (bq + r)$ and hence $d \mid a$. So the two pairs have exactly the same common divisors, and therefore the same greatest one.

The method: divide the bigger by the smaller, keep the remainder, repeat — the pair shrinks each round until the remainder is 0, and then $\gcd(x, 0) = x$.

$\gcd(5859, 1232)$**:**

Division	Consequence
$5859 = 1232 \cdot 4 + 931$	$\gcd(5859, 1232) = \gcd(1232, 931)$
$1232 = 931 \cdot 1 + 301$	$\gcd(1232, 931) = \gcd(931, 301)$
$931 = 301 \cdot 3 + 28$	$\gcd(931, 301) = \gcd(301, 28)$
$301 = 28 \cdot 10 + 21$	$\gcd(301, 28) = \gcd(28, 21)$
$28 = 21 \cdot 1 + 7$	$\gcd(28, 21) = \gcd(21, 7)$
$21 = 7 \cdot 3 + 0$	$\gcd(21, 7) = \gcd(7, 0) = 7$

So $\gcd(5859, 1232) = 7$.

$\gcd(4131, 2431)$**:**

$$4131 = 2431 \cdot 1 + 1700, \quad 2431 = 1700 \cdot 1 + 731, \quad 1700 = 731 \cdot 2 + 238,$$
$$731 = 238 \cdot 3 + 17, \quad 238 = 17 \cdot 14 + 0$$

so $\gcd(4131, 2431) = \gcd(17, 0) = 17$.

$\gcd(14, 3003)$**:** $3003 = 14 \cdot 214 + 7$, then $14 = 7 \cdot 2 + 0$, so the gcd is 7.

$\gcd(931, 301)$**:** $931 = 301 \cdot 3 + 28$, $301 = 28 \cdot 10 + 21$, $28 = 21 \cdot 1 + 7$, $21 = 7 \cdot 3 + 0$, so gcd = 7. Using that, $7 \mid 931$ and $931 = 7 \cdot 133 = 7 \cdot 7 \cdot 19 = 7^2 \cdot 19$, which has $(2 + 1)(1 + 1) = 6$ positive divisors.

$\gcd(116, 88)$**:** $116 = 88 \cdot 1 + 28$, $88 = 28 \cdot 3 + 4$, $28 = 4 \cdot 7 + 0$, so gcd = 4; hence $\operatorname{lcm}(116, 88) = \frac{116 \cdot 88}{4} = 2552$.

As pseudocode

```
Input: A, B (integers with A > B >= 0)
a := A; b := B; r := B
while b != 0:
    r := a mod b
    a := b
    b := r
gcd := a
Output: gcd
```

Trace table for $A = 1001$, $B = 871$:

	0	1	2	3	4	5
a	1001	871	130	91	39	13
b	871	130	91	39	13	0
r	871	130	91	39	13	0
gcd						13

Proofs about gcd and lcm

For all positive integers a and b, $a \mid b$ if and only if $\mathrm{lcm}(a, b) = b$.

A biconditional can be proved either way round, but **proving each direction separately is the recommended method** — proving both simultaneously by chaining "iff"s is quicker but easy to get logically wrong (every link in the chain must genuinely be reversible).

> ($\Rightarrow$) Suppose $a, b \in \mathbb{Z}^+$ and $a \mid b$. Then $b = ka$ for some $k \in \mathbb{Z}$. So $\mathrm{lcm}(a, b) = \mathrm{lcm}(a, ka)$. Since $a \mid ka$ and $ka \mid ka$, and no smaller $n > 0$ has $ka \mid n$, we get $\mathrm{lcm}(a, ka) = ka = b$.
>
> ($\Leftarrow$) Suppose $\mathrm{lcm}(a, b) = b$. By the definition of lcm, $a \mid \mathrm{lcm}(a, b)$; substituting the hypothesis gives $a \mid b$. $\square$

For all positive integers a and b, $\gcd(a, b) = \mathrm{lcm}(a, b)$ if and only if $a = b$.

> ($\Leftarrow$) If $a = b$ then both equal a.
>
> ($\Rightarrow$) Assume $\gcd(a, b) = \mathrm{lcm}(a, b)$ and set $g = \gcd(a, b)$, so $a = gm$ and $b = gn$ for positive integers m, n with $\gcd(m, n) = 1$. Since gm and gn share no prime factors beyond those in g, the lcm uses all primes from both: $\mathrm{lcm}(a, b) = gmn$. From $g = gmn$ we get $mn = 1$, so $m = n = 1$ and $a = b = g$. $\square$

Extended Euclidean algorithm (non-assessed)

Theorem: for $a, b, c \in \mathbb{Z}$, if $\gcd(a, b) \mid c$ then there exist integers x and y with $ax + by = c$.

Running the Euclidean algorithm's steps **in reverse** finds them. For $1232x + 5859y = 14$:

1. Run the algorithm (as above) to get $\gcd(1232, 5859) = 7$.
2. Work backwards from the second-last equation, substituting each remainder in turn:

$$\begin{aligned} 7 &= 28 - 21 \\ &= 28 - (301 - 28 \cdot 10) = 28 \cdot 11 - 301 \\ &= (931 - 301 \cdot 3) \cdot 11 - 301 = 931 \cdot 11 - 301 \cdot 34 \\ &= 931 \cdot 45 - 1232 \cdot 34 \\ &= (5859 - 1232 \cdot 4) \cdot 45 - 1232 \cdot 34 = 5859 \cdot 45 - 1232 \cdot 214 \end{aligned}$$

3. Scale to the target: $7 = 1232(-214) + 5859(45)$, so $14 = 1232(-428) + 5859(90)$.

This content is **not examinable**, but it's where gcd earns its keep in practice. It is used to determine whether certain types of equations have solutions (the linear Diophantine equations $ax + by = c$), and it has applications in cryptography (the modular inverses this same reversal computes).

Where this gets used

Adding fractions and other everyday arithmetic; deciding whether certain equations have integer solutions; applications in cryptography.

See also

- divisibility-and-factorisation[2] · modular-arithmetic[3] · proof-techniques[4]
- integers-modulo-n[5] — multiplicative inverses mod p, found there by search, which the reversed algorithm also computes
- inclusion-exclusion[6] — divisible by both a and b means divisible by $\text{lcm}(a, b)$, the step that counts the overlaps of sets of multiples
- practice-problems[7] — §15 The Euclidean Algorithm, with full worked solutions

[2] courses/math1061/divisibility-and-factorisation.pdf
[3] courses/math1061/modular-arithmetic.pdf
[4] courses/math1061/proof-techniques.pdf
[5] courses/math1061/integers-modulo-n.pdf
[6] courses/math1061/inclusion-exclusion.pdf
[7] courses/math1061/practice-problems.pdf