Lecture 12 — Modular Arithmetic and the Euclidean Algorithm

Table of contents

Learning goals . . . 1
Order, signs and uses . . . 2
Recap on mod . . . 2
$\gcd(a, b)$ . . . 3
$\text{lcm}(a, b)$ . . . 3
Relationship between gcd and lcm . . . 4
The Euclidean algorithm . . . 5
An "if and only if" proof . . . 6
Challenge: reversing the Euclidean algorithm . . . 7
See also . . . 8

Pre-work: Video 015 (The Euclidean Algorithm). See gcd-lcm-and-euclidean-algorithm[1] for the reference definitions, worked runs of the algorithm and the gcd/lcm proofs.

Learning goals

1. Continue to gain fluency in applying modular arithmetic.
2. Understand the definitions of $\gcd(a, b)$ and $\text{lcm}(a, b)$ for integers a and b.
3. Be able to apply the Euclidean algorithm to find the greatest common divisor of two integers.

[1] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf

Order, signs and uses

Is $\gcd(a, b) = \gcd(b, a)$**?** Yes.

How do you do gcd and lcm with a mix of positive and negative integers? Take absolute values, as set out below.

Where are gcd, lcm and the Euclidean algorithm used? All the time in arithmetic (adding fractions, etc.); to determine if certain types of equations have solutions; and in cryptography.

Recap on mod

For $n, d \in \mathbb{Z}$, $d > 0$: $n \bmod d = r$ indicates the remainder when n is divided by d is r, with $0 \leq r < d$. For $m, n, d \in \mathbb{Z}$, $d > 0$: $m \equiv n \pmod{d}$ indicates m and n have the same remainder when divided by d — equivalently $d \mid (m - n)$. See modular-arithmetic[2].

Worked: the remainder of $35m$

If $m \in \mathbb{Z}$ and $m \bmod 6 = 4$, what is the remainder when $35m$ is divided by 6?

2. Since $35 \bmod 6 = 5$ and $m \equiv 4$, we get $35m \equiv 5 \cdot 4 \equiv 20 \equiv 2 \pmod{6}$.

Worked: the remainder of $3m^2 + 2m + 1$

If $m \in \mathbb{Z}$ and $m \bmod 6 = 4$, what is the remainder when $3m^2 + 2m + 1$ is divided by 6?

3. $3m^2 + 2m + 1 \equiv 3(4)^2 + 2(4) + 1 \pmod{6}$. Rewrite $3 \cdot 4^2$ as $12 \cdot 4$ and the whole term goes — $12 \bmod 6 = 0$ because $6 \mid 12$, so $12(4) \equiv 0 \pmod{6}$ — leaving $8 + 1 = 9 \equiv 3 \pmod{6}$.

Rewriting $3 \cdot 16$ as $12 \cdot 4$ rather than as 48 is the cheaper move: you only need to spot a factor that is $\equiv 0$, not evaluate the product.

[2] courses/math1061/modular-arithmetic.pdf

$\gcd(a, b)$

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

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

$\text{hcf}(a, b)$, the *highest common factor*, names the same object, but gcd is the name this course uses. The order of a and b does not matter.

What if one, or both, of a and b are negative? The divisors of 15 are $1, 3, 5, 15, -1, -3, -5, -15$ — and these are also the divisors of -15. The divisors of an integer a are the same as the divisors of $-a$. Thus $\gcd(-15, 36) = \gcd(15, 36)$, and in general

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

$\gcd(0, b) = b$ for all positive integers b — this is the base case the algorithm below terminates on.

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

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

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

"Smallest such n" is doing the work: every other positive multiple of both a and b is greater than n.

Order does not matter. The multiples of 5 are $\ldots, -10, -5, 0, 5, 10, 15, \ldots$ — the same as the multiples of -5. So $\text{lcm}(-5, 36) = \text{lcm}(5, 36)$, and in general

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

Relationship between gcd and lcm

Use the unique prime factorisation of each integer (see divisibility-and-factorisation[3]). **Step 1:** write the UPF of each. **Step 2:** take the minimum exponent of each prime for the gcd and the maximum for the lcm.

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

With the two missing exponents written in, $30 = 2^1 \cdot 3^1 \cdot 5$. The lcm takes the 5 of 30 and the 2^3 and the 3^2 of 72, giving $\operatorname{lcm}(30, 72) = 2^3 \cdot 3^2 \cdot 5$. The gcd takes the 2 and the 3, giving $\gcd(30, 72) = 2^1 \cdot 3 = 6$. gcd-lcm-and-euclidean-algorithm[4] lays the same step out as aligned prime columns.

Lemma: if $a, b \in \mathbb{Z}^+$, then $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

Checking: $\gcd(30, 72) \cdot \operatorname{lcm}(30, 72) = 6 \cdot 360 = 30 \cdot 72$, since $(2 \cdot 3)(2^3 \cdot 3^2 \cdot 5) = (2 \cdot 3 \cdot 5)(2^3 \cdot 3^2)$.

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

Worked: gcd and lcm with a negative argument

$\gcd(63, -105)$ and $\operatorname{lcm}(63, -105)$:

- *Step 1*: $63 = 3^2 \cdot 7$ and $-105 = -3 \cdot 5 \cdot 7$. Keep the minus sign out the front and read the primes off the positive part, or replace -105 by 105 first.
- *Step 2*: $\gcd(63, -105) = 3 \cdot 7 = 21$; $\operatorname{lcm}(63, -105) = 3^2 \cdot 5 \cdot 7 = 315$.

Either habit gives the same answer, because $\gcd(a, b) = \gcd(|a|, |b|)$ and $\operatorname{lcm}(a, b) = \operatorname{lcm}(|a|, |b|)$ — the sign never reaches the answer.

Worked: two distinct primes

Let p and q be **distinct** primes ($p \neq q$). Then $\gcd(p, q) = 1$ and $\operatorname{lcm}(p, q) = pq$.

[3] courses/math1061/divisibility-and-factorisation.pdf
[4] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf

The Euclidean algorithm

To determine $\gcd(a, b)$ for $a, b \in \mathbb{Z}^+$, based on the fact:

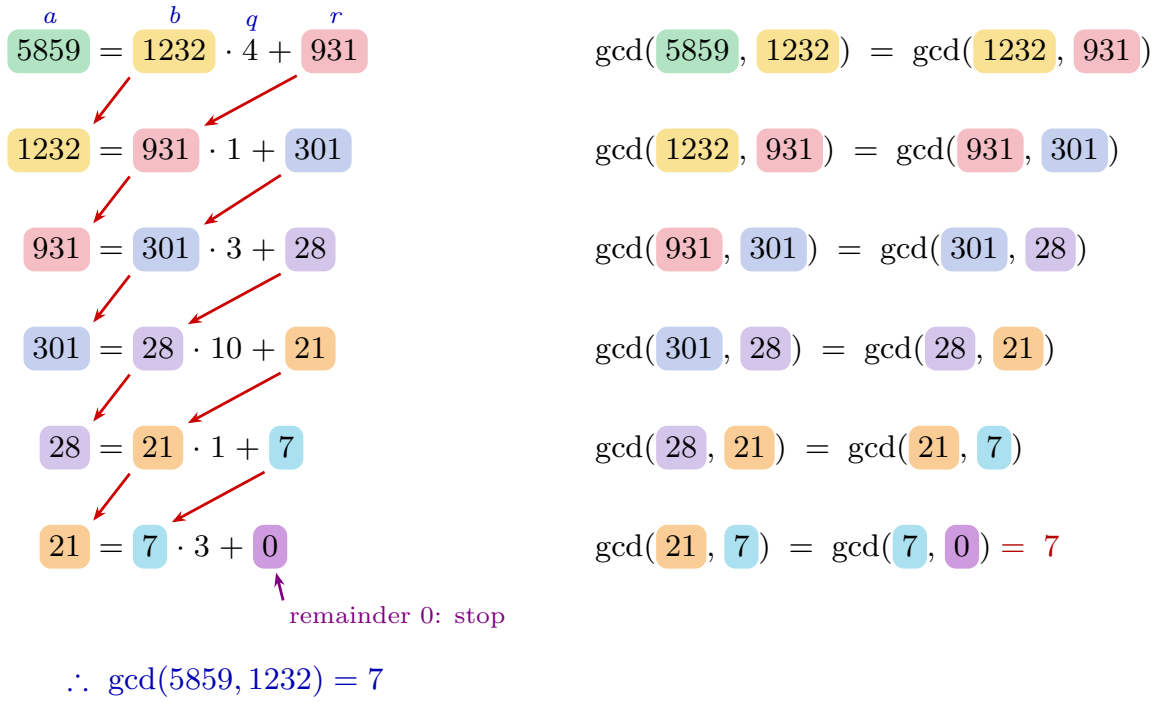
> if $a, b \in \mathbb{Z}$ are not both zero and $q, r \in \mathbb{Z}$ satisfy $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

The proof of this fact is basically showing that every divisor of a and b is also a divisor of b and r, and vice versa:

- Suppose $c \mid a$ and $c \mid b$. Then $c \mid (a - bq)$ and hence $c \mid r$.
- Suppose $d \mid b$ and $d \mid r$. Then $d \mid (bq + r)$ and hence $d \mid a$.

Divide the **big** by the **small**, then repeat on (small, remainder).

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



$\therefore\ \gcd(5859, 1232) = 7$

Figure 1: The Euclidean algorithm as a cascade of divisions. Each number is given a capsule colour and keeps it as it migrates: the divisor b of one line becomes the dividend a of the next, and the remainder r becomes the next divisor — the two red arrows per step. The right-hand column is the same movement written as $\gcd(a, b) = \gcd(b, r)$, so the pair shrinks without the gcd ever changing, until the remainder hits 0 and $\gcd(7, 0) = 7$ can be read off.

Therefore $\gcd(5859, 1232) = 7$. In $\gcd(1232, 5859)$, label 1232 as b and 5859 as a before starting, so that the first division is big-by-small.

Worked: $\gcd(4131, 2431)$

Use the Euclidean Algorithm to determine $\gcd(4131, 2431)$**.**

a	$=$	$b \times q$	$+ r$
4131	$=$	2431×1	$+ 1700$
2431	$=$	1700×1	$+ 731$
1700	$=$	731×2	$+ 238$
731	$=$	238×3	$+ 17$
238	$=$	17×14	$+ 0$

$$\gcd(4131, 2431) = \cdots = \gcd(238, 17) = \gcd(17, 0) = \mathbf{17}$$

An "if and only if" proof

Prove that for all positive integers a **and** b**,** $a \mid b$ **if and only if** $\operatorname{lcm}(a, b) = b$**.**

This calls for a **direct proof**, not a **counterexample**: the claim is universally quantified and true, so there is nothing to disprove. Both halves of the definition of lcm get used — $n > 0$, and $a \mid n$ *and* $b \mid n$ — and so does the word **smallest** in it.

Method 1: prove each direction separately. This is the **recommended method**.

The forward direction:

> ($\Rightarrow$) Suppose $a, b \in \mathbb{Z}^+$ and suppose $a \mid b$. Then $\exists k \in \mathbb{Z}$ such that $b = ka$. So $\operatorname{lcm}(a, b) = \operatorname{lcm}(a, ka)$. Since $a \mid ka$ and $ka \mid ka$ and no smaller $n > 0$ has $ka \mid n$, $\therefore \operatorname{lcm}(a, ka) = ka$ — and $b = ka$ — $\therefore \operatorname{lcm}(a, b) = b$.

The reverse direction, as a skeleton:

> ($\Leftarrow$) Suppose $a, b \in \mathbb{Z}^+$ and suppose $\operatorname{lcm}(a, b) = b$. $\vdots$ *(prove)* $\therefore a \mid b$.

Filling the gap: by the definition of lcm, $a \mid \operatorname{lcm}(a, b)$. Substituting the hypothesis $\operatorname{lcm}(a, b) = b$ gives $a \mid b$ at once. $\square$

On the forward direction: the clause "no smaller $n > 0$ has $ka \mid n$" is where the word **least** in *least common multiple* is discharged. It holds because any positive n divisible by ka satisfies $n \geq ka$.

Method 2: prove both directions simultaneously. Be careful: this is the quicker method, but it is easy to make a logical error.

This rewrites the *same* lines, replacing each connective with an "iff": "Then", "So" and "Since" become "This is true **iff**", "**which holds iff**" and "this holds **iff**", five links in all:

> Suppose $a, b \in \mathbb{Z}^+$ and suppose $a \mid b$.
>
> — **This is true iff** $\exists k \in \mathbb{Z}$ such that $b = ka$, — **which holds iff** $\text{lcm}(a, b) = \text{lcm}(a, ka)$, — **this holds iff** $a \mid ka$ and $ka \mid ka$ and no smaller $n > 0$ has $ka \mid n$, — **which holds iff** $\text{lcm}(a, ka) = ka$ — and $b = ka$ — — **which holds iff** $\text{lcm}(a, b) = b$.

One pass instead of two, at the price that *every* link must genuinely be reversible. That is the logical error to watch for: if any single line is only an implication, the chain quietly proves one direction and reads as though it proved both.

The same statement, and a second gcd/lcm biconditional, are also written out in gcd-lcm-and-euclidean-algorithm[5].

Challenge: reversing the Euclidean algorithm

Non-assessed content.

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

Given $ax + by = c$, use the Euclidean algorithm to find $\gcd(a, b)$, then run the steps in reverse to find x and y.

Example: find integers x, y satisfying $1232x + 5859y = 14$.

Step 1 — use the E.A. to find $\gcd(1232, 5859) = 7$*:*

$$5859 = 1232 \cdot 4 + 931 \quad \text{(Eqn 1)}$$
$$1232 = 931 \cdot 1 + 301 \quad \text{(Eqn 2)}$$
$$931 = 301 \cdot 3 + 28 \quad \text{(Eqn 3)}$$
$$301 = 28 \cdot 10 + 21 \quad \text{(Eqn 4)}$$
$$28 = 21 \cdot 1 + 7 \quad \text{(Eqn 5)}$$
$$21 = 7 \cdot 3 + 0$$

Step 2 — work backwards to get $1232w + 5859z = 7$*:*

[5] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf

From Eqn 5: $7 = 28 - 21$. Use Eqn 4 to replace the 21 and collect like terms: $7 = 28 - (301 - 28 \cdot 10) = 28 \cdot 11 - 301$. Use Eqn 3 to replace the 28: $7 = (931 - 301 \cdot 3) \cdot 11 - 301 = 931 \cdot 11 - 301 \cdot 34$. Use Eqn 2 to replace the 301: $7 = 931 \cdot 11 - (1232 - 931) \cdot 34 = 931 \cdot 45 - 1232 \cdot 34$. Use Eqn 1 to replace the 931: $7 = (5859 - 1232 \cdot 4) \cdot 45 - 1232 \cdot 34 = 5859 \cdot 45 - 1232 \cdot 214$.

Step 3 — multiply through to get $1232x + 5859y = 14$*:*

Therefore $7 = 1232(-214) + 5859(45)$, so $14 = 1232(-428) + 5859(90)$.

See also

- gcd-lcm-and-euclidean-algorithm[6] · modular-arithmetic[7] · divisibility-and-factorisation[8]
- 2026-08-20-modular-arithmetic[9] — Lecture 11
- practice-problems[10] — §15 The Euclidean Algorithm, with full worked solutions

[6] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[7] courses/math1061/modular-arithmetic.pdf
[8] courses/math1061/divisibility-and-factorisation.pdf
[9] courses/math1061/2026-08-20-modular-arithmetic.pdf
[10] courses/math1061/practice-problems.pdf