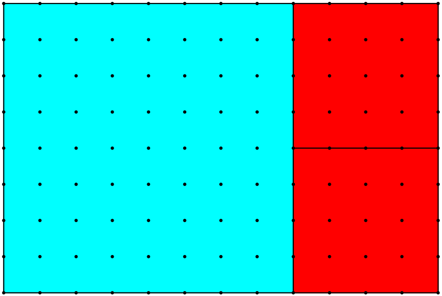
What is...an Euclidean domain?

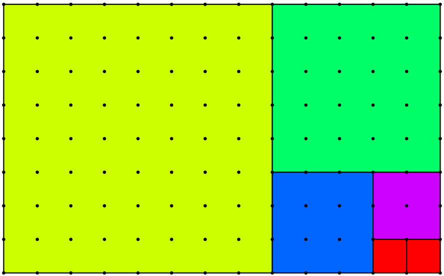
Or: Generalizing division with remainder

Euclid's algorithm – find the gcd

The greatest common divisor of 12 and 8 is 4.



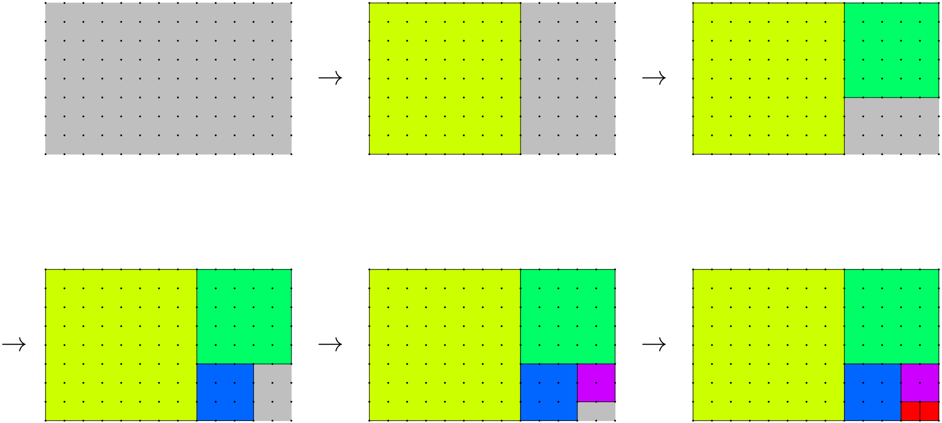
The greatest common divisor of 13 and 8 is 1.



- $a = q_0 b + r_0,\ b = q_1 r_0 + r_1,\ \ldots$
- This is eventually stabilize and $\gcd(a, b) = r_{final} \neq 0$

Question. Does this extend beyond integers?

Steadily decreasing



This terminates because the remainder keeps decreasing

gcd **for polynomials**

$$f = X^5 + X^4 - X^3 - X^2 - X - 1, \quad g = X^3 - 2 \cdot X - 1, \quad \gcd(f, g) = X + 1$$

$$(X^5 + X^4 - X^3 - X^2 - X - 1) = (X^2 + X + 1)(X^3 - 2 \cdot X - 1) + (2 \cdot X^2 + 2 \cdot X)$$

$$(X^3 - 2 \cdot X - 1) = (\tfrac{1}{2} \cdot X - \tfrac{1}{2})(2 \cdot X^2 + 2 \cdot X) + (-X - 1)$$

$$(2 \cdot X^2 + 2 \cdot X) = (-2 \cdot X)(-X - 1) + 0$$

- This terminates because the remainder keeps decreasing (degree-wise)
- We have

$$f = (X + 1)(X^4 - X^2 - 1), \quad g = (X + 1)(X^2 - X - 1)$$

- The gcd can be normalized using invertible elements $(-X - 1) = -(X + 1)$

For completeness: The formal definition

A degree function $\delta\colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ on an integral domain R is a map satisfying:

$$a = q \cdot b + r \Rightarrow \big(r = 0 \text{ or } \delta(r) < \delta(b)\big)$$

If R admits a degree function, then it is called Euclidean

(a) The Euclidean algorithm works for such R Euclid

(b) Bézout's identity holds $\gcd(a, b) = s \cdot a + t \cdot b$

(c) The $\gcd(a, b)$ is the result of the Euclidean algorithm

(d) If "$a = q \cdot b + r$" can be made algorithmic, then the Euclidean algorithm can be as well Algorithm

(e) Euclidean implies PID *e.g.* $(a_1, \dots, a_n) = \big(\gcd(a_1, \dots, a_n)\big)$

Examples. Fields, $\mathbb{Z}$, $\mathbb{K}[X]$ for a field $\mathbb{K}$, $\mathbb{Z}[i]$, $\mathbb{Z}[e^{2\pi i/3}]$, $\mathbb{Z}[\sqrt{-d}]$ for $d = 1, 2$, $\mathbb{Q}[\sqrt{-d}]$ for $d = 1, 2, 3, 7, 11$

$\gcd$ **and** lcm

Fix an integral domain R

(a) One can define $d = \gcd(a_1, ..., a_n)$ by:

- d divides all a_i Divisor
- If d' divides all a_i, then d' divides d Greatest

(b) One can define $e = \mathrm{lcm}(a_1, ..., a_n)$ by:

- e is divided by all a_i Multiple
- If e' is divided by all a_i, then e' is divided by e Lowest

(c) If they exist, then they are unique up to invertible elements

(d) If they exist, then

$$(a_1, ..., a_n) = \big(\gcd(a_1, ..., a_n)\big), \quad (a_1) \cap ... \cap (a_n) = \big(\mathrm{lcm}(a_1, ..., a_n)\big)$$

This applies, for example, to polynomial rings

Thank you for your attention!

I hope that was of some help.