Euclidean algorithm

↳ efficient algorithm to compute $\gcd(a,b)$ for (potentially large) $a,b \in \mathbb{Z}$.

↳ first need a crucial lemma:

Lemma: Fix $a,b,q,r \in \mathbb{Z}$

If $a = bq + r$

then $\gcd(a,b) = \gcd(b,r)$

Pf: Let $d = \gcd(a,b)$

$d' = \gcd(b,r)$

WTS: $d = d'$

Observe: since $a = bq + r$ and $d' \mid b$ and $d' \mid r$, we have $d' \mid a$

Hence d' is a common divisor of a, b. Hence $d' \leq d$.

OTOH: By Bezout, $\exists m,n \in \mathbb{Z}$ s.t.

$$d' = rm + bn$$

but $r = a - bq$ so:

$$d' = (a-bq)m + bn$$
$$= am + b(n - qm)$$

$\Rightarrow$ so d' is a linear combo of a, b

$\Rightarrow$ $d' \geq d$ by Bezout.

Hence $d = d'$

Lemma allows us to find $\gcd(a,b)$ by repeatedly "reducing by remainders"

Theorem (Euclidean Algorithm)

Fix $a, b \in \mathbb{N}$ with $a \geq b$.
Repeatedly using division algorithm, define a sequence of remainders and quotients as follows:

$$\underbrace{a}_{=r_0} = \underbrace{b}_{=r_1} q_1 + r_2 \qquad r_2 < b$$

$$b = r_2 q_2 + r_3 \qquad r_3 < r_2$$

$$r_2 = r_3 q_3 + r_4 \qquad r_4 < r_3$$

← remainders decrease

$$\vdots$$

$$r_{N-3} = r_{N-2} q_{N-2} + r_{N-1}$$

← last nonzero remainder

$$r_{N-2} = r_{N-1} q_{N-1} + 0$$

Then: $r_{N-1} = \gcd(a,b)$

Pf: Consider the sequence of remainders: (208)

$$\underbrace{r_0}_{=a} > \underbrace{r_1}_{=b} > r_2 > \cdots > r_{N-1} > \underbrace{r_N}_{=0}.$$

Since $r_j = r_{j+1} q_{j+1} + r_{j+2}$ $\forall j \leq N-2$

by lemma we have:

$$\gcd(r_j, r_{j+1}) = \gcd(r_{j+1}, r_{j+2}) \quad \forall j \leq N-2$$

Hence:
$$\begin{aligned} \gcd(a,b) &= \gcd(r_0, r_1) \\ &= \gcd(r_1, r_2) \\ &= \gcd(r_2, r_3) \\ &\vdots \\ &= \gcd(r_{N-1}, r_N) \\ &= \gcd(r_{N-1}, 0) \\ &= r_{N-1} \quad \checkmark \end{aligned}$$

Ex's ① Find $\gcd(68, 12)$

Sol'n $a = 68$ $b = 12$

$\underset{r_0}{68} = \underset{r_1}{12} \cdot 5 + \underset{r_2}{8}$

$\underset{r_1}{12} = \underset{r_2}{8} \cdot 1 + \underset{r_3}{4}$ ← last nonzero remainder $= \gcd$

$8 = 4 \cdot 2 + 0$

So: $\gcd(68, 12) = 4$

(2) Find $m, n \in \mathbb{Z}$ s.t.

$$68m + 12n = 4$$

Sol'n: Bezout says m, n exist. Euclid. Alg. gives us a way to find them – by "reversing" above equations.

$$4 = 12 - 8 \cdot 1 \qquad \text{and: } 8 = 68 - 12 \cdot 5$$

$$= 12 - (68 - 12\,5)\,1$$

$$= 12 - 68 \cdot 1 + 12 \cdot (5)$$

$$= 68(-1) + 12(6)$$

So $m = -1$ $n = 6$ works. ✓

this method sometimes called "extended EA"

(3) Find $k, l \in \mathbb{Z}$ s.t.

$$64k + 111l = 1$$

Sol'n: For this to be possible need gcd(64, 111) = 1. Let's do EA.

$$111 = 64 \cdot 1 + 47$$
$$64 = 47 \cdot 1 + 17$$
$$47 = 17 \cdot 2 + 13$$
$$17 = 13 \cdot 1 + 4$$
$$(*) \quad 13 = 4 \cdot 3 + 1 \leftarrow \gcd(64, 111) = 1$$
$$4 = 4 \cdot 1 + 0$$

Now we go backwards from (*)

$$1 = 13 - 4\cdot 3 \qquad (\text{and: } 4 = 17 - 13\cdot 1)$$
$$= 13 - (17 - 13\cdot 1)\cdot 3$$
$$= 17(-3) + 13(4) \qquad (\text{and: } 13 = 47 - 17\cdot 2)$$
$$= 17(-3) + (47 - 17\cdot 2)(4)$$
$$= 47(4) + 17(-11) \qquad (\text{and: } 17 = 64\cdot 1 - 47)$$
$$= 47(4) + (64\cdot 1 - 47)(-11)$$
$$= 64(-11) + 47(15) \qquad (\text{and: } 47 = 111 - 64\cdot 1)$$
$$= 64(-11) + (111 - 64\cdot 1)(15)$$
$$= 111(15) + 64(-26)$$

So $k = -26$ and $\ell = 15$ works.

Combinatorics

↳ study of counting finite sets.

↳ easy right? No.

<u>Notation</u>: if A is finite, $|A|$ denotes # of el'ts in A.

e.g. $|\{*, ♡, \Delta\}| = 3$

<u>Def'n</u>: A <u>partition</u> of a finite set A is a collection of pairwise disjoint subsets $\{A_1, \dots, A_k\}$ s.t. $\bigcup_{i=1}^{k} A_i = A$

↳ def'n same as before but now we allow some $A_i = \emptyset$.

e.g. if $A_1 = \{*, \Delta\}$ $A_2 = \emptyset$ $A_3 = \{♡\}$ then $\{A_1, A_2, A_3\}$ is a partition of $\{*, ♡, \Delta\}$

<u>Principle</u> (Rule of sum): if $\{A_1, A_2, \dots, A_k\}$ is a partition of a finite set A, then:

$$|A| = \sum_{i=1}^{k} |A_i| = |A_1| + |A_2| + \dots + |A_k|$$

Pf: obvious

Principle (Rule of Product): if the elements of a finite set A are formed by making a sequence of k choices s.t.

① the ith choice can be made in r_i-many ways

② each el't in A is uniquely formed by such a sequence of choices.

Then: $|A| = r_1 r_2 \cdots r_k$

$$= \prod_{i=1}^{k} r_i$$

Pf: not illuminating

Ex: ① How many strings of 4 letters ("4 letter words") can be formed using the English alphabet (e.g. ZZAP, EEEE)

Sol'n: by rule of product, # of such words is $26 \cdot 26 \cdot 26 \cdot 26$

$= 456{,}976$