Euclidean Algorithm.

How to efficiently find $\gcd(a,b)$ for (potentially large) $a,b \in \mathbb{Z}$. First need the following crucial:

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 and b. Hence $d' \leq d$

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

$d' = rm + bn$

but $r = a - bq$ so:

$d' = (a - bq)m + bn$

$= am + b(n - qm)$

So d' is a linear combo of a, b

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

Hence $d = d'$ ✓

This 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 the division algorithm define a sequence of remainders and quotients; as follows:

$$a = \overset{r_0}{} = b q_1 + r_2 \qquad r_2 < b$$

$$b = r_2 q_2 + r_3 \qquad r_3 < r_2 \quad \leftarrow \text{remainders decrease}$$

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

$$\vdots$$

$$r_{N-3} = r_{N-2} q_{N-2} + r_{N-1} \quad \leftarrow \text{last nonzero remainder}$$

$$r_{N-2} = r_{N-1} q_{N-1} + 0 \quad \leftarrow \text{first 0 remainder}$$

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

Pf (sketch): Consider the sequence of remainders:

$$r_0 \geq r_1 > r_2 > \cdots > r_{N-1} > r_N = 0$$
$$(r_0 = a,\ r_1 = b)$$

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

by Lemma we have

$$\gcd(r_j, r_{j+1}) = \gcd(r_{j+1}, r_{j+2})$$

$\forall j \leq N-2$

Hence: $\gcd(a,b) = \gcd(r_0, r_1)$

$= \gcd(r_1, r_2)$

$= \gcd(r_2, r_3)$

$\vdots$

$= \gcd(r_{N-1}, r_N)$

$= \gcd(r_{N-1}, 0)$

$= r_{N-1}$. ✓

Ex's ① Find $\gcd(68, 12)$

Soln $a = 68$ $b = 12$.

$68 = 12 \cdot 5 + 8$ ($r_0 = r_1 \cdot 5 + r_2$)

$12 = 8 \cdot 1 + 4$ (r_3) ← gcd

$8 = 4 \cdot 2 + 0$ (r_4)

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

② Find $m, n \in \mathbb{Z}$ s.t.

$$68m + 12n = 4$$

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

$$4 = 12 - 8 \cdot 1 \qquad \text{and: } 8 = 68 - 12 \cdot 5$$
$$= 12 - (68 - 12 \cdot 5) \cdot 1$$
$$= 12 - 68 \cdot 1 + 12 \cdot 5$$
$$= 68(-1) + 12(6)$$

So $m = -1$ $n = 6$ works.
↳ this method sometimes called "extended EA"

③ Find $k, \ell \in \mathbb{Z}$ s.t.

$$64k + 111\ell = 1$$

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

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

Now we go backwards from (*)

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

So $k = -26$ and $l = 15$ works ✓

Combinatorics

↪ study of counting finite sets

↪ easy right? no.

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

e.g. $|\{*, \heartsuit, \diamondsuit\}| = 3$.

Def'n a **partition** 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 except we allow some pieces $A_i = \emptyset$.

e.g. if $A_1 = \{*, \diamondsuit\}$ $A_2 = \emptyset$ $A_3 = \{\heartsuit\}$

then $\{A_1, A_2, A_3\}$ is a partition of $\{*, \heartsuit, \diamondsuit\}$

Principle (Rule of sum): if $\{A_1, A_2, \dots, A_k\}$ is a partition of A, A finite, 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 elt in A is uniquely formed by such a sequence of k 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)

Soln: by rule of product, # of such words is $26 \cdot 26 \cdot 26 \cdot 26$

$= 456,976.$

(2) How many strings of 4 or fewer letters can be formed.

Soln: Let A be the set of such strings

We can partition A as:

$$A = A_1 \cup A_2 \cup A_3 \cup A_4$$

where A_i = set of strings of length i.

By the rule of sum:

$$|A| = |A_1| + |A_2| + |A_3| + |A_4|$$

By rule of product:

$$|A_1| = 26 \quad |A_2| = 26^2 \quad |A_3| = 26^3$$

$$|A_4| = 26^4$$

$$\text{so } |A| = 26 + 26^2 + 26^3 + 26^4$$

$$= 475,254.$$

Permutations + Arrangements

Defn Given a finite set A, a permutation of A is an ordered list of elts of A in which every elt appears exactly once.

e.g. if $A = \{1,2,3\}$ then 213 and 321 are permutations of A, 23 and 2231 are not.

Prop'n: Fix $n \in \mathbb{N} \cup \{0\}$. If A has size n, then the # of permutations of A is n!

Pf:- If $|A| = 0$ then $A = \emptyset$ and there is $0! = 1$ permutation of A (the empty permutation)

- If $|A| = n \geq 1$ then a permutation

$a_1 a_2 \cdots a_n$ is formed (uniquely) by making a sequence of n choices.

Choose a_1, then choose a_2, ..., then choose a_n

n-choices n-1 choices ... 1 choice

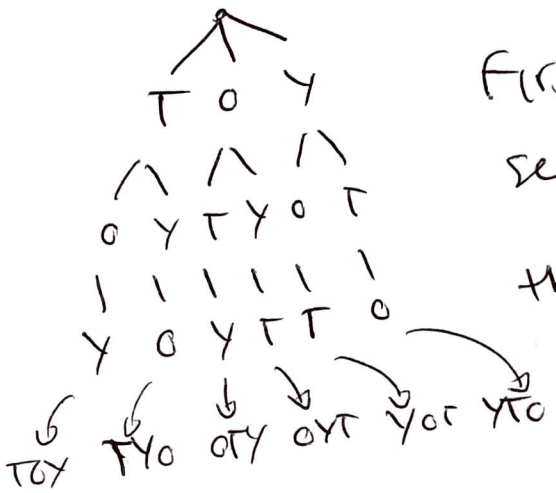
By ROP: # of perms is $n(n-1)\cdots 1 = n!$ ✓

Ex. How many anagrams of the word TOY are there?

Soln: an anagram is just a permutation of $\{T,O,Y\}$ (important! TOY has no repeated letters.) By prop'n # of anagrams is $3! = 6$.

We can list them:

TOY OTY YTO
TYO OYT YOT



Def'n Fix $k, n \in \mathbb{N} \cup \{0\}$ with $k \leq n$. Given a set A with $|A| = n$, a *k-arrangement* of A is an ordered list of k elements from A, w/ no repeats.

e.g. if $A = \{1,2,3,4,5,6\}$

- then 254 and 152 are 3-arrangements of A
- 115 and 29 are not arrangements of A.

Prop'n the # of k-arrangements of a set of size n is $\frac{n!}{(n-k)!} = n \cdot (n-1) \cdots (n-(k-1))$

Pf: a k-arrangement

$a_1 a_2 \cdots a_k$

is formed by making a sequence of k choices.

choose a_1 (↑ n choices) choose a_2 (↑ $n-1$) ... choose a_k (↑ $n-(k-1)$)

$\Rightarrow$ by ROP # of k-arrangements

$= n(n-1)\cdots(n-(k-1)) = \frac{n!}{(n-k)!}$

Ex: How many 3-letter strings w/o repeats can be formed using English alphabet? (e.g. AFG, WTS)

Soln: such strings are just 3-arrangements of $\{a, b, \ldots, z\}$

$\Rightarrow$ # of such strings

$= 26 \cdot 25 \cdot 24 = 15,600$