1 Chinese remainder theorem

Let m, n, a, b be any integers, let $g = \gcd(m, n)$, and consider the system of congruences:

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{n} \end{aligned}$$

If $a \equiv b \pmod{g}$, then this system of equations has a unique solution modulo $\operatorname{lcm}(m, n) = \frac{mn}{g}$. Otherwise, it has no solutions.
If we use Bézout's identity to write $g = um + vn$, then the solution is

$$x = \frac{avn + bum}{g}.$$

This defines an integer, as g divides both m and n. Otherwise, the proof is very similar to that for coprime moduli.

2 Eigen Decomposition

A (non-zero) vector v of dimension N is an eigenvector of a square $N \times N$ matrix A if it satisfies the linear equation

$$\mathbf{A}\mathbf{v} = \lambda\mathbf{v}$$

where λ is a scalar, termed the eigenvalue corresponding to v.
This yields an equation for the eigenvalues

$$p(\lambda) = \det(\mathbf{A} - \lambda\mathbf{I}) = 0$$

.
This equation will have $N\lambda$ distinct solutions, where $1 \leq N\lambda \leq N$. The set of solutions, that is, the eigenvalues, is called the spectrum of A.
We can factor p as

$$p(\lambda) = (\lambda - \lambda_1)^{n_1} (\lambda - \lambda_2)^{n_2} \cdots (\lambda - \lambda_{N_\lambda})^{n_{N_\lambda}} = 0$$

.
The integer n_i is termed the algebraic multiplicity of eigenvalue λ_i. If the field of scalars is algebraically closed, the algebraic multiplicities sum to N:

$$\sum_{i=1}^{N_\lambda} n_i = N.$$

For each eigenvalue λ_i, we have a specific eigenvalue equation

$$(\mathbf{A} - \lambda_i\mathbf{I})\,\mathbf{v} = 0.$$

There will be $1 \leq m_i \leq n_i$ linearly independent solutions to each eigenvalue equation. The linear combinations of the m_i solutions are the eigenvectors associated with the eigenvalue λ_i. The integer m_i is termed the geometric multiplicity of λ_i. It is important to keep in mind that the algebraic multiplicity n_i and geometric multiplicity m_i may or may not be equal, but we always have $m_i \leq n_i$. The simplest case is of course when $m_i = n_i = 1$. The total number of linearly independent eigenvectors, N_v, can be calculated by summing the geometric multiplicities

$$\sum_{i=1}^{N_\lambda} m_i = N_{\mathbf{v}}.$$

The eigenvectors can be indexed by eigenvalues, using a double index, with v_{ij} being the jth eigenvector for the ith eigenvalue. The eigenvectors can also be indexed using the simpler notation of a single index v_k, with $k = 1, 2, \ldots, N_v$.
Let A be a square $n \times n$ matrix with n linearly independent eigenvectors q_i (where $i = 1, \ldots, n$). Then A can be factorized as

$$\mathbf{A} = \mathbf{Q}\boldsymbol{\Lambda}\mathbf{Q}^{-1}$$

where Q is the square $n \times n$ matrix whose ith column is the eigenvector q_i of A, and Λ is the diagonal matrix whose diagonal elements are the corresponding eigenvalues, $\lambda_{ii} = \lambda_i$.
The n eigenvectors q_i are usually normalized, but they need not be. A non-normalized set of n eigenvectors, v_i can also be used as the columns of Q. That can be understood by noting that the magnitude of the eigenvectors in Q gets canceled in the decomposition by the presence of $Q - 1$.
The decomposition can be derived from the fundamental property of eigenvectors:

$$\begin{aligned} \mathbf{A}\mathbf{v} &= \lambda\mathbf{v} \\ \mathbf{A}\mathbf{Q} &= \mathbf{Q}\boldsymbol{\Lambda} \\ \mathbf{A} &= \mathbf{Q}\boldsymbol{\Lambda}\mathbf{Q}^{-1}. \end{aligned}$$

If a matrix A can be eigendecomposed and if none of its eigenvalues are zero, then A is nonsingular and its inverse is given by

$$\mathbf{A}^{-1} = \mathbf{Q}\boldsymbol{\Lambda}^{-1}\mathbf{Q}^{-1}$$

If $\mathbf{A}$ is a symmetric matrix, since $\mathbf{Q}$ is formed from the eigenvectors of $\mathbf{A}$ it is guaranteed to be an orthogonal matrix, therefore $\mathbf{Q}^{-1} = \mathbf{Q}^{\mathrm{T}}$. Furthermore, because Λ is a diagonal matrix, its inverse is easy to calculate:

$$\left[\Lambda^{-1}\right]_{ii} = \frac{1}{\lambda_i}$$

3 Generating function

$$\sum_{n=0}^{\infty} a^n \binom{n+k}{k} x^n = \frac{1}{(1-ax)^{k+1}} .$$

4 Partition

The number of partitions of n is the partition function $p(n)$ having generating function:

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty} (1-x^k)^{-1}$$

$$p_n = p_{n-1} + p_{n-2} - p_{n-5} - p_{n-7} + p_{n-12} + p_{n-15} - p_{n-22} - \ldots$$

$$p_k = k(3k-1)/2 \text{ with } k = 1, -1, 2, -2, 3, -3, \ldots$$

5 Center of mass + Green theorem

Let C be a positively oriented, piecewise smooth, simple closed curve in a plane, and let D be the region bounded by C. If L and M are functions of (x, y) defined on an open region containing D and having continuous partial derivatives there, then

$$\oint_C (L\,dx + M\,dy) = \iint_D \left(\frac{\partial M}{\partial x} - \frac{\partial L}{\partial y} \right) dx\,dy$$

where the path of integration along C is anticlockwise.
The centroid of a non-self-intersecting closed polygon defined by n vertices $(x_0, y_0), (x_1, y_1), \ldots, (x_{n-1}, y_{n-1})$ is the point (C_x, C_y) where

$$C_{\mathrm{x}} = \frac{1}{6A} \sum_{i=0}^{n-1} (x_i + x_{i+1})(x_i\ y_{i+1} - x_{i+1}\ y_i), \text{and}$$
$$C_{\mathrm{y}} = \frac{1}{6A} \sum_{i=0}^{n-1} (y_i + y_{i+1})(x_i\ y_{i+1} - x_{i+1}\ y_i),$$

and where A is the polygon's signed area, as described by the shoelace formula:

$$A = \frac{1}{2} \sum_{i=0}^{n-1} (x_i\ y_{i+1} - x_{i+1}\ y_i).$$

In these formulae, the vertices are assumed to be numbered in order of their occurrence along the polygon's perimeter; furthermore, the vertex (x_n, y_n) is assumed to be the same as (x_0, y_0), meaning $i+1$ on the last case must loop around to $i = 0$. (If the points are numbered in clockwise order, the area A, computed as above, will be negative; however, the centroid coordinates will be correct even in this case.)

6 Fibonacci mod $10^9 + 9$

$$F_n \equiv 276601605(691504013^n - 308495997^n) \pmod{10^9 + 9}$$

$$F_n = \frac{\varphi^n - \psi^n}{\varphi - \psi} = \frac{\varphi^n - \psi^n}{\sqrt{5}}$$

where

$$\varphi = \frac{1+\sqrt{5}}{2} \approx 1.61803\,39887\ldots$$

$$\psi = \frac{1-\sqrt{5}}{2} = 1 - \varphi = -\frac{1}{\varphi} \approx -0.61803\,39887\ldots.$$

Properties

$$(-1)^n = F_{n+1}F_{n-1} - F_n^2.$$

$$F_m F_n + F_{m-1} F_{n-1} = F_{m+n-1},$$
$$F_m F_{n+1} + F_{m-1} F_n = F_{m+n}.$$

In particular, with $m = n$,

$$\begin{aligned} F_{2n-1} &= F_n^2 + F_{n-1}^2 \\ F_{2n} &= (F_{n-1} + F_{n+1})F_n \\ &= (2F_{n-1} + F_n)F_n. \end{aligned}$$

$$\sum_{i=1}^{n} F_i = F_{n+2} - 1$$

$$\sum_{i=0}^{n-1} F_{2i+1} = F_{2n}$$

$$\sum_{i=1}^{n} F_{2i} = F_{2n+1} - 1.$$

$$\sum_{i=1}^{n} {F_i}^2 = F_n F_{n+1}$$

7 Möbius inversion formula

The classic version states that if g and f are arithmetic functions satisfying

$$g(n) = \sum_{d|n} f(d) \quad \text{for every integer } n \geq 1$$

then

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) \quad \text{for every integer } n \geq 1$$

- ε is the multiplicative identity: $\varepsilon(1) = 1$, otherwise 0.
- Id is the identity function with value n: $\mathrm{Id}(n) = n$.
- $1 * \mu = \varepsilon$, the Dirichlet inverse of the constant function 1 is the Möbius function.
- $g = f * 1$ if and only if $f = g * \mu$, the Möbius inversion formula
- $\phi * 1 = \mathrm{Id}$, proved under Euler's totient function

8 Planar graph

Euler's formula:

$$v - e + f = 2.$$

In a finite, connected, simple, planar graph, any face (except possibly the outer one) is bounded by at least three edges and every edge touches at most two faces; using Euler's formula, one can then show that these graphs are sparse in the sense that if $v \geq 3$:

$$e \leq 3v - 6.$$

The **dual graph** of a plane graph G is a graph that has a vertex for each face of G. In the complement dual graph: (removed egdes in the original =¿ edges in dual): a **connected component** is equivalent to a **face** in dual graph.

9 Pell equation

$$x^2 - 2y^2 = 1$$

If x_1, y_1 is the minimal solution then:

$$x_{k+1} = x_1 x_k + n y_1 y_k,$$
$$y_{k+1} = x_1 y_k + y_1 x_k.$$

10 Burnside lemma

let G be a finite group that acts on a set X. For each g in G let X^g denote the set of elements in X that are fixed by g (also said to be left invariant by g), i.e. $X^g = \{x \in X | g.x = x\}$. Burnside's lemma asserts the following formula for the number of orbits, denoted $|X/G|$:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

11 Euler function

Gamma:

$$\Gamma(z) = \int_0^\infty x^{z-1} e^{-x}\, dx, \qquad \Re(z) > 0\ .$$
$$\Gamma(n) = (n-1)!\ .$$
$$\Gamma(n+1) = n\Gamma(n)$$
$$\Gamma(1-z)\Gamma(z) = \frac{\pi}{\sin(\pi z)}, \qquad z \notin \mathbb{Z}$$
$$\Gamma\left(\tfrac{1}{2}\right) = \sqrt{\pi},$$

Beta

$$\mathrm{B}(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}\, dt$$
$$\mathrm{B}(x,y) = \mathrm{B}(y,x)$$
$$\mathrm{B}(x,y) = \frac{\Gamma(x)\,\Gamma(y)}{\Gamma(x+y)}.$$
$$\Gamma(x)\Gamma(y) = \int_{\mathbb{R}} f(u)\, du \cdot \int_{\mathbb{R}} g(u)\, du = \int_{\mathbb{R}} (f * g)(u)\, du = \mathrm{B}(x,y)\,\Gamma(x+y).$$

12 3 mutually tangent circles

Given 3 mutually tangent circles. Find inner circle (touching all 3) and outer circle (touching all 3). The radius is given by:

$$k4 = |k1 + k2 + k3 \pm 2 * \sqrt{k1 * k2 + k2 * k3 + k3 * k1}|$$

where $ki = 1/r_i$
Minus → Outer

Plus → Inner
Special cases: If 1 circle → line, change k_i to 0, the radius:

$$k4 = k1 + k2 \pm 2 * \sqrt{k1 * k2}$$

13 Hacken Bush

Green Hacken Bush: subtree of u: $g(u) = \bigoplus_v g(v) + 1$ with v is a child of u.
RB Hacken Bush:

- *Rooted tree u*: $g(u) = \sum f(g(v))$ with v is a child of u.
  - If color of u, v is blue: $f(x) = \frac{x+i}{2^{i-1}}$ with smallest $i \geq 1$ such that $x + i > +1$
  - If color of u, v is red: $f(x) = \frac{x-i}{2^{i-1}}$ with smallest $i \geq 1$ such that $x - i < -1$
- *Loop*: find 2 nearest 2 points where segment change color, cut the rest in half the value of loop is sum of the 2 segments. If there are an odd number, cut the middle segment in half and treat it as two segments
- *Stalk*: Count the number of blue (or red) edges that are connected in one continuous path. If there are n of them, start with the number n. For each new edge going up, assign that value of that edge to be half of the one below it. If it is a blue edge, make it positive. If it is a red edge, make it negative.

14 Prüfer sequence

- Get prufer code of a tree
  - Find a leaf of lowest label x, connect to y. Remove x, add y to the sequence
  - Repeat until we are left with 2 nodes
- Construct a tree
  - Let the first element is X, find a node which doesn't appear in the sequence L
  - Add edge X, L
  - Remove X

Cayley's formula

- The number of trees on n labeled vertices is n^{n-2}.
- The number of labelled rooted forests on n vertices, namely $(n+1)^{n-1}$.
- The number of labelled forests on n vertices with k connected components, such that vertices $1, 2, \ldots, k$ all belong to different connected components is kn^{n-k-1}.

15 Graph realization

Erdős–Gallai theorem

A sequence of non-negative integers $d_1 \geq \cdots \geq d_n$ can be represented as the degree sequence of a finite simple graph on n vertices if and only if $d_1 + \cdots + d_n$ is even and

$$\sum_{i=1}^{k} d_i \leq k(k-1) + \sum_{i=k+1}^{n} \min(d_i, k)$$

holds for every k in $1 \leq k \leq n$.

Fulkerson–Chen–Anstee theorem

A sequence $((a_1, b_1), \ldots, (a_n, b_n))$ of nonnegative integer pairs with $a_1 \geq \cdots \geq a_n$ is digraphic if and only if $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$ and the following inequality holds for k such that $1 \leq k \leq n$:

$$\sum_{i=1}^{k} a_i \leq \sum_{i=1}^{k} \min(b_i, k-1) + \sum_{i=k+1}^{n} \min(b_i, k)$$

Gale–Ryser theorem

A pair of sequences of nonnegative integers $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ with $a_1 \geq \cdots \geq a_n$ is bigraphic if and only if $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$ and the following inequality holds for k such that $1 \leq k \leq n$:

$$\sum_{i=1}^{k} a_i \leq \sum_{i=1}^{n} \min(b_i, k).$$

16 Binomial coefficient

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$$

$$\binom{n}{h}\binom{n-h}{k} = \binom{n}{k}\binom{n-k}{h}$$

$$\sum_{j=0}^{k}\binom{m}{j}\binom{n-m}{k-j} = \binom{n}{k}$$

$$\sum_{j=0}^{m}\binom{m}{j}^2 = \binom{2m}{m},$$

$$\sum_{m=0}^{n}\binom{m}{j}\binom{n-m}{k-j} = \binom{n+1}{k+1}.$$

$$\sum_{m=k}^{n}\binom{m}{k} = \binom{n+1}{k+1}$$

$$\sum_{r=0}^{m}\binom{n+r}{r} = \binom{n+m+1}{m}.$$

$$\sum_{k=0}^{\lfloor n/2 \rfloor}\binom{n-k}{k} = F(n+1).$$

17 Kőnig's theorem

Kőnig's theorem states that, in any bipartite graph, the **minimum vertex cover set** and the **maximum matching set** have in fact the same size.

Constructive proof

The following proof provides a way of constructing a minimum vertex cover from a maximum matching. Let $G = (V, E)$ be a bipartite graph and let L, R be the two parts of the vertex set V. Suppose that M is a maximum matching for G. No vertex in a vertex cover can cover more than one edge of M (because the edge half-overlap would prevent M from being a matching in the first place), so if a vertex cover with $|M|$ vertices can be constructed, it must be a minimum cover.

To construct such a cover, let U be the set of unmatched vertices in L (possibly empty), and let Z be the set of vertices that are either in U or are connected to U by alternating paths (paths that alternate between edges that are in the matching and edges that are not in the matching). Let

$$K = (L \setminus Z) \cup (R \cap Z).$$

Every edge e in E either belongs to an alternating path (and has a right endpoint in K), or it has a left endpoint in K. For, if e is matched but not in an alternating path, then its left endpoint cannot be in an alternating path (because two matched edges can not share a vertex) and thus belongs to $L \setminus Z$. Alternatively, if e is unmatched but not in an alternating path, then its left endpoint cannot be in an alternating path, for such a path could be extended by adding e to it. Thus, K forms a vertex cover.

Additionally, every vertex in K is an endpoint of a matched edge. For, every vertex in $L \setminus Z$ is matched because Z is a superset of U, the set of unmatched left vertices. And every vertex in $R \cap Z$ must also be matched, for if there existed an alternating path to an unmatched vertex then changing the matching by removing the matched edges from this path and adding the unmatched edges in their place would increase the size of the matching. However, no matched edge can have both of its endpoints in K. Thus, K is a vertex cover of cardinality equal to M, and must be a minimum vertex cover.

18 Dilworth's theorem

Dilworth's theorem states that, in any finite partially ordered set, the largest antichain has the same size as the smallest chain decomposition. Here, the size of the antichain is its number of elements, and the size of the chain decomposition is its number of chains.

19 3D Transformation

- **Rotation** We can perform 3D rotation about X, Y, and Z axes (**counter-clockwise**). They are represented in the matrix form as below:

$$R_x(\theta) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & cos\theta & -sin\theta & 0 \\ 0 & sin\theta & cos\theta & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$R_y(\theta) = \begin{bmatrix} cos\theta & 0 & sin\theta & 0 \\ 0 & 1 & 0 & 0 \\ -sin\theta & 0 & cos\theta & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$R_z(\theta) = \begin{bmatrix} cos\theta & -sin\theta & 0 & 0 \\ sin\theta & cos\theta & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- **Scaling**:

$$S = \begin{bmatrix} S_x & 0 & 0 & 0 \\ 0 & S_y & 0 & 0 \\ 0 & 0 & S_z & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- **Shear**

$$Sh = \begin{bmatrix} 1 & sh_x^y & sh_x^z & 0 \\ sh_y^x & 1 & sh_y^z & 0 \\ sh_z^x & sh_z^y & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

20 Matroid intersection

Matroid is a pair $<X, I>$ where X is called ground set and I is set of all independent subsets of X. In other words matroid $<X, I>$ gives a classification for each subset of X to be either independent or dependent (included in I or not included in I).
Of course, we are not speaking about arbitrary classifications. These 3 properties must hold for any matroid:

- Empty set is independent.
- Any subset of independent set is independent.
- If independent set A has smaller size than independent set B, there exist at least one element in B that can be added into A without loss of independency.

Some types of matroid:

- **Uniform matroid**: Matroid that considers subset S independent if size of S is not greater than some constant k ($|S| \le k$).
- **Linear (algebra) matroid**
- **Colorful matroid**: Set of elements is independent if no pair of included elements share a color
- **Graphic matroid**:This matroid is defined on edges of some undirected graph. Set of edges is independent if it does not contain a cycle
- **Truncated matroid**: We can limit rank of any matroid by some number k without breaking matroid properties
- **Matroid on a subset of ground set**. We can limit ground set of matroid to its subset without breaking matroid properties
- **Expanded matroid. Direct matroid sum.** We can consider two matroids as one big matroid without any difficulties if elements of ground set of first matroid does not affect independence, neither intersect with elements of ground set of second matroid and vise versa. Think of two graphic matroids on two connected graphs. We can unite their graphs together resulting in graph with two connected components, but it is clear that including some edges in one component have no effect on other component. This is called direct matroid sum. Formally, $M_1 = <X_1, I_1>, M_2 = <X_2, I_2>, M_1 + M_2 = <X_1 \bigcup X_2, I_1 \times I_2>$, where × means cartesian product of two sets. You can unite as many matroids of as many different types without restrictions as you want (if you can find some use for the result).

Matroid intersection solution We are given two matroids $M_1 = <X, I_1>$ and $M_2 = <X, I_2>$ with ranking functions r_1 and r_2 respectively and independence oracles with running times $C1$ and $C2$ respectively. We need to find largest set S that is independent for both matroids.

According to algorithm we need to start with empty S and then repeat the following until we fail to do this:

- Build exchange graph $D_{(M1,M2)}(S)$
- Find "free to include vertices" sets Y_1 and Y_2
- Find **Shortest** augmenting path without shortcuts P from any element in Y_1 to any element in Y_2
- Alternate inclusion into S of all elements in P

We do this at most $O(|S|)$ times.

Exchange graph: Split elements in half: S and X
S. If we exchange $v \in X$
S and $u \in S$, add edge $u \to v$ in matroid $M_1 = <X, I_1>$ and $v \to u$ in matroid $M_2 = <X_2, I_2>$