代数结构与线性代数

Clonoth

2025.7

前言

本课件旨在让大家对基础的代数结构与线性代数有一个总体的认识，避免一些常识性的错误，如 $\mathbb{Z}_n^2$。

代数系统

- 定义：代数系统由构成成分（载体+运算）、公理组成。

代数系统

- 定义：代数系统由构成成分（载体+运算）、公理组成。
- 在 OI 中一般不讨论一般的代数系统，只关心半群、群、环、域。

半群的定义

- 称代数结构 $\langle S, \circ \rangle$ 为半群，若

半群的定义

- 称代数结构 $\langle S, \circ \rangle$ 为半群，若
  - $\forall a, b \in S, a \circ b \in S$。

半群的定义

- 称代数结构 $\langle S, \circ \rangle$ 为半群，若
  - $\forall a, b \in S, a \circ b \in S$。
  - $\forall a, b, c \in S, (a \circ b) \circ c = a \circ (b \circ c)$。

半群的定义

- 称代数结构 $\langle S, \circ \rangle$ 为半群，若
  - $\forall a, b \in S, a \circ b \in S$。
  - $\forall a, b, c \in S, (a \circ b) \circ c = a \circ (b \circ c)$。
- 一般将半群 / 群中的运算 $a \circ b$ 记为 ab。

半群的定义

- 称代数结构 $\langle S, \circ \rangle$ 为半群，若
  - $\forall a, b \in S, a \circ b \in S$。
  - $\forall a, b, c \in S, (a \circ b) \circ c = a \circ (b \circ c)$。
- 一般将半群 / 群中的运算 $a \circ b$ 记为 ab。
- 也就是说，半群满足运算封闭性、结合律。

半群的运算

- 一般将半群 / 群中的运算 $a \circ b$ 记为 ab。

半群的运算

- 一般将半群 / 群中的运算 $a \circ b$ 记为 ab。
- 定义幂运算 $a^1 = a, a^{n+1} = a^n a$。

半群的运算

- 一般将半群 / 群中的运算 $a \circ b$ 记为 ab。
- 定义幂运算 $a^1 = a, a^{n+1} = a^n a$。
- 若存在单位元 e 满足 $ae = ea = a$，那么定义 $a^0 = e$。

半群的运算

- 一般将半群 / 群中的运算 $a \circ b$ 记为 ab。
- 定义幂运算 $a^1 = a, a^{n+1} = a^n a$。
- 若存在单位元 e 满足 $ae = ea = a$，那么定义 $a^0 = e$。
- 根据半群的定义可以得到，半群满足结合律，所以能用线段树维护的信息都至少是半群。如 $\langle \mathbb{Z}, + \rangle$ 为半群。

群的定义

- 称半群 $\langle G, \circ \rangle$ 为群，若

群的定义

- 称半群 $\langle G, \circ \rangle$ 为群，若
  - $\exists e \in S, \forall a \in S, ea = ae = a$。

群的定义

- 称半群 $\langle G, \circ \rangle$ 为群，若
  - $\exists e \in S, \forall a \in S, ea = ae = a$。
  - $\forall a \in S, \exists b \in S, ab = ba = e$，此时记 $b = a^{-1}, a = b^{-1}$，称 a, b 互为逆元。

群的定义

- 称半群 $\langle G, \circ \rangle$ 为群，若
  - $\exists e \in S, \forall a \in S, ea = ae = a$。
  - $\forall a \in S, \exists b \in S, ab = ba = e$，此时记 $b = a^{-1}, a = b^{-1}$，称 a, b 互为逆元。

群的定义

- 称半群 $\langle G, \circ \rangle$ 为群，若
  - $\exists e \in S, \forall a \in S, ea = ae = a$。
  - $\forall a \in S, \exists b \in S, ab = ba = e$，此时记 $b = a^{-1}, a = b^{-1}$，称 a, b 互为逆元。
- 也就是说，群在半群的基础上满足存在单位元与逆元。如 $\langle \mathbb{Z}, + \rangle$ 为群。

群的定义

- 称半群 $\langle G, \circ\rangle$ 为群，若
  - $\exists e \in S, \forall a \in S, ea = ae = a$。
  - $\forall a \in S, \exists b \in S, ab = ba = e$，此时记 $b = a^{-1}, a = b^{-1}$，称 a, b 互为逆元。
- 也就是说，群在半群的基础上满足存在单位元与逆元。如 $\langle \mathbb{Z}, +\rangle$ 为群。
- 若 $\circ$ 满足交换律，则称 G 为交换群（或 Abel 群）。

群的定义

- 称半群 $\langle G, \circ \rangle$ 为群，若
  - $\exists e \in S, \forall a \in S, ea = ae = a$。
  - $\forall a \in S, \exists b \in S, ab = ba = e$，此时记 $b = a^{-1}, a = b^{-1}$，称 a, b 互为逆元。
- 也就是说，群在半群的基础上满足存在单位元与逆元。如 $\langle \mathbb{Z}, + \rangle$ 为群。
- 若 $\circ$ 满足交换律，则称 G 为交换群（或 Abel 群）。
- $\forall x \in G$，定义 x 的阶 $|x|$ 为最小的正整数 k 使得 $x^k = e$。

群的定义

- 称半群 $\langle G, \circ \rangle$ 为群，若
  - $\exists e \in S, \forall a \in S, ea = ae = a$。
  - $\forall a \in S, \exists b \in S, ab = ba = e$，此时记 $b = a^{-1}, a = b^{-1}$，称 a, b 互为逆元。
- 也就是说，群在半群的基础上满足存在单位元与逆元。如 $\langle \mathbb{Z}, + \rangle$ 为群。
- 若 $\circ$ 满足交换律，则称 G 为交换群（或 Abel 群）。
- $\forall x \in G$，定义 x 的阶 $|x|$ 为最小的正整数 k 使得 $x^k = e$。
- 关于子群、置换群的部分将在 Burnside 引理部分展开。

环的定义

- 称代数系统 $\langle R, +, \cdot \rangle$，若

环的定义

- 称代数系统 $\langle R, +, \cdot \rangle$，若
  - $\langle R, + \rangle$ 为 Abel 群。

环的定义

- 称代数系统 $\langle R, +, \cdot \rangle$，若
  - $\langle R, + \rangle$ 为 Abel 群。
  - $\langle R, \cdot \rangle$ 为半群。

环的定义

- 称代数系统 $\langle R, +, \cdot \rangle$，若
  - $\langle R, + \rangle$ 为 Abel 群。
  - $\langle R, \cdot \rangle$ 为半群。
  - $\cdot$ 关于 $+$ 满足分配律。
- 称 $+$ 为加法，$\cdot$ 为乘法。

环的定义

- 称代数系统 $\langle R, +, \cdot\rangle$，若
  - $\langle R, +\rangle$ 为 Abel 群。
  - $\langle R, \cdot\rangle$ 为半群。
  - $\cdot$ 关于 $+$ 满足分配律。
- 称 $+$ 为加法，$\cdot$ 为乘法。
- 称加法单位元为 0，乘法单位元（如果存在）为 1。可以发现 $0x = x0 = 0$。

环的定义

- 称代数系统 $\langle R, +, \cdot \rangle$，若
  - $\langle R, + \rangle$ 为 Abel 群。
  - $\langle R, \cdot \rangle$ 为半群。
  - $\cdot$ 关于 $+$ 满足分配律。
- 称 $+$ 为加法，$\cdot$ 为乘法。
- 称加法单位元为 0，乘法单位元（如果存在）为 1。可以发现 $0x = x0 = 0$。
- $\forall x \in R$，称 x 的加法逆元为负元，记为 $-x$，称 x 的乘法逆元为逆元（若存在），记为 x^{-1}。

特殊的环

- 若乘法单位元存在，称 R 为有 1 的环或含幺环。

特殊的环

- 若乘法单位元存在，称 R 为有 1 的环或含幺环。
- 若乘法可交换，称 R 为交换环。

特殊的环

- 若乘法单位元存在，称 R 为有 1 的环或含幺环。
- 若乘法可交换，称 R 为交换环。
- 若 R 中无零因子，即 $\forall x, y \in R, xy = 0 \Rightarrow x = 0 \vee y = 0$，称 R 为无零因子环，

特殊的环

- 若乘法单位元存在，称 R 为有 1 的环或含幺环。
- 若乘法可交换，称 R 为交换环。
- 若 R 中无零因子，即 $\forall x, y \in R, xy = 0 \Rightarrow x = 0 \vee y = 0$，称 R 为无零因子环，
- 若 R 无零因子、含幺、交换，称 R 为整环。

特殊的环

- 若乘法单位元存在，称 R 为有 1 的环或含幺环。
- 若乘法可交换，称 R 为交换环。
- 若 R 中无零因子，即 $\forall x, y \in R, xy = 0 \Rightarrow x = 0 \vee y = 0$，称 R 为无零因子环，
- 若 R 无零因子、含幺、交换，称 R 为整环。
- 若 $\langle R^* = R \setminus \{0\}, \cdot \rangle$ 为群，称 R 为除环。

特殊的环

- 若乘法单位元存在，称 R 为有 1 的环或含幺环。
- 若乘法可交换，称 R 为交换环。
- 若 R 中无零因子，即 $\forall x, y \in R, xy = 0 \Rightarrow x = 0 \vee y = 0$，称 R 为无零因子环，
- 若 R 无零因子、含幺、交换，称 R 为整环。
- 若 $\langle R^* = R \setminus \{0\}, \cdot \rangle$ 为群，称 R 为除环。
- 若 R 为交换的除环，则称 R 为域。

无零因子环的特征

- 定理：对于无零因子环 R，则 R 中所有非零元的加法阶相等，为 ∞ 或为某个素数 p。

无零因子环的特征

- 定理：对于无零因子环 R，则 R 中所有非零元的加法阶相等，为 ∞ 或为某个素数 p。
- 定义：对于无零因子环 R，称 R 中非零元的加法阶为 R 的特征，记为 $\mathrm{Char}R$；当 R 中非零元的加法阶为 ∞ 时，定义 $\mathrm{Char}R = 0$。

无零因子环的特征

- 定理：对于无零因子环 R，则 R 中所有非零元的加法阶相等，为 ∞ 或为某个素数 p。
- 定义：对于无零因子环 R，称 R 中非零元的加法阶为 R 的特征，记为 $\mathrm{Char}R$；当 R 中非零元的加法阶为 ∞ 时，定义 $\mathrm{Char}R = 0$。
- 由于域为无零因子环，所以域的特征也如上定义。

无零因子环的特征

- 定理：对于无零因子环 R，则 R 中所有非零元的加法阶相等，为 ∞ 或为某个素数 p。
- 定义：对于无零因子环 R，称 R 中非零元的加法阶为 R 的特征，记为 $\mathrm{Char}R$；当 R 中非零元的加法阶为 ∞ 时，定义 $\mathrm{Char}R = 0$。
- 由于域为无零因子环，所以域的特征也如上定义。
- 例：对于素数 p，$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ 为特征为 p 的域。

线性空间

- 对于集合 V 和域 F 及满足封闭性的运算 $+, \cdot$（称为加法和数乘），若其满足以下性质，则称之为线性空间（或向量空间）。

线性空间

- 对于集合 V 和域 F 及满足封闭性的运算 $+, \cdot$（称为加法和数乘），若其满足以下性质，则称之为线性空间（或向量空间）。
  1. $\forall \alpha, \beta \in V, \alpha + \beta = \beta + \alpha$。

线性空间

- 对于集合 V 和域 F 及满足封闭性的运算 $+, \cdot$（称为加法和数乘），若其满足以下性质，则称之为线性空间（或向量空间）。
  1. $\forall \alpha, \beta \in V, \alpha + \beta = \beta + \alpha$。
  2. $\forall \alpha, \beta, \gamma \in V, (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$。

线性空间

- 对于集合 V 和域 F 及满足封闭性的运算 $+, \cdot$（称为加法和数乘），若其满足以下性质，则称之为线性空间（或向量空间）。
  1. $\forall \alpha, \beta \in V, \alpha + \beta = \beta + \alpha$。
  2. $\forall \alpha, \beta, \gamma \in V, (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$。
  3. $\exists 0 \in V, \forall \alpha \in V, 0 + \alpha = \alpha$。

线性空间

- 对于集合 V 和域 F 及满足封闭性的运算 $+, \cdot$（称为加法和数乘），若其满足以下性质，则称之为线性空间（或向量空间）。
  1. $\forall \alpha, \beta \in V, \alpha + \beta = \beta + \alpha$。
  2. $\forall \alpha, \beta, \gamma \in V, (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$。
  3. $\exists 0 \in V, \forall \alpha \in V, 0 + \alpha = \alpha$。
  4. $\forall \alpha \in V, \exists \beta \in V, \alpha + \beta = 0$。

线性空间

- 对于集合 V 和域 F 及满足封闭性的运算 $+,\cdot$（称为加法和数乘），若其满足以下性质，则称之为线性空间（或向量空间）。
  1. $\forall\alpha,\beta\in V,\alpha+\beta=\beta+\alpha$。
  2. $\forall\alpha,\beta,\gamma\in V,(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$。
  3. $\exists 0\in V,\forall\alpha\in V,0+\alpha=\alpha$。
  4. $\forall\alpha\in V,\exists\beta\in V,\alpha+\beta=0$。
  5. $\forall\alpha\in V,1\alpha=\alpha$。

线性空间

- 对于集合 V 和域 F 及满足封闭性的运算 $+, \cdot$（称为加法和数乘），若其满足以下性质，则称之为线性空间（或向量空间）。
  1. $\forall \alpha, \beta \in V, \alpha + \beta = \beta + \alpha$。
  2. $\forall \alpha, \beta, \gamma \in V, (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$。
  3. $\exists 0 \in V, \forall \alpha \in V, 0 + \alpha = \alpha$。
  4. $\forall \alpha \in V, \exists \beta \in V, \alpha + \beta = 0$。
  5. $\forall \alpha \in V, 1\alpha = \alpha$。
  6. $\forall \alpha \in V, \forall k, l \in F, k(l\alpha) = (kl)\alpha$。

线性空间

- 对于集合 V 和域 F 及满足封闭性的运算 $+, \cdot$（称为加法和数乘），若其满足以下性质，则称之为线性空间（或向量空间）。
  1. $\forall \alpha, \beta \in V, \alpha + \beta = \beta + \alpha$。
  2. $\forall \alpha, \beta, \gamma \in V, (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$。
  3. $\exists 0 \in V, \forall \alpha \in V, 0 + \alpha = \alpha$。
  4. $\forall \alpha \in V, \exists \beta \in V, \alpha + \beta = 0$。
  5. $\forall \alpha \in V, 1\alpha = \alpha$。
  6. $\forall \alpha \in V, \forall k, l \in F, k(l\alpha) = (kl)\alpha$。
  7. $\forall \alpha \in V, \forall k, l \in F, (k + l)\alpha = k\alpha + l\alpha$。

线性空间

- 对于集合 V 和域 F 及满足封闭性的运算 $+,\cdot$（称为加法和数乘），若其满足以下性质，则称之为线性空间（或向量空间）。
  1. $\forall\alpha,\beta\in V,\alpha+\beta=\beta+\alpha$。
  2. $\forall\alpha,\beta,\gamma\in V,(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$。
  3. $\exists 0\in V,\forall\alpha\in V,0+\alpha=\alpha$。
  4. $\forall\alpha\in V,\exists\beta\in V,\alpha+\beta=0$。
  5. $\forall\alpha\in V,1\alpha=\alpha$。
  6. $\forall\alpha\in V,\forall k,l\in F,k(l\alpha)=(kl)\alpha$。
  7. $\forall\alpha\in V,\forall k,l\in F,(k+l)\alpha=k\alpha+l\alpha$。
  8. $\forall\alpha,\beta\in V,\forall k\in F,k(\alpha+\beta)=k\alpha+k\beta$。

线性相关、线性无关与向量组的秩

- 对于 V 中的向量 $\alpha_1, \ldots, \alpha_n$，若存在不全为 0 的 $k_1, \ldots, k_n$ 使得 $k_1\alpha_1 + \cdots + k_n\alpha_n = 0$，则称 $\alpha_1, \ldots, \alpha_n$ 线性相关。

线性相关、线性无关与向量组的秩

- 对于 V 中的向量 $\alpha_1, \ldots, \alpha_n$，若存在不全为 0 的 $k_1, \ldots, k_n$ 使得 $k_1\alpha_1 + \cdots + k_n\alpha_n = 0$，则称 $\alpha_1, \ldots, \alpha_n$ 线性相关。
- 对于 V 中的向量 $\alpha_1, \ldots, \alpha_n$，若不存在不全为 0 的 $k_1, \ldots, k_n$ 使得 $k_1\alpha_1 + \cdots + k_n\alpha_n = 0$，则称 $\alpha_1, \ldots, \alpha_n$ 线性无关。

线性相关、线性无关与向量组的秩

- 对于 V 中的向量 $\alpha_1, \ldots, \alpha_n$，若存在不全为 0 的 $k_1, \ldots, k_n$ 使得 $k_1\alpha_1 + \cdots + k_n\alpha_n = 0$，则称 $\alpha_1, \ldots, \alpha_n$ 线性相关。
- 对于 V 中的向量 $\alpha_1, \ldots, \alpha_n$，若不存在不全为 0 的 $k_1, \ldots, k_n$ 使得 $k_1\alpha_1 + \cdots + k_n\alpha_n = 0$，则称 $\alpha_1, \ldots, \alpha_n$ 线性无关。
- 对于 V 中的向量 $\alpha_1, \ldots, \alpha_n$，取 $\alpha_1, \ldots, \alpha_n$ 中的极大线性无关组 $\alpha_{i_1}, \ldots, \alpha_{i_m}$，则称 m 为向量组 $\alpha_1, \ldots, \alpha_n$ 的秩，记为 $\mathrm{rank}\{\alpha_1, \ldots, \alpha_n\}$。

基、维数与坐标

- 对于 V 中的极大线性无关组 $\alpha_1, \ldots, \alpha_n$，称 $\alpha_1, \ldots, \alpha_n$ 为 V 的一组基，称 n 为 V 的维数，记为 $\dim V$。

基、维数与坐标

- 对于 V 中的极大线性无关组 $\alpha_1, \ldots, \alpha_n$，称 $\alpha_1, \ldots, \alpha_n$ 为 V 的一组基，称 n 为 V 的维数，记为 $\dim V$。
- 约定：所有线性空间均为有限维线性空间。无限维线性空间在 OI 中没有应用。

基、维数与坐标

- 对于 V 中的极大线性无关组 $\alpha_1,\dots,\alpha_n$，称 $\alpha_1,\dots,\alpha_n$ 为 V 的一组基，称 n 为 V 的维数，记为 $\dim V$。
- 约定：所有线性空间均为有限维线性空间。无限维线性空间在 OI 中没有应用。
- 命题：对于 n 维线性空间 V 的线性无关组 $\alpha_1,\dots,\alpha_m$，存在 $\beta_1,\dots,\beta_{n-m}$ 满足 $\alpha_1,\dots,\alpha_m,\beta_1,\dots,\beta_{n-m}$ 为 V 的基。

基、维数与坐标

- 对于 V 中的极大线性无关组 $\alpha_1, \dots, \alpha_n$，称 $\alpha_1, \dots, \alpha_n$ 为 V 的一组基，称 n 为 V 的维数，记为 $\dim V$。
- 约定：所有线性空间均为有限维线性空间。无限维线性空间在 OI 中没有应用。
- 命题：对于 n 维线性空间 V 的线性无关组 $\alpha_1, \dots, \alpha_m$，存在 $\beta_1, \dots, \beta_{n-m}$ 满足 $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_{n-m}$ 为 V 的基。
- 对于给定的线性空间 V 中的基 $\alpha_1, \dots, \alpha_n$，对于任意 V 中的向量 β 总存在唯一的 $k_1, k_2, \dots, k_n$ 使得 $\beta = k_1\alpha_1 + \dots + k_n\alpha_n$，此时称 $\begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix}$ 为 β 在基 $\alpha_1, \dots, \alpha_n$ 下的坐标。

子空间与生成子空间

- 对于线性空间 V 的子集 $U \subseteq V$，若 U 也为线性空间，则称 U 为 V 的子空间。

子空间与生成子空间

- 对于线性空间 V 的子集 $U \subseteq V$，若 U 也为线性空间，则称 U 为 V 的子空间。
- 对于线性空间 V 中的向量组 $\alpha_1, \dots, \alpha_n$，令 $U = \{k_1\alpha_1 + \cdots + k_n\alpha_n \mid k_1, \dots, k_n \in K\}$ 为由 $\alpha_1, \dots, \alpha_n$ 生成的子空间，容易验证 U 确实为 V 子空间，记为 $L(\alpha_1, \dots, \alpha_n)$ 或 $\langle \alpha_1, \dots, \alpha_n \rangle$ 或 $\operatorname{span}\{\alpha_1, \dots, \alpha_n\}$。

子空间与生成子空间

- 对于线性空间 V 的子集 $U \subseteq V$，若 U 也为线性空间，则称 U 为 V 的子空间。
- 对于线性空间 V 中的向量组 $\alpha_1, \ldots, \alpha_n$，令 $U = \{k_1\alpha_1 + \cdots + k_n\alpha_n \mid k_1, \ldots, k_n \in K\}$ 为由 $\alpha_1, \ldots, \alpha_n$ 生成的子空间，容易验证 U 确实为 V 子空间，记为 $L(\alpha_1, \ldots, \alpha_n)$ 或 $\langle\alpha_1, \ldots, \alpha_n\rangle$ 或 $\operatorname{span}\{\alpha_1, \ldots, \alpha_n\}$。
- 命题：$\dim L(\alpha_1, \ldots, \alpha_n) = \operatorname{rank}\{\alpha_1, \ldots, \alpha_n\}$。

子空间的和与直和、补空间

- 对于线性空间 V 的子空间 U_1, U_2，设 $W = \{\alpha + \beta \mid \alpha \in U_1, \beta \in U_2\}$，称 W 为 U_1 与 U_2 的和，记为 $W = U_1 + U_2$。若 $U_1 \cap U_2 = \{0\}$，则称 $W = U_1 + U_2$ 为直和，记为 $W = U_1 \oplus U_2$。

子空间的和与直和、补空间

- 对于线性空间 V 的子空间 U_1, U_2，设 $W = \{\alpha + \beta \mid \alpha \in U_1, \beta \in U_2\}$，称 W 为 U_1 与 U_2 的和，记为 $W = U_1 + U_2$。若 $U_1 \cap U_2 = \{0\}$，则称 $W = U_1 + U_2$ 为直和，记为 $W = U_1 \oplus U_2$。
- 命题：对于 $W = U_1 + U_2$，以下命题等价。

子空间的和与直和、补空间

- 对于线性空间 V 的子空间 U_1, U_2，设 $W = \{\alpha + \beta \mid \alpha \in U_1, \beta \in U_2\}$，称 W 为 U_1 与 U_2 的和，记为 $W = U_1 + U_2$。若 $U_1 \cap U_2 = \{0\}$，则称 $W = U_1 + U_2$ 为直和，记为 $W = U_1 \oplus U_2$。
- 命题：对于 $W = U_1 + U_2$，以下命题等价。
  1. $W = U_1 \oplus U_2$。

子空间的和与直和、补空间

- 对于线性空间 V 的子空间 U_1, U_2，设 $W = \{\alpha + \beta \mid \alpha \in U_1, \beta \in U_2\}$，称 W 为 U_1 与 U_2 的和，记为 $W = U_1 + U_2$。若 $U_1 \cap U_2 = \{0\}$，则称 $W = U_1 + U_2$ 为直和，记为 $W = U_1 \oplus U_2$。
- 命题：对于 $W = U_1 + U_2$，以下命题等价。
  1. $W = U_1 \oplus U_2$。
  2. $\dim W = \dim U_1 + \dim U_2$。

子空间的和与直和、补空间

- 对于线性空间 V 的子空间 U_1, U_2，设 $W = \{\alpha + \beta \mid \alpha \in U_1, \beta \in U_2\}$，称 W 为 U_1 与 U_2 的和，记为 $W = U_1 + U_2$。若 $U_1 \cap U_2 = \{0\}$，则称 $W = U_1 + U_2$ 为直和，记为 $W = U_1 \oplus U_2$。
- 命题：对于 $W = U_1 + U_2$，以下命题等价。
  1. $W = U_1 \oplus U_2$。
  2. $\dim W = \dim U_1 + \dim U_2$。
  3. U_1 的基与 U_2 的基拼接得到 W 的基。

子空间的和与直和、补空间

- 对于线性空间 V 的子空间 U_1, U_2，设 $W = \{\alpha + \beta \mid \alpha \in U_1, \beta \in U_2\}$，称 W 为 U_1 与 U_2 的和，记为 $W = U_1 + U_2$。若 $U_1 \cap U_2 = \{0\}$，则称 $W = U_1 + U_2$ 为直和，记为 $W = U_1 \oplus U_2$。
- 命题：对于 $W = U_1 + U_2$，以下命题等价。
  1. $W = U_1 \oplus U_2$。
  2. $\dim W = \dim U_1 + \dim U_2$。
  3. U_1 的基与 U_2 的基拼接得到 W 的基。
- 对于线性空间 V 的子空间 $U \subseteq V$，若子空间 W 满足 $V = U \oplus W$，则称 W 为 U 补空间。

线性表出与等价

- 对于线性空间 V 中的向量组 $\alpha_1,\ldots,\alpha_n$ 和向量 β，若存在 $k_1,\ldots,k_n$ 使得 $k_1\alpha_1+\cdots+k_n\alpha_n=\beta$，则称 β 可以由 $\alpha_1\ldots,\alpha_n$ 线性表出。

线性表出与等价

- 对于线性空间 V 中的向量组 $\alpha_1, \ldots, \alpha_n$ 和向量 β，若存在 $k_1, \ldots, k_n$ 使得 $k_1\alpha_1 + \cdots + k_n\alpha_n = \beta$，则称 β 可以由 $\alpha_1 \ldots, \alpha_n$ 线性表出。
- 对于线性空间 V 中的向量组 $\alpha_1, \ldots, \alpha_n$ 和 $\beta_1, \ldots, \beta_m$，若对于任意 $1 \leq i \leq m$，β_i 都可以由 $\alpha_1 \ldots, \alpha_n$ ，则称 $\beta_1, \ldots, \beta_m$ 可以由 $\alpha_1 \ldots, \alpha_n$ 线性表出。

线性表出与等价

- 对于线性空间 V 中的向量组 $\alpha_1, \ldots, \alpha_n$ 和向量 β，若存在 $k_1, \ldots, k_n$ 使得 $k_1\alpha_1 + \cdots + k_n\alpha_n = \beta$，则称 β 可以由 $\alpha_1 \ldots, \alpha_n$ 线性表出。
- 对于线性空间 V 中的向量组 $\alpha_1, \ldots, \alpha_n$ 和 $\beta_1, \ldots, \beta_m$，若对于任意 $1 \leq i \leq m$，β_i 都可以由 $\alpha_1 \ldots, \alpha_n$ ，则称 $\beta_1, \ldots, \beta_m$ 可以由 $\alpha_1 \ldots, \alpha_n$ 线性表出。
- 对于线性空间 V 中的向量组 $\alpha_1, \ldots, \alpha_n$ 和 $\beta_1, \ldots, \beta_m$，若 $\alpha_1, \ldots, \alpha_n$ 可以由 $\beta_1, \ldots, \beta_m$ 线性表出，且 $\beta_1, \ldots, \beta_m$ 可以由 $\alpha_1, \ldots, \alpha_n$ 线性表出，则称向量组 $\alpha_1, \ldots, \alpha_n$ 和 $\beta_1, \ldots, \beta_m$ 等价。

线性表出与等价

- 对于线性空间 V 中的向量组 $\alpha_1, \ldots, \alpha_n$ 和向量 β，若存在 $k_1, \ldots, k_n$ 使得 $k_1\alpha_1 + \cdots + k_n\alpha_n = \beta$，则称 β 可以由 $\alpha_1 \ldots, \alpha_n$ 线性表出。
- 对于线性空间 V 中的向量组 $\alpha_1, \ldots, \alpha_n$ 和 $\beta_1, \ldots, \beta_m$，若对于任意 $1 \leq i \leq m$，β_i 都可以由 $\alpha_1 \ldots, \alpha_n$ ，则称 $\beta_1, \ldots, \beta_m$ 可以由 $\alpha_1 \ldots, \alpha_n$ 线性表出。
- 对于线性空间 V 中的向量组 $\alpha_1, \ldots, \alpha_n$ 和 $\beta_1, \ldots, \beta_m$，若 $\alpha_1, \ldots, \alpha_n$ 可以由 $\beta_1, \ldots, \beta_m$ 线性表出，且 $\beta_1, \ldots, \beta_m$ 可以由 $\alpha_1, \ldots, \alpha_n$ 线性表出，则称向量组 $\alpha_1, \ldots, \alpha_n$ 和 $\beta_1, \ldots, \beta_m$ 等价。
- 推论：等价的向量组具有相同的秩。

向量

- 命题：两个向量空间同构当且仅当它们维数相同。

向量

- 命题：两个向量空间同构当且仅当它们维数相同。
- 所以我们只需要关心形如 F^n 的向量空间，其中 F 为一般的域。

向量

- 命题：两个向量空间同构当且仅当它们维数相同。
- 所以我们只需要关心形如 F^n 的向量空间，其中 F 为一般的域。
- 约定：所有向量均为列向量。

矩阵

- $n \times m$ 的矩阵 $A = \left(a_{i,j}\right)_{n\times m} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}$，$A$ 的转置 ${}^tA = \begin{pmatrix} a_{1,1} & \cdots & a_{n,1} \\ \vdots & \ddots & \vdots \\ a_{1,m} & \cdots & a_{n,m} \end{pmatrix}$。

矩阵

- $n \times m$ 的矩阵 $A = (a_{i,j})_{n \times m} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}$，$A$ 的转置 ${}^tA = \begin{pmatrix} a_{1,1} & \cdots & a_{n,1} \\ \vdots & \ddots & \vdots \\ a_{1,m} & \cdots & a_{n,m} \end{pmatrix}$。
- A 的列向量组为 $A = (\alpha_1 \ldots \alpha_m)$，其中 $\alpha_i = \begin{pmatrix} a_{1,i} \\ \vdots \\ a_{n,i} \end{pmatrix}$。

矩阵

- $n \times m$ 的矩阵 $A = (a_{i,j})_{n\times m} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}$，$A$ 的转置 ${}^tA = \begin{pmatrix} a_{1,1} & \cdots & a_{n,1} \\ \vdots & \ddots & \vdots \\ a_{1,m} & \cdots & a_{n,m} \end{pmatrix}$。
- A 的列向量组为 $A = (\alpha_1 \ldots \alpha_m)$，其中 $\alpha_i = \begin{pmatrix} a_{1,i} \\ \vdots \\ a_{n,i} \end{pmatrix}$。
- A 的行向量组为 $A = \begin{pmatrix} {}^t\beta_1 \\ \vdots \\ {}^t\beta_n \end{pmatrix}$，其中 $\beta_i = \begin{pmatrix} a_{i,1} \\ \vdots \\ a_{i,m} \end{pmatrix}$。

矩阵的秩

- 矩阵的列向量组 $\alpha_1, \ldots, \alpha_m$ 的秩被称为矩阵的列秩。若列向量组线性无关，则称矩阵列满秩。

矩阵的秩

- 矩阵的列向量组 $\alpha_1, \ldots, \alpha_m$ 的秩被称为矩阵的列秩。若列向量组线性无关，则称矩阵列满秩。
- 矩阵的行向量组 $\beta_1, \ldots, \beta_n$ 的秩被称为矩阵的行秩。若行向量组线性无关，则称矩阵行满秩。

矩阵的秩

- 矩阵的列向量组 $\alpha_1, \ldots, \alpha_m$ 的秩被称为矩阵的列秩。若列向量组线性无关，则称矩阵列满秩。
- 矩阵的行向量组 $\beta_1, \ldots, \beta_n$ 的秩被称为矩阵的行秩。若行向量组线性无关，则称矩阵行满秩。
- 定理：矩阵的行秩等于列秩。于是可以定义矩阵的秩。

初等行 / 列变换

- 以下三种操作被称为初等行变换。

初等行 / 列变换

- 以下三种操作被称为初等行变换。
  1. 交换两行。

初等行 / 列变换

- 以下三种操作被称为初等行变换。
  1. 交换两行。
  2. 将某一行乘上一个非零数。

初等行 / 列变换

- 以下三种操作被称为初等行变换。
  1. 交换两行。
  2. 将某一行乘上一个非零数。
  3. 将某一行的任意倍加到另一行上。

初等行 / 列变换

- 以下三种操作被称为初等行变换。
  1. 交换两行。
  2. 将某一行乘上一个非零数。
  3. 将某一行的任意倍加到另一行上。
- 将“行”替换为“列”可定义初等列变换。

初等行 / 列变换

- 以下三种操作被称为初等行变换。
  1. 交换两行。
  2. 将某一行乘上一个非零数。
  3. 将某一行的任意倍加到另一行上。
- 将“行”替换为“列”可定义初等列变换。
- 定理：行向量组与进行初等行变换后的行向量组等价。

初等行 / 列变换

- 以下三种操作被称为初等行变换。
  1. 交换两行。
  2. 将某一行乘上一个非零数。
  3. 将某一行的任意倍加到另一行上。
- 将“行”替换为“列”可定义初等列变换。
- 定理：行向量组与进行初等行变换后的行向量组等价。
- 推论：初等行变换不改变矩阵的秩。

阶梯形与最简阶梯形

- 若矩阵中所有非零行的第一个非零元素的下标严格单调递增，且零行位于矩阵的最后若干行，则称其为阶梯形矩阵。

阶梯形与最简阶梯形

- 若矩阵中所有非零行的第一个非零元素的下标严格单调递增，且零行位于矩阵的最后若干行，则称其为阶梯形矩阵。
- 在阶梯形矩阵中，若非零行的第一个非零元素全是 1，且非零行的第一个元素 1 所在列的其余元素全为零，则称其为最简形阶梯形矩阵。

阶梯形与最简阶梯形

- 若矩阵中所有非零行的第一个非零元素的下标严格单调递增，且零行位于矩阵的最后若干行，则称其为阶梯形矩阵。
- 在阶梯形矩阵中，若非零行的第一个非零元素全是 1，且非零行的第一个元素 1 所在列的其余元素全为零，则称其为最简形阶梯形矩阵。
- 容易发现在阶梯形中所有非零行是行向量的一个极大线性无关组，所以非零的行数就是该矩阵的秩。

高斯消元

- 高斯消元可以用于求出给定矩阵的阶梯形。

高斯消元

- 高斯消元可以用于求出给定矩阵的阶梯形。
- 算法流程：依次扫描所有列的标号，任取一个以当前列作为第一个非零元素的行，并利用这个行将其他行的当前列的元素通过初等行变换变为 0。

高斯消元

- 高斯消元可以用于求出给定矩阵的阶梯形。
- 算法流程：依次扫描所有列的标号，任取一个以当前列作为第一个非零元素的行，并利用这个行将其他行的当前列的元素通过初等行变换变为 0。
- 容易发现执行完该算法的矩阵可以通过若干交换两行的操作变为阶梯形，且可以简单的得到最简阶梯形。

高斯消元

- 高斯消元可以用于求出给定矩阵的阶梯形。
- 算法流程：依次扫描所有列的标号，任取一个以当前列作为第一个非零元素的行，并利用这个行将其他行的当前列的元素通过初等行变换变为 0。
- 容易发现执行完该算法的矩阵可以通过若干交换两行的操作变为阶梯形，且可以简单的得到最简阶梯形。
- 对 $n \times m$ 的矩阵进行高斯消元的复杂度为 nm^2。

求线性方程组的唯一解

- 对于线性方程组 $Ax=b$，令 $\tilde{A}=\begin{pmatrix}A & b\end{pmatrix}$，称 $\tilde{A}$ 为该方程组的增广矩阵。容易发现增广矩阵与线性方程组是一一对应的。

求线性方程组的唯一解

- 对于线性方程组 $Ax=b$，令 $\tilde{A}=\begin{pmatrix} A & b \end{pmatrix}$，称 $\tilde{A}$ 为该方程组的增广矩阵。容易发现增广矩阵与线性方程组是一一对应的。
-

求线性方程组的唯一解

- 对于线性方程组 $Ax=b$，令 $\tilde{A}=\begin{pmatrix} A & b \end{pmatrix}$，称 $\tilde{A}$ 为该方程组的增广矩阵。容易发现增广矩阵与线性方程组是一一对应的。
-
- 命题：该方程组有唯一解当且仅当 $\mathrm{rank}(A)=\mathrm{rank}(\tilde{A})$。

求线性方程组的唯一解

- 对于线性方程组 $Ax = b$，令 $\tilde{A} = \begin{pmatrix} A & b \end{pmatrix}$，称 $\tilde{A}$ 为该方程组的增广矩阵。容易发现增广矩阵与线性方程组是一一对应的。
-
- 命题：该方程组有唯一解当且仅当 $\operatorname{rank}(A) = \operatorname{rank}(\tilde{A})$。
- 所以可以求解一个线性方程组是否有唯一解，且通过高斯消元即可求出方程组的解。

求齐次线性方程组的解集

- 命题：对于其次线性方程组 $Ax = 0$，对 A 做初等行变换不改变解集。

求齐次线性方程组的解集

- 命题：对于其次线性方程组 $Ax=0$，对 A 做初等行变换不改变解集。
- 将 A 变为最简阶梯形，称一个未定元 x_i 为关键的若存在 A 的某一行满足该行的第一个为 1 的元素位于第 i 列，否则称 x_i 为非关键的。

求齐次线性方程组的解集

- 命题：对于其次线性方程组 $Ax=0$，对 A 做初等行变换不改变解集。
- 将 A 变为最简阶梯形，称一个未定元 x_i 为关键的若存在 A 的某一行满足该行的第一个为 1 的元素位于第 i 列，否则称 x_i 为非关键的。
- 对于所有非关键的未定元 x_i，只将 x_i 赋值为 1 将其他非关键的未定元赋值为 0，此时存在对关键的未定元赋值的方案 η_i 使得 $A\eta_i=0$。对于关键的未定元定义 $\eta_i=0$。

求齐次线性方程组的解集

- 命题：对于其次线性方程组 $Ax=0$，对 A 做初等行变换不改变解集。
- 将 A 变为最简阶梯形，称一个未定元 x_i 为关键的若存在 A 的某一行满足该行的第一个为 1 的元素位于第 i 列，否则称 x_i 为非关键的。
- 对于所有非关键的未定元 x_i，只将 x_i 赋值为 1 将其他非关键的未定元赋值为 0，此时存在对关键的未定元赋值的方案 η_i 使得 $A\eta_i=0$。对于关键的未定元定义 $\eta_i=0$。
- 那么 $Ax=0$ 的解集为 $W=L(\eta_1,\ldots,\eta_m)$，称为 A 的核，记为 $\ker A$。

求齐次线性方程组的解集

- 命题：对于其次线性方程组 $Ax=0$，对 A 做初等行变换不改变解集。
- 将 A 变为最简阶梯形，称一个未定元 x_i 为关键的若存在 A 的某一行满足该行的第一个为 1 的元素位于第 i 列，否则称 x_i 为非关键的。
- 对于所有非关键的未定元 x_i，只将 x_i 赋值为 1 将其他非关键的未定元赋值为 0，此时存在对关键的未定元赋值的方案 η_i 使得 $A\eta_i=0$。对于关键的未定元定义 $\eta_i=0$。
- 那么 $Ax=0$ 的解集为 $W=L(\eta_1,\ldots,\eta_m)$，称为 A 的核，记为 $\ker A$。
- 定理：$m=\mathrm{rank}A+\dim\ker A$。

P3812 【模板】线性基

- 注意到 $[0, 2^m)$ 的整数与异或运算构成了向量空间，其中 $V = F_2^m, F = F_2$，F_2 为二元域。

P3812 【模板】线性基

- 注意到 $[0, 2^m)$ 的整数与异或运算构成了向量空间，其中 $V = F_2^m, F = F_2$，F_2 为二元域。

P3812 【模板】线性基

- 注意到 $[0, 2^m)$ 的整数与异或运算构成了向量空间，其中 $V = F_2^m, F = F_2$，F_2 为二元域。
- 考虑求出这 n 个数的生成子空间的基：将所有数的二进制表示视为行向量，拼接得到一个矩阵，并求出这个矩阵的阶梯形即可。

P3812 【模板】线性基

- 注意到 $[0, 2^m)$ 的整数与异或运算构成了向量空间，其中 $V = F_2^m, F = F_2$，F_2 为二元域。
- 考虑求出这 n 个数的生成子空间的基：将所有数的二进制表示视为行向量，拼接得到一个矩阵，并求出这个矩阵的阶梯形即可。
- 在求出这 n 个数的生成子空间的基后，直接按位贪心即可。

P3812 【模板】线性基

- 注意到 $[0, 2^m)$ 的整数与异或运算构成了向量空间，其中 $V = F_2^m, F = F_2$，F_2 为二元域。
- 考虑求出这 n 个数的生成子空间的基：将所有数的二进制表示视为行向量，拼接得到一个矩阵，并求出这个矩阵的阶梯形即可。
- 在求出这 n 个数的生成子空间的基后，直接按位贪心即可。
- 时间复杂度 $O(\frac{nm^2}{w}) = O(nm)$，其中 $m = O(w)$。

行列式的定义

- 一个 n 阶方阵 $A = (\alpha_1 \dots \alpha_m)$ 的行列式 $\det A$ 或 $|A|$ 为使 $\det I = 1$ 的反对称 n 重线性函数。容易证明该定义下行列式唯一。

行列式的定义

- 一个 n 阶方阵 $A=(\alpha_1\dots\alpha_m)$ 的行列式 $\det A$ 或 $|A|$ 为使 $\det I=1$ 的反对称 n 重线性函数。容易证明该定义下行列式唯一。
- 定理：$\det A=\sum\limits_{p_1,\dots,p_n\in S_n}(-1)^{\tau(p_1,\dots,p_n)}\prod_{i=1}^n a_{i,p_i}$，其中 S_n 为所有 n 阶置换的集合，$\tau(p_1,\dots,p_n)$ 为 $p_1,\dots,p_n$ 的逆序对数。

行列式的定义

- 一个 n 阶方阵 $A=(\alpha_1\ldots\alpha_m)$ 的行列式 $\det A$ 或 $|A|$ 为使 $\det I=1$ 的反对称 n 重线性函数。容易证明该定义下行列式唯一。
- 定理：$\det A=\sum\limits_{p_1,\ldots,p_n\in S_n}(-1)^{\tau(p_1,\ldots,p_n)}\prod_{i=1}^n a_{i,p_i}$，其中 S_n 为所有 n 阶置换的集合，$\tau(p_1,\ldots,p_n)$ 为 $p_1,\ldots,p_n$ 的逆序对数。
- 定理：$\det A=\det {}^tA$。

求解行列式

- 命题：上三角 / 下三角矩阵的行列式为对角元之和。

求解行列式

- 命题：上三角 / 下三角矩阵的行列式为对角元之和。
- 根据行列式的定义，可以采用高斯消元的方法使原矩阵变为上三角形，时间复杂度为 $O(n^3)$。

求解行列式

- 命题：上三角 / 下三角矩阵的行列式为对角元之和。
- 根据行列式的定义，可以采用高斯消元的方法使原矩阵变为上三角形，时间复杂度为 $O(n^3)$。
- 命题：$\det A \neq 0 \Leftrightarrow \mathrm{A} = n$。

余子式与代数余子式

- 设 $A=\left(a_{i,j}\right)_{n\times n}$，则 $\forall 1\le i,j\le n$，将矩阵 A 去掉第 i 行和第 j 列后的矩阵的行列式称为 $a_{i,j}$ 元的余子式。

余子式与代数余子式

- 设 $A=\left(a_{i,j}\right)_{n\times n}$，则 $\forall 1\leq i,j\leq n$，将矩阵 A 去掉第 i 行和第 j 列后的矩阵的行列式称为 $a_{i,j}$ 元的余子式。
- 将 $a_{i,j}$ 元的余子式乘上 $(-1)^{i+j}$ 后的结果称为 $a_{i,j}$ 的代数余子式，记为 $A_{i,j}$。

余子式与代数余子式

- 设 $A=\left(a_{i,j}\right)_{n\times n}$，则 $\forall 1\leq i,j\leq n$，将矩阵 A 去掉第 i 行和第 j 列后的矩阵的行列式称为 $a_{i,j}$ 元的余子式。
- 将 $a_{i,j}$ 元的余子式乘上 $(-1)^{i+j}$ 后的结果称为 $a_{i,j}$ 的代数余子式，记为 $A_{i,j}$。
- 定理（一阶 Laplace 展开）：
  $\forall 1\leq i\leq n, \det A=\sum_{j=1}^{n} a_{i,j}A_{i,j}$。对列也成立。

一般的子式、余子式

- 对于 $1 \leq i_1 < \cdots < i_k \leq n, 1 \leq j_1 < \cdots < j_k \leq n$，将只保留 $i_1, \ldots, i_k$ 行和 $j_1, \ldots, j_k$ 列的元素的矩阵的行列式称为 $i_1, \ldots, i_k$ 行和 $j_1, \ldots, j_k$ 列的子式，记为 $A\begin{pmatrix} i_1, \ldots, i_k \\ j_1, \ldots, j_k \end{pmatrix}$。

一般的子式、余子式

- 对于 $1 \le i_1 < \cdots < i_k \le n, 1 \le j_1 < \cdots < j_k \le n$，将只保留 $i_1, \ldots, i_k$ 行和 $j_1, \ldots, j_k$ 列的元素的矩阵的行列式称为 $i_1, \ldots, i_k$ 行和 $j_1, \ldots, j_k$ 列的子式，记为 $A\begin{pmatrix} i_1, \ldots, i_k \\ j_1, \ldots, j_k \end{pmatrix}$。
- 设 $\{u_1, \ldots, u_{n-k}\} = \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}, \{v_1, \ldots, v_{n-k}\} = \{1, \ldots, n\} \setminus \{j_1, \ldots, j_k\}, 1 \le u_1 < \cdots < u_{n-k} \le n, 1 \le v_1 < \cdots < v_{n-k} \le n$，将子式 $A\begin{pmatrix} u_1, \ldots, u_{n-k} \\ v_1, \ldots, v_{n-k} \end{pmatrix}$ 称为 $i_1, \ldots, i_k$ 行和 $j_1, \ldots, j_k$ 列的余子式。

Laplace 展开

- 定理（Laplace 展开）：对于任意的 $1 \le i_1 < \cdots < i_k \le n, \{u_1, \dots, u_{n-k}\} = \{1, \dots, n\} \setminus \{i_1, \dots, i_k\}, 1 \le u_1 < \cdots < u_{n-k} \le n$， $\det A = \sum_{1 \le j_1 < \cdots < j_k \le n} A\begin{pmatrix} i_1, \dots, i_k \\ j_1, \dots, j_k \end{pmatrix} (-1)^{(i_1+\cdots+i_k)+(j_1+\cdots+j_k)} A\begin{pmatrix} u_1, \dots, u_{n-} \\ v_1, \dots, v_{n-} \end{pmatrix}$
  其中 $\{u_1, \dots, u_{n-k}\} = \{1, \dots, n\} \setminus \{i_1, \dots, i_k\}, \{v_1, \dots, v_{n-k}\} = \{1, \dots, n\} \setminus \{j_1, \dots, j_k\}, 1 \le u_1 < \cdots < u_{n-k} \le n, 1 \le v_1 < \cdots < v_{n-k} \le n$。对列也成立。

Laplace 展开

- 定理（Laplace 展开）：对于任意的 $1 \leq i_1 < \cdots < i_k \leq n, \{u_1, \ldots, u_{n-k}\} = \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}, 1 \leq u_1 < \cdots < u_{n-k} \leq n$，$\det A = \sum_{1 \leq j_1 < \cdots < j_k \leq n} A\begin{pmatrix} i_1, \ldots, i_k \\ j_1, \ldots, j_k \end{pmatrix} (-1)^{(i_1+\cdots+i_k)+(j_1+\cdots+j_k)} A\begin{pmatrix} u_1, \ldots, u_{n-} \\ v_1, \ldots, v_{n-} \end{pmatrix}$
  其中 $\{u_1, \ldots, u_{n-k}\} = \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}, \{v_1, \ldots, v_{n-k}\} = \{1, \ldots, n\} \setminus \{j_1, \ldots, j_k\}, 1 \leq u_1 < \cdots < u_{n-k} \leq n, 1 \leq v_1 < \cdots < v_{n-k} \leq n$。对列也成立。
- 推论：$\det\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \det\begin{pmatrix} A & 0 \\ D & B \end{pmatrix} = \det\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \det A \det B$。

Laplace 展开

- 定理（Laplace 展开）：对于任意的 $1 \leq i_1 < \cdots < i_k \leq n, \{u_1, \ldots, u_{n-k}\} = \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}, 1 \leq u_1 < \cdots < u_{n-k} \leq n$，$\det A = \sum_{1 \leq j_1 < \cdots < j_k \leq n} A\begin{pmatrix} i_1, \ldots, i_k \\ j_1, \ldots, j_k \end{pmatrix} (-1)^{(i_1+\cdots+i_k)+(j_1+\cdots+j_k)} A\begin{pmatrix} u_1, \ldots, u_{n-} \\ v_1, \ldots, v_{n-} \end{pmatrix}$
  其中 $\{u_1, \ldots, u_{n-k}\} = \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}, \{v_1, \ldots, v_{n-k}\} = \{1, \ldots, n\} \setminus \{j_1, \ldots, j_k\}, 1 \leq u_1 < \cdots < u_{n-k} \leq n, 1 \leq v_1 < \cdots < v_{n-k} \leq n$。对列也成立。
- 推论：
  $\det\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \det\begin{pmatrix} A & 0 \\ D & B \end{pmatrix} = \det\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \det A \det B$。
- 命题：对于方阵 A, B，都有 $\det(AB) = \det A \det B$。

可逆矩阵

- 称 n 阶方阵 A 可逆，当且仅当存在 n 阶方阵 A^{-1} 满足 $AA^{-1} = A^{-1}A = I$。

可逆矩阵

- 称 n 阶方阵 A 可逆，当且仅当存在 n 阶方阵 A^{-1} 满足 $AA^{-1}=A^{-1}A=I$。
- A 的伴随矩阵 $A^*=\begin{pmatrix} A_{1,1} & A_{2,1} & \cdots & A_{n,1} \\ A_{1,2} & A_{2,2} & \cdots & A_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1,n} & A_{2,n} & \cdots & A_{n,n} \end{pmatrix}$，容易发现 $AA*=A*A=(\det A)I$，所以 A 可逆 $\Leftrightarrow \det A\neq 0 \Leftrightarrow \mathrm{rank}A=n$，且若 A 可逆，$A^{-1}=\frac{1}{\det A}A^*$，直接求解时间复杂度 $O(n^4)$。

可逆矩阵

- 称 n 阶方阵 A 可逆，当且仅当存在 n 阶方阵 A^{-1} 满足 $AA^{-1}=A^{-1}A=I$。
- A 的伴随矩阵 $A^*=\begin{pmatrix} A_{1,1} & A_{2,1} & \cdots & A_{n,1} \\ A_{1,2} & A_{2,2} & \cdots & A_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1,n} & A_{2,n} & \cdots & A_{n,n} \end{pmatrix}$，容易发现 $AA* = A*A = (\det A)I$，所以 A 可逆 $\Leftrightarrow \det A \neq 0 \Leftrightarrow \mathrm{rank} A = n$，且若 A 可逆，$A^{-1}=\frac{1}{\det A}A^*$，直接求解时间复杂度 $O(n^4)$。
- 对于矩阵 $C=\begin{pmatrix} A & B \end{pmatrix}$，则通过初等行变换将 C 的左 n 列变为 I 后，C 的剩下的列为 $A^{-1}B$，令 $B=I$ 即可求出 A^{-1}，时间复杂度 $O(n^3)$。

正交空间

- 在 OI 中，我们一般考虑正定（或半正定）的正交空间，即度量为正定（或非退化半正定）对称双线性函数的度量空间，其中该函数称为内积，记为 (α, β)。

正交空间

- 在 OI 中，我们一般考虑正定（或半正定）的正交空间，即度量为正定（或非退化半正定）对称双线性函数的度量空间，其中该函数称为内积，记为 (α, β)。
- 标准内积的性质：

正交空间

- 在 OI 中，我们一般考虑正定（或半正定）的正交空间，即度量为正定（或非退化半正定）对称双线性函数的度量空间，其中该函数称为内积，记为 (α, β)。
- 标准内积的性质：
    1. 非退化：$\forall \alpha \in V, \exists \beta \in V, (\alpha, \beta) = ne0$。

正交空间

- 在 OI 中，我们一般考虑正定（或半正定）的正交空间，即度量为正定（或非退化半正定）对称双线性函数的度量空间，其中该函数称为内积，记为 (α, β)。
- 标准内积的性质：
  1. 非退化：$\forall \alpha \in V, \exists \beta \in V, (\alpha, \beta) = ne0$。
  2. 对称性：$(\alpha, \beta) = (\beta, \alpha)$。

正交空间

- 在 OI 中，我们一般考虑正定（或半正定）的正交空间，即度量为正定（或非退化半正定）对称双线性函数的度量空间，其中该函数称为内积，记为 (α, β)。
- 标准内积的性质：
  1. 非退化：$\forall \alpha \in V, \exists \beta \in V, (\alpha, \beta) = ne0$。
  2. 对称性：$(\alpha, \beta) = (\beta, \alpha)$。
  3. 双线性：$(k\alpha, \beta) = k(\alpha, \beta), (\alpha_1 + \alpha_2, \beta) = (\alpha_1, \beta) + (\alpha_2, \beta)$，对于第二个分量同理。

正交

- 对于向量 α, β，若 $(\alpha, \beta) = 0$，则称 α, β 正交，记为 $\alpha \perp \beta$。

正交

- 对于向量 α, β，若 $(\alpha, \beta) = 0$，则称 α, β 正交，记为 $\alpha \perp \beta$。
- 对于向量组 $\alpha_1, \ldots, \alpha_n$，若 $\forall 1 \leq i < j \leq n$，都有 $\alpha_i \perp \alpha_j$，则称 $\alpha_1, \ldots, \alpha_n$ 为正交向量组。若 $\alpha_1, \ldots, \alpha_n$ 为一组基，则称 $\alpha_1, \ldots, \alpha_n$ 为一组正交基。

正交

- 对于向量 α, β，若 $(\alpha, \beta) = 0$，则称 α, β 正交，记为 $\alpha \perp \beta$。
- 对于向量组 $\alpha_1, \dots, \alpha_n$，若 $\forall 1 \leq i < j \leq n$，都有 $\alpha_i \perp \alpha_j$，则称 $\alpha_1, \dots, \alpha_n$ 为正交向量组。若 $\alpha_1, \dots, \alpha_n$ 为一组基，则称 $\alpha_1, \dots, \alpha_n$ 为一组正交基。
- 对于向量 α 和子空间 $U \subset V$，若 $\forall \beta \in U$ 都有 $\alpha \perp \beta$，则称 $\alpha \perp U$。

正交

- 对于向量 α, β，若 $(\alpha, \beta) = 0$，则称 α, β 正交，记为 $\alpha \perp \beta$。
- 对于向量组 $\alpha_1, \dots, \alpha_n$，若 $\forall 1 \le i < j \le n$，都有 $\alpha_i \perp \alpha_j$，则称 $\alpha_1, \dots, \alpha_n$ 为正交向量组。若 $\alpha_1, \dots, \alpha_n$ 为一组基，则称 $\alpha_1, \dots, \alpha_n$ 为一组正交基。
- 对于向量 α 和子空间 $U \subset V$，若 $\forall \beta \in U$ 都有 $\alpha \perp \beta$，则称 $\alpha \perp U$。
- 对于子空间 $U \subseteq V$，定义 U 的正交补 $U^\perp = \{\alpha \mid \alpha \perp U\}$。

正交

- 对于向量 α, β，若 $(\alpha, \beta) = 0$，则称 α, β 正交，记为 $\alpha \perp \beta$。
- 对于向量组 $\alpha_1, \ldots, \alpha_n$，若 $\forall 1 \leq i < j \leq n$，都有 $\alpha_i \perp \alpha_j$，则称 $\alpha_1, \ldots, \alpha_n$ 为正交向量组。若 $\alpha_1, \ldots, \alpha_n$ 为一组基，则称 $\alpha_1, \ldots, \alpha_n$ 为一组正交基。
- 对于向量 α 和子空间 $U \subset V$，若 $\forall \beta \in U$ 都有 $\alpha \perp \beta$，则称 $\alpha \perp U$。
- 对于子空间 $U \subseteq V$，定义 U 的正交补 $U^{\perp} = \{\alpha \mid \alpha \perp U\}$。
- 命题：$\dim V = \dim U + \dim U^{\perp}, U^{\perp\perp} = U$。

正交

- 对于向量 α,β，若 $(\alpha,\beta)=0$，则称 α,β 正交，记为 $\alpha\perp\beta$。
- 对于向量组 $\alpha_1,\dots,\alpha_n$，若 $\forall 1\le i<j\le n$，都有 $\alpha_i\perp\alpha_j$，则称 $\alpha_1,\dots,\alpha_n$ 为正交向量组。若 $\alpha_1,\dots,\alpha_n$ 为一组基，则称 $\alpha_1,\dots,\alpha_n$ 为一组正交基。
- 对于向量 α 和子空间 $U\subset V$，若 $\forall\beta\in U$ 都有 $\alpha\perp\beta$，则称 $\alpha\perp U$。
- 对于子空间 $U\subseteq V$，定义 U 的正交补 $U^{\perp}=\{\alpha\mid\alpha\perp U\}$。
- 命题：$\mathrm{dim}V=\mathrm{dim}U+\mathrm{dim}U^{\perp},U^{\perp\perp}=U$。
- 命题：$U\cap W=(U^{\perp}+W^{\perp})^{\perp}$

施密特正交化

- 施密特正交化用于求出一组与给定向量组等价的正交向量组，设向量组为 $\alpha_1,\ldots,\alpha_n$，则
$$\begin{cases}\beta_1 &= \alpha_1\\ \beta_2 &= \alpha_2-\frac{(\alpha_2,\beta_1)}{(\beta_1,\beta_1)}\beta_1\\ &\vdots\\ \beta_n &= \alpha_n-\sum\limits_{i=1}\frac{(\alpha_n,\beta_i)}{(\beta_i,\beta_i)}\beta_i\end{cases},$$
可以证明 $\forall 1\leq i<j\leq n,\beta_i\perp\beta_j$。

施密特正交化

- 施密特正交化用于求出一组与给定向量组等价的正交向量组，设向量组为 $\alpha_1, \ldots, \alpha_n$，则 $\begin{cases} \beta_1 &= \alpha_1 \\ \beta_2 &= \alpha_2 - \frac{(\alpha_2, \beta_1)}{(\beta_1, \beta_1)} \beta_1 \\ & \vdots \\ \beta_n &= \alpha_n - \sum\limits_{i=1} \frac{(\alpha_n, \beta_i)}{(\beta_i, \beta_i)} \beta_i \end{cases}$，
  可以证明 $\forall 1 \le i < j \le n, \beta_i \perp \beta_j$。
- 推论：正交基总是存在。

标准正交基

- 由于内积为正定或半正定的，所以 $\forall \alpha \in V, (\alpha, \alpha) \geq 0$，定义 α 的长度 $|\alpha| = \sqrt{(\alpha, \alpha)}$。若 $|\alpha| = 1$，称 α 为单位向量。

标准正交基

- 由于内积为正定或半正定的，所以 $\forall \alpha \in V, (\alpha, \alpha) \geq 0$，定义 α 的长度 $|\alpha| = \sqrt{(\alpha, \alpha)}$。若 $|\alpha| = 1$，称 α 为单位向量。
- 若一组正交基 $\eta_1, \ldots, \eta_n$ 中的向量 η_i 均为单位向量，则称 $\eta_1, \ldots, \eta_n$ 为标准正交基。

标准正交基

- 由于内积为正定或半正定的，所以 $\forall\alpha \in V, (\alpha, \alpha) \geq 0$，定义 α 的长度 $|\alpha| = \sqrt{(\alpha, \alpha)}$。若 $|\alpha| = 1$，称 α 为单位向量。
- 若一组正交基 $\eta_1, \ldots, \eta_n$ 中的向量 η_i 均为单位向量，则称 $\eta_1, \ldots, \eta_n$ 为标准正交基。
- 以下结论均在标准正交基 $\eta_1, \ldots, \eta_n$ 的前提下。

标准正交基

- 由于内积为正定或半正定的，所以 $\forall \alpha \in V, (\alpha, \alpha) \geq 0$，定义 α 的长度 $|\alpha| = \sqrt{(\alpha, \alpha)}$。若 $|\alpha| = 1$，称 α 为单位向量。
- 若一组正交基 $\eta_1, \ldots, \eta_n$ 中的向量 η_i 均为单位向量，则称 $\eta_1, \ldots, \eta_n$ 为标准正交基。
- 以下结论均在标准正交基 $\eta_1, \ldots, \eta_n$ 的前提下。
- 命题：$\forall 1 \leq i, j \leq n, (\eta_i, \eta_j) = [i = j]$。

标准正交基

- 由于内积为正定或半正定的，所以 $\forall\alpha\in V,(\alpha,\alpha)\geq 0$，定义 α 的长度 $|\alpha|=\sqrt{(\alpha,\alpha)}$。若 $|\alpha|=1$，称 α 为单位向量。
- 若一组正交基 $\eta_1,\ldots,\eta_n$ 中的向量 η_i 均为单位向量，则称 $\eta_1,\ldots,\eta_n$ 为标准正交基。
- 以下结论均在标准正交基 $\eta_1,\ldots,\eta_n$ 的前提下。
- 命题：$\forall 1\leq i,j\leq n,(\eta_i,\eta_j)=[i=j]$。
- 定理（傅里叶展开）：$\forall\alpha\in V,\alpha=\sum_{i=1}^{n}(\alpha,\eta_i)\eta_i$。

标准正交基

- 由于内积为正定或半正定的，所以 $\forall \alpha \in V, (\alpha, \alpha) \geq 0$，定义 α 的长度 $|\alpha| = \sqrt{(\alpha, \alpha)}$。若 $|\alpha| = 1$，称 α 为单位向量。
- 若一组正交基 $\eta_1, \ldots, \eta_n$ 中的向量 η_i 均为单位向量，则称 $\eta_1, \ldots, \eta_n$ 为标准正交基。
- 以下结论均在标准正交基 $\eta_1, \ldots, \eta_n$ 的前提下。
- 命题：$\forall 1 \leq i, j \leq n, (\eta_i, \eta_j) = [i = j]$。
- 定理（傅里叶展开）：$\forall \alpha \in V, \alpha = \sum_{i=1}^{n} (\alpha, \eta_i)\eta_i$。
- 推论：对于向量 $\alpha, \beta \in V$，设在该基下 α 的坐标为 ${}^t\begin{pmatrix} a_1 & \ldots & a_n \end{pmatrix}$，$\beta$ 的坐标为 ${}^t\begin{pmatrix} b_1 & \ldots & b_n \end{pmatrix}$，那么 $(\alpha, \beta) = \sum_{i=1}^{n} a_i b_i$。

求解正交补

- 对于 V 的任一子空间 W，取 W 的基 $\alpha_1, \ldots, \alpha_m$ 和 V 的标准正交基 $\eta_1, \ldots, \eta_n$，设 β_i 为 α_i 在 $\eta_1, \ldots, \eta_n$ 下的坐标，令 $A = \begin{pmatrix} {}^t\beta_1 \\ \vdots \\ {}^t\beta_m \end{pmatrix}$，则 $W^\perp = \{\begin{pmatrix} \eta_1 & \ldots & \eta_n \end{pmatrix} \gamma \mid \gamma \in \ker A\}$。

求解正交补

- 对于 V 的任一子空间 W，取 W 的基 $\alpha_1, \dots, \alpha_m$ 和 V 的标准正交基 $\eta_1, \dots, \eta_n$，设 β_i 为 α_i 在 $\eta_1, \dots, \eta_n$ 下的坐标，令 $A = \begin{pmatrix} {}^t\beta_1 \\ \vdots \\ {}^t\beta_m \end{pmatrix}$，则 $W^\perp = \{\begin{pmatrix}\eta_1 & \dots & \eta_n\end{pmatrix}\gamma \mid \gamma \in \ker A\}$。
- 在 OI 中，$F = F_2, V = F_2^n$，V 的一组单位正交基为仅有第 i 个分量为 1 的向量，其中 $1 \le i \le n$，此时向量 α 在这组基下的坐标即为 α。

P4869 albus就是要第一个出场 题意

已知一个长度为 n 的正整数序列 A（下标从 1 开始），令 $S=\{x|1\leq x\leq n\}$，S 的幂集 2^S 定义为 S 所有子集构成的集合。定义映射 $f:2^S\rightarrow Z, f(\emptyset)=0, f(T)=\mathrm{XOR}\{A_t\},(t\in T)$。现在 albus 把 2^S 中每个集合的 f 值计算出来，从小到大排成一行，记为序列 B（下标从 1 开始）。
给定一个数，那么这个数在序列 B 中第 1 次出现时的下标是多少呢？
$n\leq 10^5, A_i, Q\leq 10^9$。

P4869 albus就是要第一个出场 题解

- 设 $A_1, \ldots, A_n$ 的秩为 r，则 B 中所有数的出现次数均为 2^{n-r}。

P4869 albus就是要第一个出场 题解

- 设 $A_1, \ldots, A_n$ 的秩为 r，则 B 中所有数的出现次数均为 2^{n-r}。
- 问题转化为 $< Q$ 的 $L(A_1, \ldots, A_n)$ 中数的个数，而这个是简单的。

CF1100F Ivan and Burgers 题意

给定长为 n 的序列 $a_1, \ldots, a_n$，有 q 次询问，每次给定 l, r，询问 $a_l, a_{l+1}, \ldots, a_r$ 的最大异或和。

$n, q \le 5 \times 10^5, V = \max\{a_i\} \le 10^6$。

CF1100F Ivan and Burgers 题解

- 可以线性基合并，时间复杂度 $O((n+q\log n)\log V)$。

CF1100F Ivan and Burgers 题解

- 可以线性基合并，时间复杂度 $O((n+q\log n)\log V)$。
- 从左到右维护线性基，在线性基内对于每个基维护这个基向量是什么时候加入的。

CF1100F Ivan and Burgers 题解

- 可以线性基合并，时间复杂度 $O((n+q\log n)\log V)$。
- 从左到右维护线性基，在线性基内对于每个基维护这个基向量是什么时候加入的。
- 在新加入一个数的时候，若在某个位为 1 且这个位对应的基加入时间早于当前数，则将这个数加入线性基并将这个基继续插入。

CF1100F Ivan and Burgers 题解

- 可以线性基合并，时间复杂度 $O((n+q\log n)\log V)$。
- 从左到右维护线性基，在线性基内对于每个基维护这个基向量是什么时候加入的。
- 在新加入一个数的时候，若在某个位为 1 且这个位对应的基加入时间早于当前数，则将这个数加入线性基并将这个基继续插入。
- 在查询时只保留 $\geq l$ 的数即可，时间复杂度 $O((n+q)\log V)$。

CF1336E2 Chiori and Doll Picking 题意

给定 $a_1, \ldots, a_n, 0 \le a_i < 2^m$。
定义一个子序列的权值为子序列中所有数的异或和在二进制表示中 1 的个数。
对于 $i = 0, 1, \ldots, m$，求出有多少子序列权值为 i，对 998244353 取模。

CF1336E2 Chiori and Doll Picking 题解

- 设 $V = L(a_1, \ldots, a_n)$。

CF1336E2 Chiori and Doll Picking 题解

- 设 $V = L(a_1, \ldots, a_n)$。
- 若 $\dim V \leq \frac{m}{2}$，则 $|V| \leq 2^{\frac{m}{2}}$，直接暴力枚举即可。

CF1336E2 Chiori and Doll Picking 题解

- 设 $V = L(a_1, \ldots, a_n)$。
- 若 $\dim V \le \frac{m}{2}$，则 $|V| \le 2^{\frac{m}{2}}$，直接暴力枚举即可。
- 若 $\dim V > \frac{m}{2}$，考虑求出 V 的正交补 $V^{\perp}$，其中内积 $(x, y) = \mathrm{popcount}(x \& y) \bmod 2$。此时 $\dim V^{\perp} \le \frac{m}{2}$。

CF1336E2 Chiori and Doll Picking 题解

- 设 $V = L(a_1, \dots, a_n)$。
- 若 $\dim V \le \frac{m}{2}$，则 $|V| \le 2^{\frac{m}{2}}$，直接暴力枚举即可。
- 若 $\dim V > \frac{m}{2}$，考虑求出 V 的正交补 $V^\perp$，其中内积 $(x, y) = \operatorname{popcount}(x \& y) \bmod 2$。此时 $\dim V^\perp \le \frac{m}{2}$。
- 引理：$[x \in V^\perp] = \frac{1}{|V|} \sum_{y \in V} (-1)^{(x,y)}$。

CF1336E2 Chiori and Doll Picking 题解

- 设 $V = L(a_1, \ldots, a_n)$。
- 若 $\dim V \le \frac{m}{2}$，则 $|V| \le 2^{\frac{m}{2}}$，直接暴力枚举即可。
- 若 $\dim V > \frac{m}{2}$，考虑求出 V 的正交补 $V^\perp$，其中内积 $(x, y) = \operatorname{popcount}(x \& y) \bmod 2$。此时 $\dim V^\perp \le \frac{m}{2}$。
- 引理：$[x \in V^\perp] = \frac{1}{|V|} \sum\limits_{y \in V} (-1)^{(x,y)}$。
- 而 $[x \in V] = [x \in V^{\perp\perp}] = \frac{1}{|V^\perp|} \sum\limits_{y \in V^\perp} (-1)^{(x,y)}$。

CF1336E2 Chiori and Doll Picking 题解

- 设 $V = L(a_1, \ldots, a_n)$。
- 若 $\dim V \le \frac{m}{2}$，则 $|V| \le 2^{\frac{m}{2}}$，直接暴力枚举即可。
- 若 $\dim V > \frac{m}{2}$，考虑求出 V 的正交补 $V^\perp$，其中内积 $(x, y) = \operatorname{popcount}(x \& y) \bmod 2$。此时 $\dim V^\perp \le \frac{m}{2}$。
- 引理：$[x \in V^\perp] = \frac{1}{|V|} \sum_{y \in V} (-1)^{(x,y)}$。
- 而 $[x \in V] = [x \in V^{\perp\perp}] = \frac{1}{|V^\perp|} \sum_{y \in V^\perp} (-1)^{(x,y)}$。
- 所以在求出了 $V^\perp$ 里每个数中 1 的数量即可求出 V 中含有 i 个 1 的数的个数了。

CF1336E2 Chiori and Doll Picking 题解

- 设 $V = L(a_1, \dots, a_n)$。
- 若 $\dim V \le \frac{m}{2}$，则 $|V| \le 2^{\frac{m}{2}}$，直接暴力枚举即可。
- 若 $\dim V > \frac{m}{2}$，考虑求出 V 的正交补 $V^{\perp}$，其中内积 $(x, y) = \mathrm{popcount}(x \& y) \bmod 2$。此时 $\dim V^{\perp} \le \frac{m}{2}$。
- 引理：$[x \in V^{\perp}] = \frac{1}{|V|} \sum\limits_{y \in V} (-1)^{(x,y)}$。
- 而 $[x \in V] = [x \in V^{\perp\perp}] = \frac{1}{|V^{\perp}|} \sum\limits_{y \in V^{\perp}} (-1)^{(x,y)}$。
- 所以在求出了 $V^{\perp}$ 里每个数中 1 的数量即可求出 V 中含有 i 个 1 的数的个数了。
- 总时间复杂度 $O(nm + 2^{\frac{m}{2}})$

习题

P4151 [WC2011] 最大XOR和路径
P3292 [SCOI2016] 幸运数字
CF1336E2 Chiori and Doll Picking (hard version)
https://uoj.ac/problem/698
https://qoj.ac/contest/1096/problem/5445