抽屉原理

第一种说法

将n个物品放入n-1个抽屉中，必然有一个抽屉中存在两个物品

一些题目

在边长为1的正方形中任取五点，则其中存在两点，他们的距离小于$\frac{\sqrt{2}}{2}$

从1到200的所有整数中任取k个数，则k个整数中至少有一对数，其中一个数整除另一个数，k最小是多少?

101，取完100个奇数

反问题：从1到200最多可以取多少个数，使得两两互不整除？100个数，101-200

抽屉原理的其他形式

将n个物品放入n个抽屉中，若没有抽屉包含两个及及以上物品，则每个抽屉中恰好有一个物品

中国剩余定理

考虑a，b互素的正整数，对于$\forall\ 0 \leq x \leq a-1$，$0 \leq y \leq b-1$，存在正整数S，使得

S = x mod a 且 S = y mod b，$S \in [1, ab]$ 共 ab 个数

引理

$a \mid n \quad, b \mid n, \quad (a,b)=1 \Rightarrow ab \mid n$

抽屉原理的一般形式

考虑 n 个实数 $a_1, a_2, ... a_n$, 设其平均值为$x = \dfrac{a_1 + a_2 + ... a_n}{n}$,则$a_1, ... a_n$ 中存在一个数a_i使得$a_i \geq x$

强形式

m个物品放入n个抽屉中，存在一个抽屉有至少$[\frac{m}{n}]$个物品

例子

大小圆盘分为200个小扇形，其中100个为红色，100个为蓝色，一定存在一个位置使得大小圆盘在至少一百个扇形区域同色

Erdos-Szekeres定理

n^2+1个实数$a_1,a_2,...a_{n^2+1}$ 构成的数列中必然有一个长为 n+1的递增子序列，或必然有一个长为n+1 的递减子序列

反问题：对于n^2 个数，是否可以构造一个数列使得其中没有长为n+1的递减或递增子序列

数论

裴蜀公式

$d = gcd(a, b), \quad \exists\, s, t \in Z, \quad sa + tb = d$

$\{sa + tb \mid \forall\, s, t \in \ Z\} = A$

$\forall\, n \in A, \quad d \mid n$

整除的相关性质

$\forall\, a, b, c, x, y \in Z$

1. $a \mid a$
2. $a \mid b,\ b \mid a \Rightarrow a = \pm b$
3. $a \mid b,\ b \mid c \Rightarrow a \mid c$
4. $a \mid b \Rightarrow a \mid bc$
5. $a \mid b, \quad a \mid c \Rightarrow a \mid xb + yc$
6. $a, b > 0,\ a \mid b \Rightarrow b \geq a$

   $$\stackrel{strogner}{\Longrightarrow} a = b \quad or \quad b \geq 2a$$

7. $\forall\, a, b > 0,\ a \mid b \Leftrightarrow ac \mid bc$

最大公约数的性质

1. 裴蜀定理
2. $a, b. c \in Z, \quad m \in N^+, \quad 有\ (ma, mb) = m(a, b)$

   特别的：1. $(a, b) = d \quad \Rightarrow \quad (\frac{a}{d}, \frac{b}{d}) = 1$

   2. $c \mid a, c \mid b \Rightarrow c \mid (a, b)$
3. $(a, c) = 1,\ (b, c) = 1 \Rightarrow (ab, c) = 1$
4. $(a, b) \Rightarrow (a, b + ac)$
5. $c \mid ab,\ (c, a) = 1 \Rightarrow c \mid b$
6. $a \mid c,\ b \mid c,\ (a, b) = 1 \Rightarrow ab \mid c$
7. 辗转相除

素数的相关性质

Def

一个正整数a是素数，$if \quad \forall b \in N^+, \quad b \mid a \Rightarrow b = 1 \quad or \quad b = a$

素数的性质

1. 素数是否有无穷多个?

1. $c \mid ab,\ (c,a)=1 \Rightarrow c \mid b$

   特别的，对于素数p，$p \mid ab \Rightarrow p \mid a \quad or \quad p \mid b$

3. 算术基本定理

算术基本定理

对于任何一个整数n，都可以唯一地分解为如下形式

$n = p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}$，其中$p_1,p_2,\dots p_k$为素数，$r_1r_2\dots r_k \in N^+$

同余的基本性质

一次同余方程

求解 $ax = b \pmod{m}$

$\Rightarrow (a,m) \mid b$

求解中国剩余定理

求出一个x，使得 $x = a_1 \pmod{m_1}$

$x = a_2 \pmod{m_2}$

$\dots$

$x = a_k \pmod{m_k}$

其中 $(m_i, m_j) = 1 \quad \forall\, i, j$ 均成立

欧拉定理与费马小定理

欧拉函数

$\varphi(n)$ ：$[1,n]$ 中与n互素的整数个数

如果$(a,n)=1 \Rightarrow \quad a^{\varphi(n)}=1 \pmod{n}$

计算欧拉函数

对于$n=p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}$

$$
\begin{aligned}
\text{有}\varphi(p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}) &= \varphi(p_1^{r_1})\,\varphi(p_2^{r_2})\dots\ \varphi(p_k^{r_k}) \\
&= p_1^{r_1-1}(p_1-1)\dots\ p_k^{r_k-1}(p_k-1) \\
&= p_1^{r_1}(1-\frac{1}{p_1})\dots p_k^{r_k}(1-\frac{1}{p_k})
\end{aligned}
$$

$$= n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k})$$

RSA

1. p,q两个素数，$n = pq$
2. 取e与$\varphi(n) = (p-1)(q-1)$ 互素

3. 计算$ed = 1 \pmod{\varphi(n)}$

加密：$P(M) = M^e \mod n$

解密：$S(C) = C^d \mod n$

群论

定义

对于非空集合G，$*$是G上的乘法运算，有

1. 封闭 $\forall\, a, b \in G, \quad a * b \in G$
2. 结合律 $\forall\, a, b, c \in G, \quad a * (b * c) = (a * b) * c$
3. 单位元 $\exists\, e \in G, \forall\, a \in G, \quad e * a = a * e = a$
4. 可逆 $\forall\, a \in G, \exists\, b \in G, \quad a * b = b * a$

则称<G,∗>为一个群

若满足1，2，则称<G,∗>为半群

若满足1，2，3，则称<G,∗>为带1半群

若在群G中，对$\forall\, a,b \in G$，有$a*b=b*a$，则称<G,∗>为**交换群**

例子

$<Z_m,+>$ (Z_m：模m的余数的集合）

性质

1. 消去律：$\forall\, a,b,c \in G \quad a*b=a*c \Rightarrow b=c$

$$b*a=c*a \Rightarrow b=c$$

2. 线性方程唯一解：$\forall\, a,b \in G, \exists\, a*x=b \Rightarrow x=a^{-1}b$
3. 单位元及逆元的唯一性
4. $(a^{-1})^{-1}=a \quad (a*b)^{-1}=b^{-1}*a^{-1}$

有限群的阶

在群$<G,*>$中，G是有限集合，则称群G是有限群，其阶数为$|G|$

结论(作业): 若群G的阶$\mid G\mid$为素数，则G是循环群，且生成元是除了1以外的每一个元素

元素的阶

在有限群$<G,*>$中，$a \in G, \exists\, n, \quad st.\, n$是满足 $a^n=e$的最小正整数，则称a是n阶的。

子群

定义

对于群$< G,* >$，若H是G的子集，且H本身是群，则有$< H,* >$是G的子群

陪集分解

$\forall$群 G，$\forall$子群$H \subseteq G, \exists\, a_1, a_2 \cdots \in G, \quad st.\ G = a_1H \cup a_2H \cup \ldots$，其中

$\forall\, i, j, \quad a_iH \cap a_jH = \emptyset$

推论1：当G为有限集时$\Rightarrow \dfrac{|G|}{|H|}$为整数

推论2：$if \quad a_1' \subseteq a_1H, \quad a_1' \neq a_1 \Rightarrow a_1'H = a_1H$

商群

对于任意**可交换群**G，G的任意子群H，有G\H={ eH，a_1H，$a_2H\dots$} 构成群，称作G模H的商群

补充 代表元$<e>,<a_1>\dots$

$\forall\, i,j,\quad <a_i>*<a_j>\rightarrow a_i*a_j\in a_kH$ 定义商群在

循环群

群G，$\forall\, a\in G$, 考虑由a生成的群$\{\dots a^{-2},\ a^{-1},e,a^1,a^2\dots\}\rightarrow\quad G_a$

G_a是G的子群（满足子群定义），称G_a是循环子群

若$G_a=G$，则称G是一个循环子群，并且称a是G的一个生成元

例子

对于$<Z_m,+>$:{ 0, 1, ... m-1} a为生成元$\Leftrightarrow\forall\, b\in Z_m,\quad st.\ b=ka\pmod m$

$$\forall\, b=ka\pmod m\Leftrightarrow(a,m)=b\Leftrightarrow(a,m)=1$$

所以**Z_m的生成元有$\varphi(m)$个**

tips

无限循环群的生成元只有a,a^{-1}

n阶有限循环群的生成元有$\varphi(n)$个

群同构

Def

对于$< G_1, *_1 >, < G_2, *_2 >$，$\exists$一一映射$f: \quad G_1 \to G_2$

$st. \ \forall a, b \in G_1, \quad f(a), f(b) \in G_2, \ f(a *_1 b) = f(a) *_2 f(b)$

则称群G_1, G_2是同构的

推论

1. 无限循环群同构于Z^+

2. 任意m阶有限循环群，同构于Z_m^+

3. 任何群G都同构于一个置换群

置换群

定义

n元集合S=[n]={1, 2, 3,.....,n} 到自身的一一对应构成的群叫做S上的n元对称群，其阶数为n！，

它的每个子群叫做S上的置换群

群作用与轨道公式

群作用的定义

任意群G，任意集合X，群G在集合X上的作用

$G * X \to X$　G为n元置换群，X为n元集合

满足的条件

1. $\forall\, g \in G, \forall\, x \in X \quad \Rightarrow g(x) \in X$
2. $\forall\, g_1, g_2 \in G,\ \forall\, x \in X \quad \Rightarrow (g_1 * g_2)(x) = g_1(g_2(x))$

固定子群

$\forall\, a \in X,\quad G_a = \{g \in G \mid g(a) = a\}$

G_a 是G的子群

轨道

$\forall\, a \in X,\quad O_a = \{g(a) \mid g \in G\}$

轨道公式

对于有限群G，在集合X上的作用，对于$\forall\, a \in X,\quad |G| = |G_a| \times |O_a|$

环

定义

在具有两个二元运算$+, \times$ 的集合R中，如果

1. <R, + >是交换群，+幺元，记作O_R
2. <R，×>是带1半群，×幺元，记住1_R
3. 分配律：$\forall\, a, b, c \in R$

　　有$(b + c) \times a = b \times a + c \times a \qquad a \times (b + c) = a \times b + a \times c$

则称$< R,+,\times >$为环

域

若同时满足乘法可交换，也即$< R\backslash 0_R >$构成交换群$\Rightarrow$ 域

环上性质

1. $0_R\times a = a\times 0_R = 0_R$
2. (-1) 是(1_R) 在加法下的逆，$\forall\, a\in R,\ (-1)\times a = -a$ (a 在加法下的逆)
3. $a\times(-b) = (-a)\times b = -(a\times b)$

整环

额外满足以下条件

1. 乘法可交换
2. $\forall\, a,b\in R,\quad a\times b = 0\Rightarrow a = 0\quad or\quad b = 0$

平凡环

对于$R=\{0_R\}$，称R为理想环，此时加法幺元等于乘法幺元等于0_R

其他的环均为非平凡环，必然有$0_R\neq 1_R$

tips

1. 环一定是整环
2. 整环不一定是域，但有限整环一定是域

理想

环R，对于集合$I,\emptyset\neq I\subseteq R$,满足

1. $\forall\, x,y\in I,\quad x-y\in I$
2. $\forall\, r\in R,\,\forall\, x\in I,\quad x\times r = r\times x\in I$

则称I是R的一个理想

例子: $<Z,+,\times>$中的所有偶数

$<Z,+,\times>$中所有k的倍数

性质: $<I,+>$是$<R,+>$的子群

tips：若I_1和I_2是环R的理想

$I_1+I_2=\{r_1+r_2\mid r_1\in I_1,\ r_2\in I_2\}$

$I_1\cdot I_2=\{\sum_{i=1}^{k}r_1\cdot r_2\mid r_1\in I_1,\ r_2\in I_2\,(1\leq i\leq k),\ k\in N^+\}$

其中$I_1\cap I_2,\ I_1+I_2,\ I_1\cdot I_2$ 均为R的理想

主理想

对于交换环R，任取一个元素a，$aR=\{a\times r\mid r\in R\}$是R的一个理想，并称其为主理想

tips 由单位生成的理想是R，有单位a，任意元素b生成的理想与$a\times b$生成的理想相同

主理想环

如果一个整环中的所有理想都是主理想，则称其为主理想整环，记为***PID***

例子: $<Z,+,\times>$是主理想环

proof：I中存在最小的非零正整数a，$a\in I$

ED(可以做带余除法的环) $\Rightarrow PID$

单位

对于含幺交换环R，$a\in R$被称作R中的单位，如果$a^{-1}\in R$

由单位生成的理想（主理想），一定是R。

素元

$p\in R$ 是素元（p不是单位），则有$\forall\, a,b\in R,\quad P|_R\, a\times b\Rightarrow p\,|_R\, a\quad or\quad p\,|_R\, b$

不可约元

$a\in R$ 是不可约元（a不是单位），则若 $\exists\, b,c,\quad st.\ a=b\times c$, 则b或c为单位

素理想

$for\, I,\quad \forall\, a,b\in R,\quad if\, a\times b\in I,\quad then\, a\in I\quad or\quad b\in I$

tips 由素元生成的理想是素理想

极大理想

I 是极大理想，如果$I\neq R$，且如果存在理想J，st. $I\subseteq J$，则$J=I\quad or\quad J=R$

tips 由不可约元生成的理想是极大理想

若I 是极大理想，则I 加上任何一个不在其中的元素生成的理想后是理想，且为R

一些结论

对于R为含幺交换整环，对于任意 a ∈ R 且 a ≠ 0，令 (a) 表示由 a 生成的理想。

a 是素元当且仅当 (a) 是素理想。

若 R 是主理想整环，则 a 是不可约元当且仅当 (a) 是极大理想。

若 R 是主理想整环，则 R 中的极大理想必是素理想，进而 R 中 的不可约元必是素元。

$Z(ED) \Rightarrow PID \Rightarrow UFD$(唯一分解)