数论简介、基本定理

整除*Divisibility*

整除定义

> $a|b$ if $b = ax$ for $a, b, x \subset z$ and $a \neq 0$

整除性质

> - $\forall n \subset N, n|0$
> - $a|b, b|c \to a|c$
>   例: $3|6, 6|36 \to 3|36$
> - $a|b, a|c \to a|bx + cy \; \forall x, y \subset z$
>   例: $7|14, 7|35 \to 7|(14 \times 3 + 35 \times 2 = 112)$

同余、中国剩余定理

同余

同余定义

> 如果a%m等于b%m，那么a、b关于m同余
>
> - m|(a-b)
> - a≡b(mod m)

同余性质

> - 如果a和b关于m同余，c和d关于m同余，那么有
> - $a + c \equiv b + d(mod\; m)$
> - $ac \equiv bd(mod\; m)$
>
> 证明是:
>
> > $a = b + mk$
> >
> > $c = d + ml$
> >
> > $a + c = b + d + m(k + l)$
> >
> > $ac = db + bml + dmk + m^2kl = bd + m(bl + dk + mkl)$
>
> - 类似的，如果a和b关于m同余（ $a \equiv b(mod\; m)$ ），那么有
> - $a^k \equiv b^k(mod\; m)$
>
> 但是**没有**:
>
> - if $a \equiv b(mod\; m)$ and $c \equiv d(mod\; m)$, then $a^c \equiv b^d$

> - if $ax \equiv bx(mod\ m)$, then $a \equiv b(mod\ m)$
>
> 例如：
>
> - $4^{12} \neq 4^{1}(mod\ 11)$
> - $8^{2} \neq 3^{7}(mod\ 5)$
> - $5 \times 2 \equiv 2 \times 2(mod\ 6)$

剩余系统

剩余系统定义

> - 模M的完全剩余系统 *Complete residue system mod*
>   - 由$a_1 a_2 \cdots a_m$组成
>   - 对任意的i和j（≥ 1 且 $\leq m$），如果$i \neq j$，那么$a_i \neq a_j(mod\ M)$
>   - 对任意的n，存在a_i使得$a_i \equiv n(mod\ M)$
>   - 例如9的一个剩余系统$\{1,2,3,4,5,6,7,8,9\}$
> - 模M的精简剩余系统 *Reduced residue system mod*
>   - 由$a_1 a_2 \cdots a_m$组成
>   - 对任意的i和j（≥ 1 且 $\leq m$），如果$i \neq j$，那么$a_i \neq a_j(mod\ M)$
>   - 对任意的i（≥ 1 且 $\leq m$），$gcd(a_i,\ M) = 1$
>   - 对任意的n，如果$gcd(n,\ M) = 1$，那么存在a_i使得$a_i \equiv n(mod\ M)$
>   - 例如9的一个精简剩余系统$\{1,2,4,5,7,8\}$

欧拉函数 *Euler's Totient Function*

> - $\phi(m)$表示m的精简剩余系统中元素的个数
>   例
>   - $\phi(9) = 6$
>   - $\phi(10) = 4$
> - 若p是素数，则
>   - $\phi(p) = p - 1$
>   - $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k(1-\frac{1}{p})$，$(k \geq 1)$

欧拉定理 *Euler's Theorm*

> - if $gcd(a,\ m) = 1$, then $a^{\phi(m)} \ \equiv\ 1\ mod\ m$.
>
>   例
>   - $3^{\phi(10)}\ =\ 81\ \equiv\ 1\ mod\ 10$

费马小定理 *Fermat's little Theorem*

> - if p is a **prime** and a is an **integer**, then $a^p\ \equiv\ a(mod\ p)$
>
>   证 Proof
>   - $\phi(p)\ =\ p\ -\ 1$
>
> $\cdots$
>
>   例
>   - $3^5\ \equiv\ 3\ mod\ 5$
>   - $2^{11}\ \equiv\ 2\ mod\ 11$

模逆元 *Inverse of elements mod*

> - if $gcd(a,\ m)\ =\ 1$, then there is a unique integer b mod m such that $ab\ \equiv\ 1\ mod\ m$. The b is denoted as $\frac{1}{a}$ or a^{-1} mod m.
>
>   注意不要写成小数形式
>
>   例
>   - $\frac{1}{5}\ mod\ 7\ =\ 5^{-1}\ mod\ 7\ =\ 3.$

威尔逊定理 *Wilson's Theorem*

> - if p is a prime then $(p\ -\ 1)!\ \equiv\ -1\ mod\ p$
>
>   例
>   - $4\,!\ =\ 24\ \equiv\ -1\ mod\ 5$

同余方程 *Congruence equation*

> - 定义
>   - A **congruence equation** is of the form $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \equiv 0\ mod\ m$ where $\{a_n, a_{n-1}, \cdots, a_0\}$ are integers.
>
>   Solution of the congruence equation are integers or residue classes mod m that satisfy the equation.
> - 例
>   - $x^2 \equiv -1\ mod\ 13$. Answer is $\{5,8\}$.
>   - $x^2 \equiv 1\ mod\ 15$. Answer is $\{\pm 1, \pm 4\ mod\ 15\}$.

线性同余方程 *Linear Congruence Equation*

- 定义

  同余方程程度为1。（ $ax \equiv b \; mod \; m$ ）
- 性质

  让$g = gcd(a, m)$，则$ax \equiv b \; mod \; m$当且仅当 $g|b$。如果上式有解，则mod m下正好有g个解。
- 例
  - $4x \equiv 5 \; mod \; 10$没有解，因为$g = gcd(4, 10) \nmid 5$
  - $4x \equiv 6 \; mod \; 10$有解$x = 4$，事实上，它有$g = 2$个解。另一个解是$x = 9$

欧几里得拓展算法

> 求$a^{-1} \mod n$ when $\gcd(a, n) = 1$.
> 见Chapter02-P31

中国剩余定理

> 求符合条件的x使得$x \equiv a_i \mod m_i$ for all i.
> 见Chapter02-P36

勒让德符号

- $(\frac{a}{p}) = \begin{cases} 0 & a \equiv 0(mod \; p) \\ 1 & a \not\equiv 0(mod \; p)且存在某个整数x使得x^2 \equiv a(mod \; p) \\ -1 & 不存在整数x使得x^2 \equiv a(mod \; p) \end{cases}$
- $(a|p)(b|p) = (ab|p)$

平方剩余及它们的关系

- **平方剩余**：假设p是素数，a是整数。若存在一个整数x使得$x^2 \equiv a(mod \; p)$，则称a在p的剩余类中是平方剩余的。
- **欧拉定理**说：如果p是奇素数，则a平方剩余当且仅当$a^{\frac{p-1}{2}} \equiv 1(mod \; p)$
  在$\{1, 2, \cdots, p-1\}$中恰好有$\frac{p-1}{2}$个数是平方剩余的。
- **勒让德符号**：如果a是平方剩余的，那么$(a|p) = 1$
- 高斯的**二次互反律**告诉我们：假设p和q是2个不同的奇素数，则$(q|p)(p|q) = (-1)^{\frac{(p-1)(q-1)}{4}}$
  另一种表述是：$(\frac{p}{q}) = \begin{cases} +(\frac{q}{p}) & if \; p \equiv 1 \; mod \; 4 \; or \; q \equiv 1 \; mod \; 4 \\ -(\frac{q}{p}) & if \; p \equiv q \equiv 3 \; mod \; 4 \end{cases}$

排列与阶乘

阶乘

> $0! = 1$
>
> $n! \sim \sqrt{2\pi n}(\frac{n}{e})^n$

排列组合

- The num of k-element multisets whose elements all belong to [n] is $\begin{pmatrix} n+k-1 \\ k \end{pmatrix}$
- Theorem: Let $n > 0$, $\sum_{k=0}^{n}(-1)^k \begin{pmatrix} n \\ k \end{pmatrix} = 0$.

  Proof: $(1-1)^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} 1^{n-k}(-1)^k$.
- Theorem: $\sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} = 2^k$.

  Proof: $(1+1)^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} 1^{n-k}1^k$.
- 递推公式(*Recursive formula*): $\begin{pmatrix} n \\ k \end{pmatrix} = \begin{pmatrix} n-1 \\ k-1 \end{pmatrix} + \begin{pmatrix} n-1 \\ k \end{pmatrix}$ for all integers n, k: $1 \le k \le n-1$, with initial values $\begin{pmatrix} n \\ 0 \end{pmatrix} = \begin{pmatrix} n \\ n \end{pmatrix} = 1$ for all integers $n \ge 0$.
- $\sum_{m=k}^{n} \begin{pmatrix} m \\ k \end{pmatrix} = \begin{pmatrix} n+1 \\ k+1 \end{pmatrix}$
- $\sum_{k=0}^{n} k \begin{pmatrix} n \\ k \end{pmatrix} = n2^{n-1}$: n个人里选1个总统，其他人的身份是委员会或公民。
  左边：先从n人里选出k个人组成委员会，再从委员会里选取一个当总统。
  右边：先从n人里选一个总统，剩下的人里每个人可以是委员会也可以是公民。
- $\sum\limits_{j=0}^{k} \begin{pmatrix} m \\ j \end{pmatrix} \begin{pmatrix} n-m \\ k-j \end{pmatrix} = \begin{pmatrix} n \\ k \end{pmatrix}$.
- 多项式系数：$\begin{pmatrix} n \\ a_1, a_2, \cdots, a_k \end{pmatrix} = \frac{n!}{a_1!a_2!\cdots a_k!}$ where $\sum\limits_{i=1}^{k} a_i = n$.
  $\sum\limits_{a_1+a_2+\cdots+a_k=n} \begin{pmatrix} n \\ a_1, a_2, \cdots, a_k \end{pmatrix} \prod\limits_{1 \le i \le k} x_i^{a_i}$

划分

组成

- *k-composition*: The number of compositions of n into exactly k parts is given by the binomial coefficient $\begin{pmatrix} n-1 \\ k-1 \end{pmatrix}$.

  Example $n = 5, k = 3$,

$3+1+1, 2+2+1, 2+1+2, 1+3+1, 1+2+2, 1+1+3$
$\binom{5-1}{3-1} = \binom{4}{2} = 6.$
Proof: 插空法5个糖有4个空，分3份需要切2刀，所以C_4^2。

- A ***weak composition*** of an integer n is similar to a composition of n, but allowing terms of the sequence to be zero: it is a way of writing n as the sum of a sequence of non-vegative integers（可为0）. $\binom{n+k-1}{k-1}$
  Proof: Wach k-composition of $n+k$ corresponds to a weak compositions of n by the rule
  $[a+b+\cdots+c=n+k] \iff [(a-1)+(b-1)+\cdots+(c-1)=n]$
- Each positive integer n has 2^{n-1} distinct compositions.
  Proof: $ans = \sum_{k=1}^{n}\binom{n-1}{k-1} = \sum_{k=0}^{n-1}\binom{n-1}{k} = 2^{n-1}.$

集合划分

- **集合划分**: 斯大林数$S(n,k)$表示将n个数划分成k个集合。`if(n==k||k==1)return 1;else return S(n-1,k-1)+k*S(n-1,k)` 最大的元素独自一个集合其他$n-1$个元素$k-1$个集合 + 其他$n-1$个元素k个集合且最大元素选一个集合加入其中。
- The number of all ***surjective functions***(满射函数) $f:[n]\to[k]$ is $k!\cdot S(n,k)$
- The ***Bell number*** B_n is the bumber of partitions of a set of size n.
  $B_n = \sum_{k=0}^{n} S(n,k)$
  for example, $B_3=5$. $B_1=1$. We define $B_0=0$.
  Bell numbers satisfy the recursion $B_{n+1} = \sum_{i=0}^{n}\binom{n}{i}B_i$.

整数划分

- **整数划分**：把一个正整数n划分成一些正整数$(a_1,a_2,\cdots,a_k)$的和，其中满足$\sum_{i=1}^{k} a_i = n, a_1 \ge a_2 \ge \cdots \ge a_k$。
  Example: $n=5$,
  $5, 4+1, 3+2, 3+1+1, 2+2+1, 2+1+1+1, 1+1+1+1+1$
  记为$p(n)$，其中划分成k份的记为$p_k(n)$。$p(5)=7, p_2(5)=2$
  No closed formula, but an asymptotic expression: $p(n) \sim \frac{1}{4n\sqrt{3}}\exp(\pi\sqrt{\frac{2n}{3}})$ as $n\to\infty$.
- **费勒斯图** ***Ferrers diagram***: 可以把14的一个划分$6+4+3+1$表示成:
  ⊡⊡⊡⊡⊡⊡
  ⊡⊡⊡⊡
  ⊡⊡⊡
  ⊡

  共轭费勒斯图就是这个图关于它的主对角线对称的图。如$4+3+3+2+1+1$
  ⊡⊡⊡⊡
  ⊡⊡⊡
  ⊡⊡⊡
  ⊡⊡
  ⊡
  ⊡
  就是$6+4+3+1$的共轭费勒斯图。

  若自己跟自己共轭则为**自共轭费勒斯图**。
  把一个整数全部分成奇数因子相加的方案数，等于它自共轭费勒斯图的个数。
- 设$a=(a_1,a_2,\cdots,a_k)$是整数n的一个划分，m_i是a中值为a_i的数的个数，那么the number of **set partitions** of [n] that are of **type** a is equal to $P_a = \frac{\binom{n}{a_1,a_2,\cdots,a_k}}{\prod_{i\ge1} m_i!}$。例如$(3,2,2,2,1)$中值为2的数的个数是3(有3个2)。

对比

- **组成***composition*就是相同巧克力分不同的人(插空法)，能有两个人具有相同数量的巧克力。
- **集合划分**是不同的人登相同的火箭(斯大林数)，你也可以理解为不同的巧克力分给相同的克隆人(不同的巧克力多)。
- **整数划分**则是相同的巧克力分给相同的克隆人，或者说相同的克隆人登相同的飞船也行。

生成函数

普通生成函数

- The **ordinary generating function** of a sequence a_n is $G(a_n,x)=\sum_{n=0}^{\infty} a_n x^n$.
  Example: $a_0=50, a_{n+1}=4a_n-100$.
  令 $G(x)=\sum_{n=0}^{\infty} a_n x^n$.
  因为 $\sum_{n=0}^{\infty} a_{n+1}x^{n+1} = \sum_{n=0}^{\infty} 4a_n x^{n+1} - \sum_{n=0}^{\infty} 100x^{n+1}$
  而 $x\in(-1,1)$时(x^n是收敛的)有$\sum_{n=0}^{\infty} x^n = \frac{x}{1-x}$
  所以 $G(x)-a_0 = 4xG(x) - \frac{100x}{1-x}$
  所以 $G(x) = \frac{a_0}{1-4x} - \frac{100x}{(1-x)(1-4x)}$
  同时 $\frac{a_0}{1-4x} = 50\sum_{n=0}^{\infty}(4x)^n = 50\sum_{n=0}^{\infty}4^n x^n$, $\frac{100x}{(1-x)(1-4x)} = \frac{100}{3}(\frac{1}{1-4x}-\frac{1}{1-x}) = \frac{100}{3}(\sum_{n=0}^{\infty}4^n x^n - \sum_{n=0}^{\infty}x^n)$
  所以 $G(x) = 50\sum_{n=0}^{\infty}4^n x^n - \frac{100}{3}(\sum_{n=0}^{\infty}4^n x^n - \sum_{n=0}^{\infty}x^n) = \sum_{n=0}^{\infty}(50\cdot 4^n - 100\cdot\frac{4^n-1}{3})x^n$
  又因为 $G(x)=\sum_{n=0}^{\infty} a_n x^n$
  所以 $a_n = 50\cdot 4^n - 100\cdot\frac{4^n-1}{3}$

斐波那契数列

- Fibonacci numbers $F_n = F_{n-1}+Fn-2$，初始条件$F_1=1, F_2=1$。
- 普通生成函数
  $G(x)=\sum_{k=0}^{\infty}F_k x^k = F_0 + F_1x + \sum_{k=2}^{\infty}(F_{k-1}+F_{k-2})x^k = x + \sum_{k=2}^{\infty}F_{k-1}x^k + \sum_{k=2}^{\infty}F_{k-2}x^k = x + x\sum_{k=0}^{\infty}F_kx^k + x^2\sum_{k=0}^{\infty}F_kx^k = x + xG($

  所以$G(x)=\frac{x}{1-x-x^2}$
- 一些性质
  - $F_1+F_2+\cdots+F_n = F_{n+2}-F_2 = F_{n+2}-1$
  - $F_1+F_3+F_5+\cdots+F_{2n-1} = F_{2n}$

> - $F_2 + F_4 + F_6 + \cdots + F_{2n} = F_{2n+1} - 1$
> - $F_1 - F_2 + F_3 - F_4 + \cdots + (-1)^{n+1} F_n = (-1)^{n+1} F_{n+1} + 1$
> - $F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}$

指数生成函数

> - exponential generating function of a sequence a_n is $E(a_n, x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$