丁尧尧

一元一次同余 方程

二元一次不定 方程

欧拉定理

中国剩余定理

容斥原理

各种组合数求

数学第一讲 基础回顾

丁尧尧

上海交通大学

July 27, 2017

目录

数学第一讲

丁尧尧

一元一次同分 方程

二元一次不足 方程

.az —

中国剩余定理

中国利尔尼廷 Lucas 空珊

快速幂

容斥原理

卡特兰数

各种组合数求 法

- 1 一元一次同余方程
- 2 二元一次不定方程
- 3 欧拉定理
- 4 逆元
- 5 中国剩余定理
- 6 Lucas 定理
- 7 快速幂
- 8 容斥原理
- 9 卡特兰数
- 10 各种组合数求法

丁尧尧

一元一次同余 方程

二元一次不定 方程

吸拉中畑

EVITACIE

中国剩汞正均

Lucas 走理

快速署

谷下原理

夕轴织**今**粉寸

各种组合数求 法

考虑如何解形如

 $ax \equiv b \pmod{m}$

的同余式.

丁尧尧

一元一次同余 方程

二元一次不定 方程

欧拉定理

4/ 17 /C /Z

型兀

中国剩余定理

Lucas 定理

快速幂

容斥原理

上柱兰粉

各种组合数求

考虑如何解形如

 $ax \equiv b \pmod{m}$

的同余式. 分类讨论:

容斥原理

F 4+ 34 40

各种组合数据

考虑如何解形如

 $ax \equiv b \pmod{m}$

的同余式 分类讨论:

1 gcd(a, m) = 1,此时在模 m 意义下存在 a 的逆元,直接左右两边同乘逆元即可解出同余方程。

欧拉定理

以江石石

古园利春ウ

Lucae 🗢 🎟

....

容斥原理

卡特兰数

各种组合数据

考虑如何解形如

$$ax \equiv b \pmod{m}$$

的同余式 分类讨论:

- 1 gcd(a, m) = 1,此时在模 m 意义下存在 a 的逆元,直接 左右两边同乘逆元即可解出同余方程.
- 2 $gcd(a, m) = d \neq 1$, 此时还需要分类.

欧拉定理

以江石石

由国剩全定理

中国判示正理

Material Control

容斥原理

卡特兰数

各种组合数数法

考虑如何解形如

$$ax \equiv b \pmod{m}$$

的同余式 分类讨论:

- 1 gcd(a, m) = 1,此时在模 m 意义下存在 a 的逆元,直接 左右两边同乘逆元即可解出同余方程.
- $gcd(a,m)=d\neq 1$, 此时还需要分类.
 - **1** *d* ∤ *b* , 此时无解

卡特兰数

各种组合数求 法

考虑如何解形如

$$ax \equiv b \pmod{m}$$

的同余式. 分类讨论:

- 1 gcd(a, m) = 1,此时在模 m 意义下存在 a 的逆元,直接 左右两边同乘逆元即可解出同余方程.
- $gcd(a,m)=d\neq 1$, 此时还需要分类.
 - **1** *d*∤*b*, 此时无解
 - 2 $d \mid b$, 此时将 a, b, m 同时除以 d, 化成上面的情况

丁尧尧

一元一次同分 方程

二元一次不定 方程

欧拉定理

71,2,2

中国剩余定理

空 反 百 理

各种组合数求

考虑如何解形如

ax + by = c

的不定方程.

丁尧尧

一元一次同分 方程

二元一次不定 方程

砂拉宁珊

EV JT VE F

山田利全空期

1 ------

ウム医性

ロノトルハメエ

各种组合数求

考虑如何解形如

$$ax + by = c$$

的不定方程. 还是分类讨论 (不妨设 gcd(a,b)=d):

欧拉定理

中国剩余定**1**

....

容斥原理

F 1 + 1/ 1/1

各种组合数求

考虑如何解形如

$$ax + by = c$$

的不定方程. 还是分类讨论 (不妨设 gcd(a,b)=d)):

1 d∤c, 无解

各种组合数求 法

考虑如何解形如

$$ax + by = c$$

的不定方程. 还是分类讨论 (不妨设 gcd(a, b) = d):

- **1** *d* ∤ *c* , 无解
- 2 $d \mid c$, 用扩展欧几里得算出 x_0, y_0 满足 $ax_0 + by_0 = d$, 然后有 $x = x_0 \frac{c}{d} + k \frac{b}{d}$, 其中 $k \in \mathbb{Z}$. 对于任何一个解 x, 直接可以用原式得出 y 的值.

容斥原理 卡特兰数

各种组合数数 法

考虑如何解形如

$$ax + by = c$$

的不定方程. 还是分类讨论 (不妨设 gcd(a,b)=d):

- 1 d∤c, 无解
- ② $d \mid c$, 用扩展欧几里得算出 x_0, y_0 满足 $ax_0 + by_0 = d$, 然后有 $x = x_0 \frac{c}{d} + k \frac{b}{d}$, 其中 $k \in \mathbb{Z}$. 对于任何一个解 x, 直接可以用原式得出 y 的值.

本质上二元一次不定方程和一元一次同余方程是一个东西. 两个可以等价转化.

丁尧尧

一元一次同分 方程

二元一次不定 方程

欧拉定理

逆元

中国剩余定理

Lucas 定埋

容斥原理

上性兰粉

各种组合数求

欧拉函数定义:

$$\varphi(n) = |\{i \in [1, n] \mid gcd(i, n) = 1\}|$$

即 [1, n] 中与 n 互质的数的个数(同时也是模 n 的缩系的大小).

欧拉定理

欧拉函数定义:

$$\varphi(n) = \mid \{i \in [1, n] \mid \gcd(i, n) = 1\} \mid$$

即 [1, n] 中与 n 互质的数的个数(同时也是模 n 的缩系的大 小).

欧拉函数的一些性质:

- $\varphi(nm) = \varphi(n)\varphi(m) \quad (gcd(m,n)=1)$ 积性函数
- $\varphi(n) = n \prod_{p|n} (1 \frac{1}{p})$ 用于手算
- $n = \sum_{d|n} \varphi(d)$

丁尧尧

一元一次同余 方程

二元一次不定 方程

欧拉定理

-X 17 VC >-

市団利全中班

Lucae 中珊

At the second

☆ 長 西 珊

各种组合数求

欧拉定理:

if gcd(a, n) = 1, then $a^{\varphi(n)} \equiv 1 \pmod{n}$

欧拉定理

中国剩余定理

....

交 丘 百 珥

各种组合数据

欧拉定理:

if gcd(a, n) = 1, then $a^{\varphi(n)} \equiv 1 \pmod{n}$

这个定理一般用来求逆元或对指数取模。

欧拉定理:

if
$$gcd(a, n) = 1$$
, then $a^{\varphi(n)} \equiv 1 \pmod{n}$

这个定理一般用来求逆元或对指数取模

if
$$q \ge \varphi(n)$$
, then $a^q \equiv a^{q \mod \varphi(n) + \varphi(n)} \pmod{n}$

不需要 a 与 n 互质了.

一元一次同余 方程

二元一次不定 方程

欧拉定理

逆元

中国剩余定理

Lucas 定理

容斥原理

H / 1 ////---

各种组合数求

在模 m 意义下,如果 gcd(a, m) = 1,那么存在数 b,使得:

$$ab \equiv 1 (mod \ m)$$

并且 b 在模意义下是唯一的. 我们称 b 为 a 在模 m 的逆元, 一般记作 a^{-1} .

各种组合数数法

在模 m 意义下,如果 gcd(a, m) = 1,那么存在数 b,使得:

$$ab \equiv 1 \pmod{m}$$

并且 b 在模意义下是唯一的. 我们称 b 为 a 在模 m 的逆元, 一般记作 a^{-1} . 一般而言, 求逆元有两种方式:

1 由欧拉定理, 在 gcd(a, m) = 1 时, 有 $a^{\varphi(m)-1}a \equiv 1 \pmod{m}$, 于是 $a^{\varphi(m)-1}$ 就是 a 的逆元.

容斥原理 卡特兰数

各种组合数求 法 在模 m 意义下,如果 gcd(a, m) = 1,那么存在数 b,使得:

$$ab \equiv 1 \pmod{m}$$

并且 b 在模意义下是唯一的. 我们称 b 为 a 在模 m 的逆元, 一般记作 a^{-1} . 一般而言, 求逆元有两种方式:

- 1 由欧拉定理, 在 gcd(a,m)=1 时, 有 $a^{\varphi(m)-1}a\equiv 1 \pmod{m}$, 于是 $a^{\varphi(m)-1}$ 就是 a 的逆元.
- ② 在 gcd(a, m) = 1 时, 可由扩展欧几里得求出 x_0, y_0 使得 $ax_0 + my_0 = 1$, 于是 $ax_0 \equiv 1 \pmod{m}$, 所以 x_0 就是逆元.

谷下原均

各种组合数才法

对于同余方程组:

$$x \equiv a_i \pmod{m_i}$$

其中 m_i 两两互素.

设 $M = \prod m_i$, $M_i = \frac{M}{m_i}$, $R_i = M_i^{-1}$ (在模 m_i 的意义下) 于是可以得到下面的解:

$$x \equiv \sum a_i M_i R_i \pmod{M}$$

砂拉字皿

人拉走理

124 —

中国剩余定理

快速幂

.

各种组合数求

上面只能处理 m_i 两两互素的情况,下面介绍一种不要求两两互素的方法。 考虑两两合并。 有下面两个方程:

$$x \equiv a_1 \pmod{m_1}$$

 $x \equiv a_2 \pmod{m_2}$

欧拉定理

中国剩余定理

Lucas 定理

....

容斥原理

卡特兰数

各种组合数数 法 设

$$x = a_1 + k_1 m_1 = a_2 + k_2 m_2$$

右边是一个关于 k_1, k_2 的不定方程, 只要我们找到一组解, 那么就找到原方程的一个解.

$$k_1 m_1 - k_2 m_2 = a_2 - a_1$$

卡特兰数

各种组合数数 法 设

$$x = a_1 + k_1 m_1 = a_2 + k_2 m_2$$

右边是一个关于 k_1, k_2 的不定方程, 只要我们找到一组解, 那么就找到原方程的一个解.

$$k_1 m_1 - k_2 m_2 = a_2 - a_1$$

设 $d = gcd(m_1, m_2)$,

1 $d \nmid a_2 - a_1$, 原方程无解

各种组合数求

设

$$x = a_1 + k_1 m_1 = a_2 + k_2 m_2$$

右边是一个关于 k_1, k_2 的不定方程, 只要我们找到一组解, 那么就找到原方程的一个解.

$$k_1 m_1 - k_2 m_2 = a_2 - a_1$$

设 $d = gcd(m_1, m_2)$,

- **1** $d \nmid a_2 a_1$, 原方程无解
- ② $d \mid a_2 a_1$, 则由扩展欧几里得存在 k_{10}, k_{20} 满足 $k_{10}m_1 k_{20}m_2 = d$,

各种组合数法

设

$$x = a_1 + k_1 m_1 = a_2 + k_2 m_2$$

右边是一个关于 k_1, k_2 的不定方程, 只要我们找到一组解, 那么就找到原方程的一个解.

$$k_1 m_1 - k_2 m_2 = a_2 - a_1$$

设 $d = gcd(m_1, m_2)$,

- **1** $d \nmid a_2 a_1$, 原方程无解
- ② $d \mid a_2 a_1$,则由扩展欧几里得存在 k_{10}, k_{20} 满足 $k_{10}m_1 k_{20}m_2 = d$,于是: $k_1 = k_{10} \frac{a_2 a_1}{d} + t \frac{m_2}{acd(m_1, m_2)}$.

欧 拉 定 埋 逆 元

中国剩余定理

Lucas 定理

快速器 空戶原理

卡特兰数

各种组合数数 法 设

$$x = a_1 + k_1 m_1 = a_2 + k_2 m_2$$

右边是一个关于 k_1, k_2 的不定方程, 只要我们找到一组解, 那么就找到原方程的一个解.

$$k_1 m_1 - k_2 m_2 = a_2 - a_1$$

设 $d = gcd(m_1, m_2)$,

- **1** $d \nmid a_2 a_1$, 原方程无解
- 2 $d \mid a_2 a_1$, 则由扩展欧几里得存在 k_{10} , k_{20} 满足 $k_{10}m_1 k_{20}m_2 = d$, 于是: $k_1 = k_{10}\frac{a_2 a_1}{d} + t\frac{m_2}{\gcd(m_1, m_2)}$. 于是: $x = a_1 + (k_{10}\frac{a_2 a_1}{d} + t\frac{m_2}{\gcd(m_1, m_2)})m_1$

各种组合数据法

设

$$x = a_1 + k_1 m_1 = a_2 + k_2 m_2$$

右边是一个关于 k_1, k_2 的不定方程, 只要我们找到一组解, 那么就找到原方程的一个解.

$$k_1 m_1 - k_2 m_2 = a_2 - a_1$$

设 $d = gcd(m_1, m_2)$,

- **1** $d \nmid a_2 a_1$, 原方程无解
- ② $d \mid a_2 a_1$, 则由扩展欧几里得存在 k_{10}, k_{20} 满足 $k_{10}m_1 k_{20}m_2 = d$, 于是: $k_1 = k_{10}\frac{a_2 a_1}{d} + t\frac{m_2}{gcd(m_1, m_2)}$. 于是: $x = a_1 + (k_{10}\frac{a_2 a_1}{d} + t\frac{m_2}{gcd(m_1, m_2)})m_1$

 $x = a_1 + k_{10} \frac{a_2 - a_1}{d} m_1 + lcm(m_1, m_2)t$

各种组合数求

上面的最后一个式子等价于:

$$x \equiv a_1 + k_{10} \frac{a_2 - a_1}{d} m_1 \pmod{lcm(m_1, m_2)}$$

我们于是成功把两个式子合并成一个,这两两两合并下去就可以得到解了.

欧拉定理

中国剩余定理

Lucas 定理

快速幂

各种组合数求

卢卡斯定理:

$$\binom{n}{m} \equiv \binom{n/p}{m/p} \binom{n \ mod \ p}{m \ mod \ p} \pmod{p}$$

其中, 如果出现 $n \mod p < m \mod p$, 则把对应的组合数看成0, 表示原来的组合数是 p 的倍数.

丁尧尧

一元一次同分 方程

二元一次不定 方程

欧拉定理

中国剩余定理

快速幂

容斥原理

上井兰岩

各种组合数求

如果要求:

 a^b

其中 b 是非负整数,a 是满足加法结合律的数学对象 (数或矩阵都是).

各种组合数求 法

如果要求:

 a^b

其中 b 是非负整数,a 是满足加法结合律的数学对象 (数或矩阵都是).

可以将 b 看成一个二进制数, 然后不断计算

$$a^0, a^1, a^2, a^4, a^8, \dots$$

如果发现 b 中有对应的项, 就把它乘到答案里.

一元一次同余 方程

二元一次不定 方程

欧拉定理

₩---

中国剩余定理

Lucas 定理

快速幂

谷下原理

各种组合数求

用相同的思想,可以解决求:

 $ab \mod m$

的问题, 其中 a, b, m 都是 10^{18} 级别.

各种组合数才 法

用相同的思想, 可以解决求:

 $ab \ mod \ m$

的问题, 其中 a, b, m 都是 10^{18} 级别. 思路就是把 b 拆分成二进制, 然后依次计算:

如果 b 中有对应项就加到答案里. 因为只有加法, 所以不会爆 $long \ long$.

中国剩余定理

杜油豆

容斥原理

卡特兰数

各种组合数数 法

容斥原理:

$$|\bigcup_{i=1}^{n} A_{i}| = \sum_{i} |A_{i}| - \sum_{1 \leq i < j \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < j < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i < k \leq n} |A_{i} \cap A_{j}| + \sum_{1 \leq i <$$

鸽巢原理:将 n 个鸽子塞进 n-1 个巢中,那么必定有一个 巢有至少两个鸽子。

☆ 長 店 班

卡特兰数

各种组合数求

卡特兰数是计数问题中经常遇到的一类数.

$$C_n = \binom{2n}{n} - \binom{2n}{n+1}$$

卡特兰数是计数问题中经常遇到的一类数.

$$C_n = \binom{2n}{n} - \binom{2n}{n+1}$$

常见模型:

- 1 有 n 对括号的括号序列的方案数.
- ☑ 在一个 n×n 的棋盘从左下角走到右上角,每次只能向右或向上,且不能越过对角线的路径数。
- 3 n 个节点的带标号的二叉树种类.

还有很多, 详见 WIKI.

丁尧尧

一元一次同分 方程

二元一次不定方程

欧拉定理

7(11/2

市国剩全空期

☆ 丘 店 畑

上柱工術

各种组合数求

我们经常遇到求组合数的问题.

容斥原理 卡特兰数

各种组合数求法

我们经常遇到求组合数的问题 比较常见的几种情形及其可能解法:

- 1 $n \le 5000$,直接用 $\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m}$ 递推.
- 2 $n \leq 10^6$ 模大质数 (超过 n), 预处理阶乘及其逆元 (O(n)), 然后直接用 $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ 计算.
- 3 $n \le 10^{18}$ 模小质数 (不超过 10^6), 用 lucas 定理, 转化为上面的问题.
- 4 $n \le 10^7$, 模任意的数, 可以先用线性筛晒出 10^7 以内的素数, 然后对于每个素数, 算出其在 n! 中对应多少次方 (O(logn)), 然后指数加减, 最后取模.