

数学第一讲

丁尧尧

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

快速幂

容斥原理

卡特兰数

各种组合数求
法

积性函数

线性筛

例题选讲

数学第一讲

基础回顾

丁尧尧

上海交通大学

August 7, 2017

目录

数学第一讲

丁尧尧

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

快速幂

容斥原理

卡特兰数

各种组合数求法

积性函数

线性筛

例题选讲

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

11 积性函数

12 线性筛

13 例题选讲

考虑如何解形如

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

的同余式.

数学第一讲

丁尧尧

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

快速幂

容斥原理

卡特兰数

各种组合数求
法

积性函数

线性筛

例题选讲

考虑如何解形如

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

的同余式. 分类讨论:

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.

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.

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.
 - 1 $d \nmid b$, 此时无解

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.
 - 1 $d \nmid b$, 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

考虑如何解形如

$$ax + by = c$$

的不定方程.

考虑如何解形如

$$ax + by = c$$

的不定方程. 还是分类讨论 (不妨设 $\gcd(a, b) = d$):

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 $d \nmid c$, 无解

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 $d \nmid c$, 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.

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 $d \nmid c$, 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.

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）.

欧拉函数的一些性质：

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

欧拉定理:

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

欧拉定理：

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

这个定理一般用来求逆元或对指数取模.

欧拉定理：

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

这个定理一般用来求逆元或对指数取模.

欧拉定理还有个比较有用的扩展：

$$\text{if } q \geq \varphi(n), \text{ then } a^q \equiv a^{q \bmod \varphi(n) + \varphi(n)} \pmod{n}$$

不需要 a 与 n 互质了.

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} .

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.

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.

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:

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

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:

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

$$x \equiv a_2 \pmod{m_2}$$

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

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

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

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

$$k_{10} m_1 - k_{20} m_2 = d,$$

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

$$k_{10} m_1 - k_{20} m_2 = d,$$

$$\text{于是: } k_1 = k_{10} \frac{a_2 - a_1}{d} + t \frac{m_2}{\gcd(m_1, m_2)}.$$

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

$$k_{10} m_1 - k_{20} m_2 = d,$$

$$\text{于是: } k_1 = k_{10} \frac{a_2 - a_1}{d} + t \frac{m_2}{\gcd(m_1, m_2)}.$$

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

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

$$k_{10} m_1 - k_{20} m_2 = d,$$

$$\text{于是: } k_1 = k_{10} \frac{a_2 - a_1}{d} + t \frac{m_2}{\gcd(m_1, m_2)}.$$

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

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

上面的最后一个式子等价于:

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

上面的最后一个式子等价于:

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

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.

卢卡斯定理:

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

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

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).

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.

用相同的思想, 可以解决求:

$$ab \bmod m$$

的问题, 其中 a, b, m 都是 10^{18} 级别.

用相同的思想, 可以解决求:

$$ab \bmod m$$

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:

$$a, 2a, 4a, 8a, \dots$$

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.

容斥原理：

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_i |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \dots$$

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。

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.
- 2 在一个 $n \times n$ 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.

数学第一讲

丁尧尧

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

快速幂

容斥原理

卡特兰数

各种组合数求
法

积性函数

线性筛

例题选讲

我们经常遇到求组合数的问题.

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 $n \leq 5000$, 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 $n \leq 10^{18}$ 模小质数 (不超过 10^6), 用 lucas 定理, 转化为上面的问题.
- 4 $n \leq 10^7$, 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 ($O(\log n)$), 然后指数加减, 最后取模.

积性是函数的一种重要性态，就像单调性、周期性一样。
一个函数 $f(n)$ 如果是积性的，当且仅当：

$$f(nm) = f(n)f(m) \quad (\gcd(m, n) = 1)$$

如果 $f(n)$ 是定义在 \mathbb{Z}^+ 上的积性函数，这样定义 \mathbb{Z}^+ 上的 $g(n)$ ：

$$g(n) = \sum_{d|n} f(d)$$

那么可以证明 $g(n)$ 也是一个积性函数。

假设 n 有质因分解: $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ 。从而:

$$g(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}) = \sum_{d|p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}} f(d) = \sum_{i_1=0}^{\alpha_1} \sum_{i_2=0}^{\alpha_2} \dots \sum_{i_s=0}^{\alpha_s} f(p_1^{i_1} p_2^{i_2} \dots p_s^{i_s})$$

因为 $f(n)$ 是积性函数, 我们可以继续:

$$= \sum_{i_1=0}^{\alpha_1} \sum_{i_2=0}^{\alpha_2} \dots \sum_{i_s=0}^{\alpha_s} f(p_1^{i_1}) f(p_2^{i_2}) \dots f(p_s^{i_s})$$

由求和的性质, 又有:

$$\begin{aligned} &= \sum_{i_1=0}^{\alpha_1} f(p_1^{i_1}) \sum_{i_2=0}^{\alpha_2} f(p_2^{i_2}) \dots \sum_{i_s=0}^{\alpha_s} f(p_s^{i_s}) = \left(\sum_{i_1=0}^{\alpha_1} f(p_1^{i_1}) \right) \left(\sum_{i_2=0}^{\alpha_2} f(p_2^{i_2}) \right) \dots \\ &= g(p_1^{\alpha_1}) g(p_2^{\alpha_2}) \dots g(p_s^{\alpha_s}) \end{aligned}$$

从而有:

$$g(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}) = g(p_1^{\alpha_1}) g(p_2^{\alpha_2}) \dots g(p_s^{\alpha_s})$$

以下是常见的一些积性函数：

- $\tau(n)$ 正整数 n 的正因子个数。
- $\sigma(n)$ 正整数 n 的正因子和。
- $\mu(n)$ 正整数 n 的 Mobius 函数值。
- $\varphi(n)$ 正整数 n 的欧拉函数值，即 $[1, n]$ 中与 n 互质的数的个数。

线性筛可以 $O(n)$ 的时间和空间复杂度内筛出 $[1, n]$ 之间的所有素数。

设一个数 a 的最小素因子是 p , 则保证数 a 只会被 $\frac{a}{p}$ 筛掉。

这保证了它的时间复杂度是 $O(n)$ 的。

然后因为我们在筛一个数的时候可以知道那个数的最小素因子, 所以对于很多积性函数, 我们可以顺便筛出来。

求¹

$$\sum_{i_1|a_1} \sum_{i_2|a_2} \cdots \sum_{i_n|a_n} \varphi(i_1 i_2 \dots i_n) \mod 10^9 + 7$$

其中

$$1 \leq n \leq 10^5, \quad 1 \leq a_i \leq 10^7$$

¹BZOJ 3560

求¹

$$\sum_{i_1|a_1} \sum_{i_2|a_2} \cdots \sum_{i_n|a_n} \varphi(i_1 i_2 \dots i_n) \mod 10^9 + 7$$

其中

$$1 \leq n \leq 10^5, \quad 1 \leq a_i \leq 10^7$$

用积性函数的性质，考虑对每个素数分开做。

¹BZOJ 3560

给你一个数列 $a_n (1 \leq a_i \leq m, m \leq 10^5)$, 求存在多少个数列 b_n 满足:²

1 $1 \leq b_i \leq a_i$

2 $\gcd(b_1, b_2, b_3, \dots, b_n) \neq 1$

给你一个数列 $a_n (1 \leq a_i \leq m, m \leq 10^5)$, 求存在多少个数列 b_n 满足: ²

$$\textbf{1} \quad 1 \leq b_i \leq a_i$$

$$\textbf{2} \quad \gcd(b_1, b_2, b_3, \dots, b_n) \neq 1$$

我们设 $F(d)$ 表示 $\gcd = d$ 的数列个数, 那么显然有:

$$F(d) = \prod_{i=1}^n \lfloor \frac{a_i}{d} \rfloor$$

我们枚举 a_i , 每个 a_i 有 $O(\sqrt{n})$ 段 $\lfloor \frac{a_i}{d} \rfloor$ 值相同的区间, 然后就可以有一个 $O(n\sqrt{m})$ 的算法, 但这样会 TLE。

我们用 $\text{cnt}[a]$ 表示 a 在 a_i 中出现的次数，那么有：

$$F(d) = \prod_{a=1}^m \lfloor \frac{i}{d} \rfloor^{\text{cnt}[i]}$$

和上面一样， $\lfloor \frac{i}{d} \rfloor$ 的值也是一段一段的，我们只需要一段一段的枚举即可，然后用快速幂计算即可。

对于 d ，一共有 $\frac{m}{d}$ 段。当 d 从 2 取到 m 时，总的段数是：

$$m \left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{m} \right) = O(m \log m)$$

每段需要一次快速幂，总的复杂度 $O(m \log^2 m)$

给你一个正整数 S ，问你有多少个数 a ，满足 a 的约数和为 S 。³
输出个数及分别是哪些数。

给你一个正整数 S ，问你有多少个数 a ，满足 a 的约数和为 S 。³

输出个数及分别是哪些数。

设 $F(n)$ 表示一个数的约数和，那么显然这是个积性函数，即：

$$F(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = F(p_1^{a_1}) F(p_2^{a_2}) \cdots F(p_k^{a_k})$$

然后我们就可以爆搜了。