初等数论

张文泰

20100122-rev4

引子

- 数论在信息学中作为一个单独的题目并不是很常见，但是在解题的过程中经常可以用到相关的数论性质。在解决特定问题的时候，数论也是具有相当优势的方法。
- 本文主要介绍了一些初等数论的性质，而不是直接给出相关的代码。

引子

下面主要讲的内容有

- 整除
- 同余
- 同余方程
- 不定方程

其中整除是一些基础的内容，同余和同余方程则稍微深入一些，不定方程则大部分是在做数学推导。

引子

由于篇幅和个人能力的限制，还有很多内容没有介绍到。像下面的：

- 高次同余方程
- 数论函数
- Dirichlet 特征
- 连分数
- 复杂不定方程

有兴趣的同学可以自行学习。

引子

- 对于数论的学习，我的建议是主要在做题中积累经验，多注意一些习题中的思想方法，多看一些书。
- 比较好的书有：《Concrete Mathematics》、《初等数论》、《简明数论》。

整除

- 整除理论是数论的基础，它主要是对整数除法运算的内容作抽象的、系统的总结。
- 整除的主要内容是算术基本定理，同时有对其他基础理论的讨论。

Peano 公理

设$\boldsymbol{N}$是一个非空集合，满足以下条件：

Peano 公理

设$\boldsymbol{N}$是一个非空集合，满足以下条件：

(i) 对每一个元素$n \in \boldsymbol{N}$，一定有唯一的一个$\boldsymbol{N}$中的元素与之对应，这个元素记作n^+，称为n的后继元素。

(ii) 有元素$e \in \boldsymbol{N}$，它不是任一元素的后继。

(iii) $\boldsymbol{N}$中的元素至多是一个元素的后继。

(iv) 设S是$\boldsymbol{N}$的一个子集合，$e \in S$。如果$n \in S$，则必有$n^+ \in S$，那么，$S = \boldsymbol{N}$。

Peano 公理

设$\boldsymbol{N}$是一个非空集合，满足以下条件：

(i) 对每一个元素$n \in \boldsymbol{N}$，一定有唯一的一个$\boldsymbol{N}$中的元素与之对应，这个元素记作n^+，称为n的后继元素。

(ii) 有元素$e \in \boldsymbol{N}$，它不是任一元素的后继。

(iii) $\boldsymbol{N}$中的元素至多是一个元素的后继。

(iv) 设S是$\boldsymbol{N}$的一个子集合，$e \in S$。如果$n \in S$，则必有$n^+ \in S$，那么，$S = \boldsymbol{N}$。

这样的集合就是自然数的抽象定义。

归纳证明原理

- 设$P(n)$是关于自然数n的一种性质或者命题。如果当$n = e$时，$P(e)$成立，以及有$P(n)$成立必可推出$P(n^+)$成立，那么，$P(n)$对所有的$n \in \boldsymbol{N}$都成立。

归纳证明原理

- 设$P(n)$是关于自然数n的一种性质或者命题。如果当$n = e$时，$P(e)$成立，以及有$P(n)$成立必可推出$P(n^+)$成立，那么，$P(n)$对所有的$n \in \boldsymbol{N}$都成立。
- 归纳证明原理作为一种相当基础的证明算法，在解决一些关于集合的命题的时候往往会被使用。在验证某些恒等式的时候，由于等式的变量取值为正整数，有时候也可以巧妙地使用归纳证明原理来证明。

自然数性质

- 最小自然数原理：自然数集合$\boldsymbol{N}$的任一子集T中都存在一个最小的元素。
- 最大自然数原理：对于自然数集合$\boldsymbol{N}$的一个子集M，如果M存在上界，那么M中必定存在一个最大的元素。

这两个性质在证明存在性的时候比较有用。

整除

设$a, b \in \boldsymbol{Z}$，$a \neq 0$。如果存在$q \in \boldsymbol{Z}$使得$b = aq$，那么就说b可被a整除，记作$a|b$，且称b是a的倍数，a是b的约数。b不能被a整除就记作$a \nmid b$。

素数

- 设整数$p \neq 0, \pm 1$。如果它除了显然约数$\pm 1, \pm p$外没有其他的约数，那么p被称为是不可约数，也叫做素数。
  若$a \neq 0, \pm 1$且a不是不可约数，则a称为合数。
- 我们一般假定素数都是正整数。

素数

若整数$a \geq 2$，则a必有可以表示为若干个素数的乘积，即

$$a = p_1 p_2 p_3 \cdots p_s$$

值得注意的是，这个分解式是唯一的。

素因数分解

设整数$a \geq 2$。

- 若a是合数，则必有素数p，$p \leq a^{1/2}$；
- 若a有如上的分解式，则必有不可约数p，$p \leq a^{1/s}$。

这个结论给予了我们一种在一定范围内求素数的方法——Eratosthenes 筛法。

素数

- 一个著名的结论是：素数有无限多个。
- 证明相当简单。假设只有$p_1, \ldots, p_n$这n个素数，那么$E_n = p_1 \cdots p_n + 1$就是一个新的素数，所以结论是正确的。

素性检验

- 我们经常遇到的一个问题是“判断一个数是否是素数”。
- 对于这个问题，我们一般有试除法、Fermat 素性检验和 Miller-Rabin 素性检验等几种方法。

带余除法

- 带余除法作为数论中最常使用的基本方法，具有很高的实用性。它是数论证明中最重要、最基本、最直接的工具。
- IMO 中的大部分数论题目都可以用带余除法解决，虽然过程可能不太直观，但是并不能影响它的地位。

带余除法

- 设a, b是两个给定的整数，$a \neq 0$。那么一定存在唯一的一对整数q与r，满足

$$b = qa + r, 0 \leq r < |a|$$

- 此外，$a|b$的充要条件是$r = 0$。
- 我们在具体应用的时候，往往并不要求r满足最小性，而是根据情况选择q之后再研究r的性质。

整数分类

- 我们接下来得到一个看似简单，但是很有用的结论。
- 设$a > 0$。任一整数被a除后所得的最小非负余数是且仅是$0, 1, \ldots, a-1$这a个数中的一个。
- 这个整数分类的方法往往配合鸽巢原理使用。

辗转相除法

设u_0, u_1是给定的两个整数，$u_1 \neq 0, u_1 \nmid u_0$。我们一定可以重复应用带余除法得到下面$k+1$个等式：

$$\begin{aligned}
u_0 &= q_0 u_1 + u_2, & 0 < u_2 < |u_1|,\\
u_1 &= q_1 u_2 + u_3, & 0 < u_3 < u_2,\\
u_2 &= q_2 u_3 + u_4, & 0 < u_4 < u_3,\\
&\cdots, & \cdots,\\
u_{k-2} &= q_{k-2} u_{k-1} + u_k, & 0 < u_k < u_{k-1},\\
u_{k-1} &= q_{k-1} u_k + u_{k+1}, & 0 < u_{k+1} < u_k,\\
u_k &= q_k u_{k+1}.
\end{aligned}$$

最大公约数

- 设a_1, a_2是两个整数。如果$d|a_1$且$d|a_2$，那么，d就是a_1, a_2的公约数。
- 设a_1, a_2是两个不全为0的整数，我们把a_1, a_2的公约数中最大的那个称为a_1, a_2的最大公约数，记作(a_1, a_2)。

互素

- 一组数的最大公约数等于 1 是这组数的一个重要性质，为此我们引入一个概念。
- 若$(a_1, a_2) = 1$，则称a_1和a_2是既约的，或是互素的。

最小公倍数

- 设a_1, a_2是两个均不等于零的整数。如果$a_1|l$且$a_2|l$，则称l是a_1和a_2的公倍数。一般情况容易推出。
- 设整数a_1, a_2均不为零。我们把a_1和a_2的正的公倍数中的最小的称为a_1和a_2的最小公倍数，记作$[a_1, a_2]$。
- $[a_1, a_2](a_1, a_2) = a_1 a_2$。这个等式告诉我们两者之间的关系。

最大公约数理论

我们可以用多种方法来构建最大公约数理论，一般而言有下面几种：

- 带余除法
- 整系数线性组合
- 辗转相除法

最大公约数理论

- 用带余除法构建最大公约数理论关键在于用带余除法证明最小公倍数的性质。
- 我们在建立理论的过程中发现“最大”与“最小”其实都是相对于整除的概念。

最大公约数理论

- 用整系数线性组合来刻画最大公约数是一种非常常用的手段。
- 设$a_1, \ldots, a_k$是不全为零的整数。我们有

$$(a_1, \ldots, a_k) = \min\{s = a_1x_1 + \cdots + a_kx_k : s > 0\}$$

- 这里满足$x_j \in \boldsymbol{Z}(1 \leq j \leq k)$。

最大公约数理论

辗转相除法的刻画过程不再赘述，其主要思想是利用辗转相除所产生的等式。

$$u_{k+1} = (u_0, u_1)$$

算术基本定理

- 设$a > 1$，那么，必有

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad p_1 < p_2 < \cdots < p_s$$

- 而且，这个分解式是唯一的。我们把该式称为a的标准素因数分解式。
- 我们可以根据素数分解式的形式找到一个计算最大公约数和最小公倍数的方法。

同余

- 下面将讨论有关同余理论的基本概念和性质。
- 同余的概念主要是：同余，同余式，同余类，完全剩余系，既约剩余系。

同余

- 设$m \neq 0$。若$m|a-b$，即$a-b = km$，则称m为模，a同余于b模m，以及b是a对模m的剩余。记作

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

- 不然，则称a不同余于b模m，b不是a对模m的剩余。

同余

同余是一种等价关系，即有

$$a \equiv a \pmod{m}$$

$$a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$$

$$a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$$

同余

- 同余式可以相加，也可以相乘。

$$ca \equiv cb \pmod{m} \Rightarrow a \equiv b \pmod{m/(c,m)}$$

- 另外的一些同余的运算性质都可以用带余除法推导出来。

同余类与剩余系

- 对给定的模m，整数的同余关系是一个等价关系，因此全体整数对模m是否同余分为若干个两两不相交的集合，使得在同一个集合中的任意两个数对模m一定同余，而属于不同集合中的两个数对模m一定不同余。

同余类与剩余系

- 对给定的模m，整数的同余关系是一个等价关系，因此全体整数对模m是否同余分为若干个两两不相交的集合，使得在同一个集合中的任意两个数对模m一定同余，而属于不同集合中的两个数对模m一定不同余。
- 每一个这样的集合称为是模m的同余类。我们以$r \mod m$表示r所属的模m的同余类。

同余类与剩余系

- 模m的同余类$r \mod m$称为是模m的既约剩余类，如果$(r, m) = 1$。
- 模m的所有既约剩余类的个数记作$\varphi(m)$，通常称为 Euler 函数。
- Euler 函数$\varphi(m)$在数论中是十分重要的，有很多有关它的有趣性质。

Euler 函数

- 设$m>1$，且$m=p_1^{\alpha_1}\cdots p_s^{\alpha_s}, \quad p_1<p_2<\cdots<p_s$，
- 则$\varphi(m)=m\prod_{p|m}\left(1-\frac{1}{p}\right)$。
- Euler 函数是一个积性函数。也就是说，如果$(m_1,m_2)=1$，那么$\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$。

Fermat-Euler 定理

- 设$(a, m) = 1$，则有

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Fermat-Euler 定理

- 设$(a, m) = 1$，则有

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

- 特别的，当p为素数时, 有

$$a^{p} \equiv a \pmod{p}$$

- 这个定理在解决一些构造性问题时非常有用。RSA 系统的思想也是来自于这个定理。

Wilson 定理

- 设p是素数，$r_1, \ldots, r_{p-1}$是模p的既约剩余系，我们有

$$r_1 \cdots r_{p-1} \equiv -1 \pmod{p}$$

Wilson 定理

- 设p是素数，$r_1, \ldots, r_{p-1}$是模p的既约剩余系，我们有

$$r_1 \cdots r_{p-1} \equiv -1 \pmod{p}$$

- 特别的

$$(p-1)! \equiv -1 \pmod{p}$$

- 需要说明的是, 这个定理并不能用来高效地检验一个数是否是素数。

同余方程

- 设整系数多项式

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

- 我们可以讨论是否有整数x满足同余式

$$f(x) \equiv 0 \pmod{m}$$

- 我们把这个同余式称作模m的同余方程。

同余方程

- 解同余方程需要对方程进行一些多项式变换。
- 多项式变换主要有四种。

一次同余方程

- 设$m \nmid a$，模m一次同余方程即为

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

一次同余方程

- 设$m \nmid a$，模m一次同余方程即为

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

- 上式有解的必要条件是

$$(a, m) | b$$

- 当$(a, m) = 1$时，同余方程必定有解，且其解数为1。

一次同余方程

- 关于一次同余方程的解法，可以用扩展 Euclid 辗转相除法来做。
- 同余方程有解的充要条件是$(a, m)|b$成立。在有解时，它有(a, m)个解。
- 以及，若x_0是一个解，那么它的所有(a, m)个解是

$$x \equiv x_0 + \frac{m}{(a, m)} t \pmod{m}, \quad t = 0, \ldots, (a, m) - 1$$

一次同余方程组

设$f_j(x)$是整系数多项式$(1 \leq j \leq k)$。我们把含有变数x的一组同余式

$$f_j(x) \equiv 0 \pmod{m_j}, 1 \leq j \leq k$$

称为是同余方程组。

孙子定理

设$m_1, \ldots, m_k$是两两既约的正整数，那么，对任意整数$a_1, \ldots, a_k$，一次同余方程组

$$x \equiv a_j \pmod{m_j}, 1 \leq j \leq k$$

必有解，且解数为1。

孙子定理

- 事实上，同余方程组的解是

$$x \equiv M_1 M_1^{-1} a_1 + \cdots + M_k M_k^{-1} a_k \pmod{m}$$

的一个整数。这里$m = m_1 \cdots m_k$，
$m = m_j M_j (1 \le j \le k)$，以及$M_j^{-1}$是$M_j$的逆。

- 该定理又称为中国剩余定理。

模为素数的二次同余方程

- 下面讨论模为素数的二次同余方程的一般理论。
- 由于$p = 2$的情形比较显然，所以下面的讨论中我们均假定$p > 2$且$p \nmid a$。二次同余方程的一般形式是

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

模为素数的二次同余方程

- 由于$p \nmid 4a$，所以上式的解和同余方程

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}$$

的解相同，所以可以改写为

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$$

模为素数的二次同余方程

- 由于$p \nmid 4a$，所以上式的解和同余方程

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}$$

的解相同，所以可以改写为

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$$

- 我们令$y \equiv 2ax + b \pmod{p}$，得到

$$y^2 \equiv b^2 - 4ac \pmod{p}$$

- 因此，我们在以后的讨论中，只讨论

$$x^2 \equiv d \pmod{p}$$

形式的方程。由于当$p|d$时仅有一个平凡解，所以我们不妨再假定$p \nmid d$。

模为素数的二次同余方程

- 设素数$p > 2$，d是整数，$p \nmid d$。如果同余方程有解，则称d是模p的二次剩余；若无解，则称d是模p的二次非剩余。
- 在模p的一个既约剩余系中，恰有$(p-1)/2$个模p的二次剩余，$(p-1)/2$个模p的二次非剩余。此外，若d是模p的二次剩余，则同余方程的解数为2。

Euler 判别法

- 设素数$p > 2$，$p \nmid d$。那么，d是模p的二次剩余的充要条件是

$$d^{(p-1)/2} \equiv 1 \pmod{p}$$

Euler 判别法

- 设素数$p > 2$，$p \nmid d$。那么，d是模p的二次剩余的充要条件是

$$d^{(p-1)/2} \equiv 1 \pmod{p}$$

- d是模p的二次非剩余的充要条件是

$$d^{(p-1)/2} \equiv -1 \pmod{p}$$

Legendre 符号

- 我们在讨论模p的二次剩余、二次非剩余的时候，通常引进一个符号——Legendre 符号。

Legendre 符号

- 我们在讨论模p的二次剩余、二次非剩余的时候，通常引进一个符号——Legendre 符号。
- 设素数$p > 2$。定义整变数d的函数

$$\left(\frac{d}{p}\right) = \begin{cases} 1 & \text{当}d\text{是模}p\text{的二次剩余;} \\ -1 & \text{当}d\text{是模}p\text{的二次非剩余;} \\ 0 & \text{当}p|d, \end{cases}$$

我们把$(\frac{d}{p})$称为是**模p的 Legendre 符号**。

Legendre 符号

- 我们经过一些性质的引进，把确定 d 的问题转化为了机械计算 Legendre 符号。
- 由一些性质可以知道，只要计算出

$$\left(\frac{-1}{p}\right), \quad \left(\frac{2}{p}\right), \quad \left(\frac{q}{p}\right)$$

就可以计算出所有的$\left(\frac{d}{p}\right)$。这里$q > 2$是小于p的素数。

Gauss 二次互反定律

- 设p, q均为奇素数，$p \neq q$。那么有

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2}$$

- Gauss 二次互反定律是初等数论中最重要的基本定理之一。

不定方程

我们把变数个数多余方程个数，且取整数值的方程（组）称为不定方程（组)。这在数论中是一个非常重要的课题。

一次不定方程

设整数$k \geq 2$，c，$a_1, \ldots, a_k$是整数且不全为零，以及$x_1, \ldots, x_k$是整数变数。方程

$$a_1 x_1 + \cdots + a_k x_k = c$$

称为k元一次不定方程，$a_1, \ldots, a_k$是它的系数。

一次不定方程

不定方程有解的充要条件是$(a_1, \ldots, a_k)|c$。进而，不定方程有解时，它的解和不定方程

$$\frac{a_1}{g}x_1 + \cdots + \frac{a_k}{g}a_k = \frac{c}{g}$$

的解相同，这里$g = (a_1, \ldots, a_k)$。

一次不定方程

设二元一次不定方程

$$a_1x_1 + a_2x_2 = c$$

有解，$x_{1,0}, x_{2,0}$是它的一组解。那么，它的所有解为

$$\begin{cases} x_1 = x_{1,0} + \frac{a_2}{(a_1,a_2)}t \\ x_2 = x_{2,0} + \frac{a_1}{(a_1,a_2)}t \end{cases} \qquad t = 0, \pm 1, \pm 2, \ldots$$

Pythagoras 方程

- 下面讨论二次不定方程

$$x^2 + y^2 = z^2$$

- 它通常称为商高方程或 Pythogoras 方程。容易看出，所有的平凡解是

$$0, \pm a, \pm a; \quad \pm a, 0, \pm a, \quad a \geq 0$$

Pythagoras 方程

- 下面讨论二次不定方程

$$x^2 + y^2 = z^2$$

- 它通常称为商高方程或 Pythogoras 方程。容易看出，所有的平凡解是

$$0, \pm a, \pm a; \quad \pm a, 0, \pm a, \quad a \geq 0$$

- 为了方便讨论，我们不妨假定

$$x > 0, y > 0, z > 0, \quad (x, y, z) = 1$$

Pythagoras 方程

- 不定方程的本原解x, y, z必满足条件：

$$(x, y) = (y, z) = (z, x) = 1$$
$$2 \nmid x + y$$

Pythagoras 方程

- 不定方程的本原解x, y, z必满足条件：

$$(x, y) = (y, z) = (z, x) = 1$$
$$2 \nmid x + y$$

- 不定方程的y为偶数的全体本原解由以下公式给出

$$x = r^2 - s^2, \quad y = 2rs, \quad z = r^2 + s^2$$

- 其中r, s为满足以下条件的任意整数：

$$r > s > 0, \quad (s, r) = 1, \quad 2 \nmid r + s$$

Lagrange 定理

每个正整数一定可以表示为四个平方数之和，即对任意的$n \geq 1$，不定方程

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$$

有解。

Lagrange 定理

如果需要证明这个定理，下面的恒等式是必须引进的：

$$
\begin{aligned}
&(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2)\\
&=(a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2\\
&+(a_1b_2-a_2b_1+a_3b_4-a_4b_3)^2\\
&+(a_1b_3-a_3b_1+a_4b_2-a_2b_4)^2\\
&+(a_1b_4-a_4b_1+a_2b_3-a_3b_2)^2
\end{aligned}
$$

End

谢谢。