初等数论

张文泰
rchardx@gmail.com

20100122-rev24

目录

第一章　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。本章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。

1.1　Peano 公理

本节将会介绍自然数[1]最重要的两个性质，自然数的归纳原理和最小自然数原理。

自然数的本质属性是由归纳属性刻画的，它是自然数公理化定义的核心。自然数集合严格的抽象的定义是由 Peano 公理给出的，它刻画了自然数的本质属性，并导出有关的运算和性质。

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) （**归纳公（原）理**）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，$S = \boldsymbol{N}$。

由此立刻可以得出几个定理：

定理 1.1.1. *对任意的$n \in \boldsymbol{N}$有$n \neq n^+$。*

[1]一般情况下，0不参与数论问题的讨论，所以在以后的讨论中，把正整数和自然数看成等价的概念。

定理 1.1.2. 设$m \in \boldsymbol{N}$，$m \neq e$，那么，必有唯一的$n \in \boldsymbol{N}$使得$n^+ = m$，即$\boldsymbol{N}$中每个不等于e的元素必是某个元素的后继，e是唯一一个不是任何元素后继的元素。

定理 1.1.3 (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，也可以巧妙地使用归纳证明原理来证明。

顺序　对给定的$a, b \in \boldsymbol{N}$，如果存在$x \in \boldsymbol{N}$，使得$b = a + x$，那么，我们就说b在a之后（或a在b之前），也说b**大于**a（或者a**小于**b），记作

$$b > a \qquad or \qquad a < b$$

由此推出

定理 1.1.4. 对任意的$a, b \in \boldsymbol{N}$，$a = b$，　$a > b$，　$a < b$有且仅有一个成立。

定理 1.1.5 (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。

定理 1.1.6 (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。

最小自然数原理是常用的第二种数学归纳法的基础。

定理 1.1.7 (第二种数学归纳法)**.** 设$P(n)$是关于自然数n的一种性质或者命题。如果

(i) 当$n = 1$时，$P(1)$成立；

(ii) 设$n > 1$，若对所有的自然数$m < n$，$P(m)$成立，则必有$P(n)$成立。

那么，$P(n)$对所有自然数n成立。

这一章完全是各种基础的概念，作为一个背景简单说明一下。下面开始介绍比较重要而又很基础的一些内容。

1.2　整除与素数

这一节简单介绍了整除的概念，然后引出了素数的相关内容。

定义 1.2.1. 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$a\nmid b$。

定理 1.2.1. *(i)* $a|b\iff -a|b\iff a|-b\iff |a||b|$；

(ii) $a|b$且$b|c\Rightarrow a|c$；

(iii) $a|b$且$a|c\iff$对任意的$x,y\in\boldsymbol{Z}$有$a|bx+cy$。该定理还有其一般形式；

(iv) 设$m\neq 0$。那么，$a|b\iff ma|mb$；

(v) $a|b$且$b|a\Rightarrow b=\pm a$；

(vi) 设$b\neq 0$。那么，$a|b\Rightarrow |a|\leq|b|$。

例题 1.2.1. 设a,b是两个给定的非零整数，且有整数x,y，使得$ax+by=1$。证明：若$a|n$且$b|n$，则$ab|n$。

证. 由$n=n(ax+by)=(na)x+(nb)y$，及$ab|na$，$ab|nb$即得所要的结论[2]。□

定义 1.2.2. 设整数$p\neq 0,\pm 1$。如果它除了显然约数$\pm 1,\pm p$外没有其他的约束，那么p被称为是不可约数，也叫做素数[3]。若$a\neq 0,\pm 1$且a不是不可约数，则a称为合数。

下面几个定理是容易得到的

定理 1.2.2. 若a是合数，则必有一个素数p满足$p|a$。

定理 1.2.3. 若整数$a\geq 2$，则a必可以表示为若干个素数的乘积，即

$$a=p_1p_2p_3\cdots p_s$$

由定理1.2.3可以得到下面的推论

推论 1.2.4. 设整数$a\geq 2$。

[2]事实上，满足题中的所给条件的a,b是互素的。
[3]以后我们提到素数的时候，若无特殊情况，都假定它是正的。

1. 若a是合数，则必有素数p，$p \leq a^{1/2}$；

2. 若a有定理1.2.3中的表达式，则必有不可约数p，$p \leq a^{1/s}$。

推论1.2.4给出了一种在某一范围内寻找素数的有效方法。我们一般称之为 **Eratosthenes 筛法**。由于比较容易推出，所以不再赘述。

定理 1.2.5. *素数有无穷多个。*

证. 假设只有有限个素数，令它们为$p_1, p_2, \ldots, p_k$。考虑$E_k = p_1 p_2 \cdots p_k + 1$，可以发现，$E_k > 2$且必有某个$p_i | E_k$，所以$p_i | E_k - p_1 p_2 \cdots p_k$，而 $E_k - p_1 p_2 \cdots p_k = 1$，但$p_i \geq 2$，显然不可能，矛盾，所以假设错误。 □

我们可以类似地定义欧拉数$e_n = e_1 e_2 \cdots e_{n-1} + 1$。下面是前几项的结果：

$$e_1 = 2, e_2 = 3, e_3 = 7, e_4 = 43, e_5 = 1807, e_6 = 3263443, \ldots$$

对于欧拉数，还没有关于其中是否存在无限多素数或合数的结论。一个关于它们的显然性质是对于正整数$m \neq n$，$(e_m, e_n) = 1$。另外，对于$e_n (n > 1)$，我们可以写出表达式

$$e_n = e_1 e_2 e_3 \cdots e_{n-1} + 1 = (e_{n-1} - 1) e_{n-1} + 1 = e_{n-1}^2 - e_{n-1} + 1$$

有一个关于这个递推式的结论是存在一个常数$K \approx 1.264$，使得

$$e_n = \left\lfloor K^{2^n} + \frac{1}{2} \right\rfloor$$

我们令$\pi(x)$为不超过x的所有素数的个数总和，$P(n)$为第n个素数。我们有下面的近似：

$$P(n) \sim n \ln n, \quad \pi(x) \sim \frac{x}{\ln x}$$

定理 1.2.6 (Wilson 定理). *m为素数* $\iff m > 1, m | (m-1)! + 1$

Wilson 定理一般不用来进行素数的判别，但是作为一个重要的定理，对于研究素数的性质非常有用。这个定理的证明我们将在后面介绍剩余系的时候阐述。

我们在进行数论研究时常常要对一个数是否是素数进行判断，我们称之为素性检验。一般常用的方法有试除法、费马素性检验、Miller-Rabin 测试。试除法最简单，算法复杂度为$O(\sqrt{n})$。费马素性检验是一个随机化

算法，其根据是费马小定理[4]。费马小定理指的是如果一个n是素数，那么对于所有的$0 < a < p$，$a^{n-1} \equiv 1 \pmod{n}$。如果对于一个$n$，存在一个满足$0 < a < p$的$a$使得$a^{n-1} \equiv 1 \pmod{n}$，我们就把这个$n$称作**伪素数**。伪素数几乎肯定是素数，另一方面，不是伪素数的数一定不是素数。如果我们随机检测了一些a之后发现n是伪素数，那么，n就有很大的概率是素数。

Miller-Rabin 测试是一种非常快速的素数检验法。要测试n是否为质数，首先将$n-1$分解为$n-1 = 2^s d$的形式。在每次测试开始时，先随机选一个介于$[1, n-1]$的整数a，之后如果对所有的$r \in [0, s-1]$，若$a^d \not\equiv 1 \pmod{n}$且$a^{2^r d} \not\equiv -1 \pmod{n}$，则$n$是合数。否则，$n$有$\frac{3}{4}$的机率为质数。这个测试的实质实际上是对$a^{n-1} \equiv 1 \pmod{n}$进行开平方处理，如果所有的$a^{2^r d} \equiv -1 \pmod{n}$都不满足的话，$a^d \equiv 1 \pmod{n}$是一定满足的。

关于a的选取，下面是一个非常有用的列表：

- $n < 1,373,653$，只需要测试$a = 2, 3$。
- $n < 9,080,191$，只需要测试$a = 31, 73$。
- $n < 4,759,123,141$，只需要测试$a = 2, 7, 61$。
- $n < 2,152,302,898,747$，只需要测试$a = 2, 3, 5, 7, 11$。
- $n < 3,474,749,660,383$，只需要测试$a = 2, 3, 5, 7, 11, 13$。
- $n < 341,550,071,728,321$，只需要测试$a = 2, 3, 5, 7, 11, 13, 17$。

2002 年，印度人 M. Agrawal、N. Kayal 以及 N. Saxena 提出了 AKS 素数检验算法，证明了可以在多项式时间内检验素数。

孪生素数是指一对素数，它们之间相差2。例如3和5，5和7，11和13，10016957和10016959等等都是孪生素数。使用著名的筛选理论，挪威的布朗发现小于x的孪生素数的个数远小于$\frac{x}{(\log x)^2}$。这表明，所有孪生素数的倒数之和收敛，即收敛到布朗常数。与之相对的，所有素数的倒数之和却是发散的。

可以证明$(p, p+2)$是孪生素数，当且仅当

$$4((p-1)! + 1) \equiv -p \pmod{p(p+2)}$$

关于素数还有很多有趣的猜想：

[4]此内容将在后面介绍。

- 是否每个大于 2 的偶数都可写成两个素数之和？
- 是否存在无穷多的孪生素数？
- Fibonacci 数列内是否存在无穷多的素数？
- 是否存在无穷多的梅森素数？
- 是否存在无穷个形式如n^2+1的素数？

1.3　带余除法与辗转相除法

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，但是并不影响它的地位。

定理 1.3.1 (带余数除法). *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*

$$b=qa+r,\qquad 0\leq r<|a| \tag{1.1}$$

此外，$a|b$的充要条件是$r=0$。

在具体应用的时候，往往并不要求r满足最小性，第二种形式如下：

定理 1.3.2. *设a，b是两个给定的整数，$a\neq 0$，再设d是一给定的整数。那么一定存在唯一的一对整数q_1与r_1，满足*

$$b=q_1a+r_1,\qquad d\leq r<|a|+d \tag{1.2}$$

此外，$a|b$的充要条件是$a|r_1$。

上面的定理可以由定理1.3.1推出。我们一般把式1.1中的r称为b被a除后的**最小非负余数**。式1.2中的r_1称为**绝对最小余数**。

下面是一个关于**整数分类**的推论：

推论 1.3.3. *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。*

例题 1.3.1. *设$a>2$是奇数。证明：*

(i) 一定存在正整数$d \leq a-1$，使得$a|2^d-1$。

(ii) 设d_0是满足 *(i)* 的最小正整数d。那么，$a|2^h-1 (h \in \boldsymbol{N})$的充要条件是$d_0|h$。

证. 先证 (i)。考虑以下a个数：

$$2^0, 2^1, 2^2, \ldots, 2^{a-1}$$

显然，$a \nmid 2^j (0 \leq j < a)$。由定理1.3.1知，对于每一个$j$，$0 \leq j < a$，

$$2^j = q_j a + r_j, \quad 0 < r_j < a$$

所以a个余数$r_0, r_1, \ldots, r_{a-1}$仅可能取$a-1$个值。因此其中必有两个相等，设为$r_i, r_k$，不妨设$0 \leq i < k < a$。因而有

$$a(q_k - q_i) = 2^k - 2^i = 2^i(2^{k-i}-1)$$

所以，$a|2^{k-i}-1$，则$d = k-i \leq a-1$，(i) 得证。

下面证 (ii)。易证充分性，所以只要证必然性。

$$h = qd_0 + r, \quad 0 \leq r < d_0$$

因而有

$$2^h - 1 = 2^{qd_0+r} - 2^r + 2^r - 1 = 2^r(2^{qd_0}-1) + (2^r - 1)$$

易得$a|2^r-1$，由此及d_0的最小性得$r=0$，即$d_0|h$。 □

推论1.3.3是对**全体整数**被一个固定的正整数a除后所得的最小非负余数的情况来说的。特殊的整数被一个固定的正整数a除后所得的最小非负余数会有更特殊的性质，例如：

(i) 两个$4k+3$形式的数的乘积一定是$4k+1$形式的数；

(ii) x^2被4除后所得的非负最小余数只可能是$0, 1$；

(iii) x^2被8除后所得的非负最小余数只可能是$0, 4$（当x是偶数），及1（当x是奇数）；

(iv) x^2被3除后所得的非负最小余数只可能是$0, 1$；

(v) x^3被9除后所得的非负最小余数只可能是$0, 1, 8$。

下面介绍**辗转相除法**[5]。

定理 1.3.4 (Euclid 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定理1.3.1得到下面$k+1$个等式：

$$\begin{aligned}
u_0 &= q_0u_1 + u_2, & 0 < u_2 < |u_1|,\\
u_1 &= q_1u_2 + u_3, & 0 < u_3 < u_2,\\
u_2 &= q_2u_3 + u_4, & 0 < u_4 < u_3,\\
&\cdots & \cdots,\\
u_{k-2} &= q_{k-2}u_{k-1} + u_k, & 0 < u_k < u_{k-1},\\
u_{k-1} &= q_{k-1}u_k + u_{k+1}, & 0 < u_{k+1} < u_k,\\
u_k &= q_ku_{k+1}. &
\end{aligned} \tag{1.3}$$

定理 1.3.5. 在定理1.3.4的条件和符号下，我们有

(i) u_{k+1}是u_0和u_1的最大公约数，也就是

$$u_{k+1} = (u_0, u_1) \tag{1.4}$$

(ii) $d|u_0$且$d|u_1$的充要条件是$d|u_{k+1}$；

(iii) 存在整数x_0, x_1使

$$u_{k+1} = x_0u_0 + x_1u_1 \tag{1.5}$$

使用 Euclid 辗转相除法，我们还可以求出$ax + by = d$的解。从后面的内容我们知道，这个不定方程有解的充要条件是$(a, b)|d$。我们先求出$ax + by = (a, b)$的解，然后可以得到原方程的解。具体的做法是使用迭代。我们先考虑和原始的辗转相除法相同的过程，当最后$b = 0$时，$a'x = a'$的解是$x = 1, y = 0$。对于$ax + by = (a, b)$，下一层的运算结果是$bx' + (a \bmod b)y' = (a, b)$，那么可以解得$x = y', y = x' - \lfloor \frac{a}{b} \rfloor y'$，因为$\lfloor \frac{a}{b} \rfloor \times b + (a \bmod b) = a$。

另外，辗转相除法在编写代码时，是可以使用位运算优化的。

1.4　最大公约数和最小公倍数

下面引进最大公约数和最小公倍数的概念。

[5]本节中的辗转相除法与下面介绍的公约数概念有关，可以同时阅读两个小节

定义 1.4.1. 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。关于其一般性的定义，不再赘述。

定义 1.4.2. 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)。我们用$\mathscr{D}(a_1, a_2, \ldots, a_k)$来表示$a_1, a_2, \ldots, a_k$的公约数集合。

定理 1.4.1. *(i)* $(a_1, a_2) = (a_2, a_1) = (-a_1, a_2)$；一般地

$$\begin{aligned}(a_1, a_2, \ldots, a_i, \ldots, a_k) &= (a_i, a_2, \ldots, a_1, \ldots, a_k)\\ &= (-a_1, a_2, \ldots, a_k)\end{aligned}$$

(ii) 若$a_1|a_j, j = 2, \ldots, k$，则

$$(a_1, a_2) = (a_1, a_2, \ldots, a_k) = (a_1) = |a_1|$$

(iii) 对任意的整数$x, (a_1, a_2) = (a_1, a_2, a_1x)$，

$$(a_1, \ldots, a_k) = (a_1, \ldots, a_k, a_1x)$$

(iv) 对任意的整数$x, (a_1, a_2) = (a_1, a_2 + a_1x)$，

$$(a_1, a_2, a_3, \ldots, a_k) = (a_1, a_2 + a_1x, a_3, \ldots, a_k)$$

(v) 若p是素数，则

$$(p, a_1) = \begin{cases} p & p|a_1 \\ 1 & p \nmid a_1 \end{cases}$$

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。

定义 1.4.3. 若$(a_1, a_2) = 1$，则称a_1和a_2是既约的，或是互素的。一般性的形式不再赘述。

定理 1.4.2. 如果存在整数$x_1, x_2, \ldots, x_k$，使得$a_1x_1 + a_2x_2 + \cdots + a_kx_k = 1$，则$a_1, a_2, \ldots, a_k$是既约的。

定理 1.4.3. 设正整数$m|(a_1, \ldots, a_k)$。我们有

$$m(a_1/m, \ldots, a_k/m) = (a_1, \ldots, a_k) \tag{1.6}$$

令$m = (a_1, \ldots, a_k)$可以得到其特别情形。

定义 1.4.4. 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。此外以$\mathscr{L}(a_1, \ldots, a_k)$作为$a_1, \ldots, a_k$的所有公倍数的集合。

定义 1.4.5. 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$[a_1, a_2]$。

由定义立即推得

定理 1.4.4. *(i)* $[a_1, a_2] = [a_2, a_1] = [-a_1, a_2]$；一般地

$$\begin{aligned}[a_1, a_2, \ldots, a_i, \ldots, a_k] &= [a_i, a_2, \ldots, a_1, \ldots, a_k] \\ &= [-a_1, a_2, \ldots, a_k]\end{aligned}$$

(ii) 若$a_2|a_1$，则$[a_1, a_2] = |a_1|$；若$a_j|a_1 (2 \leq j \leq k)$，则

$$[a_1, \ldots, a_k] = |a_1|$$

(iii) 对任意的$d|a_1$，

$$[a_1, a_2] = [a_1, a_2, d]; [a_1, \ldots, a_k] = [a_1, \ldots, a_k, d]$$

定理 1.4.5. 设$m > 0$，我们有

$$[ma_1, \ldots, ma_k] = m[a_1, \ldots, a_k]$$

上面简单介绍了一些公约数和公倍数的理论和定理，下面将介绍最大公约数理论[6]。我们将用三种途径建立最大公约数理论。

第一个途径　我们通过用带余除法证明最小公倍数的性质来实现。

定理 1.4.6. $a_j|c (1 \leq j \leq k)$的充要条件是$[a_1, \ldots, a_k]|c$。

证. 充分性显然。设$L = [a_1, \ldots, a_k]$。得

$$c = qL + r, \quad 0 \leq r < L$$

由此及$a_j|c$推出$a_j|r$，所以r是公倍数。进而，又由$0 \leq r < L$得$r = 0$，所以$L|c$。 □

该定理表明公倍数一定是最小公倍数的倍数。因此，最小公倍数中的最小指的是“整除”意义下的最小。

[6]公倍数的性质并不是很重要。

定理 1.4.7. 设D是正整数。那么，$D=(a_1,\ldots,a_k)$的充要条件是：

(i) $D|a_j(1\le j\le k)$；

(ii) 若$d|a_j(1\le j\le k)$，则$d|D$。

该定理表明，公约数一定是最大公约数的约数。这也表明了最大公约数中最大的含义。

定理 1.4.8. 设$(m,a)=1$，则有$(m,ab)=(m,b)$。

证. $(m,b)=(m,b(m,a))=(m,(mb,ab))=(m,mb,ab)=(m,ab)$ □

定理 1.4.9. 设$(m,a)=1$。那么，若$m|ab$，则$m|b$。

定理 1.4.10. $[a_1,a_2](a_1,a_2)=|a_1a_2|$

这个定理刻画了最大公约数和最小公倍数之间的关系。

例题 1.4.1. 设p是素数。证明：

(i) $p|\binom{p}{j}$，$1\le j\le p-1$；

(ii) 对任意正整数a，$p|a^p-a$；

(iii) 若$(a,p)=1$，则$p|a^{p-1}-1$。

证. 已知组合数

$$\binom{p}{j}=\frac{p!}{j!(p-j)!}$$

是整数，即$j!(p-j)!|p!$。由于p是素数，所以，对任意$1\le i\le p-1$有$(p,i)=1$。因此

$$(p,j!(p-j)!)=1,\quad 1\le j\le p-1$$

进而推出，当$1\le j\le p-1$时$j!(p-j)!|(p-1)!$，(i) 得证。

下面用归纳法证明 (ii)。$a=1$时显然成立。

$$\begin{aligned}(n+1)^p-(n+1)&=n^p+\binom{p}{1}n^{p-1}+\cdots+\binom{p}{p-1}n+1-(n+1)\\&=n^p-n+p\times A\end{aligned}$$

这里 A 是一个整数。(ii) 得证。由 (ii) 可以得到 (iii)。 □

第二个途径　我们用关于$a_1,\dots,a_k$的整系数线性组合来刻画。

定理 1.4.11. *设$a_1,\dots,a_k$是不全为零的整数。我们有*

(i) $(a_1,\dots,a_k)=\min\{s=a_1x_1+\cdots+a_kx_k : x_j\in \boldsymbol{Z}(1\le j\le k), s>0\}$，*即$a_1,\dots,a_k$的最大公约数等于$a_1,\dots,a_k$的所有整系数线性组合组成的集合$S$中最小的整数。*

(ii) 一定存在一组整数$x_{1,0},\dots,x_{k,0}$使得

$$(a_1,\dots,a_k)=a_1x_{1,0}+\cdots+a_kx_{k,0} \tag{1.7}$$

证. 由于$0<a_1^2+\cdots+a_k^2\in S$，所以集合$S$中有正整数。由最小自然数原理得$S$中必有最小数$s_0$。显然，对于任一公约数$d|a_j(1\le j\le k)$，则必有$d$整除$S$任一元素，那么$d|s_0$。所以，$|d|\le s_0$。另外

$$a_j=q_js_0+r_j,\quad 0\le r_j<s_0$$

因为s_0可以被$x_1,\dots,x_k$表示，a_j也可以，而$r_j=a_j-q_js_0$，所以$r_j\in S$。如果$r_j>0$，则与s_0最小矛盾，所以$r_j=0$。即s_0是最大公约数。　□ y 有了这一个基础性的定理，前面已经介绍过的有关最大公约数的定理都可以重新建立。虽然证明过程中没有介绍如何求出$x_{1,0},\dots,x_{k,0}$，但是应用辗转相除法，我们可以求出这种线性组合的解[7]。

第三个途径　我们用辗转相除法来刻画。由定理1.3.5作为基础，引出相关的定理、性质。具体不再赘述。

1.5　算术基本定理

定理 1.5.1. *设p是素数，$p|a_1a_2$。那么，$p|a_1$或$p|a_2$至少有一个成立。一般地，若$p|a_1\cdots a_k$，则$p|a_1,\dots,p|a_k$至少有一个成立。*

定理 1.5.2 (算术基本定理)**.** *设$a>1$，那么，必有*

$$a=p_1p_2\cdots p_s \tag{1.8}$$

其中，$p_j(1\le j\le s)$是素数，且在不计次序的前提下，表示式1.8是唯一的。

[7]方法就留给大家思考，比较简单。

这个定理的证明可以用反证法得到。该定理非常重要，尤其是它告诉我们，这种表达式具有唯一性和必然存在性。我们把1.8中的相同素因数合并，得到

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad p_1 < p_2 < \cdots < p_s \tag{1.9}$$

我们把式1.9称为a的**标准素因数分解式**。

推论 1.5.3. 设a由式1.9给出。那么，d是a的正除数的充要条件是

$$d = p_1^{e_1} \cdots p_s^{e_s}, \quad 0 \le e_j \le \alpha_j, 1 \le j \le s \tag{1.10}$$

推论 1.5.4. 设a由式1.9给出，

$$b = p_1^{\beta_1} \cdots p_s^{\beta_s}$$

这里允许某个α_j或β_j为零。那么

$$(a,b) = p_1^{\delta_1} \cdots p_s^{\delta_s}, \quad \delta_j = \min(\alpha_j, \beta_j), 1 \le j \le s \tag{1.11}$$

$$[a,b] = p_1^{\gamma_1} \cdots p_s^{\gamma_s}, \quad \gamma_j = \max(\alpha_j, \beta_j), 1 \le j \le s \tag{1.12}$$

以及

$$(a,b)[a,b] = ab$$

推论 1.5.5. 设a是正整数，$\tau(a)$表示a的所有正除数的个数（也叫做除数函数）。若a有标准因数分解式1.9，则

$$\tau(a) = (\alpha_1 + 1) \cdots (\alpha_s + 1) = \tau(p_1^{\alpha_1}) \cdots \tau(p_s^{\alpha_s})$$

推论 1.5.6. 设a是正整数，$\sigma(a)$表示a的所有正除数之和（也叫做除数和函数）。那么，$\sigma(1) = 1$，当a有标准因数分解式1.9时

$$\begin{aligned} \sigma(a) &= \frac{p_1^{a_1+1}}{p_1 - 1} \cdots \frac{p_s^{a_s+1}}{p_s - 1} = \prod_{j=1}^{s} \frac{p_j^{a_j+1}}{p_j - 1} \\ &= \sigma(p_1^{\alpha_1}) \cdots \sigma(p_s^{\alpha_s}) \end{aligned} \tag{1.13}$$

例题 1.5.1. 求$\sum_{d|180} \frac{1}{d}$。

证. 题目中所给的符号表示对于 180 的所有约数求和。

$$\sum_{d|a} \frac{1}{d} = \sum_{d|a} \frac{1}{a/d} = \frac{1}{a} \sum_{d|a} d = \frac{1}{a} \sigma(a)$$

所以我们得到

$$\sum_{d|180}\frac{1}{d}=\frac{1}{180}\sigma(180)=\frac{91}{30}$$

□

一个正整数m被称为完全数当$\sigma(m)=2m$。我们所知道的完全数有$6,28,496,8128,33550336,\ldots$，一共有47个。目前发现的所有完全数都是偶数，有定理证明，如果存在奇完全数，其形式必然是12^p+1或36^p+9，其中p是素数。完全数有许多有趣的性质:

(i) 都可以表示为连续的自然数和。

(ii) 它们的全部因数的倒数之和都是2，因此每个完全数都是调和数。

(iii) 除6以外的完全数，还可以表示成连续奇立方数之和。

(iv) 完全数都可以表达为2的一些连续正整数次幂之和。

(v) 完全数都是以6或8结尾。如果以8结尾，那么就肯定是以28结尾。

(vi) 除6以外的完全数，被9除都余1。

1.6　阶乘的分解式

这一节的内容比较简单，主要是对$n!$的讨论。

若素数$p|n!$，则必有$p|k,1\leq k\leq n$；另一方面，任一素数$p\leq n$必有$p|n!$。所以，$n!$的标准素因数分解式必为

$$n!=p_1^{\alpha_1}\cdots p_s^{\alpha_s},\quad 2=p_1<p_2<\cdots<p_s\leq n$$

因此，我们求$n!$的分解式的问题被转化为了求所有的$\alpha_j(1\leq j\leq s)$。我们先引进一个符号，记号

$$a^k\parallel b$$

表示b恰好被a的k次方整除，也就是

$$a^k|b,a^{k+1}\nmid b$$

定理 1.6.1. *设n是正整数，p是素数。再设$\alpha=\alpha(p,n)$满足$p^\alpha\parallel n!$，那么*

$$\alpha=\alpha(p,n)=\sum_{j=1}^{\infty}\left[\frac{n}{p^j}\right]$$

这个定理的证明非常“直观”，基本上不需要太复杂的推导。

推论 1.6.2. *设n是正整数。我们有*

$$n! = \prod_{p \le n} p^{\alpha(p,n)}$$

我们如果想要求$\alpha(p,n)$，可以令

$$\epsilon_p(n!) = \alpha(p,n)$$

那么

$$\begin{aligned} \epsilon_p(n!) &< \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots \\ &= \frac{n}{p}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \\ &= \frac{n}{p} \cdot \frac{p}{n-1} \\ &= \frac{n}{p-1} \end{aligned} \tag{1.14}$$

这是一个很精确的上界。

推论 1.6.3. *m个相邻整数的乘积可以被$m!$整除。*

我们对于$n!$还有一个近似公式，就是：

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

这个界我们称之为 Stirling 近似公式。相对于这个比较精确的界，我们可以得到一些不太精确的界，比如

$$n! \le \frac{(n+1)^n}{2^n}$$

我们如果把 Stirling 近似公式和刚才的$\epsilon_p(n!)$的近似公式结合起来，又可以得到一个$\pi(x)$的下界。因为

$$p^{\epsilon_p(n!)} < p^{n/(p-1)}$$

所以，如果一个整数n有k个不同的素因数，那么$n! < 2^{nk}$。我们把k用$\pi(n)$替换，得到

$$n! < 2^{n\pi(n)}$$

所以

$$n\pi(n) > n\lg(n/e) + \frac{1}{2}\lg(2\pi n)$$

推得

$$\pi(n) > \lg(n/e)$$

不过这个下界比较弱。

第二章　同余

本章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。

2.1　同余

定义 2.1.1 (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

$$a \equiv b \pmod{m} \tag{2.1}$$

不然，则称a不同余于b模m，b不是a对模 m 的剩余，记作

$$a \not\equiv b \pmod{m}$$

式2.1称为模m的同余式。

定理 2.1.1. a同余于b模m的充要条件是a和b被m除后的余数相等。也就是如果

$$a = q_1 m + r_1, \quad 0 \leq r_1 < m$$
$$b = q_2 m + r_2, \quad 0 \leq r_2 < m$$

则$r_1 = r_2$。

性质 2.1.1. 同余是一种等价关系，即有

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

性质 2.1.2. 同余式可以相加，即若有

$$a \equiv b \pmod{m}, \quad c \equiv d \pmod{m} \tag{2.2}$$

则

$$a + c \equiv c + d \pmod{m}$$

性质 2.1.3. 同余式可以相乘，即若有式2.2，则

$$ac \equiv cd \pmod{m}$$

性质 2.1.4. 设$f(x) = a_n x^n + \cdots + a_0$，$g(x) = b_n x^n + \cdots + b_0$是整系数多项式[1]，满足

$$a_j \equiv b_j \pmod{m}, \quad 0 \le j \le n \tag{2.3}$$

那么，若$a \equiv b \pmod{m}$，则

$$f(a) \equiv g(b) \pmod{m}$$

特别的，对所有整数x，有

$$f(x) \equiv g(x) \pmod{m} \tag{2.4}$$

由性质2.1.4可以引进

定义 2.1.2. 设$f(x) = a_n x^n + \cdots + a_0$，$g(x) = b_n x^n + \cdots + b_0$。当满足式2.3时，称多项式$f(x)$同余于多项式$g(x)$模$m$，记作

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

当满足式2.4时，称多项式$f(x)$等价于多项式$g(x)$模m。

性质 2.1.5. 设$d \ge 1$，$d|m$。那么，若式2.1成立，则

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

性质 2.1.6. 设$d \ne 0$。那么同余式2.1等价于

$$da \equiv db \pmod{dm}$$

下面要介绍的是由进一步的整除知识推导出的结论。

[1]以后如果无特殊说明，多项式都是整系数.

性质 2.1.7. 同余式

$$ca \equiv cb \pmod{m} \tag{2.5}$$

等价于

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

特别的，当$(c,m)=1$时，可以从两边约去c。

性质 2.1.8. 若$m \geq 1$，$(a,m)=1$，则存在c使得

$$ca \equiv 1 \pmod{m} \tag{2.6}$$

我们把c称为是a对模m的逆，记作$a^{-1} \pmod{m}$或a^{-1}。

性质 2.1.9. 同余式组

$$a \equiv b \pmod{m_j}, \quad j = 1, 2, \ldots, k$$

同时成立的充要条件是

$$a \equiv b \pmod{[m_1, \ldots, m_k]}$$

2.2　同余类与剩余系

定义 2.2.1 (同余类（剩余类）). 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$r \bmod m$表示r所属的模m的同余类。

由定义立即推出

定理 2.2.1. *(i)* $r \bmod m = \{r + km : k \in \boldsymbol{Z}\}$；

(ii) $r \bmod m = s \bmod m$的充要条件是$r \equiv s \pmod{m}$；

(iii) 对任意的r, s，要么$r \bmod m = s \bmod m$，要么$r \bmod m$与$s \bmod m$的交为空集。

定理 2.2.2. 对给定的模m，有且恰有m个不同的模m的同余类，它们是

$$0 \mod m, 1 \mod m, \ldots, (m-1) \mod m \tag{2.7}$$

我们记由这些同余类为元素所组成的集合为

$$\boldsymbol{Z}/m\boldsymbol{Z} = \boldsymbol{Z}_m = \{j \mod m : 0 \leq j \leq m-1\} \tag{2.8}$$

由鸽巢原理立即推出

定理 2.2.3. *(i)* 在任意取定的$m+1$个整数中，必有两个数对模m同余；

(ii) 存在m个数两两对模m不同余。

定义 2.2.2 (完全剩余系)**.** 一组数$y_1, \ldots, y_s$称为是模m的完全剩余系（或者简称为剩余系），如果对于任意的a有且仅有一个y_j是a对模m的剩余，即a同余于y_j模m。

定理 2.2.4. 设$m_1|m$。那么，对任意的r有

$$r \mod m \subseteq r \mod m_1$$

即

$$r + m\boldsymbol{Z} \subseteq r + m_1\boldsymbol{Z}$$

上面的定理用同余式的语言可以重新描述为

定理 2.2.5. 设$m_1|m$。那么，对任意的r，

$$n \equiv r \pmod{m_1}$$

成立的充要条件是以下$d = m/m_1$个同余式有且仅有一个成立：

$$n \equiv r + jm_1 \pmod{m}, \quad 0 \leq j < d$$

定理 2.2.6. 模m的一个同余类中的任意两个整数a_1, a_2与m的最大公约数相等，即$(a_1, m) = (a_2, m)$。

定义 2.2.3. 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。

定义 2.2.4. 一组数$z_1, \ldots, z_t$称为是模m的既约剩余系，如果$(z_j, m) = 1, 1 \leq j \leq t$；以及对任意的$a$，$(a, m) = 1$，有且仅有一个$z_j$是$a$对模$m$的剩余，即$a$同余于$z_j$模$m$。

定理 2.2.7. 模 m 的所有不同的既约同余类是：

$$r \mod m, \quad (r, m) = 1, \quad 1 \leq r \leq m \tag{2.9}$$

$\varphi(m)$等于$1, 2, \ldots, m$中和m既约的数的个数。

定理 2.2.8. *(i)* 在任意取定的$\varphi(m) + 1$个均和m既约的整数中，必有两个数对模m同余；

(ii) 存在$\varphi(m)$个数两两对模m不同余且均和m既约。

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。

定理 2.2.9. 设p是素数，$k \geq 1$，那么，

$$\varphi(p^k) = p^{k-1}(p-1)$$

以及模p^k的既约同余类是：

$$(a + bp) \mod p^k, \quad 1 \leq a \leq p-1, 0 \leq b \leq p^{k-1} - 1$$

2.3 Euler 函数的性质与 Fermat-Euler 定理

定理 2.3.1. 设$m = m_1 m_2$。

(i) 若m_1与m_2有相同的素因数，那么

$$\varphi(m) = m_2 \varphi(m_1) \tag{2.10}$$

(ii) 若$(m_1, m_2) = 1$，则

$$\varphi(m) = \varphi(m_1)\varphi(m_2) \tag{2.11}$$

那么，若有

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

则

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right) \tag{2.12}$$

由此可见，Euler 函数是一个积性函数。

定理 2.3.2. 对任意正整数m有

$$\sum_{d|m}\varphi(d)=m$$

下面将介绍 **Fermat-Euler 定理**。

定理 2.3.3 (Fermat-Euler). 设$(a,m)=1$，则有

$$a^{\varphi(m)}\equiv 1 \pmod{m} \tag{2.13}$$

特别的，当p为素数时，有

$$a^{p-1}\equiv 1 \pmod{p} \tag{2.14}$$

证. 首先，我们阐明一个性质。若$r_1,\dots,r_{\varphi(m)}$和$r'_1,\dots,r'_{\varphi(m)}$都是模$m$的既约剩余系，那么

$$\prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{j=1}^{\varphi(m)} r'_j \pmod{m}$$

下面，我们取模m的一组既约剩余系$r_1,\dots,r_{\varphi(m)}$。当$(a,m)=1$时，$ar_1,\dots,ar_{\varphi(m)}$也是模$m$的既约剩余系。由此得

$$\prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{j=1}^{\varphi(m)} (ar_j) = a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} r_j$$

立刻得到式2.13。式2.14也可以由此推出。 □

我们一般称式2.13为 Euler 定理，而称式2.14为 Fermat 小定理。

如果$m=p_1^{\alpha_1}\cdots p_s^{\alpha_s}, p_1<\cdots<p_s$，另外

$$c_j=\varphi(p_j^{\alpha_j}), \alpha=\max(\alpha_1,\dots,\alpha_s)$$

那么，对任意整数a有如下的性质

(i) $a^{\alpha+\varphi(m)}\equiv a^{\alpha} \pmod{m}$;

(ii) $a^m\equiv a^{m-\varphi(m)} \pmod{m}$;

(iii) $a^{\alpha}f(a)\equiv 0 \pmod{m}$，其中$f(x)$是多项式$x^{c_1}-1,\dots,x^{c_s}-1$的最小公倍式;

(iv) 如果$\alpha_1 = \cdots = \alpha_s = 1$，那么$a^{1+\varphi(m)} \equiv a \pmod{m}$。

我们把令$a^d \equiv 1 \pmod{m}$成立的最小正整数d称为$\delta_m(a)$。这里必有

$$\delta_m(a) | \varphi(m)$$

定理 2.3.4. *设$(a, m) = 1$。那么，$d_0 = \delta_m(a)$的充要条件是*

$$a^{d_0} \equiv 1 \pmod{m} \tag{2.15}$$

及

$$a^0 = 1, a, \ldots, a^{d_0 - 1} \tag{2.16}$$

对模m两两不同余。特别的，$d_0 = \varphi(m)$的充要条件是式2.16给出了m的一组既约剩余系。

本节介绍的内容有一个非常著名的应用——**RSA 密钥系统**。该系统由 R.L.Rivest，A.Shamir，L.Adleman 于 1978 年提出。

设$n = pq$，p, q是两个不同的大素数，再设正整数α, β满足

$$\begin{aligned} \alpha\beta &\equiv 1 \pmod{\varphi(n)} \\ &\equiv 1 \pmod{(p-1)(q-1)} \end{aligned} \tag{2.17}$$

这样，对任一整数A，$0 \le A < n$，必有唯一的整数B满足

$$B \equiv A^\alpha \pmod{n}, \quad 0 \le B < n$$

容易证明：对任意整数k有

$$k^{\alpha\beta} \equiv k \pmod{n}$$

因此，有

$$B^\beta \equiv A^{\alpha\beta} \equiv A \pmod{n}$$

这样，如果某甲知道了α, n（不知道p, q），他为了把A发给知道p, q的某乙而不让别人知道，可以把B发给某乙，因为乙可以通过式2.17来确定β，从而由B得到A。由于大整数的素因数分解是很困难的，所以，不知道p, q的人很难获得 A。这就是 RSA 密钥系统。

2.4　Wilson 定理

定理 2.4.1 (Wilson). 设p是素数，$r_1, \ldots, r_{p-1}$是模p的既约剩余系，我们有

$$r_1 \cdots r_{p-1} \equiv -1 \pmod{p} \tag{2.18}$$

特别的

$$(p-1)! \equiv -1 \pmod{p} \tag{2.19}$$

证. 当$p = 2$时，结论成立。所以设$p \geq 3$。

对这一组给定的既约剩余系中每一个r_i，必然存在一个唯一的r_j使得

$$r_i r_j \equiv 1 \pmod{p} \tag{2.20}$$

使$r_i = r_j$的充要条件是

$$r_i^2 \equiv 1 \pmod{p}$$

即

$$(r_i - 1)(r_i + 1) \equiv 0 \pmod{p}$$

由于p是素数且$p \geq 3$，所以上式成立当且仅当

$$r_i - 1 \equiv 0 \pmod{p}$$

或

$$r_i + 1 \equiv 0 \pmod{p}$$

由于$p \geq 3$，所以这两个条件不能同时成立。因此，在既约剩余系中，除了

$$r_i \equiv 1, -1 \pmod{p}$$

这两个数以外，对其它的r_i必有$r_j \neq r_i$使得式2.20成立。不妨设$r_1 \equiv 1 \pmod{p}$，$r_{p-1} \equiv -1 \pmod{p}$。这样，在这组剩余系中除去满足上式的两个数以外，其它的数恰好可以按照式2.20两两分完，即满足

$$r_2 \cdots r_{p-2} \equiv 1 \pmod{p}$$

所以定理得证。 □

需要说明的是，这个定理并不能用来检验一个数是否是素数。

定理 2.4.2. 设素数$p \geq 3$，$l \geq 1$。$c = \varphi(p^l)$，以及$r_1, \ldots, r_c$是模p^l的一组既约剩余系。我们有

$$r_1 \cdots r_c \equiv -1 \pmod{p^l} \tag{2.21}$$

特别的

$$\prod_{r=1}^{p-1} \prod_{s=0}^{p^{l-1}-1} (r + ps) \equiv -1 \pmod{p^l} \tag{2.22}$$

定理 2.4.3. 设素数$p \geq 3$，$l \geq 1$。$c = \varphi(2p^l)$，以及$r_1, \ldots, r_c$是模$2p^l$的一组既约剩余系。我们有

$$r_1 \cdots r_c \equiv -1 \pmod{2p^l} \tag{2.23}$$

Wilson 定理在数论证明中比较有用。

例题 2.4.1. 设p是奇素数，证明

$$1^2 \cdot 3^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

证. 注意到当p是奇素数时

$$\begin{aligned}(p-1)! &= (1 \cdot (p-1))(3 \cdot (p-3)) \cdots ((p-2)(p-(p-2))) \\ &\equiv (-1)^{(p-1)/2} \cdot 1^2 \cdot 3^2 \cdots (p-2)^2 \pmod{p}\end{aligned}$$

由此可以得证。 □

第三章　同余方程

3.1　同余方程基本概念

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

$$f(x) \equiv 0 \pmod{m} \tag{3.1}$$

我们把这个同余式称作模m的**同余方程**[1]。若整数c满足这个同余方程，则称c是这个方程的解。显然，这是同余类$c \mod m$中的任一整数都是这个方程的解，我们把它们的全体看作一个解，记作

$$x \equiv c \pmod{m}$$

由于我们显然只会在模m的一组完全剩余系中讨论解的情况，所以模m的同余方程的解至多只有m个。

解同余方程需要对方程进行一些多项式变换，我们介绍几个最常用的形式：

(i) 设$s(x)$也是整系数多项式，则式3.1的解与$f(x) + ms(x) \equiv 0 \pmod{m}$的解相同。[2]

(ii) 设$s(x)$也是整系数多项式，则式3.1的解与$f(x) + s(x) \equiv s(x) \pmod{m}$的解相同。

(iii) 设$(a, m) = 1$，则式3.1的解与$af(x) \equiv 0 \pmod{m}$的解相同。

[1] 注意到同样存在多元的同余方程。

[2] 这里要说明的是，同余方程的次数取决于方程的最高**有效**次数，因为有些高次项会被化简。

(iv) 设同余方程

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

的解数为m，即是一个**恒等同余式**。若整系数多项式$q(x), r(x)$满足

$$f(x) = q(x)h(x) + r(x)$$

则式3.1的解与

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

的解一样。

由这些性质可以得到下面这个定理。

定理 3.1.1. *若$(a_n, m) = 1$及*

$$a_n^{-1} a_n \equiv 1 \pmod{m}$$

则式3.1的解与

$$x^n + a_n^{-1}a_{n-1}x^{n-1} + \cdots + a_n^{-1}a_1 x + a_n^{-1}a_0 \equiv -1 \pmod{m}$$

的解一样。

定理 3.1.2. *设正整数$d|m$。那么同余方程3.1有解的必要条件是同余方程*

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

有解。

3.2　一次同余方程

设$m \nmid a$，这一节讨论最简单的模m一次同余方程

$$ax \equiv b \pmod{m} \tag{3.2}$$

式3.2有解的必要条件是

$$(a, m)|b \tag{3.3}$$

定理 3.2.1. *当$(a, m) = 1$时，同余方程3.2必定有解，且其解数为1。*

定理 3.2.2. 同余方程3.2有解的充要条件是式3.3成立。在有解时，它有(a,m)个解。以及，若x_0是式3.2的解，那么它的(a,m)个解是

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

证. 要是x是式3.2的解，那么一定存在一个整数y使得$ax = b + my$。我们要求解式3.2，就是要求这个不定方程[3]。这里若x_0, y_0是不定方程的一个解，则

$$y_0 = (ax_0 - b)/m$$

进而可以解得该不定方程的所有解是

$$x = x_0 + \frac{m}{(a,m)}t, \quad y = y_0 + \frac{a}{(a,m)}t, \quad t = 0, \pm 1, \pm 2, \ldots$$

立刻推出该定理的结论。 □

关于一次同余方程的解法，可以用扩展 Euclid 辗转相除法来做。

3.3　一次同余方程组，孙子定理

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

$$f_j(x) \equiv 0 \pmod{m_j}, \quad 1 \le j \le k \tag{3.4}$$

称为是**同余方程组**。若整数c同时满足

$$f_j(c) \equiv 0 \pmod{m_j}, \quad 1 \le j \le k \tag{3.5}$$

则称c是同余方程组3.4的解，显见，这时同余类

$$c \mod m, \quad m = [m_1, \ldots, m_k]$$

中的任一整数也是同余方程组3.4的解。

定理 3.3.1 (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

$$x \equiv a_j \pmod{m_j}, \quad 1 \le j \le k \tag{3.6}$$

[3]关于不定方程，以后会做详细讨论。

必有解，且解数为1. 事实上，同余方程组3.6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。

证. 这个定理的证明可以直接代入检验，容易得到它的正确性。 □

该定理又称为**中国剩余定理**。孙子定理告诉我们，如果同余方程模数比较大，有时候需要采取分解素因数的办法分而解之。

中国剩余定理也为我们表示大数字提供了一个方法。如果选定了一些两两互素的m_i，那么可以用这些数作为模，再以多元组的形式来表示数字。比如选定了$99, 98, 97, 95$，那么所有小于$99 \times 98 \times 97 \times 95 = 89403930$的非负整数都可以唯一的表示出来。例如，$123684 = (33, 8, 9, 89)$。整数原来的四则运算并没有变化。

3.4　模为素数的二次同余方程

本节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

$$ax^2 + bx + c \equiv 0 \pmod{p} \tag{3.7}$$

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

$$x^2 \equiv d \pmod{p} \tag{3.8}$$

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$p \nmid d$。

定义 3.4.1. 设素数$p > 2$，d是整数，$p \nmid d$。如果同余方程3.8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。

定理 3.4.1. 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3.8的解数为2。

定理 3.4.2 (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

$$d^{(p-1)/2} \equiv 1 \pmod{p} \tag{3.9}$$

d是模p的二次非剩余的充要条件是

$$d^{(p-1)/2} \equiv -1 \pmod{p} \tag{3.10}$$

证. 我们先证明上述两个式子有且仅有一个成立。我们有

$$d^{p-1} \equiv 1 \pmod{p}$$

所以

$$(d^{(p-1)/2} - 1)(d^{(p-1)/2} + 1) \equiv 0 \pmod{p}$$

由于素数$p > 2$以及

$$(d^{(p-1)/2} - 1, d^{(p-1)/2} + 1) | 2$$

所以，上面两个判别式有且仅有一个成立。

下面证式3.9成立是d为p的二次剩余的充要条件。先证必要性。若d是p的二次剩余，则必有x_0使得

$$x_0^2 \equiv d \pmod{p}$$

因而

$$x_0^{p-1} \equiv d^{(p-1)/2} \pmod{p}$$

由于$p \nmid d$，所以$p | x_0$，因而

$$x_0^{p-1} \equiv 1 \pmod{p}$$

必要性得证。

再证充分性。证明方法和我们证明 Wilson 定理的方法一样。设式3.9成立，此时必然有$p \nmid d$。考虑

$$ax \equiv d \pmod{p}$$

对于$1 \leq i < j \leq (p-1)/2$，我们有

$$i^2 \not\equiv j^2 \pmod{p}$$

所以，p的既约剩余系中两两可以搭配成上式的解，所以

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

矛盾，充分性得证。 □

推论 3.4.3. -1是模p的二次剩余的充要条件是$p \equiv 1 \pmod 4$；当$p \equiv 1 \pmod 4$时

$$\left(\pm\left(\frac{p-1}{2}\right)\right)^2 \equiv -1 \pmod{p} \tag{3.11}$$

推论 3.4.4. 设素数$p > 2$，$p \nmid d_1$，$p \nmid d_2$。那么，

(i) 若d_1, d_2均为模p的二次剩余，那么$d_1 d_2$也是模p的二次剩余；

(ii) 若d_1, d_2均为模p的二次非剩余，那么$d_1 d_2$是模p的二次剩余；

(iii) 若d_1为模p的二次剩余，d_2为模p的二次非剩余，那么$d_1 d_2$是模p的二次非剩余；

以上的一个定理和两个推论介绍了如何从理论上判断一个数是否是二次剩余或者二次非剩余。推论3.4.4是一个 Legendre 符号的粗略雏形。

3.5　Legendre 符号，Gauss 二次互反律

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**。

定义 3.5.1. 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$\left(\frac{d}{p}\right)$称为是模p的 ***Legendre*** 符号。

定理 3.5.1. *Legendre* 符号有以下性质：

(i) $\left(\frac{d}{p}\right)=\left(\frac{p+d}{p}\right)$；

(ii) $\left(\frac{d}{p}\right)\equiv d^{(p-1)/2} \pmod p$；

(iii) $\left(\frac{dc}{p}\right)=\left(\frac{d}{p}\right)\left(\frac{c}{p}\right)$；

(iv) 当$p\nmid d$时，$\left(\frac{d^2}{p}\right)=1$；

(v) $\left(\frac{1}{p}\right)=1$，$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}$。

这些性质的证明是十分简单的。

这样，我们就把确定d的问题转化为了机械计算 Legendre 符号。由上面的性质可以知道，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。解决这个问题的基础是下面的 Gauss 引理。

引理 3.5.2. 设素数$p>2$，$p\nmid d$，再设$1\le j<p/2$,

$$t_j\equiv jd \pmod p,\quad 0<t_j<p \tag{3.12}$$

以n表示这$(p-1)/2$个$t_j(1\le j<p/2)$中大于$p/2$的t_j的个数。那么有

$$\left(\frac{d}{p}\right)=(-1)^n$$

由该引理可以得到

定理 3.5.3. 我们有

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$$

定理 3.5.4. 设素数$p>2$。当$(d,2p)=1$时

$$\left(\frac{d}{p}\right)=(-1)^T \tag{3.13}$$

其中

$$T=\sum_{j=1}^{(p-1)/2}\left[\frac{jd}{p}\right] \tag{3.14}$$

由这些定理可以得到著名的 **Gauss 二次互反定律**[4]。

定理 3.5.5. *设p, q均为奇素数，$p \neq q$。那么有*

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2} \tag{3.15}$$

该定理表明：两个奇素数p, q，只要有一个数$\equiv 1 \pmod 4$，就必有

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

当且仅当它们都是$4k+3$形式的数时，才有

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$$

Gauss 二次互反定律是初等数论中最重要的基本定理之一。

Legendre 符号的计算需要求出d的素因数分解式后才能用 Gauss 二次互反定律，这当d较大时是不方便的。为了克服这个问题，产生了 Jacobi 符号。由于本文篇幅有限，有兴趣的读者可以自行查阅。

[4]这个定理是 Gauss 在 19 岁时证明的，Gauss 在 19 岁时还得到了一个重要结果：《正十七边形尺规作图之理论与方法》。

第四章　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。

4.1　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

$$a_1 x_1 + \cdots + a_k x_k = c \tag{4.1}$$

称为k元**一次不定方程**，$a_1, \ldots, a_k$是它的系数。

定理 4.1.1. 不定方程4.1有解的充要条件是$(a_1, \ldots, a_k) | c$。进而，不定方程4.1有解时，它的解和不定方程

$$\frac{a_1}{g} x_1 + \cdots + \frac{a_k}{g} a_k = \frac{c}{g} \tag{4.2}$$

的解相同，这里$g = (a_1, \ldots, a_k)$。

定理 4.1.2. 设二元一次不定方程

$$a_1 x_1 + a_2 x_2 = c \tag{4.3}$$

有解，$x_{1,0}, x_{2,0}$是它的一组解。那么，它的所有解为

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

定理 4.1.3. 设$g_1 = a_1, g_2 = (g_1, a_2), \ldots, g_k = (g_{k-1}, a_k)$。那么不定方程4.1等价于下面的有$2(k-1)$个整数变数$x_1, \ldots, x_k, y_2, \ldots, y_{k-1}$，$k-1$个方程的不

定方程组：

$$\begin{cases} g_{k-1}y_{k-1} + a_k x_k = c \\ g_{k-2}y_{k-2} + a_{k-1}x_{k-1} = g_{k-1}y_{k-1} \\ \cdots \\ g_2 y_2 + a_3 x_3 = g_3 y_3 \\ g_1 x_1 + a_2 x_2 = g_2 y_2 \end{cases}$$

当方程4.1有解时，它的通解由有$k-1$个参数的线性表达式给出。

定理 4.1.4. 设a_1, a_2及c均为正整数，$(a_1, a_2) = 1$。那么，当$c > a_1a_2 - a_1 - a_2$时，不定方程4.3有非负解，解数等于$[c/(a_1a_2)]$或$[c/(a_1a_2)] + 1$；当$c = a_1a_2 - a_1 - a_2$时，不定方程4.3没有非负解。

定理 4.1.5. 设a_1, a_2及c均为正整数，$(a_1, a_2) = 1$。那么，当$c > a_1a_2$时，不定方程4.3有正解，解数等于$-[-c/(a_1a_2)] - 1$或$-[-c/(a_1a_2)]$；当$c = a_1a_2$时，不定方程4.3没有正解。

4.2　Pythagoras 方程

这一节讨论二次不定方程

$$x^2 + y^2 = z^2 \tag{4.4}$$

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

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

引理 4.2.1. 不定方程4.4的本原解x, y, z必满足条件：

$$(x, y) = (y, z) = (z, x) = 1 \tag{4.5}$$

$$2 \nmid x + y \tag{4.6}$$

定理 4.2.2. 不定方程4.1的y为偶数的全体本原解由以下公式给出

$$x = r^2 - s^2, \quad y = 2rs, \quad z = r^2 + s^2 \tag{4.7}$$

其中r,s为满足以下条件的任意整数：

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

下面我们介绍一种非常重要的证明方法：**Fermat 无限递降法**。

定理 4.2.3. 不定方程

$$x^4+y^4=z^2 \tag{4.8}$$

无$xyz\neq 0$的解。

证. 该命题即要证无正整数解。假若有正整数解，那么在全体正整数解中，必有一组解x_0,y_0,z_0，使得z_0取最小值。

(i) 必有$(x_0,y_0)=1$。若不然，有素数$p|x_0,p|y_0$，则推出$p^2|z_0$，与z_0的最小性矛盾。由x_0^2,y_0^2,z_0为方程4.4的本原解得，x_0,y_0必为一奇一偶，不妨设$2|y_0$，以及$(z_0,y_0)=1$。

(ii) $g_1=(z_0-y_0^2,z_0+y_0^2)=1$。因为$g_1|(2z_0,2y_0^2)=2(z_0,y_0^2)=2$，由此及$2\nmid z_0-y_0^2$即得$g_1=1$。由此及

$$(z_0-y_0^2)(z_0+y_0^2)=x_0^4$$

我们令

$$z_0-y_0^2=u^4,\quad z_0+y_0^2=v^4$$

这里$v>u>0,(u,v)=1,2\nmid uv$。进而有

$$y_0^2=(v^2-u^2)\frac{v^2+u^2}{2} \tag{4.9}$$

(iii) $g_2=(v^2-u^2,(v^2+u^2)/2)=1$。因为

$$g_2|(v^2-u^2,v^2+u^2)|(2v^2,2u^2)=2(v^2,u^2)=2$$

由$2\nmid uv$得到$2\nmid (v^2+u^2)/2$，因此$g_2=1$。我们再令

$$v^2-u^2=a^2,\quad (v^2+u^2)/2=b^2$$

这里$a>0,b>0,(a,b)=1$，及$2|a,2\nmid b$。

(iv) 由u,v满足的条件及a,b得

$$0<b<v<z_0$$

及u,a,v是方程4.4的本原解且$2|a$。因此得到

$$u=r^2-s^2,\quad a=2rs,\quad v=r^2+s^2$$

所以

$$r^4+s^4=b^2$$

而$b<z_0$，与z_0的最小性矛盾，命题得证。

□

无限递降法就是像这样，通过一个假设的存在解导出一个较小的解，再结合最小自然数原理来证明命题的一中方法。

通过证明这个定理，我们容易得到

推论 4.2.4. 不定方程

$$x^4+y^4=z^4 \tag{4.10}$$

无$xyz\neq 0$的解。

定理 4.2.5. 不定方程

$$x^2+y^2=z^4$$

的满足条件$(x,y)=1$的全部正整数解是

$$x=\left|6a^2b^2-a^4-b^4\right|, y=4ab(a^2-b^2), z=a^2+b^2$$

及

$$x=4ab(a^2-b^2), y=\left|6a^2b^2-a^4-b^4\right|, z=a^2+b^2$$

其中a,b为满足以下条件的任意整数

$$a>b>0,\quad (a,b)=1,\quad 2\nmid a+b$$

4.3　Lagrange 定理

定理 4.3.1. 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

$$x_1^2+x_2^2+x_3^2+x_4^2=n \tag{4.11}$$

有解。

如果需要证明这个定理，下面的恒等式是必须引进的：

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

由此推出，若两个整数可以表示为四个平方数之和，那么它们的乘积也一定是四个平方数之和。所以定理4.3.1等价于

定理 4.3.2. *每个素数p一定可以表示为四个平方数之和，即当$n=p$是不定方程4.11有解。*

由于$2=1^2+1^2+0^2+0^2$，所以我们可以假定$p>2$。

引理 4.3.3. *设素数$p>2$。同余方程*

$$\begin{cases}x^2+y^2+1\equiv 0 \pmod p\\0\le x,y\le (p-1)/2\end{cases}$$

有解。

引理 4.3.4. *设素数$p>2$，一定存在整数x_0,y_0及m_0，$1\le m_0<p$，使得*

$$x_0^2+y_0^2+1=m_0p,\quad m_0\ge 1$$

定理 4.3.5. *当n是形如$4^\alpha(8k+7)(\alpha\ge 0,k\ge 0)$的正整数时，$n$不能表示为三个整数的平方和。*

定理 4.3.6. *$n=2\cdot 4^\alpha(\alpha\ge 0)$不能表示为四个正平方数之和。*

这个定理可以用归纳法证明。

定理 4.3.7. *除去以下12个数：*

$$1,2,3,4,6,7,9,10,12,15,18,33$$

之外，每个正整数都可以表示为五个正平方数之和。

因为当$n>168$时，可以构造，所以只需要直接验证$n\le 168$的情况。

附录 A　初等数论主要内容

- 素数
  - 伪素数
  - 费马素数
  - 梅森素数
  - 孪生素数
- 因子
  - 整除性的问题
  - 最大公因子
  - 辗转相除法
  - 质因子分解
- 有趣的数
  - 完全数
    - K 类完全数
  - 自守数
  - 金兰数
  - 亲和数
  - 拟形数
  - 纯元数
  - 回文数
  - 卡普列加数

- 连分数
  - 佩尔方程
- 幻方
- 原根
- 同余
  - 二次剩余
  - 不定方程
- 倒数的性
- 数论函数
  - 欧拉函数
  - 取整函数
- 经典的定理
  - 欧拉定理
  - 费马小定理
  - 费马大定理
  - 中国剩余定理
  - 威尔逊定理
  - 素数定理
  - 二次互反律
  - 四平方和定理（Lagrange 定理）
  - 算术基本定理
  - 整数数列
    - 阶乘
    - Farey 数列
    - Fibonacci 数列
  - 看起来很简单的猜想

* 哥德巴赫猜想
* 卡塔兰猜想
* 角谷猜想