初等数论选讲

张起帆

四川大学数学学院

email: qifanzhang@scu.edu.cn

2019年

目录

什么是数论

- 研究整数和有理数的基本性质，特别是整数的整除性
- 小学生和大数学家都可以参与的一项“游戏”（规则简单，技术深奥）
- 各级数学竞赛的热门考点（简单的知识、高深的思想）

什么是数论

- 是最古老又不断焕发青春的学科
- 是上帝用以指引人们发展数学的诱饵
- 具有广泛应用背景的学科（特别是在信息时代）
- 数学的女皇

什么是初等数论

- 用数论本身的方法研究数论
- 数学从初等过渡到高等的最佳切入点
- 大学数学专业很多（代数类）课程的基础

本课程基本内容

- 整除性（唯一分解定理、裴蜀定理）
- 同余（费马小定理、欧拉定理、Wilson定理、孙子定理）
- 二次剩余和原根

本课程基本内容

- 二次互反律的应用
- 不定方程简介
- 数论函数简介

基本概念快速梳理及约定

我们先快速回顾一些熟知的基本概念：

设a, b 是任意两个整数,其中$b \neq 0$, 若存在一个整数q使得

$$a = bq,$$

我们就说b整除a或a 被b整除, 记作$b \mid a$, 此时b叫作a的因数或约数, a叫作b的倍数.

基本概念及约定

设$a_1, \cdots, a_n$是$n(n \geq 2)$个整数. 如果整数d是它们之中每一个的因数, 那么d叫作$a_1, \cdots, a_n$的一个公因数, 其中最大的一个叫作最大公因数, 记作$(a_1, \cdots, a_n)$.

若$(a_1, \cdots, a_n) = 1$, 我们就说$a_1, \cdots, a_n$ 互质或者互素, 若$a_1, \cdots, a_n$中每两个整数互素, 就说他们两两互素.

基本概念及约定

设$a_1, \cdots, a_n$是$n(n \geq 2)$个整数. 如果整数d是它们的倍数, 那么d叫作$a_1, \cdots, a_n$的一个公倍数. 所以公倍数中最小正数叫作最小公倍数, 记作$[a_1, \cdots, a_n]$.

一个大于1的整数, 如果它的正因数只有1和它本身, 那么称这个整数为素数, 通常我们用p表示素数; 否则, 我们称这个整数为合数.

导引问题

为什么正的有理数有唯一的既约分数表示？

这个问题虽然不难，但长期被大家默认了，其实是需要证明的，我们在下次课中回答它。

计算最大公约数

例1：求$(187, 253)$**.**

$$(187, 253) = (187, 253 - 187) = (187, 66) = (66, 187)$$

利用了性质：$(a, b) = (a, ak + b) = (a, b - a)$**.**

计算最大公约数

$$= (66, 187 - 2 \times 66) = (66, 55) = (55, 11)$$

$$= (11, 0) = 11.$$

带余除法

带余除法

对正整数a, b，其中$b > 0$，则存在两个整数q和r，使得$a = qb + r, 0 \leq r \leq b - 1$，并且$q$及$r$是惟一的．并且$r$称为$a$被$b$除的余数．

辗转相除法

利用带余除法，我们可以给出求最大公约数的**Euclid**算法，即辗转相除法. 设a_1, a_2为正整数且$a_1 > a_2$，则可不断做带余除法

$$a_1 = a_2 \cdot * + a_3,$$

$$a_2 = a_3 \cdot * + a_4,$$

$$\cdots\cdots$$

$$a_{k-2} = a_{k-1} \cdot * + a_k$$

直到$a_k = 0$. 那么我们可得出$a_{k-1} = (a_1, a_2)$.

辗转相除法

因为

$$(a_1, a_2) = (a_2, a_3) = \cdots = (a_{k-1}, a_k) = (a_{k-1}, 0) = a_{k-1},$$

追踪上述过程, 可得如下定理.

裴蜀定理

裴蜀定理

对任意整数a, b，存在整数u, v使得

$$au + bv = (a, b).$$

特殊裴蜀定理

对整数a, b，若$(a, b) = 1$，则存在整数u, v使得

$$au + bv = 1.$$

重要应用

推论1.

对整数a, b, c，若$(a, b) = 1$，则

$$a|bc \Longrightarrow a|c.$$

辗转相除法

推论1的证明 因为$(a,b)=1$，故存在整数u,v 满足

$$1=au+bv$$

即

$$c=acu+bcv.$$

由于两项都是a的倍数，故$a|c$.

辗转相除法

推论2.

对素数p有

$$p|ab \Longrightarrow p|a\text{或}p|b.$$

唯一分解定理

唯一分解定理

任意大于1的整数都可以唯一地分解为素数之积. 即

$$a = p_1 p_2 \cdots p_n,$$

其中$p_1, p_2, \cdots, p_n$是素数, 并且该表示唯一.

唯一分解定理的证明

证明 存在性. 当$n = 2$时, 显然成立. 假设一切小于n的正整数均可以分解为素数的乘积. 对整数$n > 1$, 考虑n是否素数? 若是, 则完成; 若不是, 则存在整数a, b, 使得

$$n = ab.$$

利用归纳假设, 那么a和b可以写为素数的乘积. 因此n可以写为素数的乘积.

唯一分解定理的证明(续)

唯一性. 设有两种分解

$$n = p_1 \cdots p_s = q_1 \cdots q_t,$$

则$p_1 | q_1 \cdots q_t$, 利用推论2可推出p_1整除某一q_i,不妨设$p_1 | q_1$,再由p_1, q_1是素数知$p_1 = q_1$. 因此

$$p_2 \cdots p_s = q_2 \cdots q_t.$$

依此类推可完成证明.

应用举例-1

下面我们回答开始提出的问题: 例**1**. 正的有理数有唯一的既约分数表示.

证明 设$\alpha = \frac{a}{b} = \frac{c}{d}$, 且$(a,b) = (c,d) = 1$, 则

$$ad = bc.$$

那么$a|bc$, 结合$(a,b) = 1$ 知$a|c$. 同理$c|a$. 故$a = c$.进而$b = d$. 即有理数α有唯一的既约分数表示.

应用举例-2

例2. 对任意正整数n，1000^n-1不整除1978^n-1.

证明 假设$1000^n-1|1978^n-1$. 则

$$1000^n-1|1978^n-1-(1000^n-1)=1978^n-1000^n$$

$$=2^n(989^n-500^n).$$

但$(1000^n-1,2^n)=1$，故

$$1000^n-1|989^n-500^n.$$

这是不可能的，因为

应用举例-3

例3. 对任意正整数a, b，有$(a, b)[a, b] = ab$.

证明 设$a = p_1^{a_1} \cdots p_n^{a_n}, b = p_1^{b_1} \cdots p_n^{b_n}$.

$$a_i, b_j \geq 0$$

则

$$(a, b) = p_1^{\min\{a_1, b_1\}} \cdots p_n^{\min\{a_n, b_n\}}$$

$$[a, b] = p_1^{\max\{a_1, b_1\}} \cdots p_n^{\max\{a_n, b_n\}}.$$

这就归结为证明

导引问题

在上一讲中，我们知道任何一个有理数既约分数表示是唯一的. 在中学的时候我们就知道有理数不仅可以表示为既约分数，还可以表为有限小数或无限循环小数，那么为什么这两种表示方式是等价的呢？在本节课，我们将回答这个问题. 在这之前，我们首先引入同余的概念.

同余的概念

■ 对整数a, b, m，称a模m同余于b，是指a和b用m除的余数相同，记为$a \equiv b \pmod{m}$，换句话说$m|a-b$.

■ 同余思想简单来说就是在带余除法中忽略商，只关心余数，在某些场合，这就突出了重点，看问题更清晰.

同余的性质

- 同余关系是等价关系；
- $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Longrightarrow a + c \equiv b + d \pmod{m}$；
- $a \equiv b \pmod{m}, c \equiv d \pmod{m}, \Longrightarrow ac \equiv bd \pmod{m}$；
- 若$(a, m) = 1$，则

$$ax \equiv ay \pmod{m} \Longleftrightarrow x \equiv y \pmod{m};$$

- $a^n \equiv b^n \pmod{m}$，在一定条件下有$a \equiv b \pmod{m}$.

同余

裴蜀定理

对任意整数a, b，存在整数v使$bv \equiv (a, b) \pmod{a}$. 特别地，若$(a, b) = 1$，则有$bv \equiv 1 \pmod{a}$.

推论1.

对整数a, b, c，若$(a, b) = 1$，则

$$bc \equiv 0 \pmod{a} \Longrightarrow c \equiv 0 \pmod{a}.$$

同余

推论1的证明 因$(a,b)=1$, 故存在v满足

$$bv \equiv 1 \pmod{a}.$$

在$bc \equiv 0 \pmod{a}$两边同乘v有

$$c \equiv bvc \equiv 0 \pmod{a}.$$

- 引入同余使得证明更简洁, 思路更清晰.

例子

问题: 有理数的以下两种常见的定义等价

1) 可以表为分数形式;
2) 可以表为有限小数或无限循环小数的形式.

证明 整个证明的关键是以下两种数可以互相转化:

1) 既约真分数$\frac{n}{m}$, $(m, 10) = 1$.
2) 纯循环小数.

问题的证明

- **2) $\Rightarrow$ 1)是分析方法.**

希望大家自己回顾纯循环小数如何化成分数的，例如

$$0.\dot{7}\dot{3} = \frac{73}{99}$$

- **1) $\Rightarrow$ 2)关键是找到r使得**

$$10^r \equiv 1 \pmod{m}.$$

问题的证明

由于模m只有m个类，所以在序列

$$10, 10^2, 10^3, ...$$

中必有元素模m是重复的. 即存在$i < j$使得

$$10^i \equiv 10^j = 10^i \times 10^{j-i} \pmod{m}.$$

故

$$10^{j-i} \equiv 1 \pmod{m}.$$

一个问题

在上一讲，我们知道一个既约分数可以写为有限小数或者无限循环小数．如果写为无限循环小数，那么自然有这个问题：

这个循环小数的长度是多长呢？

本节课将回答上述问题．在回答之前，我们引入一些新的概念．

基本概念

- 将集合$a+m\mathbb{Z}$（简记为$\overline{a}$）称为一个模m的剩余类，a 称为这个剩余类的一个代表元.
- 模m的剩余类有m个，可记为$\overline{0},\overline{1},...,\overline{m-1}$，其中与$m$互素的类的个数记为$\phi(m)$，函数$\phi$称为Euler函数.
- 对素数p和正整数n，有

$$\phi(p)=p-1$$

和

$$\phi(p^n)=p^n-p^{n-1}.$$

基本概念

- 若有$a_1, ..., a_m$分别是模m的各个剩余类的一个代表元，称$a_1, ..., a_m$组成一个模m的完全剩余系.
- 若有$a_1, ..., a_{\phi(m)}$分别是模m的各个与m互素的剩余类的一个代表元，称$a_1, ..., a_{\phi(m)}$ 组成一个模m的（完全）剩余缩系.
- 对$(a, m) = 1$，将最小的满足$a^r \equiv 1 \pmod{m}$的正整数r称为a模m的阶.

欧拉定理

欧拉定理

设m是大于1的整数，若$(a,m)=1$，则有$a^{\phi(m)} \equiv 1 \pmod{m}$.

证明 取$a_1, a_2, ..., a_{\phi(m)}$为模$m$的一组剩余缩系，则

$$aa_1, aa_2, ..., aa_{\phi(m)}$$

为另一组剩余缩系. 因此

$$a_1 a_2 \cdots a_{\phi(m)} \equiv aa_1 aa_2 \cdots aa_{\phi(m)} \equiv a^{\phi(m)} a_1 a_2 \cdots a_{\phi(m)} \pmod{m}$$

所以$a^{\phi(m)} \equiv 1 \pmod{m}$.

Fermat小定理

Fermat小定理

对素数p, 若$(a,p)=1$, 则有$a^{p-1}\equiv 1 \pmod{p}$.

也可以叙述为

Fermat小定理

对任意素数p和整数a, 有$a^{p}\equiv a \pmod{p}$.

例子

例：$\frac{1}{7}, \frac{1}{7^2}$各是多少位循环小数.

解 既约分数$\frac{n}{m}$写为循环小数的长度就是最小的满足$m|10^r-1$的正整数r, 即10 模m的阶.

经计算可知10模7的阶是6, 因此$\frac{1}{7}$是6位循环小数. 为了更多计算，先做如下准备

命题1

对整数a, m, 若$(a, m)=1$, a模m的阶是r, 则对整数n有

$$a^n \equiv 1 \pmod{m} \Longleftrightarrow r|n.$$

例子(续)

现在研究$\frac{1}{7^2}$，设它的循环小数长度是r，由于$10^r \equiv 1 \pmod{49}$，因此

$$10^r \equiv 1 \pmod{7}$$

故$6|r$. 通过**Euler**定理(详细说明自己补充)可知

$$r|7 \times 6.$$

从而有$r = 6$或**42**，但$r \neq 6$（经简单计算知$10^6 \not\equiv 1 \pmod{49}$）. 故$\frac{1}{7^2}$是**42**位循环小数.

Wilson定理

Wilson定理

对任意素数p，有$(p-1)! \equiv -1 \pmod{p}$.

证明 当$p=2$时，显然成立．现在设p为奇素数．对任意$i \in A = \{1, 2, ..., p-1\}$，存在唯一$i' \in A$ 满足

$$ii' \equiv 1 \pmod{p}.$$

将每个i与i'配成一对，但当$i=i'$，即$i^2 \equiv 1$时，无其他元与i配对.故

$$(p-1)! = \prod_{i \in A} i \equiv \prod_{i \in A, i^2 \equiv 1 \pmod{p}} i \equiv 1 \times (-1) \equiv -1 \pmod{p}.$$

应用举例-1

例1. 对素数$p \equiv 1 \pmod 4$, 存在整数a使得$p|a^2+1$.

证明 由于$(p-i) \equiv -i \pmod p$对任意$i = 1, ..., \frac{p-1}{2}$成立. 因为$p \equiv 1 \pmod 4$, 故

$$(p-1)! \equiv ((\frac{p-1}{2})!)^2(-1)^{\frac{p-1}{2}} \equiv ((\frac{p-1}{2})!)^2 \pmod p.$$

结合Wilson定理知

$$((\frac{p-1}{2})!)^2 \equiv -1 \pmod p,$$

即$p|((\frac{p-1}{2})!)^2+1$. 因此取$a = (\frac{p-1}{2})!$.

应用举例-2

例2. 对任意整数a, 有

$$a^9 \equiv a^3 \pmod{7 \times 8 \times 9}.$$

证明 需要分别证明三个同余式

$$a^9 \equiv a^3 \pmod{7}, \tag{1}$$

$$a^9 \equiv a^3 \pmod{8} \tag{2}$$

和

$$a^9 \equiv a^3 \pmod{9} \tag{3}$$

成立.

应用举例-2

- 由**Fermat**小定理直接有$a^7 \equiv a \pmod 7$. 所以**(1)**成立.
- 证明**(2)**需分a奇和a偶两种情形. 在奇情形, 由

$$a^2 \equiv 1 \pmod 8$$

立得; 偶情形则直接验证.

- 证明**(3)**按a模**3**的余数分三种情形,一种直接验证, 两种由**Euler**定理得到.

应用举例-3

例3. 求方程$x^2+y^2=z^2$的整数解.

解 首先简化为这种特殊情形：

$$x>0,y>0,z>0,x,y,z\text{两两互素}.$$

因此x,y,z必须两奇一偶，通过考察用4 除的余数知z奇，不失一般性可设x偶，y奇.

所以将方程变形为

$$x^2=z^2-y^2$$

$$(\frac{x}{2})^2=(\frac{z+y}{2})(\frac{z-y}{2})$$

但由$(z,y)=1$可知$(\frac{z+y}{2},\frac{z-y}{2})=1$.

应用举例–3

进一步有

$$\frac{z+y}{2}=a^2,\frac{z-y}{2}=b^2,x=2ab.$$

所以可得解为

$$x=2ab,y=a^2-b^2,z=a^2+b^2,$$

其中$(a,b)=1$.要得全部整数解, 可乘任意整数.

孙子定理

在《孙子算经》里提出过以下问题：

今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？

这本质上就是要求解不同模的同余式组

$$x \equiv a_1 \pmod{m_1}, \cdots, x \equiv a_n \pmod{m_n}. \tag{4}$$

孙子定理

中国古人的贡献是找到一种有效的解法，即**孙子定理**(中国剩余定理).

孙子定理

设$m_1, m_2, ..., m_n$两两互素，$m = m_1 \cdots m_n$，$M_i = \frac{m}{m_i}$，则同余式组(4)的解是

$$x \equiv a_1 M_1 M_1' + \cdots + a_n M_n M_n' \pmod{m},$$

其中

$$M_i M_i' \equiv 1 \pmod{m_i}, i = 1, 2, \cdots, n.$$

孙子定理的证明

证明：首先注意到若整数a是同余式组的一个解，那么同余式组就可变为

$$\begin{cases} x-a\equiv 0 \pmod{m_1} \\ \cdots \\ x-a\equiv 0 \pmod{m_n}, \end{cases}$$

于是整个解为$x\equiv a \pmod{M}$

强烈建议

请与线性方程相应理论比较

孙子定理的证明

接下来就是想法找到一个特解。首先考虑n个特殊情形，即

$$\begin{cases} x \equiv 0 \pmod{m_1} \\ \cdots \\ x \equiv a_i \pmod{m_i} \\ \cdots \\ x \equiv 0 \pmod{m_n}, \end{cases}$$

其中$i = 1, ..., n$. 只要将这n个解相加即可得出**(4)**的解.

孙子定理的证明

对$i \in \{1, ..., n\}$，继续简化为：

$$\begin{cases} x \equiv 0 \pmod{m_1} \\ \cdots \\ x \equiv 1 \pmod{m_i} \\ \cdots \\ x \equiv 0 \pmod{m_n}. \end{cases}$$

孙子定理的证明

最后简化为：

$$\begin{cases} x \equiv 1 \pmod{m_i} \\ x \equiv 0 \pmod{M_i}. \end{cases} \tag{5}$$

(5)又可以写为: $M_i y \equiv 1 \pmod{m_i}$. 有解性由$(m_i, M_i) = 1$保证. 当得到最后一个的解$M_i'$, 倒回去即得定理的证明.

孙子定理的解读

证明思想简单说来就是：

$$(a_1, ..., a_n) = a_1(1, 0, ..., 0) + \cdots a_n(0, ...0, 1)$$

定理内容简单说来就是对不同的i,模m_i的信息是互相独立的，合起来就是模M的信息

应用举例-1

例1. 求$76^{2009}+25^{2009}$的最后两位数字.

解 由

$$\begin{cases} 76 \equiv 0 \pmod 4 \\ 76 \equiv 1 \pmod{25}, \end{cases}$$

知$76^2 \equiv 76 \pmod{100}$. 同理$25^2 \equiv 25 \pmod{100}$.

应用举例-1

故

$$76^{2009} + 25^{2009} \equiv 76 + 25 \equiv 1 \pmod{100},$$

因此, 最后两位数字是**0**和**1**.

实际上**76**和**25**就是通过$x^2 \equiv x \pmod{100}$解出的.

应用举例-2

例2 解方程

$$\begin{cases} x \equiv 2 \pmod 4, \\ x \equiv 3 \pmod{25}. \end{cases}$$

解 由定理知解为

$$x \equiv 2 \times 25 + 3 \times 76 \equiv 78 \pmod{100}$$

应用举例-3

例3. 求1000以内的一个非负整数x使得

$$x \equiv 1 \pmod 7, x \equiv 2 \pmod{11}, x \equiv 9 \pmod{13}$$

韩信点兵的故事

练习1

求正整数n满足

$$n-1|n^3+n+1 \tag{6}$$

解法

解法一： $n^3+n+1=(n-1)(n^2+n+2)+3$，故由条件可知$n-1|3$，可知$n=2,4$.

解法二： $n^3+n+1=n^3-1+n-1+3=(n-1)(*)+3$，接方法一。

解法三： 由于$n\equiv 1 \pmod{n-1}$，因此$n^3+n+1\equiv 1^3+1+1\equiv 3 \pmod{n-1}$，条件等价于$n-1|3$，接方法一。

解法二比解法一少计算了一些无用的量，解法三把解法二的想法规范了。

练习2

哪些正整数n满足$2n-1|n^3+1$.

分析：该题出现了新困难，不知$n \equiv ?\pmod{2n-1}$，只知道$2n \equiv 1 \pmod{2n-1}$.故先将条件化为$2n-1|8(n^3+1)=(2n)^3+8$，
但$(2n)^3+8 \equiv 1^3+8 \equiv 9 \pmod{2n-1}$，因此$2n-1|9$

练习3

哪些正整数m,n满足$mn-1|n^3+1$.

分析：本题比上题复杂得多，因为2换成了一个未知数m. 用类似上题的方法得$mn-1|n^3+1 \Longrightarrow mn-1|m^3(n^3+1)=m^3+(mn)^3\equiv m^3+1 \pmod{mn-1}$，即

$$mn-1|n^3+1 \Longleftrightarrow mn-1|m^3+1$$

说明条件中m与n有同等的地位，不妨设$m\geq n$，这就意味着

练习3

$$\frac{n^3+1}{mn-1} \leq n$$

另外因为$n^3+1 \equiv 1 \pmod{n}, mn-1 \equiv -1 \pmod{n}$，故

$$\frac{n^3+1}{mn-1} \equiv \frac{1}{-1} = -1 \pmod{n}$$

（这一步推理不严格，请同学们自己把它严格化，同时想想不严格在什么地方）所以

$$\frac{n^3+1}{mn-1} = n-1$$

小结

本题的难度大了不少，但基本思想只多了一个：同余关系加上一个不等式可精确确定一个整数.

思考题**1**：$\frac{a^2+b^2}{ab+1}$若为整数，则必为平方数。

思考题**2**：把一个正整数n的十进制表示的各位数字相加得一个新的数，叫$f(n)$，现在从4444^{4444}出发，不断地做$f(n)$运算，依次得出A, B, C

$$4444^{4444} \longrightarrow A \longrightarrow B \longrightarrow C$$

求C

练习1

对非正整数a, b, c，有

$$\frac{(a,b)(b,c)(c,a)}{(a,b,c)^2} = \frac{[a,b][b,c][c,a]}{[a,b,c]^2}$$

分析：这是算术基本定理的标准应用，只要假设

$$a = p_1^{\alpha_1} \cdots$$

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

$$c = p_1^{\gamma_1} \cdots$$

需证的结论变为对任意非负整数α, β, γ有

$$\min(\alpha,\beta)\min(\beta,\gamma)\min(\alpha,\gamma) - 2\min(\alpha,\beta,\gamma) =$$

练习1

不失一般性，可设$\alpha \leq \beta \leq \gamma$，容易验证两边都是$2\beta$.

练习2

若整数a, b, c满足$(a, b, c) = 1$，则

$$(a, bc) = (a, b)(a, c)$$

同余方程的定义

方程

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \equiv 0 \pmod{m}$$

叫作模m的同余方程，这里所有系数a_i是整数，m是正整数，$a_n \not\equiv 0 \pmod{m}$，称$n$是方程的次数．现在我们讨论同余方程的解数和解法．当然我们谈论解数时是在一个剩余系中去数，或说是模m的剩余类的个数。

一次同余方程

定理2.5.1

一次同余方程

$$ax \equiv b \pmod{m}, a \not\equiv 0 \pmod{m}$$

有解的充分必要条件是$(a, m) \mid b$. 若有解, 则解的个数为$d = (a, m)$.

高次同余方程

本节我们讨论高次同余方程的解数和解法. 基本方法是先把合数模的同余式化成素数模的同余式, 然后讨论素数模的同余式的解法.

高次同余方程

定理2.5.2

设$m = p_1^{l_1} \cdots p_r^{l_r}$，那么方程

$$f(x) \equiv 0 \pmod{p_i^{l_i}}, i = 1, \cdots, r \tag{7}$$

与

$$f(x) \equiv 0 \pmod{m} \tag{8}$$

等价.并且若(9)有n_i个解，$i = 1, ..., r$，那么(8) 有$n_1 \cdots n_r$个解.

高次同余方程

证明 先证(9)与(8)等价. 利用同余的性质和$p_1, \cdots, p_r$两两互素可推得等价.

利用孙子定理可得(9)与(8)的解数.

Hensel引理

由于

$$f(x) \equiv 0 \pmod{p^l} \Longrightarrow f(x) \equiv 0 \pmod{p^{l-1}},$$

因此我们在解方程$f(x) \equiv 0 \pmod{p^l}$时，应该逐次解

$$f(x) \equiv 0 \pmod{p}, f(x) \equiv 0 \pmod{p^2}, ...$$

Hensel引理

著名的**Hensel引理**说从$f(x) \equiv 0 \pmod{p}$的一个好的解可以提升得到$f(x) \equiv 0 \pmod{p^l}$的一个解.

Hensel引理

Hensel引理

如果整数a_0满足$f(a_0) \equiv 0 \pmod{p}$，而$f'(a_0) \not\equiv 0 \pmod{p}$，则存在唯一的整数序列$a_1, a_2, \ldots$，$0 \leq a_i \leq p-1$使对任意$l > 1$，以下方程**(3)**

$$\begin{cases} f(x) \equiv 0 \pmod{p^l} \\ x \equiv a_0 \pmod{p} \end{cases}$$

有唯一解$x \equiv a_0 + a_1 p + \cdots + a_{l-1} p^{l-1} \pmod{p^l}$.

Hensel引理的证明

证明 思路就是逐次解方程

$$f(x) \equiv 0 \pmod{p^l}, l = 2, 3, ...$$

记$x = a_0 + px_1$，代入方程$f(x) \equiv 0 \pmod{p^2}$得

$$f(a_0 + px_1) \equiv f(a_0) + f'(a_0)px_1 \equiv 0 \pmod{p^2},$$

Hensel引理的证明

因此

$$f'(a_0)x_1 \equiv -\frac{f(a_0)}{p} \pmod{p}.$$

该方程有唯一解，记为$x_1 \equiv a_1 \pmod{p}$. 从而得到方程(3)在$l = 2$时的唯一解

$$x \equiv a_0 + a_1 p \pmod{p^2}.$$

Hensel引理的证明

递归地解方程, 若解出

$$x \equiv \alpha_{l-2} = a_0 + a_1 p + \cdots + a_{l-2} p^{l-2} \pmod{p^{l-1}}$$

为

$$\begin{cases} f(x) \equiv 0 \pmod{p^{l-1}} \\ x \equiv a_0 \pmod{p} \end{cases}$$

的解.

Hensel引理的证明

设$x = \alpha_{l-2} + p^{l-1}x_{l-1}$, 代入$(3)$式并化简得

$$f'(\alpha_{l-2})x_{l-1} \equiv -\frac{f(\alpha_{l-2})}{p^{l-1}} \pmod{p}$$

也有唯一解$x_{l-1} \equiv a_{l-1} \pmod{p}$ (因为$f'(\alpha_{l-2}) \equiv f'(a_0) \not\equiv 0 \pmod{p}$), 由此得到$(3)$的唯一解

$$x \equiv \alpha_{l-2} + p^{l-1}a_{l-1} = a_0 + a_1 p + \cdots + a_{l-1}p^{l-1} \pmod{p^l}.$$

应用举例

例1. 解方程$x^2 - x \equiv 0 \pmod{100}$

解 先解$x^2 - x \equiv 0 \pmod{4}$**和**$x^2 - x \equiv 0 \pmod{25}$**，分别得到**

$$x \equiv 0, 1 \pmod{4}$$

和

$$x \equiv 0, 1 \pmod{25}.$$

再通过孙子定理得到四个解$x \equiv 0, 1, 76, 25 \pmod{100}$

应用举例

例2. 解同余方程

$$7x^4 + 19x + 25 \equiv 0 \pmod{27}$$

解 先解

$$7x^4 + 19x + 25 \equiv 0 \pmod{3}$$

易知有唯一解$x \equiv 1 \pmod{3}$**.**

应用举例

令$x = 1 + 3y$, 代入

$$7x^4 + 19x + 25 \equiv 0 \pmod 9 \tag{4}$$

并化简得

$$6 + 6y \equiv 0 \pmod 9,$$

即$y \equiv 2 \pmod 3$. 那么(4)的解为$x \equiv 7 \pmod 9$.

应用举例

再设$x = 7 + 9z$, 代入原方程并化简得

$$18 + 9z \equiv 0 \pmod{27},$$

解得$x \equiv 1 \pmod{3}$. 因此原方程有唯一解

$$x \equiv 16 \pmod{27}.$$

应用举例

例3，对任意1到$p-1$之间的任意a，下列同余方程

$$x^{p-1} \equiv 1 \pmod{p^2}$$

有唯一的满足条件$x \equiv a \pmod{p}$，且解可以表为a^p

拉格朗日定理

本讲主要介绍模素数的同余方程.

拉格朗日定理

方程$f(x) \equiv 0 \pmod{p}$解数不超过$f(x)$的次数$\deg f$.

拉格朗日定理的证明

这个定理的证明与通常证明一个数域上的代数方程相应结论是一样的. 因为

$$ab \equiv 0 \pmod{p} \Longrightarrow a \equiv 0 \text{或} b \equiv 0 \pmod{p},$$

对任意整系数多项式$f(X), g(X)$, 有

$$f(x)g(x) \equiv 0 \pmod{p} \Rightarrow f(x) \equiv 0 \text{或} g(x) \equiv 0 \pmod{p}. \tag{9}$$

拉格朗日定理的证明

令A_f 表示$f(x) \equiv 0 \pmod{p}$的解的集合, 由**(9)**则有

$$A_{f\cdot g} = A_f \cup A_g.$$

$$|A_{f\cdot g}| \leq |A_f| + |A_g|.$$

另一方面, 由于任何$f(X)$总可表为

$$f(X) = (X-a)g(X) + f(a).$$

拉格朗日定理的证明

故从$f(a) \equiv 0 \pmod{p}$可推出存在$g(X)$，使得

$$f(X) \equiv (X-a)g(X) \pmod{p}.$$

用以上两点通过归纳法可得定理证明.

注记 若$f(x) \equiv 0 \pmod{p}$恰有$\deg f$个根，那么对任意$g(x) \mid f(x)$，都有$g(x) \equiv 0 \pmod{p}$ 的解数等于$\deg g$.

拉格朗日定理

下面利用拉格朗日定理重证**Wilson**定理.

由**Fermat**小定理知$x^{p-1}-1\equiv 0 \pmod p$有$p-1$个根$1,2,...,p-1$, 再用拉格朗日定理知必有

$$X^{p-1}-1\equiv (X-1)(X-2)\cdots(X-(p-1)) \pmod p.$$

比较常数项知

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

模素数的同余方程

定理

对正整数$d|p-1$，有

(1)方程$x^d - 1 \equiv 0 \pmod{p}$恰有$d$个根；

(2)对给定整数a，若存在b满足$a \equiv b^d \pmod{p}$，则称a是模p的d次剩余.

$$a\text{是}d\text{次剩余} \iff a^{\frac{p-1}{d}} \equiv 1 \pmod{p}.$$

模素数的同余方程

证明 **(1)** 因为$x^{p-1}-1\equiv 0 \pmod p$有$p-1$个根，而$x^d-1$是$x^{p-1}-1$的因子，由注记立得

$$x^d-1\equiv 0 \pmod p$$

的根数亦为次数，即d.

模素数的同余方程

证明 (2) 先证$\Longrightarrow$. 若$a \equiv b^d$, 则$a^{\frac{p-1}{d}} \equiv b^{p-1} \equiv 1 \pmod{p}$.

然后证明满足两边条件的数（在一个剩余系内）一样多. 由**(1)**已知右边的有$\frac{p-1}{d}$个. 为了数左边的个数, 写出全部d次剩余

$$1^d, 2^d, ..., (p-1)^d,$$

这$p-1$个列出的对象并不表示$p-1$个剩余类.

模素数的同余方程

因为对任意b, 满足$x^d \equiv b^d \pmod{p}$的x恰有d个类$x \equiv b\alpha_i, i = 1, ..., d$, 这里$\alpha_i$表$x^d - 1 \equiv 0 \pmod{p}$的那$d$个根. 说明

$$1^d, 2^d, ..., (p-1)^d$$

中每d个同余, 那么d次剩余一共是$\frac{p-1}{d}$个.

特别地, 当$d = 2$时, 我们称(2)式的判别法为欧拉判别法.

定义

定义

设整数a和m满足$(a,m)=1$，称a是模m的**原根**，如果$a^i, i=1,...,\phi(m)$正好构成模m的一个剩余缩系.换句话说：若a模m的阶是$\phi(m)$则称a是模m的原根.

原根

问题

对什么整数m，原根存在？若存在，如何判别和寻找？

原根

首先回顾以下命题.

命题

设整数$(a,m)=1$, 那么a模m的阶是n的充分必要条件是

1) $a^n \equiv 1 \pmod{m}$,

2) 对n的任一素因子q, 有$a^{\frac{n}{q}} \not\equiv 1 \pmod{m}$.

原根

特别地有,

命题

设有互素的整数a和m, 那么a是模m的原根的充分必要条件是: 对$\phi(m)$的任一素因子q, 有$a^{\frac{\phi(m)}{q}} \not\equiv 1 \pmod{m}$.

模p的原根的存在性

定理

模素数p的原根的存在.

我们用不同的方法证明. 只证明梗概, 细节由大家作为练习.

模p的原根的存在性

方法一 记A表一个模p的剩余缩系，A_d表A中阶为d的元的集合，那么

$$A = \bigcup_{d|p-1} A_d.$$

所以

$$|A| = \sum_{d|p-1} |A_d| \qquad (1).$$

我们将会看到$|A_d| = \phi(d)$.

模p的原根的存在性

只要存在元素a的阶为d，则方程$x^d \equiv 1 \pmod{p}$恰有d个解，于是可数出全体d阶元个数为$\phi(d)$. 可以得出

$$|A_d| > 0 \Longrightarrow |A_d| = \phi(d),$$

即$|A_d| = 0$或$\phi(d)$，总之$|A_d| \leq \phi(d)$.

模p的原根的存在性

于是由**(1)**有

$$p-1=\sum_{d|p-1}|A_d|\leq\sum_{d|p-1}\phi(d)=p-1.$$

说明$|A_d|=\phi(d)$, 即阶为任意$d|p-1$的都有$\phi(d)$个, 原根也一定有$\phi(p-1)$个.

模p的原根的存在性

方法二 设$p-1$的标准分解式为$p-1=p_1^{l_1}\cdots p_r^{l_r}$，若$a_i$的阶为$p_i^{l_i}$，那么$a_1\cdots a_r$的阶为$p-1$. 先用拉格朗日定理证明存在阶为$p_i^{l_i}$的元. 因为由$p_i^{l_i}|p-1$，用拉格朗日定理可知: 对$d=p_i^{l_i}$，同余式

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

恰有d个解.

模p的原根的存在性

说明一定有元素满足

$$x^{p^{l_i}} \equiv 1 \pmod{p}$$

且

$$x^{p^{l_i-1}} \not\equiv 1 \pmod{p}.$$

这就是我们要的阶为$p_i^{l_i}$的元a_i.

模素数幂的原根存在性

当$p = 2$时, 模2^2的原根存在, 但当$l > 2$时, 不存在模2^l的原根. 因为对任意奇数a有

$$a^{2^{l-2}} \equiv 1 \pmod{2^l}.$$

模素数幂的原根存在性

定理

若p为奇素数，$l > 1$，a是一整数，则a是模p^l的原根当且仅当下列两条同时成立

1) **a是模p的原根；**

2) $a^{p-1} \not\equiv 1 \pmod{p^2}$.

模素数幂的原根存在性

- 对$l > 1$, a是模p^l的原根等价于a是模p^2的原根.
- 保证了模p^2 的原根存在性, 因为对满足**1)**的a总可取适当的t**(**$p-1$种取法**)**使得

$$(a+tp)^{p-1} \not\equiv 1 \pmod{p^2}.$$

- 特别地, a和$a+p$必有一个满足**2).**
- 给出了寻找原根的方法. 先找模p的原根a, 再用a和$a+p$检查条件**2).**

模素数幂的原根存在性

先看例子，下讲介绍证明.

例1. 求模25的原根.

解 先找模**5**的原根**2**，计算知$2^4 \equiv 16 \not\equiv 1 \pmod{25}$，故$2$是模**25**的原根. 利用**Hensel**引理可知，$2+5t$（$t=0,1,2,3,4$）中恰有一个不是模**25**的原根.

模素数幂的原根存在性

例2.

$$1/7 = 0.\dot{1}42857\dot{}$$

$$2/7 = 0.\dot{2}85714\dot{}$$

$$3/7 = 0.\dot{4}28571\dot{}$$

$$\cdots$$

如何解释这个现象？根本原因是：10是模7的原根.

模素数幂的原根存在性的证明

本讲先介绍证明上讲定理需要用到的引理.

引理1.

设p为素数, n是正整数, 则

$$a \equiv b \pmod{p^n} \Longrightarrow a^p \equiv b^p \pmod{p^{n+1}}.$$

Proof.

利用二项式定理即可证明. □

模素数幂的原根存在性的证明

引理2.

设p为素数，n是正整数，则有

$$a\text{是模}p^{n+1}\text{的原根} \Longrightarrow a\text{是模}p^{n}\text{的原根}.$$

模素数幂的原根存在性的证明

Proof.

若a不是模p^n的原根, 则有正整数$r < \phi(p^n)$, 满足

$$a^r \equiv 1 \pmod{p^n}.$$

再由引理**1.** 知

$$a^{rp} \equiv 1 \pmod{p^{n+1}},$$

而$rp < p\phi(p^n) = \phi(p^{n+1})$与$a$是模$p^{n+1}$的原根矛盾. □

模素数幂的原根存在性的证明

引理3.

设p为奇素数，n是正整数，若$(a,p)=(b,p)=1$，则

$$a^p \equiv b^p \pmod{p^{n+1}} \Longrightarrow a \equiv b \pmod{p^n}.$$

模素数幂的原根存在性的证明

Proof.

记设$p^r||a-b$. 设

$$a = b + tp^r, t \not\equiv 0 \pmod{p}.$$

所以有

$$a^p = (b+tp^r)^p \equiv b^p + tb^{p-1}p^{r+1} \pmod{p^{r+2}}.$$

由于$tb^{p-1} \not\equiv 0 \pmod{p}$, 上式意味着$p^{r+1}||a^p - b^p$. 结合$a^p \equiv b^p \pmod{p^{n+1}}$知$r+1 \geq n+1$, 即$r \geq n$.

□

模素数幂的原根存在性的证明

定理

若p为奇素数，$l>1$，a是一整数，则a是模p^l的原根当且仅当下列两条同时成立

1) a**是模**p**的原根；**

2) $a^{p-1}\not\equiv 1 \pmod{p^2}$**.**

证明 先证必要性. 假设a是模p^n的原根，由引理2 已知a是模p^2的原根，那么也是模p的原根. 由a是模p^2的原根可得出条件2).

模素数幂的原根存在性的证明

充分性. 要证a是模p^n的原根, 即证对$\phi(p^n) = p^{n-1}(p-1)$的任一素因子q, 均有

$$a^{\frac{p^{n-1}(p-1)}{q}} \not\equiv 1 \pmod{p^n}.$$

不停地用引理3知这等价于$n = 2$的情形，即：

模素数幂的原根存在性的证明

$$a^{\frac{p(p-1)}{q}} \not\equiv 1 \pmod{p^2}.$$

$q = p$时就变成条件**2)**，而$q|p-1$时，（继续用引理**3**知）这就变成

$$a^{(p-1)/q} \not\equiv 1 \pmod{p}.$$

这恰好由条件**1**）保证。

模任意整数的情形

命题1.

设$m_1, ..., m_k$是两两互素的整数，整数a模m_i的阶是r_i，则a模$m_1 \cdots m_k$的阶是$[r_1, ..., r_k]$.

模任意整数的情形

Proof.

对整数n,

$$a^n \equiv 1 \pmod{m_1 \cdots m_k} \Longleftrightarrow a^n \equiv 1 \pmod{m_i}\text{对每个}i\text{成立}$$

$$\Longleftrightarrow r_i | n\text{对每个}i\text{成立} \Longleftrightarrow [r_1, ..., r_k] | n.$$

故a模$m_1 \cdots m_k$的阶是$[r_1, ..., r_k]$ □

模任意整数的情形

推论1.

设$m_1, ..., m_k$是两两互素的整数，整数a是模$m_1 \cdots m_k$的原根当且仅当对每个i，a是模m_i的原根，且$\phi(m_i)$两两互素.

模任意整数的情形

Proof.

设a模m_i的阶是r_i，于是a模$m_1 \cdots m_k$的阶是

$$[r_1, ..., r_k] \leq r_1 \cdots r_k \leq \phi(m_1) \cdots \phi(m_k) = \phi(m).$$

因此a是模$m_1 \cdots m_k$的原根当且仅当$r_i = \phi(m_i)$，且$\phi(m_i)$两两互素.

模任意整数的情形

定理2.

模m的原根存在当且仅当m是以下几类之一：**2, 4,** p^l**,** $2p^l$**.**

指数

定义

设g是模m的原根，$(a,m)=1$，则存在唯一整数d，满足$0 \le d < \phi(m)$和$g^d \equiv a \pmod{m}$，称d为a对g的**指数**（或离散对数），记为$\mathrm{ind}_g a$，有时可简单记为$\mathrm{ind}a$.

指数

指数有以下性质：

$$\mathbf{ind}ab \equiv \mathbf{ind}a + \mathbf{ind}b \pmod{\phi(m)}.$$

$$\mathbf{ind}a^n \equiv n\mathbf{ind}a \pmod{\phi(m)}.$$

对$d|\phi(m)$，有a是模m的d次剩余当且仅当$d|\mathbf{ind}a$，特别地对奇素数p，有：

a是模p的2次剩余当且仅当$2|\mathbf{ind}a$.

定义

设p为奇素数，与p互素的a称为模p的二次剩余，如果方程

$$x^2 \equiv a \pmod{p} \tag{1}$$

有解；若(1)无解，则称a是模p的非二次剩余.

欧拉判别条件

定理1 (欧拉判别条件)

若$(a,p)=1$, 那么

$$a\text{是二次剩余} \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

并且

$$a\text{是非二次剩余} \iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \tag{2}$$

勒让德符号

勒让德符号

勒让德符号$(\frac{a}{p})$是对于给定的奇素数p定义在一切整数a上的函数，规定：

$$\left(\frac{a}{p}\right)=\begin{cases}1, a\text{是模}p\text{二次剩余}\\ -1, a\text{是模}p\text{非二次剩余}\\ 0, p\mid a\end{cases}$$

勒让德符号的性质

- $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$
- $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$
- $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$
- $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$

二次互反律

二次互反律

对不同的奇素数p和q，有

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

等价地

$$\left(\frac{q}{p}\right)=\begin{cases}\left(\frac{p}{q}\right), & p\equiv 1 \pmod 4 \text{或} q\equiv 1 \pmod 4;\\ -\left(\frac{p}{q}\right), & p\equiv q\equiv 3 \pmod 4\end{cases}$$

例子

计算$(\frac{5}{353})$.

解 因为

$$(\frac{5}{353}) = (\frac{353}{5}) = (\frac{3}{5}) = -1.$$

故5是模353的非二次剩余.

Gauss引理

接下来主要证明二次互反律, 采用**Gauss**的初等证明, 这需要一个关键的**Gauss**引理**(**不仅是结论, 包括思想**)**. 我们从计算$(\frac{2}{p})$开始, 它的思想非常有启发性。我们先从计算具体的$(\frac{2}{13})$开始. 由**Euler**判别法知只只需计算$2^6 \equiv ?\pmod{13}$.

Gauss引理

记$A=\{1,2,3,4,5,6\}$，当然$A\bigcup(-A)$是一剩余缩系.

$$2A=\{2,4,6,8,10,12\}\equiv\{2,4,6,-5,-3,-1\}\pmod{13},$$

因此

$$2^6\prod_{i\in A}i=\prod_{i\in 2A}i\equiv(-1)^3\prod_{i\in A}i\pmod{13}$$

故$2^6\equiv-1\pmod{13}$. 这样$(\frac{2}{13})=-1$.

Gauss引理

记$A = \{1, 2, ..., \frac{p-1}{2}\}$, 模$p$有两个最简单的缩系:

$$\{1, 2, ..., p-1\} = A \bigcup (p - A)$$

和

$$A \bigcup (-A).$$

Gauss引理

设$2A = \{x_1, ..., x_s, y_1, ..., y_t\}$，其中

$$x_1 < \cdots < x_s < \frac{p}{2} < y_1 < \cdots < y_t$$

$$A = \{x_1, ..., x_s, p - y_1, ..., p - y_t\}.$$

简单理由：$A \bigcup (-A)$是一个模p的剩余缩系，$2A \bigcup (-2A)$也是。

Gauss引理

于是

$$\prod_{i\in A} i \equiv (-1)^t x_1 \cdots x_s y_1 \cdots y_t \pmod{p}.$$

另一方面，

$$2^{\frac{p-1}{2}} \prod_{i\in A} i = \prod_{i\in 2A} i = x_1 \cdots x_n y_1 \cdots y_m \pmod{p}.$$

Gauss引理

综上两式知

$$2^{\frac{p-1}{2}} \equiv (-1)^t,$$

即$(\frac{2}{p}) = (-1)^t$. t是$2A$中$> \frac{p}{2}$的元的个数, 即A中$> \frac{p}{4}$的元的个数.

Gauss引理

因此

$$t = [\frac{p}{2}] - [\frac{p}{4}] \equiv \frac{p^2-1}{8} \pmod 2,$$

所以

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}.$$

这样我们就证明了勒让德符号的一个重要性质. 我们继续证明Gauss引理.

Gauss引理

- 称集合$A = \{a_1, ..., a_{\frac{p-1}{2}}\}$为模$p$的一个半系，若$A \bigcup (-A)$是一剩余缩系.
- 对任意$a \not\equiv 0 \pmod{p}$，aA仍是半系.
- $aa_i \equiv \varepsilon_i b_i \pmod{p}, \varepsilon_i = \pm 1, b_1, ..., b_{\frac{p-1}{2}}$为$a_1, ..., a_{\frac{p-1}{2}}$的一个置换.

Gauss引理

因此，考察 $\prod_{i\in aA} i$ 可得

$$a^{\frac{p-1}{2}} \equiv \varepsilon_1 \cdots \varepsilon_{\frac{p-1}{2}} \equiv (-1)^m,$$

这里m为$\varepsilon_1, ..., \varepsilon_{\frac{p-1}{2}}$中$-1$的个数，即在模$p$下$aA$与$-A$相交的元素个数.

Gauss引理

Gauss引理

设A为模p的一个半系，$a \not\equiv 0 \pmod{p}$，$aA = \{x_1, ..., x_s, y_1, ..., y_t\}$，其中$\{x_1, ..., x_s\}$同余于$A$的一个子集，$\{y_1, ..., y_t\}$同余于$-A$的一个子集. 则

$$(\frac{a}{p}) = (-1)^t.$$

Gauss引理

取$A = \{1, 2, ..., \frac{p-1}{2}\}$, 得到如下特殊形式的**Gauss引理**

Gauss引理

设$a, 2a, ..., \frac{p-1}{2}a$这些数对$p$的最小非负剩余中$> \frac{p}{2}$的个数为$t$, 则

$$(\frac{a}{p}) = (-1)^t.$$

Gauss引理

例子:用Gauss引理计算$(\frac{3}{13})$

令

$$A = \{1, 2, 3, 4, 5, 6\}.$$

那么

$$3A = \{3, 6, 9, 12, 15, 18\} \equiv \{3, 6, 9, 12, 2, 5\} \equiv \{3, 6, -4, -1, 2, 5\}.$$

考察$\prod_{i\in 3A} i$可知$3^6 \equiv (-1)^2 = 1 \pmod{13}$. 故$(\frac{3}{13}) = 1$.

练习：用Gauss引理计算$(\frac{3}{17})$

二次互反律的证明

首先我们利用Gauss引理计算$(\frac{3}{17})$.

1	2	3	4	5	6	7	8	π_1	S_1
3	6	9	12	15	18	21	24	π_2	S_2
3	6	9	12	15	1	4	7	π_3	S_3
1	3	4	6	7	9	12	15	π_4	S_4
1	3	4	6	7	8	5	2	π_5	S_5

其中π_i表示第i行前8个元素相乘，S_i表示第i行前8个元素相加.

二次互反律的证明

上表中，我们可得关系

$$3^8\pi_1 \equiv \pi_2 \equiv \pi_3 \equiv \pi_4 \equiv (-1)^3\pi_5 \pmod{p},$$

$$\pi_5 \equiv \pi_1 \pmod{p}.$$

所以

$$3^8 \equiv (-1)^3 = -1 \pmod{p}.$$

二次互反律的证明

计算一般的$(\frac{q}{p})$. 记$n = \frac{p-1}{2}$

1	2	3	4	$\cdots$	n	π_1	S_1
q	$2q$	$3q$	$4q$	$\cdots$	nq	π_2	S_2
r_1	r_2	r_3	r_4	$\cdots$	r_n	π_3	S_3
x_1	$\cdots$	x_s	y_1	$\cdots$	y_t	π_4	S_4
x_1	$\cdots$	x_s	$p-y_1$	$\cdots$	$p-y_t$	π_5	S_5

π_i表示第i行前n个元素相乘, S_i表示第i行前n个元素相加.

二次互反律的证明

利用Gauss引理可得

$$(\frac{q}{p}) \equiv q^{\frac{p-1}{2}} \equiv (-1)^t \pmod{p}.$$

即$(\frac{q}{p}) = (-1)^t$.只需计算$t \pmod 2$的值.

记

$$kq = pq_k + r_k, 0 < r_k < p.$$

二次互反律的证明

注意各行的S_i的关系

$$S_3 = S_4$$

$$S_1 = S_5$$

$$S_2 = qS_1 \equiv S_1 \pmod 2$$

$$S_5 \equiv S_4 + t \pmod 2$$

二次互反律的证明

因此

$$t \equiv S_2 - S_3 = \sum_{k=1}^{n} pq_k \equiv \sum_{k=1}^{n} q_k \pmod 2$$

改写为

$$t \equiv \sum_{k=1}^{\frac{p-1}{2}} [\frac{kq}{p}] \pmod 2,$$

二次互反律的证明

即

$$(\frac{q}{p}) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} [\frac{kq}{p}]}.$$

同理

$$(\frac{p}{q}) = (-1)^{\sum_{k=1}^{\frac{q-1}{2}} [\frac{kp}{q}]}.$$

二次互反律的证明

于是

$$(\frac{q}{p})(\frac{p}{q}) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]+\sum_{k=1}^{\frac{q-1}{2}}[\frac{kp}{q}]}.$$

剩下只需证

$$\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}] + \sum_{k=1}^{\frac{q-1}{2}}[\frac{kp}{q}] = \frac{p-1}{2}\frac{q-1}{2}.$$

二次互反律的证明

这只需要将长方形$\{(x,y)|0<x<\frac{p}{2},0<y<\frac{q}{2}\}$沿对角线$y=\frac{q}{p}x$分成两个三角形，分别数长方形内部的整点数目和两个三角形内部的整点数目就可以完成。

注意：对角线上无整点。

应用举例

例1. 判别3是否模23的原根.

解 $23-1=22$**有两个素因子2和11. 因为**

$$3^{22/11}=3^2\not\equiv 1 \pmod{23}$$

$$3^{22/2}\equiv(\frac{3}{23})=-(\frac{23}{3})=-(\frac{2}{3})=1 \pmod{23}$$

故3不是模23的原根.

应用举例

例2. 判别3是否模Fermat素数$p = 2^n + 1, n > 1$的原根.

解 $(\frac{3}{p}) = (\frac{p}{3}) = (\frac{2}{3}) = -1$ **即**$3^{\frac{p-1}{2}} \equiv -1 \pmod{p}$**. 由于**$p-1$**只有素因子2, 故3是模**$p$**的原根.**

推广的二次互反律

定义

设$n = p_1^{l_1} \cdots p_r^{l_r}$为奇数，则可对与$n$互素的$m$定义Jacobi符号$\left(\frac{m}{n}\right)$

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{l_1} \cdots \left(\frac{m}{p_r}\right)^{l_r}.$$

推广的二次互反律

Jacobi符号具有勒让德符号的相应的性质:

(1) 若$a \equiv b \pmod{n}$, 则$(\frac{a}{n}) = (\frac{b}{n})$

(2) $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$

(3) $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$

(4) $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$

(5) 推广的二次互反律 对互素的奇数m和n, 有

$$(\frac{m}{n})(\frac{n}{m}) = (-1)^{(\frac{m-1}{2})(\frac{n-1}{2})}.$$

推广的二次互反律

上述性质的证明都留作练习，此处仅证明**(3)**. 设$n = p_1^{l_1} \cdots p_r^{l_r}$，则**(3)**归结为证明

$$\frac{p_1^{l_1} \cdots p_r^{l_r} - 1}{2} \equiv l_1 \frac{p_1 - 1}{2} + \cdots + l_r \frac{p_r - 1}{2} \pmod 2.$$

从而归结为证明对任意奇数a, b有

$$\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod 2.$$

推广的二次互反律

用**Jacobi**符号，计算勒让德符号会更方便，因为算$(\frac{a}{p})$时不必分解a.

例如$(\frac{143}{353}) = (\frac{353}{143}) = (\frac{67}{143}) = -(\frac{143}{67}) = -(\frac{9}{67}) = -1.$

$$\begin{aligned}(\frac{129}{353}) &= (\frac{353}{129}) = (\frac{95}{129}) = (\frac{129}{95}) = (\frac{34}{95}) = (\frac{2}{95})(\frac{17}{95}) \\ &= (\frac{17}{95}) = (\frac{95}{17}) = (\frac{10}{17}) = (\frac{5}{17}) = (\frac{17}{5}) \\ &= (\frac{2}{5}) = -1.\end{aligned}$$

推广的二次互反律

例：证明若$n > 1$，则$2^n - 1$不整除$3^n - 1$.

首先，若n为偶数，显然成立（因$3|2^n - 1$）.下面设n奇。

若$2^n - 1|3^n - 1$，则

$$3^n \equiv 1 \pmod{2^n - 1}$$

计算Jacobi符号得出矛盾，因

$$(\frac{3^n}{2^n - 1}) = (\frac{3}{2^n - 1})^n = (\frac{3}{2^n - 1})$$

$$= -(\frac{2^n - 1}{3}) = -(\frac{1}{3}) = -1$$

特殊二次同余方程的解法

用二次互反律很容易判别二次同余方程

$$x^2 \equiv n \pmod{p} \tag{1}$$

是否有解，但如何解却不容易，在某些特殊情形下，解有某种表达式.

特殊二次同余方程的解法

定理1.

设p为奇素数，$(\frac{n}{p})=1$，则

1) 当$p\equiv 3 \pmod 4$时，方程(1)的解为

$$x\equiv \pm n^{\frac{p+1}{4}} \pmod p;$$

2) 当$p\equiv 5 \pmod 8$时，方程(1)的解为

$$x\equiv \begin{cases} \pm n^{\frac{p+3}{8}} \pmod p, \text{若} n^{\frac{p-1}{4}}\equiv 1 \pmod p \\ \pm n^{\frac{p+3}{8}}(\frac{p-1}{2})! \pmod p, \text{若} n^{\frac{p-1}{4}}\equiv -1 \pmod p. \end{cases}$$

特殊二次同余方程的解法

证明：1) 因$n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, 但$\frac{p-1}{2}$是奇数(加1后变成偶数), 故

$$n \equiv n^{\frac{p-1}{2}+1} = (\pm n^{\frac{p+1}{4}})^2 \pmod{p}$$

得出1)的解.

特殊二次同余方程的解法

2) 因为$n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, 但$\frac{p-1}{2}$是偶数, 不过只有一个2因子, 此时

$$n^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}.$$

分两种情形：若$n^{\frac{p-1}{4}} \equiv 1 \pmod{p}$, 因$\frac{p-1}{4}$是奇数, 故由**1)**的方法可得解为

$$x \equiv \pm n^{\frac{p+3}{8}} \pmod{p}.$$

特殊二次同余方程的解法

若$n^{\frac{p-1}{4}} \equiv -1 \pmod{p}$, 则

$$n \equiv -(n^{\frac{p+3}{8}})^2 \equiv (p-1)!\left(n^{\frac{p+3}{8}}\right)^2 \equiv \left(\frac{p-1}{2}!\right)^2 (n^{\frac{p+3}{8}})^2 \pmod{p}$$

从而得出方程2)的解.

特殊二次同余方程的解法

问题.

当$p-1=2^rk$，k奇，$r\geq 3$时，如何推广上述解法？如果已知一个非二次剩余b，利用b^k阶为2^r可以解相应的方程。请同学们思考。

特殊二次同余方程的解法

定理2.

设p为奇素数，$(\frac{n}{p}) = 1$，则对任意正整数l，方程

$$x^2 \equiv n \pmod{p^l} \tag{2}.$$

有两个解.

证明：由**Hensel**引理得到所要结论.

素数表平方和

定理3.

设p为素数，则p可表为平方和当且仅当$p = 2$或$p \equiv 1 \pmod 4$.

素数表平方和

定理4.

m^2+1形的数的素因子都是平方和.

素数表平方和

这个定理的证明只需要一个引理

Lemma

若$(x,y)=1$，称x^2+y^2为**本原平方和**. 如果一个本原平方和x^2+y^2的素因子p可表为平方和，则$\frac{x^2+y^2}{p}$也可表为本原平方和.

引理的证明

证明 设$p = a^2 + b^2$, 则

$$a^2 \equiv -b^2 \pmod{p}.$$

又有

$$x^2 \equiv -y^2 \pmod{p}.$$

于是

$$a^2x^2 \equiv b^2y^2 \pmod{p}.$$

从而$ax \equiv \pm by \pmod{p}$.

引理的证明

若$ax \equiv by \pmod{p}$(另一种情形同样证明), 则有

$$\frac{x^2+y^2}{p} = \frac{(a^2+b^2)(x^2+y^2)}{p^2} = \frac{(ax-by)^2+(ay+bx)^2}{p^2}$$
$$= (\frac{ax-by}{p})^2 + (\frac{ay+bx}{p})^2.$$

但$p|ax-by$和

$$p^2|(a^2+b^2)(x^2+y^2) = (ax-by)^2+(ay+bx)^2$$

知$p|ay+bx$.

引理的证明

因此$\frac{x^2+y^2}{p}$可表为平方和

$$(\frac{ax-by}{p})^2+(\frac{ay+bx}{p})^2.$$

现证明这种表示是本原的，若有$d|(\frac{ax-by}{p},\frac{ay+bx}{p})$，则

$$d|a\frac{ax-by}{p}+b\frac{ay+bx}{p}=x.$$

同理$d|y$. 由于$(x,y)=1$，故$d=1$. 所以表示是本原的.

定理4的证明

对m作归纳. $m=1$时显然成立. 假设对$<m$的整数成立. 任取素数$p|m^2+1$, 若$p<m$, 则由$p|(m-p)^2+1$和归纳假设知p是平方和.
若$p>m$, 则

$$\frac{m^2+1}{p}=p_1\cdots p_r<m,$$

当然每个$p_i<m$, 于是p_i是平方和, 再由引理可得$p=\frac{m^2+1}{p_1\cdots p_r}$是（本原）平方和.

定理3的证明

必要性是显然的.

由于$p \equiv 1 \pmod 4 \Longrightarrow$ 存在整数m, 有$p|m^2+1$.再由定理**4**可得.

Gauss整数环

记**Gauss**整数$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$. 可以验证$\mathbb{Z}[i]$中元素的加法和乘法性质和整数的情形类似, 我们称$\mathbb{Z}[i]$为**Gauss整数环**.

Gauss整数环

命题1.

$\mathbb{Z}[i]$上的单位(即可以求倒数的元)只有$\pm 1, \pm i$.

证明 设$a+bi$是$\mathbb{Z}[i]$上的单位, 则

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} \in \mathbb{Z}[i],$$

即

$$\frac{a}{a^2+b^2}, \frac{b}{a^2+b^2} \in \mathbb{Z}.$$

从而$a+bi = \pm 1, \pm i$.

Gauss整数环

定义

称α为$\mathbb{Z}[i]$上的**素元**，如果α的每一个因子β，都有β 或$\frac{\alpha}{\beta}$ 是单位.

Gauss整数环

对复数$\alpha = a + bi$，用$N(\alpha)$表$a^2 + b^2$.

定理1.

对任意$\alpha, \beta \in \mathbb{Z}[i]$，$\beta \neq 0$，存在$\gamma, \lambda \in \mathbb{Z}[i]$，满足

$$\alpha = \lambda\beta + \gamma \text{和} N(\gamma) < N(\beta);$$

换句话说，存在$\gamma \in \mathbb{Z}[i]$满足

$$\alpha \equiv \gamma \pmod{\beta} \text{和} N(\gamma) < N(\beta).$$

Gauss整数环

推论1.

对$\alpha, \beta \in \mathbb{Z}[i]$, 集合$\alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i]$一定形如$\gamma\mathbb{Z}[i]$

注记 这样的γ称为α和β的最大公因子, 它是集合$\alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i]$中$N(\gamma)$最小的(即复绝对值最小).

Gauss整数环

推论2.

($\mathbb{Z}[i]$上的唯一分解定理) $\mathbb{Z}[i]$上的任何非零元可唯一分解为“素元”之积.

注: 证明就是平推旧的证明(因为有带余除法).

Gauss整数环

定义

$a+bi \in \mathbb{Z}[i]$**称为本原的，若**a**与**b**互素.**

问题

任何一个**Gauss**整数可写为一个普通整数乘一个本原的**Gauss**整数，因此需问什么普通素数还是‘素的’，一个本原的**Gauss**整数何时是‘素的’**?**

Gauss整数环

命题2.

普通素数p是'素的'当且仅当p不是平方和.

证明：必要性, 因为若$p = a^2 + b^2$, 则$p = (a + bi)(a - bi)$.

充分性：若p不是'素的', 则$p = (a + bi)(c + di)$, 因而

$$p^2 = (a^2 + b^2)(c^2 + d^2), a^2 + b^2 > 1, c^2 + d^2 > 1.$$

说明$a^2 + b^2 = p = c^2 + d^2$, 矛盾.

Gauss整数环

命题3.

本原的Gauss整数$a+bi$是“素的”当且仅当a^2+b^2是素数.

Gauss整数的应用

现在我们利用**Gauss**整数的算术理论证明上讲定理.

定理

设p为素数, 则p可表为平方和当且仅当$p = 2$或$p \equiv 1 \pmod 4$.

Gauss整数的应用

证明 若$p|m^2+1=(m+i)(m-i)$, 显然

$$p\nmid m+i, p\nmid m+i.$$

由Gauss整数的唯一分解性知p不是‘素的’. 再由命题2 知p是平方和.

Gauss整数的应用

例1 在整数范围内解方程$y^2+1=x^3$.

解： 经过简单讨论知y为偶数. 将方程变形为

$$(y+i)(y-i)=x^3.$$

说明$y+i$与$y-i$“互素”. 若它们有公共“素因子”π, 则$\pi|2i=(1+i)^2$, 即$\pi=1+i$, 但因$y=2n=-i(1+i)^2n$, 故$y+i\equiv i\pmod{1+i}$, 说明$1+i\nmid y+i$. 综上, $y+i$与$y-i$“互素”.

Gauss整数的应用

由唯一分解定理知

$$y+i=u(a+bi)^3, u\text{是一单位}$$

由于所有单位$\pm 1, \pm i$都是某元的三次方，故可设

$$y+i=(a+bi)^3.$$

比较虚部知$1=3a^2b-b^3=b(3a^2-b^2)$. 说明$b=\pm 1$，进一步讨论知必须

$$b=-1, a=0.$$

原方程解为

$$x=1, y=0.$$

不定方程的解法

要证明某方程$f(x_1, ..., x_n) = 0$无整数解，一个常见的想法是找一个适当的m使

$$f(x_1, ..., x_n) \equiv 0 \pmod{m}$$

无解.

不定方程的解法

例1 求方程$x^2+y^2=3z^2$的非零整数解.

解法一： 假设有解，不妨设x,y,z两两互素，取$p=3$，将原方程模3得

$$x^2\equiv -y^2 \pmod 3,$$

从而得到-1是模3的二次剩余，不可能.

解法二： 取$p=2$，将原方程模2^2得

$$x^2+y^2+z^2\equiv 0 \pmod 4,$$

无解.

柯召方法

不定方程的柯召方法是柯先生在研究**Catalan**猜想时首创的.

Catalan猜想, 1842

8和9是仅有的两个连续正整数, 它们都是整数方幂.

柯召方法

用不定方程的语言描述: 当$m, n > 1$时, 方程

$$x^m + 1 = y^n$$

除了$m = 3, n = 2, x = 2, y = 3$以外没有其他的正整数解.

柯召方法

首先将Catalan猜想归结为看似特殊的方程

$$x^p + 1 = y^q,$$

其中p, q是不同的素数，再按p, q分成两类：

(1) p, q之一为2，

(2) p, q都是奇.

柯召方法

(1)的$p = 2$情形由**Lebesque**很快解决**(**只需在**Gauss**整环上进行即可**).**

(1)的$q = 2$情形, 即下述柯召方程

$$x^p + 1 = y^2. \tag{1}$$

其中$p = 3$的情形在猜想提出之前已解决, 剩下情形由柯召先生在**1962**年解决. 方法是完全初等的, 称为柯召方法.

柯召方法

在柯先生的工作之前, 数学大师**Selberg**(菲尔兹和沃尔夫双奖获得者)曾证明了较弱的情形, 即方程

$$x^p + 1 = y^4$$

无解. 在**2002**年, **Catalan**猜想的最后情形也解决了.

柯召方法

定理

方程

$$x^p + 1 = y^2 \tag{1}$$

没有满足$(x+1, \frac{x^p+1}{x+1}) > 1$**，** $p > 3$**的正整数解，**

注：$(x+1, \frac{x^p+1}{x+1}) = 1$的情形用其他方法证(先于我们这种情形解决)，我们这种情形代表了柯召方法的精华.

柯召方法

证明：由于$\frac{x^p+1}{x+1} \equiv p \pmod{x+1}$**，因此**$(x+1, \frac{x^p+1}{x+1}) = 1$**或**$p$**，故**$(x+1, \frac{x^p+1}{x+1}) = p$**. 但**

$$y^2 = (x+1)\frac{x^p+1}{x+1},$$

故有

$$x + 1 = py_1^2 \tag{2}$$

$$\frac{x^p+1}{x+1} = py_2^2. \tag{3}$$

柯召方法

由**1)**知x为偶数**(**否则y为偶数**,** 从而$(y+1, y-1) = 1$**,** 从而$y \pm 1$都是p次幂**,** 很容易得矛盾**),** 再结合**2)**知

$$x + 1 \equiv p \pmod 8 \qquad 4).$$

下面的主要思路是在原方程**1)**上造矛盾**,** 取适当的模$f(x)$对两边算**Jacobi**符号**,** 右边是**1,** 如果证明左边是-1即可**.**

柯召方法

(1)当$p \equiv 5, 7 \pmod 8$**时**

取模$f(x) = x - 1$**, 因**$x^p + 1 \equiv 2 \pmod{x-1}$**, 故**

$$(\frac{x^p+1}{x-1}) = (\frac{2}{x-1}) = (\frac{2}{p-2})$$

$$= -1, \text{当} p \equiv 5, 7 \pmod 8 \text{时}.$$

柯召方法

(2) 当$p \equiv 3 \pmod 8$**时**

取模$f(x) = x^3 - 1$**. 因**$p \equiv 1, 2 \pmod 3$**，故**$x^p + 1 \equiv x + 1$**或**$x^2 + 1 \pmod{x^3 - 1}$**. 注意**x**是偶数且**$x + 1 \equiv p \pmod 8$**，分别计算**

$$(\frac{x+1}{x^3-1}) = (-1)^{\frac{x+1-1}{2}}(\frac{x^3-1}{x+1}) = (\frac{-1}{x+1})(\frac{-2}{x+1}) = (\frac{2}{p}).$$

柯召方法

$$(\frac{x^2+1}{x^3-1}) = (\frac{x^3-1}{x^2+1}) = (\frac{-x-1}{x^2+1}) = (\frac{x+1}{x^2+1}) = (\frac{x^2+1}{x+1}) = (\frac{2}{p}).$$

即

$$(\frac{x^p+1}{x^3-1}) = (\frac{2}{p}) = -1.$$

柯召方法

(3) 当$p \equiv 1 \pmod 8$时，出现了新困难，因为如果想取另外的$x^a - 1$来模的话，计算发现（细节作为练习）

$$(\frac{x^p + 1}{x^a - 1}) = (\frac{2}{x \pm 1})$$

但此时$x \pm 1 \equiv \pm 1 \pmod 8$，从而有

$$(\frac{2}{x \pm 1}) = 1$$

那就需要新思路了。

柯召方法

现在转向方程3)造矛盾. 记

$$E(a) = \frac{(-x)^a - 1}{-x - 1}.$$

a为奇时$E(a) = \frac{x^a+1}{x+1}$. 取模$E(a)$计算Jacobi符号, 柯先生发现对$a < p$, 总有$(\frac{E(p)}{E(a)}) = 1$.但取适当的a, 可使

$$(\frac{py_2^2}{E(a)}) = (\frac{p}{E(a)}) = (\frac{E(a)}{p}) = (\frac{a}{p}) = -1$$

从而得到矛盾.

柯召方法

观察：因为对任意正整数m, n, t，只要$m \equiv n \pmod{t}$，就有

$$(-x)^m - 1 \equiv (-x)^n - 1 \pmod{(-x)^t - 1}.$$

从而

$$E(m) \equiv E(n) \pmod{E(t)}$$

$$(E(m), E(n)) = E((m, n)).$$

柯召方法

当$(m,n)=1$时，有

$$(E(m),E(n))=E(1)=1.$$

对$0<a<p$，有$(a,p)=1$，故可做辗转相除法．这样我们就能得到$(\frac{E(p)}{E(a)})=1$.

数论函数

称自变量取正整数的函数为数论函数. 常见数论函数:

- 取整函数$[\cdot]$. 具有以下性质:

(1) $[x+y] \geq [x]+[y]$

(2) 对整数n, 有$[x+n]=[x]+n$

(3) $[\frac{[\frac{x}{a}]}{b}]=[\frac{x}{ab}]$

数论函数

对任意整数a和素数p, 如果

$$a = p^l \cdot a', (a', p) = 1,$$

则定义$\mathbf{ord}_p a = l$, 称l为a对素数p的指数.

数论函数

ord且有如下性质：对任意整数a, b,

(1) $\mathbf{ord}_p ab = \mathbf{ord}_p a + \mathbf{ord}_p b$,

(2) $\mathbf{ord}_p(a+b) \geq \min\{\mathbf{ord}_p a, \mathbf{ord}_p b\}$, 且当

$$\mathbf{ord}_p a \neq \mathbf{ord}_p b,$$

一定取等号.

数论函数

推广到a为有理数时，只要规定

$$\mathbf{ord}_p\frac{n}{m}=\mathbf{ord}_p n-\mathbf{ord}_p m.$$

由定义可知：

1) 对任意整数a，$\mathbf{ord}_p a\geq 0$

2) 对有理数a，$\mathbf{ord}_p a\geq 0\Longleftrightarrow a$的分母不是$p$的倍数.

数论函数

例1.求$a = 1 + \frac{1}{2} + \cdots + \frac{1}{10}$的分母.

解 首先分母的素因子只能是10以内的素数, 因此只要对所有10以内素数p, 求出$\mathbf{ord}_p a$即可.

1) 对素数2, 8是含2最多的, 故

$$\mathbf{ord}_2 a = \mathbf{ord}_2 \frac{1}{8} = -3.$$

数论函数

2) 对素数**3**, **9**是含**3**最多的, 故

$$\mathbf{ord}_3 a = \mathbf{ord}_2 \frac{1}{9} = -2.$$

3) 对素数**5**, **5**和**10**并列含**5**最多, 故应具体计算得

$$\mathbf{ord}_5(\frac{1}{5} + \frac{1}{10}) = \mathbf{ord}_5 \frac{3}{10} = -1.$$

典型例子

由于其余部分分母都不含**5**, 故

$$\mathbf{ord}_5 a = -1.$$

4) 只有**7**含有**7**, 故

$$\mathbf{ord}_7 a = -1.$$

综上, a的分母是$8 \times 9 \times 5 \times 7$.

数论函数

定理1.

对任意素数p和正整数n，有

$$\mathbf{ord}_p n! = [\frac{n}{p}] + [\frac{n}{p^2}] + \cdots .$$

数论函数

证明：设$m = [\frac{n}{p}]$, 则因

$$n! = 1 \cdots p \cdots 2p \cdots mp \cdot (mp+1) \cdots n.$$

可知

$$\mathbf{ord}_p n! = \mathbf{ord}_p(p^m m!) = m + \mathbf{ord}_p m!.$$

归纳并注意到$[\frac{n}{ij}] = [\frac{[\frac{n}{i}]}{j}]$可得定理1.需要的公式.

数论函数

定理2.

对任意素数p和正整数n，记$A(n,p)$为n的p进展开式的各位数字之和，则有下列公式

$$\mathbf{ord}_p n! = \frac{n - A(n,p)}{p-1}.$$

数论函数

证明: 利用

$$\mathbf{ord}_p n! = \mathbf{ord}_p(p^m m!) = m + \mathbf{ord}_p m!$$

进行归纳, 因此只需检查

$$m + \frac{m - A(m,p)}{p-1} = \frac{n - A(n,p)}{p-1}$$

是否成立?其中$n = pm + a_0$, 那么$A(n,p) = a_0 + A(m,p)$, 简单计算可知上式成立.

常见数论函数

- 因子函数$d(n) := n$的因子个数.
- 素因子函数$\omega(n) := n$的素因子个数.
- 因子和函数$\sigma(n) := \sum\limits_{d|n} d$.
- $I(n) = \begin{cases} 1, n = 1 \\ 0, n > 1. \end{cases}$
- $e(n) = 1$.

常见数论函数

- **Mobius函数μ:**

$$\mu(n)=\begin{cases}1, n=1\\ 0, n\text{有平方因子}\\ (-1)^r, n\text{是}r\text{个不同素数之积}.\end{cases}$$

常见数论函数

定理

$$\sum_{d|n}\mu(d)=\begin{cases}1, n=1\\ 0, n>1\end{cases}$$

证明：对$n>1$，设$n=p_1^{l_1}\cdots p_r^{l_r}$，则

$$\sum_{d|n}\mu(d)=\sum_{d|p_1\cdots p_r}\mu(d)=\sum_{i=0}^{r}(-1)^i\binom{r}{i}=0.$$

常见数论函数

- **Euler函数ϕ.**

(1) 积性: 对$(m,n)=1$, 有

$$\phi(mn)=\phi(m)\phi(n).$$

(2) $\sum\limits_{d|n}\phi(d)=n$**.**

将一个模n的完全剩余系里的数按照与n的最大公约数分类计数可证.

(3) 用$\mu(n)$的语言重新表述

$$\phi(n)=\sum_{d|n}\mu(d)\frac{n}{d}.$$

积性函数和完全函数

给定数论函数f.

(1)若对$(m,n)=1$，有

$$f(mn)=f(m)f(n),$$

称f为积性函数。

(2) 若对任意正整数m,n，有

$$f(mn)=f(m)f(n),$$

称f为完全积性函数。

(3)前面讲的$\sigma(n),\phi(n),\mu(n)$都是积性函数，但不是完全积性函数。$e(n),I(n)$及幂函数n^a都是完全积性函数。

数论函数和Dirichlet级数

- 对数论函数$f(n)$和$g(n)$, 定义函数

$$(f*g)(n)=\sum_{d|n}f(d)g(\frac{n}{d})=\sum_{d_1d_2=n}f(d_1)g(d_2)$$

为$f(n)$和$g(n)$的**Dirichlet乘积**.

- **Dirichlet乘积的背景是Dirichlet对数论函数$f(n)$引进Dirichlet级数**

$$D_f(s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s}.$$

数论函数和Dirichlet级数

数论函数		Dirichlet级数
$f+g$	$\longleftrightarrow$	D_f+D_g
$f*g$	$\longleftrightarrow$	$D_f\cdot D_g$

$(f*g)*h=f*(g*h) \longleftrightarrow (D_f\cdot D_g)\cdot D_h=D_f\cdot(D_g\cdot D_h).$

$I(n) \longleftrightarrow D_I=1.$

$I*f=f \longleftrightarrow D_I D_f=D_f.$

$e*\mu=I \longleftrightarrow D_e D_\mu=1.$

数论函数和Dirichlet级数

对数论函数$f(n)$, 称数论函数

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

为$f(n)$的**Mobius变换**. 反过来

$$f=g*\mu$$

即

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

这就是通常说的**Mobius反演公式**，称$g*\mu$为g的**Mobius变换逆变换**。

数论函数和Dirichlet级数

Euler函数满足$\sum_{d|n}\phi(d)=n$表明ϕ的Mobius变换是恒等函数$h(n)=n$.

Euler函数满足

$$\phi(n)=\sum_{d|n}\mu(d)\frac{n}{d}$$

意味着ϕ可由h得到.

素数分布

令$\pi(n)$表示不超过n的素数的个数. 具有下列性质:

- $\pi(n) \longrightarrow \infty$, 这就是说素数有无限多.
- $\frac{\pi(n)}{n} \longrightarrow 0$.
- $\frac{1}{8} \cdot \frac{n}{\log n} < \pi(n) < 6\frac{n}{\log n}$.
- 素数定理$\pi(n) \sim \frac{n}{\log n}$.
- **Riemann**假设: 对任意$\varepsilon > 0$, $\pi(n) - \frac{n}{\log n} = O(n^{\frac{1}{2}+\varepsilon})$. 即存在常数$C$使$|\pi(n) - \frac{n}{\log n}| < Cn^{\frac{1}{2}+\varepsilon}$

素数分布

第一条性质Eucilid已经证明了，下面我们给出Euler的分析方法证明.

记

$$\zeta(s) = \sum_{i=1}^{\infty} \frac{1}{n^s}.$$

把它当成关于s的实函数，当$s > 1$时，级数收敛，且（由算术基本定理知）

$$\zeta(s) = \prod_{p}(1 + p^{-s} + p^{-2s} + \cdots) = \prod_{p}(1 - p^{-s})^{-1}.$$

素数分布

对上式两边取对数可得,

$$\log\zeta(s)=\sum_p(-\log(1-p^{-s}))=\sum_p\sum_{m=1}^{\infty}\frac{p^{-ms}}{m} \tag{10}$$
$$=\sum_p p^{-s}+\sum_p\sum_{m=2}^{\infty}\frac{p^{-ms}}{m}.$$

素数分布

现对$\sum\limits_{p}\sum\limits_{m=2}^{\infty}\frac{p^{-ms}}{m}$做简单估计：

$$0<\sum_{p}\sum_{m=2}^{\infty}\frac{p^{-ms}}{m}<\sum_{p}\sum_{m=2}^{\infty}p^{-m}=\sum_{p}\frac{p^{-2}}{1-p^{-1}}=\sum_{p}\frac{1}{p(p-1)}$$
$$<\sum_{n=2}^{\infty}\frac{1}{n(n-1)}=1.$$

素数分布

当$s \longrightarrow 1^+$时**(1)**式左边是无穷，说明$\sum\limits_p p^{-s}$也是无穷，说明素数必须是无限多，且

$$\sum_p p^{-1} = \infty.$$

素数分布

Dirichlet定理

当$(a,m)=1$时, 满足$x\equiv a\pmod m$的素数有无限个.

证明思路：推广**Euler**证明素数无限的方法.

Euler用$\zeta(s)=D_e$数所有的素数。

Dirichlet用某些特殊的D_f定义的函数来数一个剩余类里的素数。

素数分布

特殊情形的Dirichlet定理

对素数q时，满足$p \equiv 1 \pmod{q}$的素数p有无限个.

Dirichlet注意到对完全积性函数$f(n)$可以得到

$$L(f,s) := D_f = \sum_{i=1}^{\infty} \frac{f(n)}{n^s} = \prod_p (1 - f(p)p^{-s})^{-1}.$$

素数分布

后面的证明步骤是模拟**Euler**的做法. 只要f有界，可做类似分析得

$$\log L(f,s)=\sum_p(-\log(1-f(p)p^{-s}))=\sum_p f(p)p^{-s}+\text{有界量}$$

如果f满足

$$f(n)=\begin{cases}1, n\equiv 1 \pmod q\\ 0, \text{其它}\end{cases} \tag{4}$$

那么需证的结果归结为:左边是无穷(当s趋于**1**时).

素数分布

以上就是**Dirichlet**的基本思想，但一个函数f难以兼顾两条好性质，而改用几个函数联手.

首先取定一个模q的原根g，对任意给定的$q-1$次复单位根ω，可定义一个从$(\mathbb{Z}/q\mathbb{Z})^\times$到$\mathbb{C}^\times$的乘法群同态$\chi_\omega$

$$\chi_\omega(g^m)=\omega^m$$

即

$$\chi_\omega(n)=\omega^{ind_g n}.$$

令$\chi_\omega(0)=0$将χ_ω的定义域扩充到$\mathbb{Z}/q\mathbb{Z}$上.

素数分布

再通过与自然映射$\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z}$ 的合成将χ_ω看作定义在$\mathbb{Z}$上, 从而得到完全积性的（复值）数论函数(仍记为χ_ω).虽然χ_ω不满足(4)式的性质, 但$\sum\limits_{\omega} \chi_\omega$却具有类似性质, 即

$$\sum_{\omega} \chi_\omega(n) = \begin{cases} q-1, n \equiv 1 \pmod{q} \\ 0, \text{其它} \end{cases}$$

素数分布

于是

$$\sum_{\omega} \log L(\chi_\omega, s) = \sum_{p} (\sum_{\omega} \chi_\omega(p)) p^{-s} + \text{有界量}$$

$$= \sum_{p \equiv 1 \pmod q} (q-1) p^{-s} + \text{有界量}.$$

最终需证明$\prod_{\omega} L(\chi_\omega, s)$趋于无穷. 易知

$$L(1, s) = (1 - q^{-s}) \zeta(s).$$

下列关键的分析性质给出一切：当$\omega \neq 1$时, $L(\chi_\omega, 1) \neq 0$.

综合例题

例1. 证明$x^2+y^2=z^2$的整数解满足性质：x,y,z中必有一个3的倍数，一个4的倍数，一个5的倍数。

证明 先化简为$x,y,x>0$且x,y,z两两互素. 经观察可得x,y一奇一偶(不妨设x奇y偶)，z为奇数.对上式 $\mod 8$可得$y^2\equiv 0 \mod 8$. 因此$y\equiv 0 \mod 4$.

由于对任意整数n都有$n^2\equiv 0,1 \mod 3$，所以对上式 $\mod 3$可得x^2,y^2中有一个元素$\equiv 0 \mod 3$. 因此$x\equiv 0 \mod 3$或$y\equiv 0 \mod 3$.

综合例题

对任意整数n，若$(n,5)=1$，那么$n^4 \equiv 1 \mod 5$，因此$n^2 \equiv \pm 1 \pmod 5$,对原方程模5讨论可得x,y,z中必有一个5的倍数

综合例题

例2. 证明对$n > 1$, $a = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$不是整数.

证明 说明1到n中只有一个数含有最多的2.

由于存在唯一的r满足$2^r \leq n < 2^{r+1}$, 于是任意1到n中非2^r的其它数m, 有$\mathbf{ord}_2 m < r$.

典型例子

利用性质: 若$\mathbf{ord}_p a \neq \mathbf{ord}_p b$, 则有

$$\mathbf{ord}(a+b) = \min\{\mathbf{ord}_p a, \mathbf{ord}_p b\}$$

可得

$$\mathbf{ord}_2 a = \mathbf{ord}_2 \frac{1}{2^r} = -r.$$

典型例子

例3. 设p是奇素数, 若

$$a \equiv b \not\equiv 0 \pmod{p},$$

证明对任意n, 有

$$\mathbf{ord}_p(a^n - b^n) = \mathbf{ord}_p(a-b) + \mathbf{ord}_p n.$$

典型例子

证明 首先注意到

$$\begin{aligned}&\mathbf{ord}_p(a^{mn}-b^{mn})-\mathbf{ord}_p(a-b)\\&=(\mathbf{ord}_p(a^{mn}-b^{mn})-\mathbf{ord}_p(a^n-b^n))\\&+(\mathbf{ord}_p(a^n-b^n)-\mathbf{ord}_p(a-b)).\end{aligned}$$

典型例子

因此上述结论对m和n分别成立, 则对mn成立. 这样就归结为考虑n取素数时证明结论是否成立.将n分两种情形讨论：

1) $n = q \neq p$时,

$\frac{a^q - b^q}{a-b} \equiv qa^{q-1} \not\equiv 0 \pmod{p}$, 结论成立.

典型例子

2) $n = p$**时, 需证**$\mathbf{ord}_p \frac{a^p - b^p}{a-b} = 1$**.**

若$\mathbf{ord}_p(a-b) > 1$**, 即**$a \equiv b \pmod{p^2}$**, 则**

$\frac{a^p - b^p}{a-b} \equiv pa^{p-1} \not\equiv 0 \pmod{p^2}$**, 结论成立.**

典型例子

若$\mathbf{ord}_p(a-b)=1$，可设$a\equiv b+pt\pmod{p^2}$，$t\not\equiv 0\pmod{p}$，于是

$$a^p\equiv (b+pt)^p\equiv b^p+p^2b^{p-1}t\pmod{p^3}.$$

典型例子

由于$bt \not\equiv 0 \pmod{p}$, 因此上式意味着

$$\mathbf{ord}_p(a^p - b^p) = 2 = \mathbf{ord}_p(a-b) + \mathbf{ord}_p p$$

结论成立.

综合例题

例4. 证明满足$n^2 \mid 2^n + 1$的整数只有$n = 1, 3$.

证明 易验证$n = 1$上式成立. 当n是偶数时, 上式显然不成立. 下设n为大于1的奇数.

当$n = p$, 可得$2^p \equiv -1 \mod p^2$. 所以$2 \equiv 2^p \equiv -1 \mod p$. 所以$p \mid 3$. 可验证$p = 3$.

综合例题

当$n = p^r (r > 1)$, 可得

$$2^{p^r} \equiv (-1) \equiv (-1)^{p^r} \mod p^{2r}.$$

由上题结论知可得$2 \equiv -1 \mod p^r$.可得$p^r = 3$.

综合例题

当$n = p^r \cdot m$, 其中$m > 1, p \nmid m$. 可得

$$2^{p^r m} \equiv -1 \mod p^{2r} m^2.$$

因此有

$$2^{p^r m} \equiv (-1)^m \mod p^{2r} \tag{1}$$

和

$$2^{p^r m} \equiv -1 \mod m^2. \tag{2}$$

综合例题

利用同余的开方性质:

若$a^n \equiv b^n \mod m$, 且$(a,m)=1,(n,\phi(m))=1$, 则有$a \equiv b \mod m$.

不妨假设p是最小的素因子, 所以有$(m,\phi(p^{2r}))=1$. 可得

$$2^{p^r} \equiv -1 \mod p^{2r}.$$

由上述讨论可知$p^r=3$, 即$n=3m$, $(3,m)=1$ 上面的(2)式变成了

$$2^{3m} \equiv -1 \mod m^2$$

综合例题

即

$$8^m \equiv -1 \mod m^2$$

同样的讨论可以推出$3|m$，从而得到矛盾。