数论中的互反律

孙智宏

1. 二次互反律

设p为奇素数, k为自然数, $a \in \mathbb{Z}$, 若存在$x \in \mathbb{Z}$使得$p \mid x^k - a$,则说同余式$x^k \equiv a \pmod{p}$可解(有解), 并称a为p的k次剩余.

定理1(二次互反律) 设p与q为不同的奇素数,则

(i) 当p, q中至少有一个为$4k+1$形数时,

$x^2 \equiv q \pmod{p}$有解 $\Longleftrightarrow$ $x^2 \equiv p \pmod{q}$有解.

(ii) 当p, q均为$4k+3$形数时,

$x^2 \equiv q \pmod{p}$有解 $\Longleftrightarrow$ $x^2 \equiv p \pmod{q}$无解.

二次互反律由Euler在1750年提出,1785年Legendre重新发现并给出部分证明,1796年19岁的Gauss首次给出严格证明.Gauss一生共给出二次互反律八个不同的证明. Gauss称二次互反律为“算术中的宝石.”

2. 两个基本定理

定理2.(Fermat-Euler, 两平方和定理) 在不计次序和正负号情况下,每个$4k+1$形素数可唯一地表成两个整数的平方和. ($p = a^2 + b^2$)

定理3.(Euler) 设p为$3k+1$形素数,则存在唯一的一对自然数L, M使得$4p = L^2 + 27M^2$.

3.Euler关于三四次剩余的猜想

Euler猜想1(1748-1750): 设p为$3k+1$形素数,则

$x^3 \equiv 2 \pmod{p}$有解 $\iff$ $p = A^2 + 27B^2 (A, B \in \mathbb{Z})$,
$x^3 \equiv 3 \pmod{p}$有解 $\iff$ $4p = A^2 + 243B^2$.

Euler猜想2(1748-1750): 设p为$4k+1$形素数,则

$x^4 \equiv 2 \pmod{p}$有解 $\iff$ $p = A^2 + 64B^2 (A, B \in \mathbb{Z})$,
$x^4 \equiv 5 \pmod{p}$有解 $\iff$ $p = A^2 + 100B^2$.

4.Gauss与四次互反律

Gauss从1807年起开始研究三四次剩余, 1828年与1832年他出版了两篇四次剩余论文,提出四次互反律.

Gauss整数环: $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

$\mathbb{Z}[i]$中四次剩余问题: 设$\alpha, \pi \in \mathbb{Z}[i]$, 问$x^4 \equiv \alpha \pmod{\pi}$在$\mathbb{Z}[i]$中是否有解?即是否存在$x, y \in \mathbb{Z}[i]$使$x^4 = \alpha + y\pi$.

四次互反律大意: 设α, π为$\mathbb{Z}[i]$中不可分数(Gauss素数), 则$x^4 \equiv \alpha \pmod{\pi}$在$\mathbb{Z}[i]$中是否可解取决于$x^4 \equiv \pi \pmod{\alpha}$在$\mathbb{Z}[i]$中是否可解.

Gauss说四次互反律证明是算术中最深奥的秘密.四次互反律第一个出版的证明属于Eisenstein (1844). 人们在Gauss的遗稿中发现他关于四次互反律的分圆证明和几何证明. 利用四次互反律可证明Euler关于2,3,5为$4k + 1$形素数p的四次剩余猜想.

5. Eisenstein(爱森斯坦)与三次互反律

$\omega = (-1 + \sqrt{-3})/2$.

Eisenstein整数环: $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$.

在$\mathbb{Z}[\omega]$中考虑三次剩余问题, 则有三次互反律.

三次互反律大意: 设α, π为$\mathbb{Z}[\omega]$中不可分数(Eisenstein素数),则$x^3 \equiv \alpha \pmod{\pi}$在$\mathbb{Z}[\omega]$中是否可解取决于$x^3 \equiv \pi \pmod{\alpha}$在$\mathbb{Z}[\omega]$中是否可解.

1844年21岁的一年级大学生Eisenstein在著名的Crelle杂志上出版了25篇重要论文,其中包括三四次互反律的首次证明(应用Gauss和). 随后Jacobi宣称他在1837年给学生的讲课中给出过三四次互反律的证明.

1845年Eisenstein又利用Abel的椭圆函数论证明三四次互反律. 1850年Eisenstein建立一般的k次(k为素数)互反律, 即著名的Eisenstein互反律. Gauss称Eisenstein是世纪罕见的天才. 今天最一般的互反律由Artin在1927年建立.

6. Burde有理四次互反律

定理4(Burde, 1969) 设p, q为不同的$4k+1$形素数，$x^2 \equiv p \pmod{q}$有解，$p = a^2 + b^2, 2|b$, $q = c^2 + d^2, 2|d$,

(i) 若$x^2 \equiv ac - bd \pmod{q}$有解，则

$$x^4 \equiv q \pmod{p}\text{有解} \iff x^4 \equiv p \pmod{q}\text{有解}.$$

(ii) 若$x^2 \equiv ac - bd \pmod{q}$无解，则

$$x^4 \equiv q \pmod{p}\text{有解} \iff x^4 \equiv p \pmod{q}\text{无解}.$$

7. 群$G(q)$与有理三次互反律

对素数q,令$\mathbb{Z}_q$为模q的剩余类集合,即

$$\mathbb{Z}_q = \{q\mathbb{Z}, 1 + q\mathbb{Z}, \ldots, q - 1 + q\mathbb{Z}\} = \mathbb{Z}/q\mathbb{Z},$$

则$\mathbb{Z}_q$为q个元素的域.

分数同余　设p为素数, $m, n, x \in \mathbb{Z}$, $p \nmid m$, $mx \equiv n \pmod{p}$, 则定义$\frac{n}{m} \equiv x \pmod{p}$.

定义　对素数$q > 3$令

$$G(q) = \{\infty\} \cup \{x : \ x^2 \neq -3, \ x \in \mathbb{Z}_q\}.$$

对$x, y \in G(q)$规定二元运算

$$x * y = \frac{xy - 3}{x + y} \quad (\infty * x = x * \infty = x).$$

例如: (1) $G(5) = \{0, \pm 1, \pm 2, \infty\}$. 在$G(5)$中

$$1 * 2 = \frac{1 \cdot 2 - 3}{1 + 2} = -\frac{1}{3} = -2$$

$$1 * (-2) = \frac{1 \cdot (-2) - 3}{1 + (-2)} = 5 = 0.$$

(2) $G(7) = \{0, \pm 1, \pm 3, \infty\}$. 在$G(7)$中

$$3 * 3 = \frac{3 \cdot 3 - 3}{3 + 3} = 1,$$

$$1 * (-1) = \frac{1 \cdot (-1) - 3}{1 + (-1)} = \infty.$$

定理5(Z.H.Sun，1998) 设$q>3$为素数，

$$\left(\frac{q}{3}\right)=\begin{cases}1 & \text{若}q\equiv 1 \pmod 3,\\ -1 & \text{若}q\equiv 2 \pmod 3,\end{cases}$$

则$G(q)$是$q-(\frac{q}{3})$阶循环群(∞为单位元)，从而其中所有三次幂构成一个$\frac{q-(\frac{q}{3})}{3}$阶循环子群。

定理6(Z.H.Sun，1998, 有理三次互反律) 设$p,q>3$为不同素数，$p\equiv 1 \pmod 3$, $4p=L^2+27M^2$ $(L,M\in\mathbb{Z})$,则

$x^3\equiv q \pmod p$有解

$$\iff \frac{L}{3M}\text{是}G(q)\text{中三次幂}$$

$$\iff q\mid M \text{ or } \frac{L}{3M}\equiv\frac{s^3-9s}{3s^2-3} \pmod q \text{ for } s\in\mathbb{Z}.$$

对素数$q > 3$, 记$G(q)$中三次幂构成的子群为$G_0(q)$, 则

$G_0(5) = G_0(7) = \{0, \infty\},\ G_0(11) = \{0, \pm 5, \infty\},$
$G_0(13) = \{0, \pm 4, \infty\},$

故当p为$3k+1$形素数且$4p = L^2 + 27M^2$时

$x^3 \equiv 5 \pmod{p}$有解 $\iff$ $5 \mid L$ or $5 \mid M$,
$x^3 \equiv 7 \pmod{p}$有解 $\iff$ $7 \mid L$ or $7 \mid M$,
$x^3 \equiv 11 \pmod{p}$有解 $\iff$ $11 \mid L,\ 11 \mid M$
or $L \equiv \pm 5 \cdot 3M \pmod{11}$,
$x^3 \equiv 13 \pmod{p}$有解 $\iff$ $13 \mid L,\ 13 \mid M$,
or $L \equiv \pm 4 \cdot 3M \pmod{13}$.

8. 群$H(q)$与有理四次互反律

定义　对奇素数q,令

$$H(q)=\{\infty\}\cup\{x:\ x^2\neq -1,\ x\in\mathbb{Z}_q\}.$$

对$x,y\in H(q)$规定二元运算

$$x*y=\frac{xy-1}{x+y}\quad(\infty*x=x*\infty=x).$$

例如：$H(5)=\{0,\pm1,\infty\}$. 在$H(5)$中

$$1*0=\frac{0\cdot1-1}{0+1}=-1,$$
$$1*(-1)=\frac{1\cdot(-1)-1}{1+(-1)}=\infty.$$

定理7(Z.H.Sun，2001) 设q为奇素数，则$H(q)$是$q-(-1)^{\frac{q-1}{2}}$阶循环群(∞为单位元)，从而其中所有四次幂构成一个$(q-(-1)^{\frac{q-1}{2}})/4$阶循环子群。

定理8(Z.H.Sun，2001，有理四次互反律) 设p,q为不同奇素数，$p\equiv 1 \pmod 4$，$p=a^2+b^2(a,b\in\mathbb{Z})$，$2\mid b$，则

$$x^4\equiv(-1)^{\frac{q-1}{2}}q \pmod p\text{有解}$$
$$\Longleftrightarrow \frac{a}{b}\text{是}H(q)\text{中四次幂}$$
$$\Longleftrightarrow q\mid b \text{ or } \frac{a}{b}\equiv\frac{s^4-6s^2+1}{4s^3-4s} \pmod q \text{ for } s\in\mathbb{Z},$$

且

$$x^2\equiv(-1)^{\frac{q-1}{2}}q \pmod p\text{有解}$$
$$\Longleftrightarrow \frac{a}{b}\text{是}H(q)\text{中二次幂(平方)}$$
$$\Longleftrightarrow q\mid b \text{ or } \frac{a}{b}\equiv\frac{s^2-1}{2s} \text{ for some } s\in\mathbb{Z}.$$

对奇素数q记$H(q)$中四次幂构成的子群为$H_0(q)$, 则

$$H_0(3) = H_0(5) = \{\infty\},\ H_0(7) = \{0, \infty\},$$
$$H_0(11) = \{\pm 2, \infty\},\ H_0(13) = \{\pm 3, \infty\}.$$

故当p为$4k+1$形素数且$p = a^2+b^2 (a, b \in \mathbb{Z}, 2 \mid b)$时

$$x^4 \equiv -3 \pmod{p} \text{有解} \iff 3 \mid b,$$
$$x^4 \equiv 5 \pmod{p} \text{有解} \iff 5 \mid b,$$
$$x^4 \equiv -7 \pmod{p} \text{有解} \iff 7 \mid a \text{ or } 7 \mid b,$$
$$x^4 \equiv -11 \pmod{p} \text{有解} \iff 11 \mid b \text{ or } a \equiv \pm 2b \pmod{11},$$
$$x^4 \equiv 13 \pmod{p} \text{有解} \iff 13 \mid b \text{ or } a \equiv \pm 3b \pmod{13}.$$