

# 剩余和互反律

剩余问题、互反律问题，是初等数论计划系列的最后一篇。

这一篇是前三篇的集大成者，基本上会应用到前三篇的所有知识。如果您阅读本文有困难，可以参考前三篇的内容：

[初等数论三大定理和缩系乘法群](#)中的缩系乘法群部分。

[素数幂次与p进数问题](#)中的p进数部分。

[二次域及有理逼近相关问题](#)中的高斯整数与艾森斯坦整数部分以及二次域部分。

至此，初等数论中，除了数论函数（我还不太会）的部分，其余的部分全部成体系按线索地叙述完毕。在算法层面，本文到二次互反律部分即已经结束了，后面的部分为较为前沿的内容，无需掌握。

写完这四篇基本上可以出版一本初等数论教科书了。

## 二次剩余与互反律

### 二次Kronecker符号

剩余符号一般分为Legendre符号、Jacobi符号和Kronecker符号，三者为包含关系，前一个是后一个的特例，后一个是前一个的推广。勒让德符号要求下方为非分歧本原素数（二次为正奇素数），雅可比符号要求下方为非分歧本原数（二次为正奇数），而Kronecker符号什么限制都没有。当然，绝大多数剩余都能轻易地推广到Jacobi符号，这是为了计算互反律方便，但是推广到Kronecker符号就很困难。

高次剩余符号要加下角标3、4等等，而二次剩余符号中的下角标2可以省略。如果没有下角标，默认为二次剩余符号。

二次克罗内克符号是一种二次剩余符号。它含有两个变元n和m对于n和m均是完全积性的。也就是说，如果把n分解为a个数相乘、m分解为b个数相乘，那么n与m的二次克罗内克符号可以分解为相应的ab个二次克罗内克符号的乘积。

$$n = n_1 n_2$$

$$m = m_1 m_2$$

$$\left(\frac{n}{m}\right) = \left(\frac{n_1}{m_1}\right) \left(\frac{n_2}{m_1}\right) \left(\frac{n_1}{m_2}\right) \left(\frac{n_2}{m_2}\right)$$

为了介绍初值和定律，还需要借助类似于Gauss整数中的本原数的概念。在这里要给一般的整数定义本原数

规定2是分歧数。本原数去掉所有的因子2之后除以4余1，而非本原数去掉所有的因子2之后除以4余3，并规定0是本原数。具体来讲：

本原数：……-6, -3, 0, 1, 2, 4, 5, 8, 9, 10, 13, ……

非本原数：……-5, -4, -2, -1, 3, 6, 7, 11, 12, 14, ……

除了0以外，两整数分类相同，乘积为本原数；分类不同，乘积为非本原数。由于-1是非本原数，整数n和-n被分到不同类中。

对于奇素数 $p$ 就有了它的相伴本原素数 $\square$

$$p_0 = \left(\frac{-1}{p}\right) p = \begin{cases} p \quad & p \equiv 1 \pmod{4} \\ -p \quad & p \equiv 3 \pmod{4} \end{cases}$$

相当于通过配正负号，将 $p$ 强行转换为 $4k+1$ 形式。

定义以下初值：

只要有1，值就为1。

$$\left(\frac{n}{1}\right) = \left(\frac{1}{m}\right) = 1$$

在 $n$ 和 $m$ 都不是正负1的时候，有：

$$\left(\frac{n}{0}\right) = \left(\frac{0}{m}\right) = 0$$

下方为-1的时候，用于区分负数和非负数。

$$\left(\frac{n}{-1}\right) = \begin{cases} 1 \quad & n \geq 0 \\ -1 \quad & n < 0 \end{cases}$$

而上方为-1的时候，不仅要看负数或非负数，还要看 $m$ 是否本原数。

当 $m$ 为本原数或负非本原数时：

$$\left(\frac{-1}{m}\right) = 1$$

当 $m$ 为正非本原数或负本原数时：

$$\left(\frac{-1}{m}\right) = -1$$

最后，关于2的结论，上下方是相同的。

$$\left(\frac{n}{2}\right) = \left(\frac{2}{n}\right) = \begin{cases} 0 \quad & n \equiv 0 \pmod{2} \\ n \equiv 1, 7 \pmod{8} \quad & n \equiv 3, 5 \pmod{8} \end{cases}$$

由于二次克罗内克符号不仅满足完全积性，还满足以下的两个性质，因此可以通过递归的方式简捷地计算二次克罗内克符号。

### 循环律 $\square$

当 $m$ 是正奇数时，固定 $m \mid n$ 与 $m$ 的二次克罗内克符号是关于 $n$ 的周期为 $m$ 的函数。

$$\left(\frac{n}{m}\right) = \left(\frac{n+km}{m}\right)$$

这个性质用于缩小 $n$ 通过取余数的方法，使得 $n$ 落入0到 $m-1$ 之间。

另一个性质是互反律，在下文的二次互反律再介绍。

## Gauss引理

将奇素数 $p$ 的缩系分为前后两个区间：前半区间是1到二分之 $p-1$ 后半区间是二分之 $p+1$ 到 $p-1$

用 $n$ 乘前半个区间的数，有 $m$ 个落到了后半个区间，则：

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

为了下文的证明方便，引入一个模 $p$ 意义下的除2运算□

$$k/2 = \begin{cases} \frac{k}{2} \quad & 2|k \\ \frac{k+p}{2} \quad & \text{others} \end{cases}$$

接下来再引入一个多项式 $h$ □需要借助模 $p$ 意义下的除2运算：

$$h(x) = \prod_{k=1}^{\frac{p-1}{2}} (x^{p-k/2} - x^{k/2})$$

最终乘积展开后，仍旧要对多项式 $h$ 的指数部分做模 $p$ 操作，使得最终多项式 $h$ 次数不超过 $p-1$ □

第一步，要计算多项式 $h$ 在单位根处的值：

$$h(\zeta_p) = \prod_{k=1}^{\frac{p-1}{2}} (\zeta_p^{p-k/2} - \zeta_p^{k/2})$$

我们发现，由于代入的自变量是 $p$ 次单位根，对指数部分的模 $p$ 操作不影响最终取值。并且乘积的每一项都是纯虚数，是 $2i$ 或 $-2i$ 乘以对应角度的正弦值，如果规定正弦值全部取正，则它跑遍了所有的正弦值，不重不漏。

于是将注意力集中到辐角，即统计里面出现了多少个 $-2i$ □出现 $-2i$ □当且仅当函数 $f$ 落到前半个区间，即：

$$k/2 < \frac{p}{2}$$

因此 $-2i$ 的个数恰好就是：前半个区间的数，有多少个乘2之后还落在前半个区间。这个东西很容易让我们联想到这里的Gauss引理。

如果只关注 $-2i$ 中的负号，即关注个数奇偶性，由于总个数 $p-1$ 是偶数，因此两半区间的奇偶性应当相同。

综上，多项式 $h$ 在该点的值是：

$$h(\zeta_p) = \left(\frac{2}{p}\right)^{\frac{p-1}{2}} (2^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} \sin \frac{k}{p} 2\pi)$$

分成了辐角和模长两部分。

根据 $p$ 是奇素数，模8无非就只有1、3、5、7四种情况，简单讨论可以得到：

$$\left(\frac{2}{p}\right)^{\frac{p-1}{2}} = \begin{cases} 1 \quad & p \equiv 1 \pmod{4} \\ & p \equiv 3 \pmod{4} \end{cases}$$

辐角部分就解决了。

模长部分是多少呢？首先它一定是个正实数。如果我们在复平面单位圆中观察这部分，会发现它是一大堆弦长的乘积。我们之前见过一大堆弦长的乘积：

$$\sum_{k=0}^{p-1} x^k = \prod_{k=1}^{p-1} (x - \zeta_p^k)$$

在式中，代入 $x$ 等于1，并取模长。那么，等式左边是 $p$ □右边是 $p-1$ 条弦长的乘积。我们要求的模长部分，弦长恰好有二分之 $p-1$ 条，不重不漏，因此相当于上式的一半。所以模长部分是：

$$2^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} \sin \frac{k}{p} 2\pi = \sqrt{p}$$

综上：

$$\$h(\zeta_p)=\begin{cases}\sqrt{p}\quad & p\equiv 1\pmod 4 \\ \sqrt{p}\quad & p\equiv 3\pmod 4\end{cases}\$$$

观察多项式 $h(x)$

$$\$h(1+u)=\prod_{k=1}^{\frac{p-1}{2}}((1+u)^{\frac{p-k}{2}}-(1+u)^{\frac{k}{2}})\$$$

由二项式展开，在对多项式系数模 $p$ 时，无论除 $2$ 运算为何值，总有：

$$\$u^2 | ((1+u)^{\frac{p-k}{2}}-(1+u)^{\frac{k}{2}})+2(\frac{k}{2}u)\$$$

除 $2$ 运算乘 $2$ 会得到 $k$ 本身。因此：

$$\$u^{\frac{p+1}{2}} | h(1+u)-u^{\frac{p-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}(-k)\$$$

由威尔逊定理，乘积部分简化为：

$$\$u^{\frac{p+1}{2}} | h(1+u)+u^{\frac{p-1}{2}} \frac{1}{(\frac{p-1}{2}!)}\$$$

## Gauss和

要想讲解二次互反律，首先必须讲高斯和，从其根源处讲起。

观察三角函数表：

$$\$\cos\frac{1}{5}2\pi+\cos\frac{4}{5}2\pi=\frac{-1+\sqrt{5}}{2}\$$$

$$\$\cos\frac{2}{5}2\pi+\cos\frac{3}{5}2\pi=\frac{-1-\sqrt{5}}{2}\$$$

$$\$\cos\frac{1}{13}2\pi+\cos\frac{3}{13}2\pi+\cos\frac{4}{13}2\pi+\cos\frac{9}{13}2\pi+\cos\frac{10}{13}2\pi+\cos\frac{12}{13}2\pi=\frac{-1+\sqrt{13}}{2}\$$$

$$\$\cos\frac{2}{13}2\pi+\cos\frac{5}{13}2\pi+\cos\frac{6}{13}2\pi+\cos\frac{7}{13}2\pi+\cos\frac{8}{13}2\pi+\cos\frac{11}{13}2\pi=\frac{-1-\sqrt{13}}{2}\$$$

$$\$\cos\frac{1}{17}2\pi+\cos\frac{2}{17}2\pi+\cos\frac{4}{17}2\pi+\cos\frac{8}{17}2\pi+\cos\frac{9}{17}2\pi+\cos\frac{11}{17}2\pi+\cos\frac{15}{17}2\pi+\cos\frac{16}{17}2\pi=\frac{-1+\sqrt{17}}{2}\$$$

$$\$\cos\frac{3}{17}2\pi+\cos\frac{5}{17}2\pi+\cos\frac{6}{17}2\pi+\cos\frac{7}{17}2\pi+\cos\frac{10}{17}2\pi+\cos\frac{12}{17}2\pi+\cos\frac{13}{17}2\pi+\cos\frac{14}{17}2\pi=\frac{-1-\sqrt{17}}{2}\$$$

我们发现，每一组有两个等式，分母为 $4k+1$ 型素数，而第一行的分子全部为它的二次剩余，第二行则全部不是。更多的不再枚举，总之全部符合这个规律。

首先，全体余弦值的和（两行等式的和）是 $-1$ 。这一点非常容易。既然有了和，只需证明差就可以了。以 $5$ 为例，相当于：

$$\$\cos\frac{1}{5}2\pi-\cos\frac{2}{5}2\pi-\cos\frac{3}{5}2\pi+\cos\frac{4}{5}2\pi=\sqrt{5}\$$$

由于规律与二次剩余相关，引入二次剩余符号Legendre符号，上面Kronecker符号退化至下方为奇素数的情形），并且将余弦式用单位根表示，就变成：

$$\sum_{k=1}^4 \left(\frac{k}{5}\right) \zeta_5^k = \sqrt{5}$$

很令人惊讶，等式的左端出现了高斯和。因此，这个规律的本质，就是要计算高斯和的值。

定义多项式g

$$g(x) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) x^k$$

引入p次单位根，高斯和就是该多项式在单位根处的值。

$$\zeta_p = e^{\frac{2\pi i}{p}}$$

$$g(\zeta_p) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \zeta_p^k$$

因此高斯和是一个具体的数值。

高斯和的平方很好计算，不断地交换求和次序即可。

$$\begin{aligned} g(\zeta_p)^2 &= \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{mn}{p}\right) \zeta_p^{m+n} \\ &= \sum_{s=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{m(s-m)}{p}\right) \zeta_p^s \\ &= \sum_{s=0}^{p-1} \zeta_p^s \sum_{m=1}^{p-1} \left(\frac{s-m}{p}\right) \\ &= \left(\frac{-1}{p}\right)(p-1) + \sum_{s=1}^{p-1} \zeta_p^s \sum_{n=0}^{p-2} \left(\frac{n}{p}\right) \\ &= \left(\frac{-1}{p}\right)p \end{aligned}$$

至此，已经知道在p为4k+1型素数时，高斯和的值要么是根号p要么是负根号p了。然而要想证明本节开头发现的规律，仅凭这些是不够的。我们需要将目标锁定到根号p排除负根号p的情况才行。因此，问题最终归结为“高斯和的符号问题”。

这是关于多项式g在x+1处取值的结论。交换求和次序：

$$g(x+1) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) (x+1)^k = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \sum_{r=0}^{p-1} C_k^r x^r = \sum_{r=0}^{p-1} \sum_{k=0}^{p-1} C_k^r \left(\frac{k}{p}\right) x^r$$

约定当下标溢出的时候，组合数值为0。对于给定的r可以把组合数看成关于k的多项式。这对于下标模p也成立，并且上述约定0结论不变。

一个有趣的事实是，模p意义下：

$$\sum_{k=0}^{p-1} k^r = -1 \pmod{p-1} \text{ or } 0 \pmod{p-1}$$

根据欧拉判别法，模p意义下：

$$\sum_{k=0}^{p-1} k^r \left(\frac{k}{p}\right) = -1 \pmod{p-1} \text{ or } 0 \pmod{p-1}$$

那么先对组合数部分求和，消去k最终就有：

$$x^{\frac{p+1}{2}} |g(x+1) + x^{\frac{p-1}{2}} \frac{1}{(p-1)!}|$$

这个结论的意思是，多项式g在1+x处，低于二分之p-1次数项的系数均被p整除，二分之p-1次数项的系数为一个阶乘的逆的相反数。

最后，只需要证明这两个多项式是相等的，就是h的展开。即：

$$g(x)=h(x)$$

这需要用到多项式的整除理论。首先我们已经证明了，在一个单位根处的平方相等。

$$g(\zeta_p)^2=h(\zeta_p)^2$$

由于两边都是整系数多项式，必然有整除关系：

$$\sum_{k=0}^{p-1} x^k |(g(x)+h(x))(g(x)-h(x))$$

左边是不可约多项式，因此右边两个因式必有一个被它整除。换句话说：

$$\sum_{k=0}^{p-1} x^k |(g(x)-h(x))$$

$$\sum_{k=0}^{p-1} x^k |(g(x)+h(x))$$

必然有一个成立。当然，由于多项式g也是p-1次，并且不等于左边，两结论有且仅有一个成立。

如果我们对多项式系数采取模p操作，有结论：

$$\sum_{k=0}^{p-1} x^k \equiv (x-1)^{p-1} \pmod p$$

设u为x-1，即在对多项式系数模p情形下：

$$u^{p-1} |(g(1+u)-h(1+u))$$

$$u^{p-1} |(g(1+u)+h(1+u))$$

有且仅有一个成立。

上文已经证明了：

$$u^{\frac{p+1}{2}} |h(1+u)+u^{\frac{p-1}{2}} \frac{1}{(\frac{p-1}{2}!)}$$

$$u^{\frac{p+1}{2}} |g(1+u)+u^{\frac{p-1}{2}} \frac{1}{(\frac{p-1}{2}!)}$$

结合之前有且仅有一个成立的两个整除式，一路逆推，我们最终证明了：

$$u^{p-1} |(g(1+u)-h(1+u))$$

$$\sum_{k=0}^{p-1} x^k |(g(x)-h(x))$$

两多项式均不超p-1次，最终只能相等。

## 二次互反律

根据上面多项式g与高斯和的定义，可以证明二次互反律。对于奇素数p，q模q意义下有：

$$\left(\frac{p_0}{q}\right)g(\zeta_p) \equiv p_0^{\frac{q-1}{2}}g(\zeta_p) = \{g(\zeta_p)\}^q \equiv g(\zeta_p^q) \pmod q$$

这个方法也可以用于计算2的情形，即辅助定理，模p意义下：

$$\begin{aligned} \left(\frac{2}{p}\right)\sqrt{2} &\equiv 2^{\frac{p}{2}} = \left(\left(\frac{\sqrt{2}}{2}\right)^2 + \frac{\sqrt{2}}{2}i\right) + \left(\frac{\sqrt{2}}{2}\right)^2 - \\ &\frac{\sqrt{2}}{2}i)^p \equiv \left(\frac{\sqrt{2}}{2}\right)^2 + \frac{\sqrt{2}}{2}i)^p + \left(\frac{\sqrt{2}}{2}\right)^2 + \\ &\frac{\sqrt{2}}{2}i)^p = \begin{cases} \sqrt{2} & p \equiv 1, 7 \pmod 8 \\ -\sqrt{2} & p \equiv 3, 5 \pmod 8 \end{cases} \end{aligned}$$

用文字叙述出来，二次互反律的完整版是这样的：

如果n和m有一个大于0，那么当且仅当n和m都是非本原数的时候n与m位置互换需要乘-1；否则只要n和m有一个本原数n与m位置互换的二次克罗内克符号函数值相同。

如果n和m均小于0，那么当且仅当n和m都是非本原数的时候n与m位置互换的二次克罗内克符号函数值相同；否则只要n和m有一个本原数n与m位置互换需要乘-1。

这个定律用于递归，使得从n比m小的状态开始，通过n与m交换位置，新的n比新的m大。这样就可以重复应用循环律，将n与m都缩小至初值范围内。

可以将计算得到的一部分二次克罗内克符号的值排成表。表的第一行写n，第一列写m



表中0的位置标蓝了，而对角线对称后不相同的元素标成了黄色，为了更加直观地看到二次互反律。

## 二次Hilbert符号

事实上纯数学的美感到这里顶多展示了一半，甚至可以说才刚刚开始。接下来的结论更加适合科普。如果愿意写个算法研究一下，其实也无所谓。事实上学算法的话，看到上文的二次互反律就足够了，只是互反律深刻的本质还没有被揭示出来，甚至到今天仍旧是纯数学的最艰深的课题之一。毕竟在Hilbert的23问中，第6个问题就是在任意数域中证明最一般的互反律，即Artin大佬百年前解决的问题。可知，互反律是数论的核心之一。

要想解释上文二次Kronecker符号中，为什么互反律不仅与本原数有关，还与数的正负有关，参考后文三四次互反律只与本原数有关，这点确实令人匪夷所思。那么要想解释这个问题，就不得不提到p进数，以及后文的Hilbert符号，还有前文中二次曲线上的整点问题一起讨论，才能解释清楚。

二次Hilbert符号中的变元是上方的a和b，范围不仅限于整数，而是要求a和b非零，并且使得a和b有意义的数。

二次Hilbert符号的值域只有1或-1。

考察这条二次曲线。

$$ax^2 + by^2 = 1$$

这条二次曲线在实数范围有没有点？这与a和b的取值有关。因此定义Hilbert符号，看起来像是二次剩余符号的上方变为两个的样子：

$$\left(\frac{a,b}{\infty}\right)$$

这个符号下方是无穷，表示实数范围。当a与b存在一个是非负数的时候，取值为1；仅当a和b都是负数的时候，取值为-1。

看起来怎么这么简单？这是因为这里考察的范围是实数。下面转到p进数域，对应这个符号：

$$\left(\frac{a,b}{p}\right)$$

同样考察同一个方程（二次曲线）。

$$ax^2+by^2=1$$

这条二次曲线在p进数范围有没有点？同样与a和b的取值有关。这时，需要将同样的a和b改写为p进数的形式。

$$a=p^iu$$

$$b=p^jv$$

其中p的幂次i和j要保证u和v在p进数中，小数点后没有内容，小数点前一位非0。这样的表示类似于科学记数法，是唯一的。

于是给出一个表达式r

$$r=\frac{(-a)^j}{(-b)^i}=\frac{(-u)^j}{(-v)^i}=(-1)^{ij}\frac{u^j}{v^i}$$

那么二次Hilbert符号的计算就有了，直接给出结论。

当p是奇素数时：

$$\left(\frac{a,b}{p}\right)=\left(\frac{r}{p}\right)$$

等式的右端就是一般的Kronecker二次剩余符号，上方的p进数r只取最后一位，代表模p

当p是2的时候：

$$\left(\frac{a,b}{2}\right)=(-1)^{\frac{r^2-1}{8}+\frac{u-1}{2}\frac{v-1}{2}}$$

这里-1的指数是2进数，只取2进数最后一位，代表模2。

那么二次Hilbert符号就有如下性质，用v代表素数或无穷符号：

对称性

$$\left(\frac{a,b}{v}\right)=\left(\frac{b,a}{v}\right)$$

完全积性

$$\left(\frac{a,bc}{v}\right)=\left(\frac{a,b}{v}\right)\left(\frac{a,c}{v}\right)$$

化归二次剩余情况

这里a为p进数中，小数点后没有内容而前一位非0的数。当其中含一个p的时候，无论p是奇素数还是2：

$$\left(\frac{a,p}{p}\right)=\left(\frac{a}{p}\right)$$

右边就是一般的二次剩余符号，例如二次Kronecker符号。

双可逆元情况

对于奇素数p如果a和b均为p进数中，小数点后没有内容而前一位非0的数，就有：

$$\left(\frac{a,b}{p}\right)=1$$

原因很简单。式子算出r的uv部分指数ij都是0，因此r就是1。

对于2的情况是这样的，如果a和b均为2进数中，小数点后没有内容而前一位为1：

$$\left(\frac{a,b}{2}\right)$$

当且仅当a和b都模4余3的时候，值为-1，否则值为1。

到这里，与利用完全积性计算二次Hilbert符号的目标，还差最后一步。

相等数情况□

$$\left(\frac{a,a}{v}\right)=\left(\frac{a,-1}{v}\right)$$

当a就是下方的素数p的时候，代入公式得：

$$\left(\frac{p,p}{p}\right)=\left(\frac{p,-1}{p}\right)=\left(\frac{-1}{p}\right)$$

至此就可以借助完全积性来计算二次Hilbert符号了。

根据方程含义，还可以推出以下初值：

$$\left(\frac{a,1-a}{v}\right)=1$$

注意定义要求自变量非0，即a不能是0或1。

## 二次互反律与p进数的关系

这里是本篇最精华的部分。

由于上一部分二次Hilbert符号里面直接给出了结论，略去了证明，于是这部分的难度被大大降低了，似乎随便写写就能写明白了。

对于方程：

$$ax^2+by^2=1$$

我们利用下方为无穷的二次Hilbert符号就可以判定它是否有实数解，当然这一步多此一举，直接正负讨论即可。

那么，上面有没有有理解呢？结论是这样的：

对于给定的非0有理数a和b□二次曲线上有有理点，等价于首先有实数点，并且其次对于所有的p进数域中都有点。

那么有理解的判定方法是怎样的？有下面的Hilbert乘积公式。不过先说一个显然的结论：

对于给定的非0有理数a和b□至多只有有限个p使得a和b的二次Hilbert符号值为-1。

这是因为定义中a和b非0，至多只有有限个p整除a或b□于是对于剩余的p均既不整除a□也不整除b□符号的值就为1了。

## Hilbert乘积公式

$$\prod_v \left(\frac{a,b}{v}\right) = 1$$

乘积的范围是全体 $v$ 即 $v$ 取无穷以及全体素数。

考虑完全积性的性质以及 $a$ 和 $b$ 的素因子分解，只需要对以下三种情形证明即可。

当 $a$ 和 $b$ 为相异奇素数时：

$$\left(\frac{a,b}{v}\right) = \begin{cases} \left(\frac{b}{a}\right) & v=a \\ \left(\frac{a}{b}\right) & v=b \\ (-1)^{\frac{a-1}{2}\frac{b-1}{2}} & v=2 \\ \text{others} \end{cases}$$

这种情况Hilbert乘积公式恰好就是二次互反律。

当 $a$ 为奇素数 $b$ 为-1或2时：

$$\left(\frac{a,-1}{v}\right) = \begin{cases} \left(\frac{-1}{a}\right) & v=a \\ (-1)^{\frac{a-1}{2}} & v=2 \\ \text{others} \end{cases}$$

$$\left(\frac{a,2}{v}\right) = \begin{cases} \left(\frac{2}{a}\right) & v=a \\ (-1)^{\frac{a^2-1}{8}} & v=2 \\ \text{others} \end{cases}$$

这种情况Hilbert乘积公式恰好就是二次互反律的补充定律。

当 $a$ 为-1 $b$ 均为-1或2时，这种情形最简单了。

$$\left(\frac{-1,-1}{v}\right) = \begin{cases} -1 & v=2 \text{ or } \infty \\ 1 & \text{others} \end{cases}$$

$$\left(\frac{-1,2}{v}\right) = 1$$

这个乘积公式统一了二次互反律。它的意义就是：对于给定的非0有理数 $a$ 和 $b$ 不存在有理点的 $p$ 进数域加实数域的数量是偶数。

因此验证有理点，只需验证实数域，以及除一个素数以外所有的 $p$ 进数域即可。

## Cipolla平方根算法

由于三次方程的解法较为复杂，开三次方根的算法并不容易。但是在这里有一种简洁有效的开平方根的算法，它需要将研究对象进行域扩张，扩张到 $Q(\sqrt{a^2-n})$ 上。

对于一个二次剩余 $n$ 我们想对它开平方根，即求解：

$$t^2 \equiv n \pmod{p}$$

考虑方程：

$$x^2 - 2ax + n = 0$$

这个方程的两根之积是 $n$ 因此根据Fermat-Eular定理，两根之积的 $p$ 次方应该也是 $n$

$$x_1^p \equiv x_2^p \pmod{p}$$

注意这里的两个根都未必是整数。下面分别考虑两个根单独的p次方是什么，即考虑：

$$x_1^p \pmod{p}$$

如果这个根本身是整数，那么根据Fermat-Eular定理，它的值应当回到这个根本身。

不是整数的情形会怎样？在扩域 $Q(\sqrt{a^2-n})$ 当中，没有引入p分之1作为因子。因此，下面的常见二项式展开结论应当成立：

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

这里的取模是对两个分量1和根号的系数取模。不妨取比较大的根 $x_1$ （较小的根同理），于是：

$$x_1^p = (a + \sqrt{a^2-n})^p \equiv a^p + (\sqrt{a^2-n})^p \equiv a^p + (a^2-n)^{\frac{p}{2}} \pmod{p}$$

由于a是整数，根据Fermat-Eular定理 $a^p \equiv a \pmod{p}$ 因此关键在于后面根号部分的p次方是多少，这部分未必满足Fermat-Eular定理。事实上，这一部分不满足Fermat-Eular定理。

根据Euler判别法，根号下的部分的半群阶次方很好计算。在是二次剩余的时候为1，否则二次非剩余的时候为-1。即：

$$(a^2-n)^{\frac{p-1}{2}} \equiv 1 \text{ or } -1 \pmod{p}$$

两边再乘一个这个数的根号就有：

$$(a^2-n)^{\frac{p}{2}} \equiv \sqrt{a^2-n} \text{ or } -\sqrt{a^2-n} \pmod{p}$$

上文中，根是整数的情形，即根号可以被开出来，那么这里就是二次剩余，右面的根号系数为1，代回原式可以得到p次方后不变的结果，与之前结论吻合。

但是，根不是整数的情形，对应根号下为二次非剩余，这里的同余式右端根号为负，即：

$$(\sqrt{a^2-n})^p \equiv -\sqrt{a^2-n} \pmod{p}$$

因此，在p次方作用下，原方程的两个根交换了位置

$$x_1^p \equiv a - \sqrt{a^2-n} = x_2 \pmod{p}$$

换位的前提，是根号下的数为二次非剩余，即这个根号开不出来的情形。

那么这个结论有什么用呢？我们在两边再同乘一个 $x_1$

$$x_1^{p+1} \equiv x_1 x_2 = n \pmod{p}$$

发现p+1恰好是偶数，而右边恰好是要开方的整数n因此最开始的开方值t就应该是：

$$t_1 \equiv x_1^{\frac{p+1}{2}} \pmod{p}$$

这就是Cipolla平方根算法。第一步随机出一个a使得a的平方减n是二次非剩余。然后只需计算 $x_1$ 的二分之p加1次方即可。由于二次剩余和二次非剩余恰好各占总体的一半，一般认为随机一次的a符合条件的概率是50%。

对于四次方根的求解，可以用两次Cipolla算法来解决，也不算困难。然而对于三次方根就麻烦得多。

# 高次剩余与互反律

## 一一映射情形的求根

这里指当素数 $p$ 不是 $tk+1$ 情形的时候 $t$ 次方运算在 $p$ 的缩系中是一一映射。那么这种情形的求根相当容易，甚至不需要用到上文的扩域。

这里仅举个简单的例子作为参考。对于 $p$ 是 $3k+2$ 情形的时候，3次方运算是——对应。我们已知下面的 $n$ 要求解 $x$

$$x^3 \equiv n \pmod p$$

首先根据Fermat-Eular定理，这个同余式一定是成立的：

$$x^{3k+1} \equiv 1 \pmod p$$

那么对 $n$ 作 $k$ 次方，就有：

$$n^k \equiv x^{3k} \equiv x^{-1} \pmod p$$

那么再来一次数论倒数就完事了。即完整的式子是：

$$n^{3k^2} = n^{k(p-2)} \equiv x \pmod p$$

其实上面的操作，就是缩系循环群里面，取对数之后，对3进行的数论倒数操作，即寻找一个逆映射。我们看到，3乘以 $3k$ 方是 $9k$ 方，再减去1之后，恰好是 $p-1$ 即 $3k+1$ 的倍数。因此，在缩系循环群的观点下，这样的逆映射就是跑了若干个整循环之后，恰好多跑出了一个幂次。这样类似于不定方程的思想就求解出了逆映射。

同时也看到，当 $p$ 是 $tk+1$ 情形的时候，这个映射不是一一映射，那么就不能采用这种办法了。即 $p$ 是 $3k+1$ 情形的时候，无法用这种办法开三次方。

## Peralta算法开立方

Cipolla算法开平方是一种特别优秀的算法，时间复杂度很低。而这里写出的Peralta算法仍旧属于一种暴力算法，比用原根与对数计算（至少根号量级）要优秀，相对Cipolla算法（对数量级）时间复杂度比较高。

它的思路是这样的。要求解：

$$x^3 \equiv n \pmod p$$

其中 $p$ 是 $3k+1$ 形式，即3次方不是一一对应，并且 $n$ 是三次剩余，即满足Euler判别法：

$$n^k \equiv 1 \pmod p$$

那么对 $x$ 进行待定系数。考虑全体 $x$ 的整系数二次多项式：

$$y = ax^2 + bx + c$$

因此记录 $y$ 的时候只需记录整数三元组 $abc$ 即可。利用最开始的方程关系：

$$x^3 \equiv n \pmod p$$

可以对指数模3，即计算多项式的乘法之后，仍旧还是二次三项式，即y的幂还是整数三元组abc对于这样的多项式y也满足Fermat-Euler定理：

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

即p-1次方(3k次方)之后，整数三元组abc变为001。那么在这个多项式空间里就有三次单位根：

$$y^k \equiv w \pmod p$$

那么w也是二次三项式w的三次方是1，即整数三元组001。

如果随机生成一个y即随机生成一组初始三元组abc使得w恰好满足w的abc三元组中a和c都是0，即：

$$w = bx$$

那么根据w的三次方是1，我们计算出的b恰好就是x的数论倒数。

进一步分析表明，这种随机生成y的方法里，最终计算出的w中a和c都是0的概率只有九分之一，即平均随机九次才能算出一个合格的w

当然一个优势是，这种暴力算法是可推广的，即可以轻松推广到任意次数的剩余中，只是时间复杂度会非常高。它退化二次的形式的时候，其实和上文的Cipolla算法比较接近，相当于Cipolla的弱化版。

### 三四次剩余的初步介绍

我们看到优秀的Cipolla算法的关键是，在Euler判别法中，二次非剩余的二分之p-1次方恰好回到了-1，即-1是二次单位根。因此，在一开始考察的方程中，做p次方之后x1和x2恰好互换了位置。这是Cipolla算法的关键。

然而，三四次剩余不是这样。问题在于在缩系乘法群当中，三四次单位根并不固定，并非像二次单位根一样一直是-1。

解决这个问题的办法还是扩域。三四次单位根不固定的原因，是因为固定的三次单位根和四次单位根本就不在考察范围里。因此需要将分圆域添加进来，才能在新范围中实现固定。

之前提到的高斯整环就是四次分圆整环，艾森斯坦整环就是三次（也是六次）分圆整环。

于是在这种情形下引入三次剩余符号和四次剩余符号(Legendre符号)，要求符号下方的数必须是新数域中的非分歧本原素数（可推广至Jacobi符号，下方为不含分歧数的本原数），则总有：

$$\left(\frac{\xi}{\pi}\right)_3 = 0 \text{ or } 1 \text{ or } \frac{-1 + \sqrt{3}}{2} \text{ or } \frac{-1 - \sqrt{3}}{2}$$

$$\left(\frac{\xi}{\pi}\right)_4 = 0 \text{ or } 1 \text{ or } -1 \text{ or } i \text{ or } -i$$

0总代表整除（不互素），1代表是三次剩余或四次剩余，-1代表是二次剩余但不是四次剩余，其余均为非剩余。

例如，对于3k+2型素数p扩充根号3i之后仍为新数域中的素数，其中每个原来的整数都是三次剩余，在新数域中由原来的一一对应变为三一对应，因为新数域中完系扩充到了p的平方个。于是三次剩余性质不变，每一个原来的整数代入符号之后右端为1。原来的三次单位根只有1一个，现在多了复平面上的两个。

对于3k+1型素数p扩充根号3i之后不为素数，分裂为两个共轭的新素数，原来的三次剩余性质由新素数

继承了。这时，原来看似混乱的三次单位根在模新素数的情况下，同余于复平面上的单位根。

综上所述，在扩域后三次或四次剩余符号里面（下方未扩展至Jacobi符号欧拉判别法仍然是成立的。

$$\left(\frac{\xi}{\pi}\right)_3 \equiv a^{\frac{N(\pi)-1}{3}} \pmod{\pi}$$

$$\left(\frac{\xi}{\pi}\right)_4 \equiv a^{\frac{N(\pi)-1}{4}} \pmod{\pi}$$

## 三四次互反律简介

有了前面的铺垫，这部分就简单了。

三四次互反律的主体部分特别简单：非分歧本原数可以直接颠倒。

$$\left(\frac{\xi_1}{\xi_2}\right)_k = \left(\frac{\xi_2}{\xi_1}\right)_k$$

这里的应用范畴是Jacobi符号。如上所见，二次互反律中的Kronecker符号的相应形式都不太一样，因此个人感觉不太可能直接推广到相应的Kronecker符号形式。

与二次互反律一样，除了主体部分，一定还有一个辅助定理，用于处理上方是分歧数的情形。对于二次互反律，就是上方是2的情形作为辅助定理。而三四次互反律的这部分比较复杂，就先不再给出了。

（缺了辅助定理这部分，计算可能会变得较为繁杂呢）

到更难的一类域论的部分，阿廷Artin为每一个数域上都推广出了相应的互反律，称为阿廷互反律。这就实在太难了，估计即使是数学系也得要博士才会研究，本科和研究生肯定不会去研究这些（所以我当然不会喽）。

至此，有关互反律的全部内容介绍完毕。完结撒花！

From: <https://wiki.cvbbacm.com/> - CVBB ACM Team

Permanent link: <https://wiki.cvbbacm.com/doku.php?id=2020-2021:teams:namespace:%E5%89%A9%E4%BD%99%E5%92%8C%E4%BA%92%E5%8F%8D%E5%BE%8B&rev=1592905359>

Last update: 2020/06/23 17:42