组合数学第十二讲

授课时间: 2018年12月10日 授课教师: 孙晓明 记录人: 於修远

1 勒让德符号(Legendre Symbol)与欧拉判别法(Euler Criterion)

首先，让我们来回顾一下勒让德符号的定义:

$$(\frac{a}{p}) = \begin{cases} 1 & (p \nmid a且x^2 \equiv a \pmod p有解) \\ -1 & (x^2 \equiv a \pmod p无解) \\ 0 & (p \mid a) \end{cases}.$$

注意:勒让德符号$(\frac{a}{p})$中的p必须为素数，而a可以是任意整数。
为了计算勒让德符号，我们先考虑一个特殊的例子。

定理 1. *对$4k+3$型的素数p，$(\frac{-1}{p}) = -1$。*

证明 这里我们依旧采用反证法。若不然，则存在$4k+3$型的素数p，使得$(\frac{-1}{p}) = 1$。也就是说，

$$\exists a,\ a^2 \equiv -1 \pmod p,$$

两边同时取$\frac{p-1}{2}$次方(p显然是奇素数，所以这一步操作可行)，得到

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

结合费马小定理(显然，a不会是p的倍数)，并将p的形式带入，就得到

$$1 \equiv a^{p-1} \equiv (-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1 \pmod p.$$

矛盾!假设不成立，从而$(\frac{-1}{p}) = -1$恒成立。 □

利用类似的思路，我们可以证明

定理 2 (欧拉判别法)**.** *对于整数a以及奇素数p*

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

在证明欧拉判别法的过程中，要用到威尔逊定理及相关思想。这里给出一个简单的证明。

定理 3 (威尔逊定理(Wilson's theorem))**.** *设p为素数，那么*

$$(p-1)! \equiv -1 \pmod p.$$

证明 $p = 2$时，结论平凡。当p为奇素数时，不难证明当p为素数时$\mathbb{Z}_p \setminus \{0\}$是一个域。现在，我们将集合$\mathbb{Z}_p \setminus \{0\}$ 中的所有元素与各自的逆配对，它们的逆两两不同。除去1和$p-1$的逆恰好为自身外，其他所有元素的逆都不是自身。于是便有

$$(p-1)! \equiv p-1 \equiv -1 \pmod p.$$

□

欧拉判别法的证明 首先我们需要证明$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$。这是因为当$p$为奇素数时，由费马小定理，我们有

$$0 \equiv a^{p-1} - 1 \equiv (a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \pmod p.$$

于是定理的证明可以分为两个部分。首先我们证明:$(\frac{a}{p}) = 1 \Rightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p$。

若$(\frac{a}{p}) = 1$，则存在整数b，使得$b^2 \equiv a \pmod p$。显然地，$p \nmid b$。结合费马小定理并对两边同时取$\frac{p-1}{2}$次方，马上得到

$$1 \equiv b^{p-1} \equiv a^{\frac{p-1}{2}} \pmod p.$$

然后证明$(\frac{a}{p}) = -1 \Rightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod p$。这里借鉴了费马小定理的一种证明，简述如下。

> *费马小定理的一种证明.* 在威尔逊定理的证明中已经得到，当$p \nmid a$时，在模p的意义下，有$\mathbb{Z}_p = a\mathbb{Z}_p$。将两个集合中的非零元素各自相乘，在模$p$意义下也应是相等的，即$a^{p-1}(p-1)! \equiv (p-1)! \pmod p$，也即费马小定理的$a^{p-1} \equiv 1 \pmod p$。

设已经有$(\frac{a}{p}) = -1$。类似地，联想到威尔逊定理的形式，我们也希望构造合适的$\frac{p-1}{2}$元集$\mathbb{S}$，通过$a\mathbb{S} = \bar{\mathbb{S}}$来证明$a^{\frac{p-1}{2}} \equiv -1 \pmod p$。我们来考察一个这样的集合(在模$p$意义下):

$$\mathbb{S} = \{1^2, 2^2, \cdots, (\frac{p-1}{2})^2\}.$$

显然$\mathbb{S}$中的元素都是模p的二次剩余。同时，它们两两不同，否则不妨设$i^2 \equiv j^2 \pmod p$，于是有$(i-j)(i+j) \equiv 0 \pmod p$。但$i \neq j$ 且$0 < i + j < p$，得到矛盾。利用这一方法同样可以证明

$$\mathbb{S} = \{(\frac{p+1}{2})^2, (\frac{p+3}{2})^2, \cdots, (p-1)^2\}.$$

所以$\mathbb{S}$确定了模p的所有二次剩余，$|\mathbb{S}| = \frac{p-1}{2}$。

现在由$(\frac{a}{p}) = -1$ 可知a 是模p的一个二次非剩余，我们断言:任取$\mathbb{S}$ 中的元素i^2，则ai^2 是模p 的一个二次非剩余。若不然，则存在整数b，使得$b^2 \equiv a \cdot i^2 \pmod p$。由于$\mathbb{Z}_p \setminus \{0\}$是一个域，所以存在$i$对于$p$的模逆$r = i^{-1}$。在上述同余式两边同乘$r^2$，则有$(rb)^2 \equiv a \pmod p$。这与$a$是二次非剩余相矛盾。

又由于$ai^2 - aj^2 = a(i+j)(i-j)$，故与上面证明$\mathbb{S}$中的元素两两不同一样，可以证明$a\mathbb{S}$中的元素两两不同，于是也有$|a\mathbb{S}| = \frac{p-1}{2}$。这样一来，$|a\mathbb{S}| + |\mathbb{S}| = p + 1$，也就意味着$\mathbb{S}$和$a\mathbb{S}$分别是$p$的所有二次剩余和二次非剩余的集合。特别地，$a\mathbb{S}$又可以表示为$\mathbb{Z}_p \setminus \mathbb{S}$。也就是说，

$$a\mathbb{S} = \mathbb{Z}_p \setminus \mathbb{S}.$$

另一方面，注意到若$t \in \mathbb{S}$，即存在$m^2 \equiv t \pmod p$，那么必定有t的模逆$m^{-2} \equiv t^{-1} \pmod p$，即$t^{-1} \in \mathbb{S}$。记$\mathbb{S}$中所有元素的模逆构成的集合为$\mathbb{S}^{-1}$，则有$\mathbb{S}^{-1} = \mathbb{S}$。代回之前的式子，得到

$$a\mathbb{S} = \mathbb{Z}_p \setminus \mathbb{S}^{-1}.$$

至此，我们依然模仿费马小定理的证明，将两边集合的所有元素各自相乘，得到

$$a^{\frac{p-1}{2}} \cdot \prod_{t \in \mathbb{S}} t \equiv \frac{(p-1)!}{\prod\limits_{t \in \mathbb{S}} t^{-1}} \pmod p,$$

结合威尔逊定理便得到

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

综合上述两种情况，欧拉判别法得证。 □

我们先看欧拉判别法的一个应用。

例1 对奇素数p，用欧拉判别法计算$(\frac{2}{p})$的值。

解 根据欧拉判别法，得到

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

为了计算$2^{\frac{p-1}{2}}$，我们采用和欧拉判别法的证明相似的集合法。有一点不同的是，由于这里不再需要用到太多二次剩余的性质，所以我们无需构造平方元素。取集合

$$\mathbb{S} = \{1, 2, \cdots, \frac{p-1}{2}\} \pmod{p},$$

对其中每个数乘二，得到

$$2\mathbb{S} = \{2, 4, \cdots, p-1\} \pmod{p}.$$

显然，$2\mathbb{S}$中的元素两两模p不同余。并且对其中大于$[\frac{p}{2}]$的所有元素减去p，就得到了一个这样的集合

$$2\mathbb{S} = \{-1, 2, -3, 4, \cdots, \frac{p-1}{2}\} \pmod{p}.$$

注意绝对值为$1, \cdots, \frac{p-1}{2}$的元素恰好各出现了一次，其中负数的个数恰好等于$\frac{p}{2}$和p之间偶数的个数：

$$\#\{k|\frac{p}{2} < 2k < p\} = [\frac{p}{2}] - [\frac{p}{4}] = \frac{p-1}{2} - [\frac{p}{4}] = [\frac{p+1}{4}],$$

故有:

$$2^{\frac{p-1}{2}} \cdot (\frac{p-1}{2})! \equiv (-1)^{[\frac{p+1}{4}]} \cdot (\frac{p-1}{2})! \pmod{p},$$

而$\gcd(p, (\frac{p-1}{2})!) = 1$，所以可以在两边约去相同项，得到

$$2^{\frac{p-1}{2}} \equiv (-1)^{[\frac{p+1}{4}]} \pmod{p}.$$

对p模8的结果分别进行讨论，得

$$(\frac{2}{p}) = \begin{cases} 1 & (p = 8k \pm 1) \\ -1 & (p = 8k \pm 3) \end{cases}.$$

定理 4. $8k-1$型素数有无穷多个。

证明 我们用反证法。如果$8k-1$型素数只有有穷多个。不妨设为p_1，p_2，$\cdots$，p_n。考虑数

$$N = 8p_1^2 p_2^2 \cdots p_n^2 - 1.$$

显而易见地，$N \equiv -1 \pmod 8$，并且对任意$1 \le i \le n$，$p_i \nmid N$。考虑N的素因子q，我们有

$$q \mid 2N = (4p_1p_2\cdots p_n)^2 - 2,$$

即$(\frac{2}{q}) = 1$。由之前的论断，可知q必为$8k+1$型的素数。但若干个$8k+1$型的素数相乘，我们有

$$N \equiv 1 \pmod 8,$$

矛盾!所以假设不成立，即$8k-1$型素数有无穷多个。 □

事实上，更一般地，我们可以证明这样一个定理:

定理 5 (狄利克雷定理(Dirichlet's theorem on arithmetic progressions))**.** *对互素的正整数a和b，在等差数列$\{an+b\}_{n=1}^{\infty}$中，有无穷多个素数存在。*

欧拉判别法不仅为我们提供了勒让德符号数值计算的方法，进一步外推还可以得到一些化简勒让德符号的重要公式。例如

引理6. *对素数$p \ge 3$，若$a \equiv b \pmod p$，那么$(\frac{a}{p}) = (\frac{b}{p})$。*

证明 由欧拉判别法，有

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv (\frac{b}{p}) \pmod p \Rightarrow (\frac{a}{p}) - (\frac{b}{p}) \equiv 0 \pmod p.$$

但另一方面，根据勒让德符号的定义，有

$$|(\frac{a}{p}) - (\frac{b}{p})| \le 2.$$

对照条件的$p \ge 3$，便有$(\frac{a}{p}) = (\frac{b}{p})$。 □

引理7. *对素数$p \ge 3$，$(\frac{a_1a_2\cdots a_n}{p}) = (\frac{a_1}{p})(\frac{a_2}{p})\cdots(\frac{a_2}{p})$。特别地，$(\frac{ab^2}{p}) = (\frac{a}{p})$。*

证明 由欧拉判别法，有

$$\begin{aligned}(\frac{a_1a_2\cdots a_n}{p}) &\equiv (a_1a_2\cdots a_n)^{\frac{p-1}{2}} \\ &= a_1^{\frac{p-1}{2}} \cdot a_2^{\frac{p-1}{2}} \cdot \cdots \cdot a_n^{\frac{p-1}{2}} \\ &\equiv (\frac{a_1}{p})(\frac{a_2}{p})\cdots(\frac{a_2}{p}) \pmod p,\end{aligned}$$

也即

$$(\frac{a_1a_2\cdots a_n}{p}) - (\frac{a_1}{p})(\frac{a_2}{p})\cdots(\frac{a_2}{p}) \equiv 0 \pmod p.$$

仿照上一引理的证明。就得到了$(\frac{a_1a_2\cdots a_n}{p}) = (\frac{a_1}{p})(\frac{a_2}{p})\cdots(\frac{a_2}{p})$。作为特殊情况有$(\frac{ab^2}{p}) = (\frac{a}{p})$成立。 □

定理 8. *给定奇素数p和正整数n，满足$\gcd(p,n) = 1$。记$\frac{p-1}{2}$个整数$n, 2n, \cdots, \frac{p-1}{2}n$对模$p$的最小剩余分别为$r_1, r_2, \cdots, r_u, -r_1', -r_2', \cdots, -r_v'$，其中$r_i, r_j' \in \{1, 2, \cdots, \frac{p-1}{2}\}$，则$u+v = \frac{p-1}{2}$且$(\frac{n}{p}) = (-1)^v$。*

证明 与$n=2$的情况类似，取集合

$$\mathbb{S}=\{1,2,\cdots,\frac{p-1}{2}\} \pmod p.$$

对其中每个数乘n，得到

$$n\mathbb{S}=\{n,2n,\cdots,\frac{p-1}{2}n\} \pmod p.$$

显然，$n\mathbb{S}$中的元素两两模p不同余。所以我们可以断言，任取i,j，必定有$r_i\neq r_j$且$r'_i\neq r'_j$。接下来，假设存在$r_i\neq r'_j$，从而存在不超过$\frac{p-1}{2}$的正整数a和b，分别满足

$$an\equiv r_i \pmod p, \quad bn\equiv -r'_j \pmod p.$$

两式相加，结合假设，得到$(a+b)n\equiv 0 \pmod p$。然而$\gcd(n,p)=1$且$0<a+b<p$，矛盾。所以r_i和r'_j两两不同，从而$u+v=\frac{p-1}{2}$。

与此同时，这也说明$r_1,r_2,\cdots,r_u,r'_1,r'_2,\cdots,r'_v$恰好是$1,2,\cdots,\frac{p-1}{2}$的一个排列。于是将两边的元素在模$p$的意义下相乘，得到

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

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

结合$|(\frac{n}{p})-(-1)^v|\leq 2$和$p$为奇素数，便得到

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

□

2 二次互反律(Law of Quadratic Reciprocity)

首先给出二次互反律的完整表达及其证明。

二次互反律 任给两个不同的奇素数p和q，有

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

证明 首先考虑$(\frac{q}{p})$的计算。由欧拉判别法，有$(\frac{q}{p})=q^{\frac{p-1}{2}}$。与上一节最后的做法类似，我们构造集合

$$q\mathbb{S}=\{q,2q,\cdots,(\frac{p-1}{2})q\} \pmod p,$$

其中$\mathbb{S}=\{1,2,\cdots,\frac{p-1}{2}\}$。把上式两边集合中各元素全部相乘，得到

$$q^{\frac{p-1}{2}}\cdot(\frac{p-1}{2})!\equiv(\frac{p-1}{2})!\cdot(-1)^{\#\{j|\{\frac{qj}{p}\}>\frac{1}{2}\}}.$$

其中$\{x\}$表示数x的小数部分。同样，我们可以在两边约去$(\frac{p-1}{2})!$项，即

$$q^{\frac{p-1}{2}}\equiv(-1)^{\#\{j|\{\frac{qj}{p}\}>\frac{1}{2}\}}.$$

现在问题转换为对$\#\{j|\{\frac{qj}{p}\}>\frac{1}{2}\}$的计算。根据高斯取整符号的定义，我们有

$$qj=p[\frac{qj}{p}]+p\{\frac{qj}{p}\}.$$

注意到$p\{\frac{qj}{p}\}$对任意j为整数。方便起见，记$A=\{j|\{\frac{qj}{p}\}>\frac{1}{2}\}$，其补集$B=\mathbb{S}\setminus\{j|\{\frac{qj}{p}\}>\frac{1}{2}\}$。对上式的两边从$j=1$ 到$j=\frac{p-1}{2}$ 求和，得

$$q\sum_{j=1}^{\frac{p-1}{2}}j=p\sum_{j=1}^{\frac{p-1}{2}}[\frac{qj}{p}]+\sum_{j\in B}p\{\frac{qj}{p}\}+\sum_{j\in A}p\{\frac{qj}{p}\}.$$

对于最后一项，我们做如下变形

$$\begin{aligned}\sum_{j\in A}p\{\frac{qj}{p}\} &= \sum_{j\in A}(p\{\frac{qj}{p}\}+p-p)\\ &= p|A|-\sum_{j\in A}p(1-\{\frac{qj}{p}\}).\end{aligned}$$

将此变形代回求和式，即

$$q\sum_{j=1}^{\frac{p-1}{2}}j=p\sum_{j=1}^{\frac{p-1}{2}}[\frac{qj}{p}]+p|A|+\sum_{j\in B}p\{\frac{qj}{p}\}-\sum_{j\in A}p(1-\{\frac{qj}{p}\}).$$

对两边同时取模2，即得

$$\sum_{j=1}^{\frac{p-1}{2}}j\equiv\sum_{j=1}^{\frac{p-1}{2}}[\frac{qj}{p}]+|A|+\sum_{j\in B}p\{\frac{qj}{p}\}+\sum_{j\in A}p(1-\{\frac{qj}{p}\})\pmod 2.$$

在$1-\{\frac{qj}{p}\}$的作用下，对应的小数部分可以被映射到正的$\{\frac{j}{p}\}$上$(1\le j\le\frac{p-1}{2})$。结合$q\mathbb{S}$中的元素的绝对值在模p 意义下构成的集合恰为$\mathbb{S}$ 的结论，有

$$\sum_{j=1}^{\frac{p-1}{2}}j\equiv\sum_{j=1}^{\frac{p-1}{2}}[\frac{qj}{p}]+|A|+\sum_{j=1}^{\frac{p-1}{2}}p\{\frac{j}{p}\}\equiv\sum_{j=1}^{\frac{p-1}{2}}[\frac{qj}{p}]+|A|+\sum_{j=1}^{\frac{p-1}{2}}j\pmod 2.$$

从而$\sum\limits_{j=1}^{\frac{p-1}{2}}[\frac{qj}{p}]\equiv|A|\pmod 2$，即

$$(\frac{q}{p})\equiv q^{\frac{p-1}{2}}\equiv(-1)^{\sum\limits_{j=1}^{\frac{p-1}{2}}[\frac{qj}{p}]}\pmod p.$$

同理有

$$(\frac{p}{q})\equiv p^{\frac{q-1}{2}}\equiv(-1)^{\sum\limits_{k=1}^{\frac{q-1}{2}}[\frac{pj}{q}]}\pmod q.$$

由于p和q均为奇素数，故以上两式均可写成等式形式:

$$(\frac{q}{p})=(-1)^{\sum\limits_{j=1}^{\frac{p-1}{2}}[\frac{qj}{p}]}\text{fi}\ (\frac{p}{q})=(-1)^{\sum\limits_{k=1}^{\frac{q-1}{2}}[\frac{pk}{q}]}.$$

两式相乘，得到

$$(\frac{q}{p})\cdot(\frac{p}{q})=(-1)^{\sum\limits_{j=1}^{\frac{p-1}{2}}[\frac{qj}{p}]+\sum\limits_{k=1}^{\frac{q-1}{2}}[\frac{pk}{q}]}.$$

最后为了得到二次互反律，我们只需证明等式

$$\sum_{j=1}^{\frac{p-1}{2}}[\frac{qj}{p}]+\sum_{k=1}^{\frac{q-1}{2}}[\frac{pk}{q}]=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

在这里我们直接证明一个更强的命题:任取正奇数m,n，满足$\gcd(m,n)=1$，则

$$\sum_{0<s<m/2}[\frac{n}{m}s]+\sum_{0<t<n/2}[\frac{m}{n}t]=\frac{m-1}{2}\cdot\frac{n-1}{2}.$$

考虑正方形格点图中过原点的一条斜率为$\frac{n}{m}$的直线l。(如图所示)

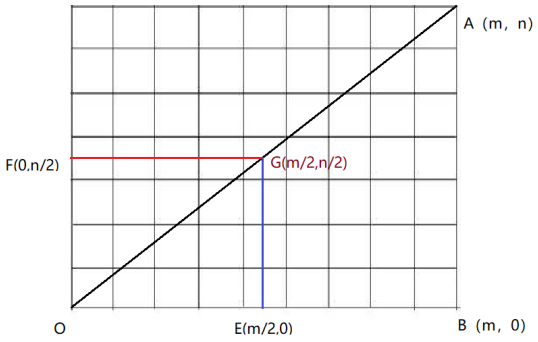

Figure 1: 格点计数示意

接下来，我们对矩形$OEGF$内部的格点进行两种不同方法的计数，来得到要证的式子。首先由奇数条件可知G不是格点，并且由于$\gcd(m,n)=1$，可得三角形OEG内部的格点数为$\sum\limits_{0<s<m/2}[\frac{n}{m}s]$以及，三角形$OFG$内部的格点数为$\sum\limits_{0<t<n/2}[\frac{m}{n}t]$。这样一来，矩形$OEGF$内部的格点数也就可以表示为$\sum\limits_{0<s<m/2}[\frac{n}{m}s]+\sum\limits_{0<t<n/2}[\frac{m}{n}t]$。另一方面，$\{(x,y)|0<s<\frac{m}{2},0<t<\frac{n}{2}\}$表示的矩形$OEGF$内部的格点数显然为$\frac{m-1}{2}\cdot\frac{n-1}{2}$。结合上述两式即得。 □

最后，通过一道例题来说明如何结合欧拉判别法和二次互反律来计算二次剩余。

例2 求$(\frac{40}{67})$。

解

$$\begin{aligned}(\frac{40}{67}) &= (\frac{10}{67})=(\frac{2}{67})\cdot(\frac{5}{67})\\ &= (-1)^{33-16}\cdot(-1)^{2\times33}\cdot(\frac{67}{5})\\ &= (-1)\cdot(\frac{2}{5})=1.\end{aligned}$$