二次互反律

Law of Quadratic Reciprocity

二次互反律：设 p,q 均为奇素数，则有：

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

其中，$\left(\frac{p}{q}\right)$ 表示 **Legendre** 符号。

第一补充定律：

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

第二补充定律：

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

高斯引理 Gauss's Lemma

设 p 是一个奇素数，$p\nmid a$（即 $a\perp p$），考虑如下 $\frac{p-1}{2}$ 个数：

$$a \bmod p,\ 2a \bmod p,\ \cdots,\ \left(\frac{p-1}{2}\right)a \bmod p$$

设 n 是它们中大于 $\frac{p}{2}$ 的数的个数，那么有：

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

证：（以下运算均在模 p 意义下进行）这 $\frac{p-1}{2}$ 个数的乘积是 $a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!$. 但是我们还可以换个角度看它们的乘积。易知这 $\frac{p-1}{2}$ 个数是从 p 的完全剩余系中选出的互不相同的数，所以每一个数要么是 x_i，要么是 $p-x_i$（这里 $x_i\leqslant\frac{p-1}{2}$），且 x_i 互不相同（反证法可证）。于是它们的乘积等于 $\left(\frac{p-1}{2}\right)!$ 乘上 $(-1)^n$，其中 n 是形如 $p-x_i$ 的数，也即 $>\frac{p}{2}$ 的数的个数。于是乎，$a^{\frac{p-1}{2}}=(-1)^n$，由欧拉判别准则知：$\left(\frac{a}{p}\right)=(-1)^n$. 证毕。