数学新星网 ※ 张瑞祥专栏
www.nsmath.cn/zrxzl

模 p 特征与 Polya-Vinogradov 不等式

张瑞祥

对于奇素数 p, 我们知道由二次剩余定义的 Legendre 符号:

$$\left(\frac{n}{p}\right)=\begin{cases}0, & p\mid n\\ 1, & \exists\, m \text{ 使得 } m^2\equiv n \pmod p\\ -1, & \text{否则}\end{cases}$$

是一个非常神奇的函数. 著名的二次互反律告诉我们它有一个很不平凡的性质, 而关于它的其它性质则不那么容易了. 例如, 如果我们取模 p 的最小正二次非剩余, 它会是多大呢? 能不能给出一个不平凡的上界?

一个办法是对任意正整数 $n<p$, 考虑如下的和:

$$T(n)=\sum_{k=1}^{n}\left(\frac{k}{p}\right).$$

显然, 若 $T(n)<n$, 则模 p 的最小正二次非剩余 $\le n$, 反之亦然.

那么如何估计 $T(n)$ 的大小呢? 今天我们要讨论的 Polya-Vinogradov 不等式告诉我们, 引入复数对估计这个实值函数竟然是有帮助的! 为此我们作一些准备工作, 引入 $\{1,\cdots,p\}$ 上的 p 个复值函数 χ_j, $1\le j\le p$. 它们称为模 p 的 **(加性) 特征**.

定义 1. 设 p 为素数, **特征** χ_j $(1\le j\le p)$ 定义为从 $\{1,\cdots,p\}$ 到 $\mathbb{C}$ 的函数:

$$\chi_j(k)=e^{\frac{2\pi ijk}{p}},\quad 1\le j\le p, 1\le k\le p.$$

这里 i 是虚数单位.

定义 2. 定义 **Gauss 和**: $S_j=\sum\limits_{k=1}^{p}\chi_j(k)\cdot\left(\frac{k}{p}\right),\quad 1\le j\le p.$

对于 Gauss 和 S_j, 我们有很好的估计, 这也是我们估计 $T(n)$ 的方法的核心.

收稿日期: **2016-12-05.**

引理 3. $S_p = 0; |S_j| = \sqrt{p},\ \ 1 \leq j < p.$

证明

$$\begin{aligned}
&\sum_{j=1}^{p} |S_j|^2 = \sum_{j=1}^{p} \left| \sum_{k=1}^{p} e^{\frac{2\pi \mathrm{i} jk}{p}} \left(\frac{k}{p}\right) \right|^2 \\
&= \sum_{j=1}^{p} \left(\sum_{k=1}^{p} e^{\frac{2\pi \mathrm{i} jk}{p}} \left(\frac{k}{p}\right) \right) \left(\sum_{l=1}^{p} e^{-\frac{2\pi \mathrm{i} jl}{p}} \left(\frac{l}{p}\right) \right) \\
&= \sum_{1 \leq k,l \leq p} \left(\frac{k}{p}\right) \left(\frac{l}{p}\right) \sum_{j=1}^{p} e^{\frac{2\pi \mathrm{i}(k-l)j}{p}} \\
&= \sum_{1 \leq k \leq p} p \left(\frac{k}{p}\right)^2 \qquad \text{(等比数列求和多数时候为 0)} \\
&= p^2 - p. \qquad (1)
\end{aligned}$$

又显然 $S_p = 0$, 对于 $1 \leq j < p$,

$$\begin{aligned}
S_j &= \left(\sum_{k=1}^{p} e^{\frac{2\pi \mathrm{i} jk}{p}} \left(\frac{jk}{p}\right) \right) \left(\frac{j}{p}\right) \\
&= S_1 \cdot \left(\frac{j}{p}\right).
\end{aligned}$$

故对任意 $1 \leq j < p$, 有 $\left|S_j\right| = \left|S_1\right|$. 因此由 (1) 必有

$$\left|S_1\right| = \left|S_2\right| = \cdots = \left|S_{p-1}\right| = \sqrt{p}. \qquad \square$$

我们现在设法使 $T(n)$ 被诸 S_j $(1 \leq j \leq p)$ 表出. 如果复数 $\lambda_1 = \lambda_1(n), \cdots, \lambda_p = \lambda_p(n)$ 使得方程组

$$\begin{cases} \sum_{j=1}^{p} \lambda_j \chi_j(k) = 1, & 1 \leq k \leq n \\ \sum_{j=1}^{p} \lambda_j \chi_j(k) = 0, & n < k \leq p \end{cases} \qquad (2)$$

成立, 则

$$\begin{aligned}
T(n) &= \sum_{k=1}^{p} \left(\frac{k}{p}\right) \sum_{j=1}^{p} \lambda_j \chi_j(k) \\
&= \sum_{j=1}^{p} \lambda_j \sum_{k=1}^{p} \chi_j(k) \left(\frac{k}{p}\right) \\
&= \sum_{j=1}^{p} \lambda_j S_j.
\end{aligned}$$

从而由引理 3,

$$\left|T(n)\right| \leq \sqrt{p}\sum_{j=1}^{p-1}\left|\lambda_j\right|. \tag{3}$$

现在估计 $\left|\lambda_j\right|$, 我们希望用消元法从 (2) 中反解出 λ_j. 考虑

$$\begin{aligned}\left|\sum_{k=1}^{n}\overline{\chi_{j_0}(k)}\right| &= \left|\sum_{k=1}^{p}\overline{\chi_{j_0}(k)}\sum_{j=1}^{p}\lambda_j\chi_j(k)\right| \\ &= \left|\sum_{j=1}^{p}\lambda_j\sum_{k=1}^{p}\overline{\chi_{j_0}(k)}\chi_j(k)\right| \\ &= \left|\sum_{j=1}^{p}\lambda_j\sum_{k=1}^{p}e^{2\pi \mathrm{i}k(j-j_0)}\right| \\ &= \left|p\lambda_{j_0}\right|. \end{aligned} \tag{4}$$

(**注**. 不难检验这样反解出的 $\{\lambda_j\}$ 确实是 (2) 的解, 证明留给读者.)

而由等比数列求和, 当 $j_0 \neq p$ 时上式左端 $\leq \max\left\{\frac{C_1 p}{j_0}, \frac{C_1 p}{p-j_0}\right\}$. 其中 C_1 是正常数 (细节请读者自行补出). 故

$$\left|\lambda_{j_0}\right| \leq \max\left\{\frac{C_1}{j_0}, \frac{C_1}{p-j_0}\right\}. \tag{5}$$

代入 (3), 熟知调和级数的部分和是 log 级别大小, 我们知存在正常数 C_2 使得 $|T(n)| \leq C_2\sqrt{p}\log p$. 我们得到了数论中 Polya-Vinogradov 不等式的一个最简单情形.

因此当 $n > C_2\sqrt{p}\log p$ 时, $|T(n)| < n$. 这样, 我们就知道模 p 的最小二次非剩余至多大约是 $p^{\frac{1}{2}+\varepsilon}$ 量级的 ($\varepsilon > 0$ 任意小).

最后要说明的是: 这里我们“解方程”的过程用到了线性代数中“标准正交基”的性质. 适当乘以一个数后, (加性) 特征构成一组标准正交基, 给了我们很好的代数结构 (见引理 3 及 (4) 式), 才使得我们的证明得以成立. (5) 式的估计是所谓“Fourier 系数”的估计. 有兴趣的同学可以查阅相关文献.

我们估计部分和 $T(n)$ 的技巧称为“补全求和”: 既然对于 $\left(\frac{k}{p}\right)$ 的部分和我们不好估计, 那么就设法把它转化为在整段 $1-p$ 上的求和 (Gauss 和), 从而利用 Gauss 和的结构性估计达到目的.

我们得到的指标 $\frac{1}{2}+\varepsilon$ 很不平凡, 但它也不是最好的. Vinogradov 曾将此指标降到 $\frac{1}{4\sqrt{e}}+\varepsilon$. 我们猜想它可被改进为任意 $\varepsilon > 0$. 但这个问题很难, 目前大家还找不到办法证明它.