关于特征和的估計及其应用*

王　元

(中国科学院数学研究所)

1. 介紹.　运用 Weil[1] 关于有限代数函数体上的 Riemann 猜想的貢献，Burgess[2] 首先引进了一个估計特征和的方法，对于模 p（素数）的实原特征的情形，他改进了熟知的 Pólya 的結果．以后，作者[4]及他本人[5,6]又推广与改进了他的結果，并得到了一系列应用．他的方法的最后形式可以表述为

定理 A[6].　命 χ 为模 k 之原特征．又命 η，r 分別为任意給予的正数与正整数．若 k 无平方因子或 $r=2$，則对于任意一对整数 N，$H\,(H>0)$ 皆有

$$\left|\sum_{n=N+1}^{N+H}\chi(n)\right|\leqslant c_1(r,\eta)H^{1-\frac{1}{r+1}}k^{\frac{1}{4r}+\eta}.$$

由此吾人有下面两个推論：

推論 1[6].　若 $\chi(n)=\left(\frac{f}{n}\right)$ 为模 f 的实原特征，則

$$\left|\sum_{n=1}^{H}\left(\frac{f}{n}\right)\right|\leqslant c_2(r,\eta)H^{1-\frac{1}{r+1}}f^{\frac{1}{4r}+\eta},$$

此处 $\left(\frac{f}{n}\right)$ 为 Kronecker 符号．

推論 2[4].　若 χ 为模 p 的非主特征，則当 $H>p^{\frac{1}{4}+\eta}$ 时

$$\left|\sum_{n=1}^{H}\chi(n)\right|<c_3(\eta)\frac{H}{p^{\eta^2/6}}.$$

本文的目的在于将这些估計用于 Pell 氏方程的最小解問題及模 p 的最小 n 次非剩余問題．此外本文还要在广义 Riemann 猜想之下来討論最小 n 次非剩余問題．

命 d 为正整数但非完全平方，$d\equiv 0$ 或 $1\pmod 4$．整点 $(x_0,\,y_0)\,(x_0>0,\,y_0>0)$ 为下面 Pell 氏方程

$$x^2-dy^2=4$$

的解，使 $x_0+\sqrt{d}\,y_0$ 最小者．命

$$\varepsilon=\frac{x_0+\sqrt{d}\,y_0}{2}.$$

定理 1.　对于任意 $\delta>0$，皆存在 $c_4(\delta)$，当 $d>c_4(\delta)$ 时

$$\ln\varepsilon<\left(\frac{1}{4}+\delta\right)\sqrt{d}\ln d.$$

这一結果改良了华罗庚[7]的結果．

* 1962 年 9 月 25 日收到．

命 $n \geqslant 2$ 及 $n \mid (p-1)$. 若同余式

$$x^n \equiv c \pmod p, \quad 1 \leqslant x \leqslant p$$

无解，则称 c 为模 p 之 n 次非剩余，否則，称 c 为模 p 的 n 次剩余. 記最小的正 n 次非剩余为 $N(p, n)$.

定理 2. 命 δ 为任意給予的正数，则当 p 充分大时有

(i) $N(p, n) \leqslant p^{\frac{1}{4e^{\frac{n-1}{n}}}+\delta} \quad (n \geqslant 2)$,

(ii) $N(p, n) \leqslant p^{\frac{1}{12}} \quad (n \geqslant 21)$

及

(iii) $N(p, n) \leqslant p^{\frac{\ln\ln n+2}{4\ln n}} \quad (n > e^{33})$.

(i) (ii) 与 (iii) 分别是 Виноградов[8] 与 Бухштаб[9] 的結果的改良.

II. 定理 1 的証明. 命

$$\sigma(a) = \sum_{n=1}^{a} \left(\frac{d}{n}\right), \quad K(d) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) \frac{1}{n}.$$

引 1. 命 $r \geqslant 4$ 为任意整数及 $\tau = \frac{1}{r}$. 則当 $a \geqslant d^{\frac{1}{4}+\tau}$ 时

$$|\sigma(a)| \leqslant c_5(\tau) a d^{-\tau^2/6}.$$

証. 命 $d = fm^2$，此处 f 为基本判别式，则

$$\sigma(a) = \sum_{n=1}^{a} \left(\frac{d}{n}\right) = \sum_{\substack{n=1 \\ (n,m)=1}}^{a} \left(\frac{f}{n}\right) = \sum_{n=1}^{a} \left(\frac{f}{n}\right) \sum_{k \mid (n,m)} \mu(k) =$$

$$= \sum_{k \mid m} \mu(k) \left(\frac{f}{k}\right) \sum_{n \leqslant a/k} \left(\frac{f}{n}\right).$$

因此

$$|\sigma(a)| \leqslant \sum_{k \mid m} \left| \sum_{n \leqslant a/k} \left(\frac{f}{n}\right) \right|.$$

故由推理 1 可知

$$|\sigma(a)| \leqslant \sum_{k \mid m} c_6(\tau) \left(\frac{a}{k}\right)^{1-\frac{1}{r+1}} f^{\frac{1}{4r}+\frac{1}{4r(r+1)}} \leqslant c_5(\tau) a^{1-\frac{1}{r+1}} d^{\frac{1}{4r}+\frac{1}{2r(r+1)}} \leqslant$$

$$\leqslant c_5(\tau) a d^{-\frac{1}{4(r+1)}-\frac{1}{r(r+1)}+\frac{1}{4r}+\frac{1}{2r(r+1)}} = c_5(\tau) a d^{-\frac{1}{4r(r+1)}} < c_5(\tau) a d^{-\tau^2/6}.$$

引理証完.

引 2. 对任意給予 $0 < \delta < \frac{1}{2}$，皆存在 $c_7(\delta)$，当 $d > c_7(\delta)$ 时

$$K(d) < \left(\frac{1}{4} + \delta\right) \ln d.$$

証. $K(d) = \sum_{n=1}^{\infty} \frac{\sigma(n) - \sigma(n-1)}{n} = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n(n+1)} = \Sigma_1 + \Sigma_2 + \Sigma_3.$

命 $\tau=\frac{1}{r}\leqslant\frac{\delta}{2}<2\tau$,此处 r 为一个整数. 则

$$|\Sigma_1|\leqslant\left|\sum_{1\leqslant n<d^{\frac{1}{4}+\tau}}\frac{\sigma(n)}{n(n+1)}\right|\leqslant\sum_{1\leqslant n<d^{\frac{1}{4}+\tau}}\frac{1}{n+1}<$$

$$<\int_1^{d^{\frac{1}{4}+\tau}}\frac{dt}{t}+\frac{1}{d^{\frac{1}{4}+\tau}}\leqslant\left(\frac{1}{4}+\frac{\delta}{2}\right)\ln d+\frac{1}{d^{\frac{1}{4}+\frac{\delta}{4}}},$$

故由引 1 可知

$$|\Sigma_2|=\left|\sum_{d^{\frac{1}{4}+\tau}\leqslant n<d}\frac{\sigma(n)}{n(n+1)}\right|\leqslant c_8(\delta)d^{-\frac{\delta^2}{96}}\sum_{1\leqslant n<d}\frac{1}{n+1}<c_8(\delta)d^{-\frac{\delta^2}{96}}\ln d.$$

最后,由 Pólya 定理可知

$$|\sigma(a)|\leqslant\sum_{k|m}\sqrt{f}\ln f<\sqrt{d}\ln d.$$

因此

$$|\Sigma_3|\leqslant\sqrt{d}\ln d\cdot\sum_{n>d}\frac{1}{n(n+1)}=\frac{\ln d}{\sqrt{d}}.$$

綜合上述,即得引理.

定理 1 是引 2 的推論(見[10]).

III. 定理 2 的証明.

引 3[9]. 命 $\Psi(x,y)$ 表示不超过 x 且仅含有 $\leqslant y$ 的素因子的正整数的个数. 则

$$\Psi(x,x^{\frac{1}{a}})=\rho(a)x+O\left(\frac{x}{\sqrt{\ln x}}\right),$$

此处与“O”有关的常数仅依于 a,而

$$\rho(a)=\begin{cases}1, & \text{若 } 0<a\leqslant 1;\\ 1-\int_1^a\frac{dz_1}{z_1}+\int_2^a\int_1^{z_1-1}\frac{dz_1dz_2}{z_1z_2}-\cdots+ & \\ \qquad+(-1)^{[a]}\int_{[a]}^a\int_{[a-1]}^{z_1-1}\cdots\int_1^{z_{[a-1]}-1}\frac{dz_1\cdots dz_{[a]}}{z_1\cdots z_{[a]}}, & \text{若 } a>1.\end{cases}$$

由此可見 $\rho(a)$ 为一个連續单調递減函数,且当 $a\geqslant 6$ 时

$$\rho(a)>e^{-a\left(\ln a+\ln\ln a+\frac{6\ln\ln a}{\ln a}\right)}.$$

引 4. 命 R 表示模 p 在区間 $1\leqslant c\leqslant H$ 中的 n 次剩余的个数. 若 $n|(p-1)$, $n\geqslant 2$ 及 $H>p^{\frac{1}{4}+\eta}$ $(\eta>0)$,则

$$R=\frac{H}{n}+S,$$

此处

$$|S|<c_9(\eta)Hp^{-\eta^2/6}.$$

証. 命 $\chi(x)=e^{2\pi i\,\mathrm{Ind}\,x/n}$. 则由推論 2 可知

$$R=\sum_{x=1}^{H}\frac{1}{n}\sum_{a=1}^{n}e^{2\pi ia\,\mathrm{Ind}\,x/n}=\frac{H}{n}+\frac{1}{n}\sum_{a=1}^{n-1}\sum_{x=1}^{H}\chi(x)^a=\frac{H}{n}+S,$$

此处

$$|S| < c_9(\eta)Hp^{-\eta^2/6}.$$

引理証完.

引 5. 若 $n \geqslant 2$, $n|(p-1)$ 及 $\rho(\alpha) > \frac{1}{n} + \delta(\delta > 0)$, 则存在 $c_{10}(\alpha, \delta)$, 当 $p > c_{10}(\alpha, \delta)$ 时, $N(p, n) \leqslant p^{\frac{1}{4\alpha}}$.

証. 取 $H = [p^{\frac{1}{4}+\eta}] + 1(\eta > 0)$. 若 $N(p, n) > p^{\frac{1}{4\alpha}}$,则不超过$H$且仅含有 $\leqslant p^{\frac{1}{4\alpha}}$ 的素因子的正整数都是 n 次剩余. 定义R如引 4, 則当 $\eta = \eta(\delta)$ 充分小时

$$R \geqslant \Psi(H, p^{\frac{1}{4\alpha}}) \geqslant \rho((1+5\eta)\alpha)H + O\left(\frac{H}{\sqrt{\ln p}}\right) >$$

$$> \left(\frac{1}{n} + \frac{\delta}{2}\right)H + O\left(\frac{H}{\sqrt{\ln p}}\right),$$

故由引 4 可知

$$\frac{H}{n} + O(Hp^{-\eta^2/6}) \geqslant \left(\frac{1}{n} + \frac{\delta}{2}\right)H + O\left(\frac{H}{\sqrt{\ln p}}\right),$$

此处与“O”有关的常数仅依于 α 及 δ. 当 p 充分大时,上式是不可能的. 故明所欲証.

現在我們来証明定理 2 如下:

(i) 取 $\alpha = e^{\frac{n-1}{n}-\tau}\left(\frac{1}{2} > \tau > 0\right)$, 則

$$\rho(\alpha) \geqslant 1 - \ln \alpha = \frac{1}{n} + \tau.$$

故有 $c_{11}(n, \tau)$,当 $p > c_{11}(n, \tau)$ 及 $n \geqslant 2$ 时

$$N(p, n) \leqslant p^{\frac{1}{4e^{\frac{n-1}{n}}}+\delta},$$

此处 $\delta > 0$ 而且 $\lim\limits_{\tau\to 0}\delta = 0$.

(ii) 取 $\alpha = 3$. 則

$$\rho(3) = 1 - \ln 3 + \int_2^3\int_1^{z_1-1}\frac{dz_1dz_2}{z_1z_2} > 0.4804 > \frac{1}{21}.$$

因此存在 c_{12},当 $p > c_{12}$ 及 $n \geqslant 21$ 时

$$N(p, n) \leqslant p^{\frac{1}{12}}.$$

(iii) 取 $\alpha = \frac{\ln n}{\ln\ln n + 2}$. 則当 $n > e^{33}$ 吾人恆可选取 $\delta = \delta(n) > 0$ 使

$$\rho(\alpha) > \frac{1}{n} + \delta.$$

故存在 $c_{13}(n)$,当 $p > c_{13}(n)$ 及 $n > e^{33}$ 时

$$N(p, n) \leqslant p^{\frac{\ln\ln n + 2}{4\ln n}}.$$

IV. 条件結果.

引 6.[4,11] 在广义 Riemann 猜想之下,

$$\sum_{n=1}^{\infty} \Lambda(n)\chi(n)e^{-\frac{n}{x}} = \begin{cases} x + O(x^{\frac{1}{2}}\ln p), \text{若 } \chi \text{ 为模 } p \text{ 的主特征 } \chi_0; \\ O(x^{\frac{1}{2}}\ln p), \text{若 } \chi \text{ 为模 } p \text{ 的非主特征,} \end{cases}$$

此处及以后与"O"有关的常数皆絕对常数.

定理 3. 在广义 Riemann 猜想之下

$$N(p, n) = O(\ln^2 p) \quad (n \geqslant 2).$$

証. 习知当 $x \geqslant 2$ 时,有 $c_{14} > 0$ 使

$$\Psi(x) = \sum_{n \leqslant x} \Lambda(n) \leqslant c_{14}x.$$

由分部求和可知当 $c_{15} > 1$ 时

$$\sum_{n > c_{15}x} \Lambda(n)e^{-\frac{n}{x}} \leqslant c_{14}e^{-c_{15}}(c_{15} + 1)x.$$

考虑

$$R(x) = \sum_{r_n \leqslant c_{15}x} \chi_0(r_n)\Lambda(r_n)e^{-\frac{r_n}{x}},$$

此处 $\sum\limits_{r_n \leqslant c_{15}x}$ 表示通过所有 $\leqslant c_{15}x$ 的正 n 次非剩余求和. 則

$$R(x) \geqslant \sum_{r_n \geqslant 1} \chi_0(r_n)\Lambda(r_n)e^{-\frac{r_n}{n}} - \sum_{m > c_{15}x} \Lambda(m)e^{-\frac{m}{x}} \geqslant$$

$$\geqslant \sum_{m=1}^{\infty} \chi_0(m)\Lambda(m)e^{-\frac{m}{x}}\left(1 - \frac{1}{n}\sum_{a=1}^{n} e^{2\pi i a \operatorname{Ind} m/n}\right) - c_{14}e^{-c_{15}}(c_{15} + 1)x =$$

$$= \left(1 - \frac{1}{n}\right)\sum_{m=1}^{\infty} \chi_0(m)\Lambda(m)e^{-\frac{m}{x}} - \frac{1}{n}\sum_{a=1}^{n-1}\sum_{m=1}^{\infty} \Lambda(m)\chi_0(m)e^{2\pi i a \operatorname{Ind} m/n}e^{-\frac{m}{x}} -$$

$$- c_{14}e^{-c_{15}}(c_{15} + 1)x \geqslant \left(1 - \frac{1}{n} - c_{14}e^{-c_{15}}(c_{15} + 1)\right)x + O(x^{\frac{1}{2}}\ln p).$$

取 $x = c_{16}\ln^2 p$. 当 c_{15}, c_{16} 充分大时可知

$$R(x) > 0.$$

换言之

$$N(p, n) \leqslant c_{15}c_{16}\ln^2 p.$$

定理証完.

参　考　文　献

[1] Weil, A., Sur les courbes algébriques et les variétés qui s'en déduisent, *Pub. Inst. Math. Strasbourg*, (N. S. Nr. 2) (1948), 1—85.

[2] Burgess, D. A., The distribution of quadratic residues and non-residues, *Mathematica*, London, **4** (1957), 106—112.

[3] P. Pólya, Über die Verteilung der Quadratischen Reste und Nichtreste, *Nachr. Ges. Wiss. Göttingen* (1918), 21—29.

[4] 王 元, 論素数的最小正原根, 数学学报, **9**:4 (1959), 432—441.

[5] Burgess, D. A., On character sums and primitive roots, *Proc. Lond. Math. Soc.*, **XII** (1962), 179—192.
[6] Burgess, D. A., On character sums and L-series, *Proc. Lond. Math. Soc.*, **XII** (1962), 193—206.
[7] Hua Loo-keng (华罗庚), On the least solution of Pell's equation, *Bull. Amer. Math. Soc.*, **48** (1942), 731—735.
[8] Виноградов, И. М., О границе наименьшего невычета n-й степени, *ИАН СССР, Серия Матем.*, **20** (1926), 47—58.
[9] Бухштаб, А. А., О числах арифметической прогрессии у которых все простые множители малы по порядку роста, *ДАН СССР*, **67**, 1 (1947), 5—8.
[10] 华罗庚，数論导引，第 12 章，科学出版社，1957.
[11] Ankeny, N. C., The least quadratic non-residue, *Ann. of Math.*, **55** (1952), 65—72.