第 21 卷 第 3 期 华侨大学学报(自然科学版) Vol. 21 No. 3
2000 年 7 月 Journal of Huaqiao University (Natural Science) Jul. 2000

文章编号 1000-5013(2000)03-0234-05

Bernoulli 数与判别素数的充要条件

王云葵 马武瑜

(广西民族学院数学与计算机科学系, 南宁 530006)

摘要 利用等幂和与判别素数的充要条件及等幂和与 Bernoulli 数的同余关系, 获得与 Bernoulli 数有关的判别素数的充要条件, 还得到整除 Bernoulli 数的充要条件.

关键词 等和幂和, Bernoulli 数, 充要条件

中图分类号 O 156 文献标识码 A

著名的 Bernoulli 数 B_m 与等幂和 $S_m(n)=1^m+2^m+\cdots+n^m$ 有着密切联系[1], 其关系式为

$$nB_{2m}+nmS_{2m-1}(n-1)=\sum_{j=0}^{m}C_{2m}^{2j}B_{2j}n^{2j}S_{2m-2j}(n-1). \tag{1}$$

等幂和与 Bernoulli 数在数论研究中占有极其重要的地位. 例如, 它们与丢番图方程、Giuga 猜想[2]、Bowen 猜想[3]及素数判别[4]等密切相关, 特别是 Bernoulli 数在 Fermat 大定理的研究中很有用. 1857 年 Kummer 证明[5] $p>3$ 为正规素数的充要条件, 是 p 不整除 Bernoulli 数 B_{2k} $(2\leq 2k\leq p-3)$ 的分子, 并且若 p 为正规素数, 则 Fermat 大定理成立. 1929 年 Vandiver 证明了[5]若 $p^3\mid B_{2pk}(2\leq 2k\leq p-3)$ 的分子, 则 Fermat 大定理成立. 1999 年, 我们获得了 Bernoulli 数的同余关系[6]. 本文利用等幂和与 Bernoulli 数的同余关系, 获得 Bernoulli 数与判别素数的充要条件, 得到整除 Bernoulli 数的充要条件, 还给出 Giuga 猜想的等价命题.

1 等幂和与 Bernoulli 数的同余关系

引理 **1**[2] $m\geq 1, n\geq 2$, 则 $n\mid nB_{2m}$ 的分母.

引理 **2**[4] p 为素数的充要条件是满足: (1) 当 $(p-1)\mid m$ 时, $S_m(p-1)\equiv 0\pmod p$; (2) 当 $(p-1)\mid m$ 时, $S_m(p-1)\equiv -1\pmod p$.

引理 **3**[4] 奇数 p 为素数的充要条件是满足: (1) 对 $2\leq 2m\leq \frac{p}{5}-1$ 有 $S_{2m}(p-1)\equiv 0\pmod p$; (2) $S_{p-1}(p-1)\equiv -1\pmod p$.

引理 **4**[7] $m\geq 1, p\geq 3$ 为奇数, 则

$$S_{2m}(p-1)\equiv 2S_{2m}\left(\frac{p-1}{2}\right)-2mpS_{2m-1}\left(\frac{p-1}{2}\right)+$$

收稿日期 1999-11-18 作者简介 王云葵(1965-), 男, 讲师

基金项目 广西民族学院重点科研基金资助项目

$$p^2C_{2m}^2S_{2m-2}\left(\frac{p-1}{2}\right)\ (\mathrm{mod}\ p^3), \tag{2}$$

$$S_{2m+1}(p-1)\equiv(2m+1)pS_{2m}\left(\frac{p-1}{2}\right)-p^2C_{2m+1}^2S_{2m-1}\left(\frac{p-1}{2}\right)(\mathrm{mod}\ p^3), \tag{3}$$

$$2S_{2m+1}(p-1)\equiv(2m+1)pS_{2m}(p-1)-\frac{1}{2}p^3C_{2m+1}^3S_{2m-2}(p-1)\ (\mathrm{mod}\ p^4). \tag{4}$$

定理 **1**　$m\geq 2, p\geq 3$ 为奇数, 则

$$S_{2n}(p-1)\equiv pB_{2m}+\frac{1}{3}p^2C_{2m}^2S_{2m-2}(p-1)(\mathrm{mod}\ p^3), \tag{5}$$

$$S_{2m}(p-1)\equiv pB_{2m}+\frac{1}{3}p^3C_{2m}^3B_{2m-2}(\mathrm{mod}\ p^3). \tag{6}$$

证明　由引理 1 有 $p^3\mid p^{2j}B_{2j}(2\leq j\leq m)$ 的分子, 从而由式(1)有

$$S_{2m}(p-1)\equiv pB_{2m}+mpS_{2m-1}(p-1)-\frac{1}{6}p^2C_{2m}^2S_{2m-2}(p-1)\ (\mathrm{mod}\ p^3). \tag{7}$$

因 $m\geq 2$, 由式(4)得 $2S_{2m-1}(p-1)\equiv(2m-1)pS_{2n-2}(p-1)\ (\mathrm{mod}\ p^2)$, 即

$$2mpS_{2m-1}(p-1)\equiv p^2C_{2m}^2S_{2m-2}(p-1)\ (\mathrm{mod}\ p^3). \tag{8}$$

将式(8)代入式(7)即得式(5), 从而有 $S_{2n-2}(p-1)\equiv pB_{2m-2}(\mathrm{mod}\ p^2)$. 将它代入式(5), 即得式(6).

定理 **2**　$m\geq 2$, $p\geq 5$ 为奇数, 并且 $p\mid C_{2m}^2$, 则

$$S_{2m}(p-1)\equiv pB_{2m}+\frac{1}{3}p^2C_{2m}^2S_{2n-2}(p-1)\ (\mathrm{mod}\ p^4), \tag{9}$$

$$S_{2m}(p-1)\equiv pB_{2m}+\frac{1}{3}p^2C_{2m}^2S_{2m-2}(\mathrm{mod}\ p^4). \tag{10}$$

证明　由引理 1 有 $p^5\mid p^{2j}B_{2j}(3\leq j\leq m)$ 的分子. 利用式(1)及 $B_2=\frac{1}{6}$, $B_4=-\frac{1}{30}$, 得

$$S_{2m}(p-1)\equiv pB_{2m}+mpS_{2n-1}(p-1)-\frac{1}{6}p^2C_{2m}^2S_{2m-2}(p-1)+$$

$$\frac{1}{30}p^4C_{2m}^4S_{2m-4}(p-1)\ (\mathrm{mod}\ p^5). \tag{11}$$

因 $p\geq 5$, 为奇数, $p\mid C_{2n}^2$, 故 $p\mid C_{2m}^4$, $p\mid C_{2n+1}^3$. 由式(4)和式(11), 得

$$S_{2m}(p-1)\equiv pB_{2m}+mpS_{2m-1}(p-1)-\frac{1}{6}p^2C_{2m}^2S_{2m-2}(p-1)\ (\mathrm{mod}\ p^4), \tag{12}$$

$$2mS_{2n-1}(p-1)\equiv pC_{2m}^2S_{2m-4}(p-1)\ (\mathrm{mod}\ p^4). \tag{13}$$

将式(13)代入式(12)即得式(9), 从而有 $S_{2m-2}(p-1)\equiv pB_{2m-2}(\mathrm{mod}\ p^3)$. 再代入式(9), 即得式(10).

2　Bernoulli 数与判别素数的充要条件

1950 年 Giuga 猜想, p 为素数的充要条件是 $S_{p-1}(p-1)\equiv -1\ (\mathrm{mod}\ p)$. 对此, 文献[8]等有关学者曾进行过大量的研究, 1998 年文献[9]又利用 Bernoulli 数获得了 Giuga 猜想的深刻结果.

引理 **5**　奇数 p 为素数的充要条件是满足: (1)　当 $(p-1)\mid 2m$ 时, 与 B_{2m} 的分母互素;

(2) 当$(p-1)\mid 2m$时,$(p\mid pB_{2m}+1)$的分子.

引理**6**[9] 奇数p为素数的充要条件是满足:(1) 对$2\leq 2m\leq \frac{p}{5}-1$有$p$与$B_{2m}$的分母互素;(2) $p\mid pB_{p-1}+1)$的分子.

引理**7**[2] $m\geq 1$,设满足$(p-1)\mid 2m$的所有不同的素数为$p_1,p_2,\cdots,p_s$,则有:(1) B_{2m}的分母是$p_1p_2\cdots p_s(S\geq 2)$;(2) $B_{2m}=a_{2m}-\sum_{j=1}^{s}\frac{1}{p_j}$,$a_{2m}$为整数.

定理**3** 奇数p为素数的充要条件是满足:(1) 当$(p-1)\mid 2m$时,$S_{2m}(p-1)\equiv 0\pmod p$;(2) 当$(p-1)\mid 2m$时,$S_{2m}(p-1)\equiv -1\pmod p$.

证明 对任何奇数$p\geq 3$有$(p-1)\mid(2m+1)$,由式(4)有$S_{2m+1}(p-1)\equiv 0\pmod p$,故由引理2即得证.

定理**4** 奇数p为素数的充要条件是满足:(1) 当$(p-1)\mid 2m$时,$S_{2m}(\frac{p-1}{2})\equiv 0\pmod p$;(2) 当$(p-1)\mid 2m$时,$S_{2m}(\frac{p-1}{2})\equiv(\frac{p-1}{2})\pmod p$.

证明 由式(2)知,对奇数$p\geq 3$有$S_{2m}(p-1)\equiv 2S_{2m}(\frac{p-1}{2})\pmod p$. 因此,$S_{2m}(p-1)\equiv 0\pmod p\Leftrightarrow S_{2m}(\frac{p-1}{2})\equiv 0\pmod p$,$S_{2m}(p-1)\equiv -1\pmod p\Leftrightarrow S_{2m}(\frac{p-1}{2})\equiv\frac{p-1}{2}\pmod p$. 再由定理3即得证.

定理**5** $m\geq 2,(p,3)=1,p\mid C_{2m}^2$,则奇数$p$为素数的充要条件是满足:(1) 当$(p-1)\mid(2m-2)$时,$S_{2m}(p-1)\equiv pB_{2m}\pmod{p^3}$;(2) 当$p-1\mid 2m-2$时,$S_{2m}(p-1)\equiv pB_{2m}-\frac{1}{3}p^2C_{2m}^2\pmod{p^3}$.

证明 因$(p,3)=1,p\mid C_{2m}^2$,故对奇数$p\geq 3$有

$$S_{2m-2}(p-1)\equiv 0\pmod p\Leftrightarrow\frac{1}{3}p^2C_{2m}^2S_{2m-2}(p-1)\equiv 0\pmod{p^3},$$

$$S_{2m-2}(p-1)\equiv -1\pmod p\Leftrightarrow\frac{1}{3}p^2C_{2m}^2S_{2m-2}(p-1)\equiv -\frac{1}{3}p^2C_{2m}^2\pmod{p^3}.$$

再由式(5)及定理3即得证.

定理**6** $m\geq 2,(p,3)=1,p\parallel C_{2m}^2$,则奇数$p$为素数的充要条件是满足:(1) 当$(p-1)\mid(2m-2)$时,$S_{2m}(p-1)\equiv pB_{2m}\pmod{p^4}$,(2) 当$(p-1)\mid(2m-2)$时,$S_{2m}(p-1)\equiv pB_{2m}-\frac{1}{3}p^2C_{2m}^2\pmod{p^4}$.

证明 因$(p,3)=1,p\parallel C_{2m}^2$,故对任何奇数$p$有

$$S_{2m-2}(p-1)\equiv 0\pmod p\Leftrightarrow\frac{1}{3}p^2C_{2m}^2S_{2m-2}(p-1)\equiv 0\pmod{p^4},$$

$$S_{2m-2}(p-1)\equiv -1\pmod p\Leftrightarrow\frac{1}{3}p^2C_{2m}^2S_{2m-2}(p-1)\equiv -\frac{1}{3}p^2C_{2m}^2\pmod{p^4}.$$

故由式(9)及定理3即得证.

定理**7** $(3,p)=1$,则奇数p为素数的充要条件是满足:(1) 对$4\leq 2m\leq\frac{p}{5}+1$有$S_{2m}(p$

$-1)\equiv pB_{2m}(\mathrm{mod}\ p^3)$; (2) $S_{p+1}(p-1)\equiv pB_{p+1}-\frac{1}{6}p^3(\mathrm{mod}\ p^4)$.

证明　因 $2\leq 2m-2\leq \frac{p}{5}-1$ 且 $p\mid C_{2m}^2$, 故由式(5)得

$$S_{2m-2}(p-1)\equiv 0\ (\mathrm{mod}\ p)\Leftrightarrow S_{2m}(p-1)\equiv pB_{2m}(\mathrm{mod}\ p^3).$$

当 $2m=p+1$ 时 $p\mid C_{p+1}^2$, 由式(9)得 $S_{p+1}(p-1)\equiv pB_{p+1}+\frac{1}{6}p^3S_{p-1}(p-1)\ (\mathrm{mod}\ p^4)$, 故

$$S_{p-1}(p-1)\equiv -1\ (\mathrm{mod}\ p)\Leftrightarrow S_{p+1}(p-1)\equiv pB_{p+1}-\frac{1}{6}p^3(\mathrm{mod}\ p^4).$$

于是, 由引理 3 即得证.

定理 8　$m\geq 1$, 设满足 $p_i-1\mid 2m$ 的所有素数为 $p_1, p_3, \cdots, p_s$, 则奇数 p 为素数的充要条件是满足: (1) 当 $(p-1)\mid 2m$ 时, $(p, p_1p_2\cdots p_s)=1$; (2) 当 $(p-1)\mid 2m$ 时, $\sum_{j=1}^{s}\frac{p}{p_j}\equiv 1\ (\mathrm{mod}\ p)$.

证明　由引理 7 可知, B_{2m} 的分母是 $p_1p_2\cdots p_s$, 并且 $B_{2m}=a_{2m}-\sum_{j=1}^{s}\frac{p}{p_j}$, a_{2m} 为整数, 故 p 与 B_{2m} 的分母互素 $\Leftrightarrow (p, p_1p_2\cdots p_s)=1, p\mid (pB_{2m}+1)$ 的分子 $\Leftrightarrow \sum_{j=1}^{s}\frac{p}{p_j}\equiv 1\ (\mathrm{mod}\ p)$. 再由引理 5 即得证.

定理 9　设 $2\leq 2m\leq \frac{p}{5}-1$, 满足 $(p_i-1)\mid (p-1)$ 的素数为 $p_1, p_2, \cdots, p_s$, 满足 $(q_i-1)\mid 2m$ 的素数为 $p_1, p_2, \cdots, p_r$)$=1$. 因此, 奇数 p 为素数的充要条件是满足: (1) $(p, p_1p_2\cdots p_r)=1$; (2) $\sum_{j=1}^{s}\frac{p}{p_j}\equiv 1\ (\mathrm{mod}\ p)$.

证明　利用引理 6 和引理 7, 完全类似于定理 8 的方法则得证.

3　整除 Bernoulli 数的充要条件

1874 年, Kummer 发现 164 以内的非正规素数只有 8 个, 即 $37\mid B_{32}$, $59\mid B_{44}$, $67\mid B_{58}$, $101\mid B_{68}$, $103\mid B_{24}$, $131\mid B_{22}$, $149\mid B_{130}$, $157\mid B_{62}$, $157\mid B_{110}$. 对此, 我们给出 3 个判别方法.

定理 10　$m\geq 2$, $p\geq 5$ 为素数, 因此 $p\mid B_{2m}$ 的充要条件是 $(p-1)\mid 2m$, $S_{2m}(p-1)\equiv 0\ (\mathrm{mod}\ p^2)$.

证明　由式(5), 对任何素数 $p\geq 5$ 有 $S_{2m}(p-1)\equiv pB_{2m}(\mathrm{mod}\ p^2)$.

(1) 必要性. $p\mid B_{2m}$ 则 $p\mid B_{2m}$ 的分母, 由引理 7 有 $(p-1)\mid 2m$, 从而 $S_{2m}(p-1)\equiv pB_{2m}\equiv 0\ (\mathrm{mod}\ p^2)$.

(2) 充分性. $(p-1)\mid 2m$, 则 $p\mid B_{2m}$ 的分母, 即有 $pB_{2m}\equiv S_{2m}(p-1)\equiv 0\ (\mathrm{mod}\ p^2)$. 故 $B_{2m}\equiv 0\ (\mathrm{mod}\ p)$. 完全类似地, 利用定理 5 和定理 6 即得.

定理 11　$m\geq 2$, $p\geq 5$ 为素数, $p\mid C_{2m}^2$. 因此, $p^2\mid B_{2m}$ 的充要条件是 $(p-1)\mid 2m$ 且满足: (1) 当 $(p-1)\mid (2m-2)$ 时, $S_{2m}(p-1)\equiv 0\ (\mathrm{mod}\ p^3)$; (2) 当 $p-1\mid 2m-2$ 时, $S_{2m}(p-1)\equiv -\frac{1}{3}p^2C_{2m}^2(\mathrm{mod}\ p^3)$.

定理 12　$m\geq 2$, $p\geq 5$ 为素数, $p\parallel C_{2m}^2$. 因此, $p^2\mid B_{2m}$ 的充要条件是 $(p-1)\mid 2m$ 且满足: (1) 当 $(p-1)\mid (2m-2)$ 时, $S_{2m}(p-1)\equiv 0\ (\mathrm{mod}\ p^3)$; (2) 当 $(p-1)\mid (2m-2)$ 时, $S_{2m}(p-1)\equiv$

$-\frac{1}{3}p^2C_{2m}^2 \pmod{p^4}$.

猜想 **1** 素数 $p \mid 2m$, $(p-1) \mid 2m$, 则必有 $p \mid B_{2m}$.

猜想 **2** p 为素数, $(p-1) \mid 2m$, 则必 $B_{2mp} \equiv pB_{2m} \pmod{p^2}$.

猜想 **3** 奇数 p 为素数的充要条件是, $S_{p-1}(\frac{p-1}{2}) \equiv \frac{p-1}{2} \pmod{p}$.

猜想 **4** 奇数 p 为素数的充要条件是, $S_p(\frac{p-1}{2}) \equiv \frac{p^2(p-1)}{2} \pmod{p^3}$.

猜想 **5** 奇数 p 为素数的充要条件是, $p \mid (pB_{p-1}+1)$ 的分子.

参 考 文 献

1 邓培民, 王云葵. 关于伯努利数结构的讨论[J]. 广西师范大学学报(自然科学版), 1995, 13(4): 4～9

2 邓培民, 王云葵. 关于伯努利数结构的讨论(续)[J]. 广西师范大学学报(自然科学版), 1996, 13(4): 1～5

3 王云葵. 等幂和与波文猜想[J]. 广西教育学院学报, 1998, (1): 105～111

4 王云葵. 等幂和与判别素数的充要条件[J]. 数学通报, 1996, (6): 46～47

5 胡作玄. 350 年历程 —— 从费尔马到维尔斯[M]. 济南: 山东教育出版社, 1996. 121～130

6 王云葵. 关于 Bernoulli 数的同余关系[J]. 广西科学, 1999, 6(4): 250～252

7 王云葵. 等幂和的分解及其同余式链[J]. 天中学刊, 1999, 14(5): 1～3

8 王云葵. 居加猜想研究及其新进展[A]. 见: 杨世明主编. 全国第三届初等数学研究学术交流会论文集[C]. 北京: 首都师范大学出版社, 1996. 482～491

9 王云葵. 伯努利数与判别素数的充要条件[J]. 广西民族学院学报(自然科学版), 1998, 4(1): 11～13

Necessary and Sufficient Condition for Bernoulli´s Numbers and Discriminant Prime Numbers

Wang Yunkui Ma Wuyu

(Dept. of Math. & Comput. Sci., Guangxi Nationalities College, 530006, Nanning)

Abstract By using necessary and sufficient condition for sum of equal powers and discriminant prime numbers as well as congruent relations between sum of equal powers and Bernoulli´s numbers, the authors obtain necessary and sufficient condition for discriminant prime numbers relating to Bernoulli´s numbers and also necessary and sufficient condition for the exact division of Bernoulli´s numbers.

Keywords sum of equal powers, Bernoulli´s numbers, necessary and sufficient condition