关 于 Hall 问 题*

曹珍富

(哈尔滨工业大学)

Hall[1]在T型差集的研究中，产生了如下问题：方程

$$q^m = p^n + 2,\quad p,\ q \text{ 是素数},\ m>1,\ n>1, \tag{1}$$

除开$p=5$，$n=2$，$q=3$，$m=3$以外，是否还有其他的解？这是一个未决问题[2]．最近，孙琦和周小明[3]在研究不定方程

$a^x+b^y=c^z$，a，b，c是不同的素数，$\max(a,b,c)=19$时，顺便给出了方程（1）的一个结果，即

定理A 设$q=p+2$，-2模q的次数l满足了$3\nmid l$，且$f=p^2-p+1$是一个素数，满足$q^{p+1}\equiv 1(\bmod f)$，则方程（1）无解．

在本文中，我们将证明如下的

定理 设$q=p+2$，则方程（1）无解．

显然，这个结果改进了定理A．下面我们分三个引理来证明定理．

引理1 设$2\nmid mn$，$q=pt^2+2$，t为正整数，则方程（1）无解．

证 如（1）有解，显然$2\nmid pq$．在$2\nmid mn$，$q=pt^2+2$时，方程（1）可整理成

$$\left(\frac{(pt^2+2)^m+p^n}{2}\right)^2-p(pt^2+2)\left((pt^2+2)^{\frac{m-1}{2}}p^{\frac{n-1}{2}}\right)^2=1, \tag{2}$$

熟知[4]，Pell方程$x^2-\mathcal{D}y^2=1$，$\mathcal{D}=p(pt^2+2)$的基本解是$\varepsilon=1+pt^2+t\sqrt{\mathcal{D}}$．令$\bar{\varepsilon}=1+pt^2-t\sqrt{\mathcal{D}}$，则（2）给出

$$(pt^2+2)^{\frac{m-1}{2}}p^{\frac{n-1}{2}}=\frac{\varepsilon^a-\bar{\varepsilon}^a}{2\sqrt{\mathcal{D}}}=t\frac{\varepsilon^a-\bar{\varepsilon}^a}{\varepsilon-\bar{\varepsilon}}, \tag{3}$$

其中a是一个正整数．显然，如果$2\mid a$，则$\frac{\varepsilon^a-\bar{\varepsilon}^a}{2\sqrt{\mathcal{D}}}$为偶数，因此（3）给出$2\nmid a$．又，由（3）得出$t\mid p^{\frac{n-1}{2}}$，可设$t=p^s$，$0\leqslant s\leqslant\frac{n-1}{2}$．于是（3）成为

$$(p^{2s+1}+2)^{\frac{m-1}{2}}p^{\frac{n-1}{2}-s}=\frac{\varepsilon^a-\bar{\varepsilon}^a}{\varepsilon-\bar{\varepsilon}},\quad a\equiv 1(\bmod 2), \tag{4}$$

此时$q=p^{2s+1}+2$及$\varepsilon=1+p^{2s+1}+p^s\sqrt{\mathcal{D}}$，$\bar{\varepsilon}=1+p^{2s+1}-p^s\sqrt{\mathcal{D}}$．由于在$2\nmid a$时有

$$\frac{\varepsilon^a-\bar{\varepsilon}^a}{\varepsilon-\bar{\varepsilon}}=\binom{a}{1}(1+p^{2s+1})^{a-1}+\binom{a}{3}(1+p^{2s+1})^{a-3}(p^s\sqrt{\mathcal{D}})^2+\cdots+$$

* 1984年6月7日收到．

$$+\binom{a}{a-2}(1+p^{2s+1})^2(p^s\sqrt{\mathcal{D}})^{a-3}+(p^s\sqrt{\mathcal{D}})^{a-1},$$

注意到$\mathcal{D}=p(pt^2+2)=p(p^{2s+1}+2)$ 可得

$$\frac{\varepsilon^a-\bar{\varepsilon}^a}{\varepsilon-\bar{\varepsilon}}\equiv a(\mathrm{mod}\,p),\quad \frac{\varepsilon^a-\bar{\varepsilon}^a}{\varepsilon-\bar{\varepsilon}}\equiv a(\mathrm{mod}\,p^{2s+1}+2(=q)),\tag{5}$$

由（4）及$m>1$知$a\equiv 0(\mathrm{mod}q)$，$q=p^{2s+1}+2$．设$a=qa_1$，则（4）给出

$$q^{\frac{m-1}{2}}p^{\frac{n-1}{2}-s}=\frac{(\varepsilon^{a_1})^q-(\bar{\varepsilon}^{a_1})^q}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}\cdot\frac{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}{\varepsilon-\bar{\varepsilon}},\tag{6}$$

设$\varepsilon^{a_1}=u+v\sqrt{\mathcal{D}}$，则$\bar{\varepsilon}^{a_1}=u-v\sqrt{\mathcal{D}}$，$v=\frac{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}{2\sqrt{\mathcal{D}}}=p^s\frac{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}{\varepsilon-\bar{\varepsilon}}$．我们有

$$\frac{(\varepsilon^{a_1})^q-(\bar{\varepsilon}^{a_1})^q}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}=\binom{q}{1}u^{q-1}+\binom{q}{3}u^{q-3}(v\sqrt{\mathcal{D}})^2+\cdots+(v\sqrt{\mathcal{D}})^{q-1},\tag{7}$$

而$(u,v)=1$，故$\left(\frac{(\varepsilon^{a_1})^q-(\bar{\varepsilon}^{a_1})^q}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}},v\right)\Big|\binom{q}{1}=q$，即

$$\left(\frac{(\varepsilon^{a_1})^q-(\bar{\varepsilon}^{a_1})^q}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}},\frac{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}{\varepsilon-\bar{\varepsilon}}\right)=1\text{或}q.$$

由于$u=\frac{\varepsilon^{a_1}+\bar{\varepsilon}^{a_1}}{2}\equiv -1\not\equiv 0\ (\mathrm{mod}q)$，由（7）显然$q\parallel\frac{(\varepsilon^{a_1})^q-(\bar{\varepsilon}^{a_1})^q}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}$．因此，如果

$\left(\frac{(\varepsilon^{a_1})^q-(\bar{\varepsilon}^{a_1})^q}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}},\frac{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}{\varepsilon-\bar{\varepsilon}}\right)=1$，则$q\nmid\frac{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}{\varepsilon-\bar{\varepsilon}}$，由（6）给出$\frac{m-1}{2}=1$．注意到

$\frac{(\varepsilon^{a_1})^q-(\bar{\varepsilon}^{a_1})^q}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}>q$，由（6）得出

$$\frac{(\varepsilon^{a_1})^q-(\bar{\varepsilon}^{a_1})^q}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}=q\cdot p^{\frac{n-1}{2}-s},\quad\frac{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}{\varepsilon-\bar{\varepsilon}}=1,\quad\frac{n-1}{2}-s>0,\tag{8}$$

（8）的第二式显然给出$a_1=1$．在$\frac{n-1}{2}-s>0$时，（8）的第一式得出（注意$a_1=1$及（5）的第一式）

$$p\mid q\cdot p^{\frac{n-1}{2}-s}=\frac{\varepsilon^q-\bar{\varepsilon}^q}{\varepsilon-\bar{\varepsilon}}\equiv q(\mathrm{mod}\,p),$$

即$p\mid q$，显然不可能．

如果$\left(\frac{(\varepsilon^{a_1})^q-(\bar{\varepsilon}^{a_1})^q}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}},\frac{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}{\varepsilon-\bar{\varepsilon}}\right)=q$，则（6）显然给出

$$\frac{(\varepsilon^{a_1})^q-(\bar{\varepsilon}^{a_1})^q}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}=q\cdot p^{\frac{n-1}{2}-s},\quad\frac{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}{\varepsilon-\bar{\varepsilon}}=q^{\frac{m-1}{2}-1},\quad\frac{n-1}{2}-s>0,\tag{9}$$

由于$\frac{n-1}{2}-s>0$时，（4）及（5）的第一式给出

$$p\mid\frac{\varepsilon^a-\bar{\varepsilon}^a}{\varepsilon-\bar{\varepsilon}}\equiv a(\mathrm{mod}\,p),$$

故$p \mid a = qa_1$，得出$p \mid a_1$，因此$p \mid \frac{\varepsilon^{a_1} - \bar{\varepsilon}^{a_1}}{\varepsilon - \bar{\varepsilon}} = q^{\frac{m-1}{2}-1}$，这仍不可能．引理1证完．

引理2 方程

$$(p+2)^{2m_1} = p^n + 2,\ m_1 \geqslant 1,\ n > 1, \tag{10}$$

无解．

证 显然$2 \nmid n$．对（10）取模8得

$$1 \equiv p \cdot p^{n-1} + 2 \equiv p + 2 (\mathrm{mod}\, 8),$$

故$p + 1 \equiv 0 (\mathrm{mod}\, 8)$．设$p + 1 = 2^s p_1$，$s \geqslant 3$，$2 \nmid p_1$，则由于

$$(p+2)^{2m_1} = (2^s p_1 + 1)^{2m_1} \equiv 1 (\mathrm{mod}\ 2^{s+1}),$$

$$p^{n-1} = (2^s p_1 - 1)^{2 \cdot \frac{n-1}{2}} \equiv 1 (\mathrm{mod}\ 2^{s+1}),$$

故（10）给出$1 \equiv p \cdot p^{n-1} + 2 \equiv p + 2 (\mathrm{mod}\ 2^{s+1})$，即$p + 1 \equiv 0 (\mathrm{mod}\ 2^{s+1})$，此与$p + 1 = 2^s p_1$，$2 \nmid p_1$矛盾．这就证明了引理2．

引理3 设$n = 2n_1$，$q = pt^2 + 2$，t为正整数，则方程（1）无解．

证 如果$p = 3$，则$pt^2 + 2 = 3t^2 + 2 \equiv 5 (\mathrm{mod}\, 8)$．此时（1）为$(pt^2+2)^m = 3^{2n_1} + 2 \equiv 0 (\mathrm{mod}\ pt^2 + 2)$，故Legendre符号$\left(\frac{-2}{pt^2+2}\right) = 1$有$1 = \left(\frac{-2}{pt^2+2}\right) = -1$，不可能．如果$p \neq 3$，则$p^{2n_1} + 2 \equiv 0 (\mathrm{mod}\, 3)$，因此$3 \mid q = pt^2 + 2$，即$pt^2 + 2 = 3$，仍不可能．

由引理1～3立得本文的主要结果．

致谢：本文是在孙琦教授指导下写成的，作者向他表示衷心地感谢！

参 考 文 献

〔1〕Hall, M. Jr., Combinatorial Theory, 1967.
〔2〕柯召、孙琦，群论、组合论和代数数论中的一些不定方程问题，数学研究与评论，2(1983)，131—134.
〔3〕孙琦、周小明，关于丢番图方程$a^x + b^y = c^z$，科学通报，1(1984)，61.
〔4〕柯召、孙琦，谈谈不定方程，上海教育出版社，1980年，第二章24页.

On a Problem of Hall

Cao Zhenfu
(Harbin Institute of Technology)

Abstract

The author gives elementary proofs of the following theorems:

(1) If $2 \nmid mn$, $q = pt^2 + 2$, then the equation

$$q^m = p^n + 2,\ p, q \text{ are primes},\ m > 1,\ n > 1, \tag{•}$$

has no solution.

(2) The equation $(p+2)^{2m_1} = p^n + 2$ has no solution with $m_1 > 1$, $n > 1$.

(3) If $n = 2n_1$, $q = pt^2 + 2$, then the equation (•) has no solution. Clearly, if $q = p + 2$, then the equation (•) has no solution.