第3卷 第2期
1983年4月

数学研究与评论
JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION

Vol.3 No.2
Apr. 1983

群论、组合论和代数数论中的一些不定方程问题*

柯召 孙琦

(四川大学)

近年来，在群论、组合论和代数数论等分支的某些研究工作中，提出了一些不定方程问题，这不仅丰富了不定方程本身的研究课题，而且通过这些方程的解决，得到了以上诸分支中某些新结果，促进了各分支间的联系和应用．本文将扼要介绍这方面的工作以及一些尚未解决的问题．

(一)

在有限群的研究中，特别是Brauer[1],[2]和Alex[3],[4]对于群的阶的标准分解式中含有一次幂素数 p 的有限群的研究中，提出了不定方程

$$x+y=z, \tag{1}$$
$$xyz=p_1^{a_1}\cdots p_k^{a_k}, \qquad k\geqslant 1,\ a_j\geqslant 0$$

p_j 是给定的素数，$j=1,\cdots,k$，

1980年，Alex[5]给出了不定方程

$$1+y=z, \tag{2}$$
$$yz=2^a3^b5^c7^d; \qquad a\geqslant 0,\ b\geqslant 0,\ c\geqslant 0,\ d\geqslant 0$$

的全部正整数解 $(y,z)=(1,2),(2,3),(3,4),(8,9),(7,8),(63,64),(27,28),(5,6),(125,126),(49,50),(2400,2401),(4374,4375),(20,21),(14,15),(224,225)$．

Alex[5]还给出了不定方程

$$x+y=z,$$
$$xyz=2^a3^b5^c7^d, \qquad (x,y)=1,$$
$$x\leqslant y,\ a\geqslant 0,\ b\geqslant 0,\ c\geqslant 0,\ d\geqslant 0 \tag{3}$$

的全部正整数解 (x,y,z)，共62组．

不难看出，(2)和(3)均可化为指数方程，一般说来，可以用初等方法求解．但是，对于某些有限群，需要解不定方程

$$1+x=y+z, \tag{3}'$$
$$xyz=2^u3^v7^w, \qquad u\geqslant 0,\ v\geqslant 0,\ w\geqslant 0$$

*1982年10月29日收到．

求出(3)′的全部正整数解(x,y,z)是一个没有解决的问题.

在Berger关于有限群的工作中，提出了不定方程

$$p^m-2q^n=\pm1,\ p,q\text{是素数},\ m>1,\ n>1 \tag{4}$$

的问题. 1975年，Crescenzo[6]证明了

定理 除开$(239)^2-2(13)^4=-1$以外，方程(4)有解，则$m=n=2$.

证明这个定理，用到Ljunggren关于不定方程$x^2+1=2y^4$的一个深刻的结果. 我们希望找到一个不用Ljunggren的结果的初等证明，但迄今尚未找到. Crescenzo提到，是否有无穷多对素数p，q适合$p^2-2q^2=\pm1$？看来，这是一个困难的问题.

在有限群中，还用到不定方程一些熟知的结果，例如不定方程$p^m-q^n=1$，p、q是素数，$m>1$，$n>1$，仅有解$p=3$，$m=2$，$q=2$，$n=3$(这是Catalan猜想的特例，参看[7]).

(二)

众所周知，在组合论的某些构造性的结果中，不定方程的一些经典结果得到很好的应用. 例如，在阿达玛矩阵的构造中，用到Lagrange定理：每一个正整数可以表成四个平方和. 在区组设计中用到不定方程$ax^2+by^2+cz^2=0$有非零解的充分必要条件，等等. 特别在组合论的一个重要内容——差集合中，遇到许多类型的不定方程. 当我们讨论超平面差集$(v=2^n-1,\ n\geqslant2)$和Hall差集($v=4x^2+27$是一个素数)有无共公部分时，就产生了如下不定方程

$$x^2+7=2^y. \tag{5}$$

关于方程(5)，1913年，Ramanujun 发现有五组正整数解$(x,y)=(1,3),(3,4),(5,5),(11,7),(181,15)$. 他问：方程(5)除开上述五组解以外，还有没有其他的正整数解？五十年代，Nagell 首先证明了(5)仅有上述五组正整数解. 后来，Mordell, Hasse, Chowla; Lewis 等分别给出三个不同的证明，我们在[7]中介绍了Hasse的证明. 在另一些差集的讨论中将处理不定方程

$$p^n=1+4y^2, \tag{6}$$
$$n=2s+1,\ s>0,\ p\equiv1\pmod4\text{是素数}.$$

和

$$p^n=9+4y^2, \tag{7}$$
$$n=2s+1,\ s>0,\ p\equiv1\pmod4\text{是素数}$$

运用高斯整数的性质，不难证明(6)和(7)都是无解的[8].

在T型差集的讨论中，产生了不定方程

$$q^s=p^n+2,\ p,q\text{是素数},\ s>1,\ n>1 \tag{8}$$

的求解问题(参看[8]或[9])除开$p=5$，$n=2$，$q=3$，$s=3$以外，(8)是否还有其他的解，是一个尚未解决的问题.

1979年，Enomoto 等[10]在一类设计中，提出了不定方程

$$3x^4-4y^4-2x^2+12y^2-9=0, \tag{9}$$

这样一个看来如此简单的方程，他们无法解决．后来，方程(9)被Bremner[11]完全解决了，他证明了不定方程 (9) 除开$(x,y)=(1,1),(3,3)$外，无其他的正整数解．Bremner的证明较深，他用了Cassels关于四次域$R(\sqrt[4]{3})$一些较深入的结果和Skolem的p-adic方法．给出Bremner定理一个初等的证明，仍然是有意义的工作．

(三)

一方面，代数数论为不定方程提供了有力的工具．另一方面，许多不定方程的结果在代数数论中得到应用．

众所周知，Pell 方程 $x^2-Dy^2=\pm 1$，$x^2-Dy^2=\pm 4$，定出了二次域 $Q(\sqrt{D})$ 的基本单位数，从而表出了$Q(\sqrt{D})$的全部单位数．设$D>1$，且无三次方因子，不定方程

$$x^3+Dy^3=1$$

最多只有一组整数解 $xy\neq 0$，如果 x_1,y_1 是这样一组解，那么 $x_1+y_1\sqrt[3]{D}$ 或者是三次域 $Q(\sqrt[3]{D})$ 的基本单位数，或者是基本单位数的平方．

代数数论中一个著名问题是决定类数 $h(D)=1$的虚二次域$Q(D)$，这里 $D<0$且无平方因子．Gauss已经知道$D=-1,-2,-3,-7,-11,-19,-43,-67,-163$时，$Q(D)$的类数 $h(D)=1$．1934 年，Heilbronn 等证明最多只有十个D使 $h(D)=1$．多年来，第十个域是否存在，一直没有解决．1952年，Heegner[12] 发表了第十个域不存在的证明，他主要用到了不定方程和椭圆模函数的结果，但用模函数的那部分证明有漏洞．他在不定方程方面，主要研究了方程$(\beta-2a^2)^2=2a(a^3+1)$的整数解．直到1967年，Stark[13]为Heegner的使用不定方程所启发而设法避开了模函数，成功地给出了第十个域不存在的严格证明．他在证明中，用到不定方程一些基本的类型，例如方程$x^3\pm 1=y^2$和方程$x^3\pm 1=2y^2$，用初等方法或代数数论的方法，这些不定方程都不难解决．顺便指出，形如 $x^3+k=y^2$的方程也叫Mordell方程，历史上有过大量的研究，参看[14]；形如 $x^3\pm b^3=Dy^2$的不定方程，Nagell Ljungyren 有过许多工作．不久前，我们也得到一些结果，参看 [15]、[16]．1968年，Heegner 证明中的漏洞，也被成功的补充了．另外，1967 年，Baker 用他著名的“有效方法”，也独立地解决了类数为 1 的虚二次域问题．

1981年，Thomas[17]等在三次域的研究中，提出了下面不定方程组的问题：

$$\begin{aligned} xy&=v^2-vw+w^2\\ x^2+y(v+w)&\equiv 0 \pmod{vw}\\ y^2+x(v+w)&\equiv 0 \pmod{vw} \end{aligned} \tag{10}$$

其中，

$$vw\neq 0.$$

Thomas 给出了方程(10)的全部整数解．

参 考 文 献

[1] Brauer, R., On groups whose order contains a prime number to first power, I, II, *Amer. J. Math.*, 64 (1942), 401-440.

[2] Brauer, R. On Simple groups of order $5\,3^a2^b$, Bull. *Amer. Math. Soc.*, 74 (1960), 900-903.

[3] Alex, L. J., Simple groups of order $2^a3^b5^c7^dp$, *Trans. Amer. Math. Soc.*, 173 (1972), 389-399.

[4] Alex, L. J., On simple groups of order $2^a3^b7^cp$, *J. Algebra* 25 (1973), 113-124.

[5] Alex, L. J., Diophantine Equations related to finite groups, *Comm. in Algebra*, 4 (1976), 77-100.

[6] Crescenzo, P., A Diophantine equation which arises in the theory of finite groups, *Advances Math.*, 17 (1975), 25-29.

[7] 柯召，孙琦，谈谈不定方程，上海教育出版社，1980年.

[8] 四川大学数学系，组合论(讲义)，1974年.

[9] Hall. M. Jr., Combinatorial Theory, 1967.

[10] Enomoto, H., Ito, N., Noda, R., Tight 4-designs, *Osaka J. Math.*, 10 (1979), 39-43.

[11] Bremner. A., A Diophantine equation arising from tight 4-designs, *Osaka J. Math.*, 16(1979). 353-356.

[12] Heegner, H; Diophantine Analysis und Modulfunktionen, *Math. Z.*, 56 (1952), 227-253.

[13] Stark, H. M., A complete determinetion of the complex quadratic fields of class number One, *Michigan Math. J.* 14 (1967), 1-27.

[14] Mordell, L. J., Diophantine Equations, 1972.

[15] 柯召，孙琦，关于丢番图方程 $x^3\pm1=Dy^2$，中国科学，12(1981)，1453-1457.

[16] 柯召，孙琦，关于丢番图方程 $x^3\pm8=Dy^2$ 和 $x^3\pm8=3Dy^2$，四川大学学报(自然科学版)，4 (1981)，1-5.

[17] Thomas, E., Vasquez, A. T., Diophantine equations arising from Cubic number fields, *Journal of Number Theory*, 13 (1981), 398-414.