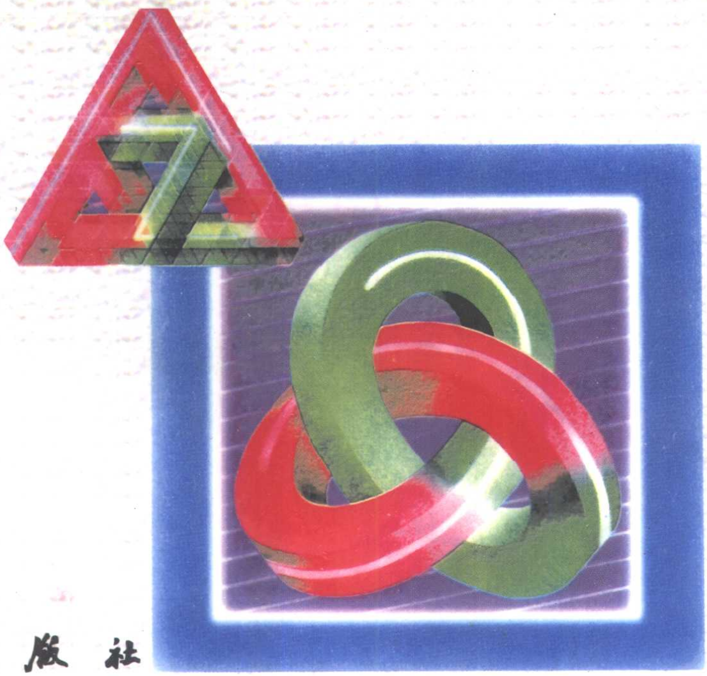
现代数学基础丛书

Gel'fond-Baker方法在丢番图方程中的应用

乐茂华 著



科学出版社

现代数学基础丛书

Gel′fond-Baker方法在丢番图方程中的应用

乐茂华 著

科学出版社

1998

内 容 简 介

本书系统论述 Gel'fond-Baker 方法在 Thue 方程、Thue-Mahler 方程、广义 Ramanujan-Nagell 方程、椭圆方程、超椭圆方程以及有理数域上的 S-单位方程中的应用，并对上述方程的历史背景、最新成果和尚待解决的问题作了全面的阐述. 书中附有详细的文献目录，以便读者做进一步的研究.

本书可供高等学校数学系学生和教师阅读和参考。

图书在版编目（CIP）数据

Gel'fond-Baker 方法在丢番图方程中的应用/乐茂华著. -北京：科学出版社，1998. 10

（现代数学基础丛书/程民德主编）

ISBN 7-03-006623-5

Ⅰ. G… Ⅱ. 乐… Ⅲ. 盖勒范德-贝克法-应用-丢番图方程 Ⅳ. O156. 7

中国版本图书馆 CIP 数据核字（98）第 07908 号

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

北京科地亚印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

1998年10月第一版 开本:850×1168 1/32

1998年10月第一次印刷 印张:8 1/8

印数:1—2 000 字数:207 000

定价:16.00元

（如有印装质量问题，我社负责调换〈新欣〉）

前　　言

1966 年，英国数学家 A. Baker 在超越数论方面作出了杰出的贡献. 他成功地将 Gel'fond 和 Schneider 有关 Hilbert 第七问题的著名结果推广到了一般的情况，并且对代数数对数线性型给出了可有效计算的下界. Baker 的出色工作不但推动了超越数论的发展，同时也给数论中包括丢番图方程在内的很多研究领域带来了突破性的进展. 近 30 年来，以上述工作为基础的 Gel'fond-Baker 方法在丢番图方程的研究中取得了一系列重要结果，日益成为该领域中的一个强有力的研究方法. 目前，这一趋势在国内已经受到越来越多的关注. 鉴于国内至今还没有这方面的专门书籍，作者根据多年来收集的资料以及为此而写的札记，在湛江师范学院数学系"数论与组合高级研讨班"部分讲义的基础上编写了本书，以供对此感兴趣的读者参考.

丢番图方程是一个非常活跃的研究领域，与此有关的文献资料浩如烟海. 本书在力求内容的完整性和关联性的前提下，根据各类方程之间的内在联系，将有关的文献资料贯穿起来，以便读者能够对问题有个全面的了解. 阅读本书除了需要具备大学数学系的代数、分析和初等数论的知识以外，还需要了解部分代数数论和超越数论方面的知识. 这些内容在讨论丢番图方程时是必不可少的. 本书的第一章对此作了简要的介绍，其中经常被引用的结果将以引理的形式给出. 本书的其余各章依次介绍了 Gel'fond-Baker 方法在 Thue 方程、Thue-Mahler 方程、广义 Ramanujan-Nagell 方程、椭圆方程、超椭圆方程、指数型超椭圆方程以及有理数域上的 S -单位方程中的应用情况，其中的主要结果都以定理的形式给出. 由于在一般情况下，有关各类方程的最好结果的证明总是十分繁琐的，需要高度复杂的技巧和计算. 因此，为了

突出 Gel′fond-Baker 方法所起到的关键作用，书中省略了定理的证明中对辅助性结果的讨论. 同时，为了使读者对问题有个整体的了解，书中每小节都对所讨论方程的历史背景、最新结果以及尚待解决的问题进行了系统的阐述. 另外，各章的末尾都附有详细的参考文献，以便读者作进一步的研究. 本书除绪论部分以外，所有的公式、引理、定理、推论、问题和猜想分别按其所在的章节编号，参考文献按每章编号.

作者在学习和研究数论的过程中，得到了中国科学院王元院士、波兰科学院 A. Schinzel 院士、北京大学潘承彪教授、同济大学陆洪文教授和中国科学院数学研究所徐广善教授的热情帮助和指教；本书的写作受到了中山大学林伟教授和邓东皋教授、广州师范学院裴定一教授以及湛江师范学院暨数学系各位领导和老师的鼓励和支持. 作者谨在此向他们表示衷心的感谢. 同时，作者还要感谢法国 Paris Ⅵ 大学 M. Waldschmidt 教授、法国 Louis Pasteur 大学 M. Mignotte 教授、匈牙利 Kossuth Lajos 大学 K. Győry 教授、荷兰 Leiden 大学 R. Tijdeman 教授和印度 Tata 研究所 T. N. Shorey 教授提供的大量论文预印本和抽印本. 这些宝贵的资料帮助作者及时了解到有关丢番图方程这一研究领域的最新动态.

本书的写作和出版分别得到国家自然科学基金、广东省自然科学基金和国家自然科学基金委员会出版基金的资助.

最后，作者希望本书的出版能够有助于国内读者对丢番图方程及其研究方法的了解. 同时，由于作者的水平所限，书中的缺点和不妥之处在所难免，切望读者不吝赐教.

乐茂华

1997 年 8 月于湛江师范学院

常用符号表

以下列出书中常用符号的定义．如果符号在个别地方有不同的含意，则将明确说明；未列入本表的符号均在使用时另行说明．

$\mathbb{N}$	全体正整数的集合
$\mathbb{Z}$	整数环
$\mathbb{Q}$	有理数域
$\mathbb{R}$	实数域
$\mathbb{C}$	复数域
$\mathbb{A}$	全体代数数的集合
$\mathbb{P}$	全体素数的集合
$\mathbb{P}'$	全体奇素数的集合
$\mathbb{P}^*$	全体素数及其方幂的集合
$\mathbb{F}_q$	q 元有限域
$R[X_1,X_2,\cdots,X_n]$	数环 R 上关于未定元 $X_1,X_2,\cdots,X_n$ 的 n 元多项式环
$a\mid b$	整数 a 整除 b
$a\nmid b$	整数 a 不能整除 b
$p^k\parallel b$	对于素数 p、正整数 k 以及整数 b，$p^k\mid b$ 且 $p^{k+1}\nmid b$
$\gcd(a_2,a_2,\cdots,a_n)$	整数 $a_1,a_2,\cdots,a_n$ 的最大公因数
$\operatorname{lcm}(a_1,a_2,\cdots,a_n)$	整数 $a_1,a_2,\cdots,a_n$ 的最小公倍数
$a\equiv b\pmod m$	整数 a 与 b 对模 m 同余
$a\not\equiv b\pmod m$	整数 a 与 b 对模 m 不同余
$[a]$	不超过实数 a 的最大整数
$\exp z$	指数函数 e^z

$C_i(i=1,2,\cdots)$	可有效计算的绝对正常数
$C_i^*(i=1,2,\cdots)$	不可有效计算的绝对正常数
$C_i(a,b,\cdots,c)(i=1,2,\cdots)$	仅与参数 $a,b,\cdots,c$ 有关的可有效计算的正常数
$C_i^*(a,b,\cdots,c)(i=1,2,\cdots)$	仅与参数 $a,b,\cdots,c$ 有关的不可有效计算的正常数

目　　录

绪　论

在数论中，通常将未知数个数多于方程个数，并且对未知数的取值加以某些限制（例如，限制为整数、正整数或有理数等）的方程和方程组统称为丢番图方程. 早在公元三世纪初，古希腊数学家 Diophantus 就已经比较系统地研究过此类方程. 我国最早的数学文献《周髀算经》也曾有过这方面的记载. 因此，丢番图方程是数论中最古老的分支，历史上的很多著名数学问题（例如 Fermat 猜想）都与此类方程有关. 几百年来，Fermat，Euler，Legendre，Gauss，Dirichlet，Hilbert 等数学大师都曾对丢番图方程的研究有过卓越的贡献. 这些开拓者的重要工作，不但丰富了丢番图方程的内容，同时也给代数数论、超越数论、代数几何等目前非常活跃的现代数学分支的产生和发展奠定了基础.

由于丢番图方程对解的特殊限制，在数论、代数、组合数学等讨论各种有限结构的数学分支中，有许多亟待解决而又相当困难的问题最终都可归结为某些丢番图方程的求解问题. 因此，丢番图方程与上述数学分支之间的紧密联系是十分自然的. 正是因为存在这种联系，关于丢番图方程的研究在本世纪，特别是近 30 年来，取得了前所未有的进展.

丢番图方程的种类异常繁多. 1920 年，Dickson[7]用了 800 多面的篇幅专门介绍了到本世纪初为止有关这方面的主要工作，其复杂程度可见一斑. 尽管如此，迄今讨论较多的单个的丢番图方程基本上都属于以下两个类型. 一类是多项式方程，它通常可表成

$$f(x_1,x_2,\cdots,x_m)=0,x_1\in\Phi_1,x_2\in\Phi_2,\cdots,x_m\in\Phi_m,\qquad(1)$$

其中 $f(X_1,X_2,\cdots,X_m)$是未定元 $X_1,X_2,\cdots,X_m$ 的整系数多项式，$\Phi_i(i=1,2,\cdots,m)$是未知数 $x_i(i=1,2,\cdots,m)$取值的集合. 如果当$(x_1,x_2,\cdots,x_m)=(a_1,a_2,\cdots,a_m)$时(1)成立，则称它是方程(1)的一

组解. 当多项式 $f(X_1,X_2,\cdots,X_m)$ 的次数等于 n 时,方程(1)称为 m 元 n 次方程. 例如,运用丢番图方程的语言,著名的 Fermat 猜想可表述为:

猜想 A 当 n 是大于 2 的正整数时,方程

$$x^n + y^n = z^n, x, y, z \in \mathbb{N} \tag{2}$$

无解 (x,y,z).

当方程(1)的元数或次数大于 2 时,该方程通常称为多元方程或高次方程. 猜想 A 中的方程(2)是三元 n 次方程,它是一个典型的多元高次方程. 在一般情况下,方程的元数越多、次数越高,就越不容易解决.

如果方程(1)中多项式 $f(X_1,X_2,\cdots,X_m)$ 的某些项的指数位置也含有未知数,则称它是指数型方程. 这是另一类讨论较多的丢番图方程. 例如,Catalan[5]在 1844 年曾经猜测:在全体正整数中,连续的完全方幂仅有 8 和 9. 上述猜想可表述为:

猜想 B 方程

$$x^m - y^n = 1, x, y, m, n \in \mathbb{N}, m > 1, n > 1 \tag{3}$$

仅有解 $(x,y,m,n)=(3,2,2,3)$.

此后,Cassels[4]又对方程(3)提出了以下较弱的猜想:

猜想 C 方程(3)仅有有限多组解 (x,y,m,n).

上述两个猜想中的方程(3)是一个典型的指数型方程. 显然,指数型方程通常要比相应的多项式方程更难解决.

对于一个具体的丢番图方程(1),我们通常需要解决下列问题:

问题 A 方程(1)是否有解 $(x_1,x_2,\cdots,x_m)$?

问题 B 当方程(1)有解时,它是否有无限多组解?

问题 C 当方程(1)有无限多组解时,是否能找到可表出它的所有解的公式?

问题 D 当方程(1)仅有有限多组解时,是否能具体求出它的全部解?

1900 年,Hilbert 在巴黎召开的第二次国际数学家大会上作

的著名演讲中提出了23个重要的数学问题，其中的第10问题就与上述的问题A有关. 该问题可表述为：

问题 E 对于一般的整系数多项式 $f(X_1,X_2,\cdots,X_m)$，能不能给出仅有有限步运算的算法来判定方程

$$f(x_1,x_2,\cdots,x_m)=0,x_1,x_2,\cdots,x_m\in\mathbb{Z} \tag{4}$$

是否有解 $(x_1,x_2,\cdots,x_m)$？

1970年，Matijasevič[18]运用数理逻辑方法对问题E给出了否定的回答，即证明了这样的算法是不存在的. 上述结果从一个侧面说明了求解丢番图方程的困难程度.

直到本世纪初，人们讨论丢番图方程的方法主要是以整除性、同余式、连分数、平方剩余、原根与指数等内容为基础的初等数论方法和以代数数域中代数整数环上理想数的基本性质为基础的代数数论方法(参见文献[19]). 从本世纪初开始，两类新的数论方法在丢番图方程的研究中崭露头角，并且逐渐成为该领域的主要研究方法. 它们分别是以代数数的有理逼近为基础的丢番图逼近方法和以代数数对数线性型的下界估计为基础的超越数论方法. 以下我们简要地回顾一下这两类方法的起源.

设 α 是 $d(d\geqslant 2)$ 次代数数. 1844年，Liouville[17]证明了：对于任何正数 δ，不等式

$$\left|\alpha-\frac{x}{y}\right|<\frac{1}{y^{d+\delta}},x,y\in\mathbb{Z},y>0,\gcd(x,y)=1 \tag{5}$$

仅有有限多组解 (x,y). 上述结果称为Liouville定理. 它揭示了代数数有理逼近的基本特性：对于任何给定的代数数，不会有很多的有理数能很好地逼近它. 设 κ 是使得当 $\upsilon>\kappa$ 时，不等式

$$\left|\alpha-\frac{x}{y}\right|<\frac{1}{y^{\upsilon}},x,y\in\mathbb{Z},y>0,\gcd(x,y)=1 \tag{6}$$

仅有有限多组解 (x,y) 的最小正数. 根据Liouville定理可知 $\kappa\leqslant d$. 在此后的一段相当长的时间里，关于 κ 的上界一直是丢番图逼近方面的中心课题. 1909年，Thue[29]进一步证明了：$\kappa\leqslant d/2+1$. 根据这一结果可以推知：Thue方程

$$f(x,y)=k, x,y \in \mathbb{Z} \tag{7}$$

仅有有限多组解(x,y)，这里$f(X,Y)$是二元$n(n\geqslant 3)$次型，k是非零整数. 1955 年，Roth[21]最终解决了上述问题. 他证明了：$\kappa\leqslant 2$. 由于已知任何无理数α都有无限多个渐近分数x/y满足

$$\left|\alpha-\frac{x}{y}\right|<\frac{1}{y^2}, x,y\in\mathbb{Z}, y>0, \gcd(x,y)=1, \tag{8}$$

因此 Roth 的结果是臻于至善的. 该结果通常称为 Roth 定理. 1970 年，Schmidt[22]将 Roth 定理推广到了多维的情况，由此可以得出一大类多元高次方程解数的有限性结果. 此类方法通常称为 Thue-Siegel-Roth-Schmidt 方法，有关它的基本原理可参考文献[23,24]，本书第 1.8 节将简要地介绍这方面的结果. 这里应该指出，Thue-Siegel-Roth-Schmidt 方法在本质上是非实效的. 例如，运用 Roth 定理可以估计出 Thue 方程(7)的解数的可有效计算的上界[6]，但不能得出它的解(x,y)的上界.

早在 1748 年，Euler[8]就已经预见到某些指数函数值和对数函数值的超越性. 然而直到百年之后，人们才能借助 Liouville 定理构造出超越数的具体例子. 此后，Hermite[13]和 Lindemann[16]分别证明了 Napier 常数e和圆周率π是超越数，其中后一结果解决了古希腊人提出的"化圆为方"问题. 这些研究成果为近代数论的一个重要分支——超越数论奠定了基础. 超越数论的进一步发展也与 Hilbert 的著名问题有关. Hilbert 的第七问题可表述为：

问题 F　当α为不等于 0 或 1 的代数数，β为非有理数的代数数时，α^β是不是超越数？

同时，Hilbert 还具体问及数$2^{\sqrt{2}}$和$e^\pi=(-1)^{-\sqrt{-1}}$的超越性. 由于当时对超越数的性质还知之甚少，所以人们普遍认为上述问题的解决要比 Fermat 猜想和 Riemann 猜想更晚. 但是，事实却大大出乎人们的预料. 1929 年，Gel'fond[9]首先证明了e^π是超越数，并且指出他的方法可以解决问题 F 在β属于虚二次域时的情况. 次年，Kuzmin[14]将 Gel'fond 的方法推广到β属于实二次域的情况，从而证明了$2^{\sqrt{2}}$是超越数. 1934 年，Gel'fond[10]和

Schneider[22]分别独立地解决了问题 F. 然而,Fermat 猜想直到最近才由 Wiles[39]给出了证明,至于 Riemann 猜想则至今尚未见到解决的迹象.

设$\mathbb{A}$是全体代数数的集合. Gel'fond 和 Schneider 的结果可以等价地表述为:

命题 A 对于非零代数数 α_1,α_2,如果 $\log\alpha_1,\log\alpha_2$ 在有理数域 $\mathbb{Q}$ 上线性无关,则它们在$\mathbb{A}$上也线性无关.

上述结果称为 Gel'fond-Schneider 定理. 在方法上,Gel'fond 和 Schneider 关于该结果的证明是不同的,前者利用了指数函数的微分特性,后者则基于指数函数的乘法性质. 这两种不同的思路及其推广形式分别称为 Gel'fond 途径和 Schneider 途径. 它们对后来许多重要结果的产生有着深远的影响,Waldschmidt[35—38]对此作了详细的分析和比较.

1952 年,Gel'fond[12]提出了以下问题:

问题 G 是否可将命题 A 中的结果推广到任意多个非零代数数的情况?

Gel'fond 指出这是一个相当困难而又非常有意义的问题,它的解决将对数论中的很多分支带来深刻的影响. 1966 年,Baker[1,1,1]完整地解决了问题 G,并且得到了更强的结果. 他用多变量辅助函数代替 Gel'fond[10]原来使用的单变量函数,并且引入了一种新的外插技巧,从而证明了:

命题 B 设 $\alpha_1,\cdots,\alpha_n$ 是非零代数数. 如果 $\log\alpha_1,\cdots,\log\alpha_n$ 在$\mathbb{Q}$上线性无关,则 $1,\log\alpha_1,\cdots,\log\alpha_n$ 在$\mathbb{A}$上同样线性无关.

上述命题称为 Baker 定理,它是超越数论中最重要的结果之一. 设 $\beta_0,\beta_1,\cdots,\beta_n$ 是非零代数数. 此时,

$$\Lambda = \beta_0 + \beta_1\log\alpha_1 + \cdots + \beta_n\log\alpha_n \tag{9}$$

称为关于代数数 $1,\alpha_1,\cdots,\alpha_n$ 的对数线性型. 从命题 B 可知:当 $\log\alpha_1,\cdots,\log\alpha_n$ 在$\mathbb{Q}$上线性无关时,必有 $\Lambda\neq 0$. 在此条件下,Gel'fond[11]首先对 $n=2$ 的情况给出了 $|\Lambda|$ 的可有效计算的下界. 他证明了:当 $n=2$ 且 $\beta_0=0$ 时,对于任何正数 δ 必有

$$\log|\Lambda| > -C_1(\delta,d,A)(\log B)^{5+\delta}, \tag{10}$$

其中 $d=[\mathbb{Q}(\alpha_1,\alpha_2,\beta_1,\beta_2):\mathbb{Q}]$，$A,B$ 分别是两组代数数 α_1,α_2 以及 β_1,β_2 的高的最大值，$C_1(\delta,d,A)$ 是仅与 δ,d,A 有关的可有效计算的正常数. 1968 年，Baker[1,2]将上述结果推广到了一般的情况. 他证明了：

命题 C 当 $\Lambda\neq0$ 时，对于任何正数 δ 必有

$$\log|\Lambda| > -C_2(\delta,n,d,A)(\log B)^{n+1+\delta}, \tag{11}$$

其中 $d=[\mathbb{Q}(\alpha_1,\cdots,\alpha_n,\beta_0,\beta_1,\cdots,\beta_n):\mathbb{Q}]$，$A,B$ 分别是代数数 $\alpha_1,\cdots,\alpha_n$ 以及 $\beta_0,\beta_1,\cdots,\beta_n$ 的高的最大值，$C_2(\delta,n,d,A)$ 是仅与 δ，n,d,A 有关的可有效计算的正常数.

上述结果在包括丢番图方程在内的许多数论问题中有着广泛的应用（参见文献[3]）. 此类方法通常称为 Gel'fond-Baker 方法，它是一类具有实效性的方法. 例如，Baker[2]将命题 C 运用于 Thue 方程（7），得到了该方程的解的可有效计算的上界. 又如，Tijdeman[30]利用命题 C 的一个改进形式，解决了有关 Catalan 方程（3）的猜想 C. 他证明了：方程（3）仅有有限多组解 (x,y,m,n)，而且这些解都满足 $\max(x,y,m,n)<C_3$，其中 C_3 是可有效计算的绝对正常数. 从上述例子可知，Gel'fond-Baker 方法可以把很多目前人们最感兴趣的丢番图方程的求解范围，由无限缩小到可以有效计算的有限范围之内；也就是说它解决了有关这些方程的求解问题 B，并且为最终解决问题 D 创造了条件. 由此可见，Gel'fond-Baker 方法是研究丢番图方程的一个强有力的工具.

近 30 年来，Gel'fond-Baker 方法在丢番图方程，特别是指数型方程的研究中不断获得卓有成效的应用. 10 年前，Shorey 和 Tijdeman[24]曾经对此有过系统的论述. 此外，文献[15]，[20]，[26]，[28]，[31]，[32]，[33]和[34]分别对近期各个阶段的工作进行了综述和总结. 本书将在上述文献的基础上，着重介绍这方面的最新成果和尚待解决的问题. 纵观 30 年来的发展历程，我们不难看到：在早期的工作中，直接利用 Gel'fond-Baker 方法得到的上界通常是相当大的，远远超出了现有的计算能力. 因而，这些结果虽

然能够说明所讨论的方程的解的有限性，但是对解的完全确定则帮助不大. 近年来，随着该方法的基本原理中关键数据的不断改进、综合运用各类方法的技巧不断提高以及各种高效率的计算手段的普及，已经有越来越多的丢番图方程问题获得了彻底的解决. 因此，这是现代数论中的一个前景十分广阔的研究领域.

参 考 文 献

[1] Baker A. ,Linear forms in the logarithms of algebraic numbers Ⅰ,Mathematika, 1966,13:204—216; Ⅱ:ibid,1967,14:102—107; Ⅲ:ibid,1967,14:220—228; Ⅳ:ibid,1968,15:204—216.

[2] Baker A. , Contribution to the theory of diophantine equation Ⅰ: On the representation of integers by binary forms,Philos Trans Roy Soc London,1968, A263:173—191.

[3] Baker A. , Transcendental Number Theory, Cambridge: Cambridge University Press,1975.

[4] Cassels,J. W. S. ,On the equation $a^x-b^y=1$,Amer J Math,1953,75:159—162.

[5] Catalan E. ,Note extraite d'une lettre adressée á l'èditeur,J Reine Angew Math, 1844,27:192.

[6] Davenport H. , Roth K. F. , Rational approximation to algebraic number, Mathematika,1955,2:160—167.

[7] Dickson L. E. ,History of the Theory of Numbers,Vol. 2,Carnegie Institution of Washington,1920.

[8] Euler L. , Introduction to Analysis of the Infinite, Book I, Berlin: Springer-Verlag,1988:80.

[9] Gel'fond A. O. ,Sur les nombres transcendants,C R Acad Sci Paris,1929,189: 1224—1226.

[10] Gel'fond A. O. , Sur le septième problème de Hilbert,Izv Akad Nauk SSSR, 1934,7:623—630.

[11] Gel'fond A. O. ,On the approximation of transcendental numbers by algebraic numbers,Dokl Akad Nauk SSSR,1935,2:177—182.

[12] Gel'fond A. O. ,Transcendental and Algebraic Numbers,New York:Dover Publ, 1960.

[13] Hermite Ch,Sur la fonction exponentielle,C R Acad Sci Paris,1873,77:18—24, 74—79,226—233,285—293.