英文版

# 古今数学思想

[美] 莫里斯·克莱因 著

第三册

上海科学技术出版社

# 古今数学思想

（英文版）

第三册

[美]莫里斯·克莱因　著

上海科学技术出版社

**图书在版编目(CIP)数据**

古今数学思想. 第三册＝Mathematical thought from ancient to modern times(volume 3):英文/(美)克莱因(Kline,M.)著. —上海:上海科学技术出版社,2014.1

ISBN 978－7－5478－2072－8

Ⅰ.①古... Ⅱ.①克... Ⅲ.①数学史－英文 Ⅳ.①O11

中国版本图书馆 CIP 数据核字(2013)第 267006 号



**古今数学思想**（英文版）第三册

[美]莫里斯·克莱因 著

上海世纪出版股份有限公司
上海科学技术出版社 出版
(上海钦州南路 71 号 邮政编码 200235)

上海世纪出版股份有限公司发行中心发行
200001 上海福建中路 193 号 www.ewen.cc
苏州望电印刷有限公司印刷
开本:787×1092 1/16 印张 28.5
字数:420 千字
2014 年 1 月第 1 版 2014 年 1 月第 1 次印刷
ISBN 978－7－5478－2072－8/O·31
定价：78.00 元

# 序

如果我们想要预见数学的将来，适当的途径是研究这门科学的历史和现状。

庞加莱(Henri Poincaré)

本书论述从古代一直到20世纪头几十年中的重大数学创造和发展。目的是介绍中心思想，特别着重于那些在数学历史的主要时期中逐渐冒出来并成为最突出的，并且对于促进和形成尔后的数学活动有影响的主流工作。本书所极度关心的还有对数学本身的看法、不同时期中这种看法的改变，以及数学家对于他们自己的成就的理解。

必须把本书看作是历史的一个概述。当人们想到欧拉（Leonhard Euler）全集满满的约70卷、柯西（Augustin-Louis Cauchy）的26卷、高斯(Carl Friedrich Gauss)的12卷，人们就容易理解只凭本书一卷的篇幅不能给出一个详尽的叙述。本书的一些篇章只提出所涉及的领域中已经创造出来的数学的一些样本，可是我坚信这些样本最具有代表性。再者，为了把注意力始终集中于主要的思想，我引用定理或结果时，常常略去严格准确性所需要的次要条件。本书当然有它的局限性，但我相信它已给出整个历史的一种概貌。

本书的组织着重在居领导地位的数学课题，而不是数学家。数学的每一分支打上了它的奠基者的烙印，并且杰出的人物在确定数学的进程方面起决定性作用。但是，特意叙述的是他们的思想，传记完全是次要的。在这一点上，我遵循帕斯卡（Blaise Pascal）的意见：“当我们援引作者时，我们是援引他们的证明，不是援引他们的姓名。”

为使叙述连贯，特别是在1700年以后的时期，对于每一发展要等到它已经成熟，在数学中占重要地位并且产生影响的时候，我才进行论述。例如，我把非欧几里得几何放在19世纪的时期介绍，虽然企图寻找欧几里得平行公

理的替代物或证明早在欧几里得（Euclid）时代就开始了并且继续不断。当然，有许多问题会在不同的时期反复提及。

为了不使资料漫无边际，我忽略了几种文化，例如中国的*、日本的和玛雅的文化，因为他们的工作对于数学思想的主流没有重大的影响。还有一些数学中的发展，例如概率论和差分演算，它们今天变得重要，但在所考虑的时期中并未起重要作用，从而也只得到很少的注意。这最后的几十年的大发展使我不得不在本书中只收入那些20世纪的，并且在该时期变成有特殊意义的创造。我没有在20世纪时期继续讨论像常微分方程或变分法的扩展，因为这将会需要很专门的资料，而它们只对于这些领域的研究工作者有兴趣，并且将会大大增加本书的篇幅。此外还考虑到，对于许多较新的发展的重要性，目前还不能做客观的估价。数学的历史告诉我们，许多科目曾经激起过很大的热情，并且得到最好的数学家的注意，但终于湮没无闻。我们只需要回忆一下凯莱（Arthur Cayley）的名言“射影几何就是全部几何”，以及西尔维斯特（James Joseph Sylvester）的断言“代数不变量的理论已经总结了数学中的全部精华”。确实，历史给出答案的有趣问题之一便是数学中哪些东西还生存着而未被淘汰？历史做出它自己的而且更可靠的评价。

通过几十项重要发展的即使是基础的叙述，也不能指望读者知道所有这些发展的内容。因此，我在本书中论述某科目的历史时，除去一些极初等的领域外，也说明科目的内容，把科目的历史叙述和内容说明融合起来。对各种数学创造，这些说明也许不能把它们完全讲清楚，但应能使读者对它们的本质得到某些概念。从而在某种程度上，本书也可作为一本从历史角度来讲解的数学入门书。这无疑是使读者能获得理解和鉴赏的最好的写法之一。

我希望本书对于专业的数学家和未来的数学家都有帮助。专业的数学家今天不得不把这么多的时间和精力倾注到他的专题上去，使得他没有机会去熟悉他的学科的历史。而实际上，这历史背景是重要的。现在的根深扎在过去，而对于寻求理解“现在之所以成为现在这样子”的人们来说，过去的每一事件都不是无关的。再者，虽然数学大树已经伸张出成百的分支，它毕竟是一个整体，并且有它自己的重大问题和目标。如果一些分支专题对于数学的心脏无所贡献，它们就不会开花结果。我们的被分裂的学科就面临着这种危险；跟这种危险做斗争的最稳妥的办法，也许就是要对于数学的过去成就、传统和目标得到一些知识，使得能把研究工作导入有成果的渠道。如同

* 中国数学史的一个可喜的叙述，已见于李约瑟（Joseph Needham）的*Science and Civilization in China*，剑桥大学出版社，1959，卷3，第1～168页。

希尔伯特（David Hilbert）所说的："数学是一个有机体，它的生命力的一个必要条件是所有各部分的不可分离的结合。"

对于学数学的学生来说，本书还会另有好处。通常一些课程所介绍的是一些似乎没有什么关系的数学片断。历史可以提供整个课程的概貌，不仅使课程的内容互相联系，而且使它们跟数学思想的主干也联系起来。

在一个基本方面，通常的一些数学课程也使人产生一种幻觉。它们给出一个系统的逻辑叙述，使人们有这种印象：数学家们几乎理所当然地从定理到定理，数学家能克服任何困难，并且这些课程完全经过锤炼，已成定局。学生被湮没在成串的定理中，特别是当他正开始学习这些课程的时候。

历史却形成对比。它教导我们，一个科目的发展是由汇集不同方面的成果点滴积累而成的。我们也知道，常常需要几十年甚至几百年的努力才能迈出有意义的几步。不但这些科目并未锤炼成无缝的天衣，就是那已经取得的成就，也常常只是一个开始，许多缺陷有待填补，或者真正重要的扩展还有待创造。

课本中的斟字酌句的叙述，未能表现出创造过程中的斗争、挫折，以及在建立一个可观的结构之前，数学家所经历的艰苦漫长的道路。学生一旦认识到这一点，他将不仅获得真知灼见，还将获得顽强地追究他所攻问题的勇气，并且不会因为他自己的工作并非完美无缺而感到颓丧。实在说，叙述数学家如何跌跤，如何在迷雾中摸索前进，并且如何零零碎碎地得到他们的成果，应能使搞研究工作的任一新手鼓起勇气。

为了使本书能包罗所涉及的这个大范围，我曾经试着选择最可靠的原始资料。对于微积分以前的时期，像希思(Thomas L.Heath)的《希腊数学史》（*A History of Greek Mathematics*）无可否认地是第二手的资料，可是我并未只依靠这样的一个来源。对于以后时期中的数学发展，通常都能直接查阅原论文；这些都幸而可以从期刊或杰出的数学家的全集中找到。对研究工作的大量报道和概述也帮助了我，其中一些实际上也就在全集里。对于所有的重要结果，我都试着给出出处。但并没有对于所有的断言都这么做；否则将会使引证泛滥，浪费篇幅，而这些篇幅还不如用来充实报道。

每章中的参考书目指出资料来源。如果读者有兴趣，他能从这些来源得到比本书中所说的更多的报道。这些书目中还包括许多不应而且没有作为来源的文献。把它们列在书目中，是因为它们供给额外的报道，或者表达的水平可以对一些读者更有帮助，或者它们比原始资料更易于找到。

在此，我想对我的同事Martin Burrow,Bruce Chandler,Martin Davis, Donald

Ludwig,Wilhelm Magnus,Carlos Moreno,Harold N.Shapiro 和Marvin Tretkoff表示谢意，感谢他们回答了大量的问题，阅读了本书的许多章节，提出了许多宝贵的批评意见。我特别感激我的妻子Helen，她以批评的眼光编辑我的手稿，广泛地核对人名、日期和出处，而且极仔细地阅读尚未分成页的校样并给它们编上页码。Eleanore M.Gross夫人做了大量的打字工作，对我是一个极大的帮助。我想对牛津大学出版社的编辑部表示感激，感谢他们细心地印刷了本书。

**莫里斯·克莱因**(Morris Kline)

纽约1972年5月

# 目　录

# 34
# The Theory of Numbers in the Nineteenth Century

> It is true that Fourier had the opinion that the principal object of mathematics was public use and the explanation of natural phenomena; but a philosopher like him ought to know that the sole object of the science is the honor of the human spirit and that under this view a problem of [the theory of] numbers is worth as much as a problem on the system of the world.
>
> C. G. J. JACOBI

## 1. *Introduction*

Up to the nineteenth century the theory of numbers was a series of isolated though often brilliant results. A new era began with Gauss's *Disquisitiones Arithmeticae*[1] which he composed at the age of twenty. This great work had been sent to the French Academy in 1800 and was rejected but Gauss published it on his own. In this book he standardized the notation; he systematized the existing theory and extended it; and he classified the problems to be studied and the known methods of attack and introduced new methods. In Gauss's work on the theory of numbers there are three main ideas: the theory of congruences, the introduction of algebraic numbers, and the theory of forms as the leading idea in Diophantine analysis. This work not only began the modern theory of numbers but determined the directions of work in the subject up to the present time. The *Disquisitiones* is difficult to read but Dirichlet expounded it.

Another major nineteenth-century development is analytic number theory, which uses analysis in addition to algebra to treat problems involving the integers. The leaders in this innovation were Dirichlet and Riemann.

## 2. *The Theory of Congruences*

Though the notion of congruence did not originate with Gauss—it appears in the work of Euler, Lagrange, and Legendre—Gauss introduced the notation

1. Published 1801 = *Werke*, 1.

in the first section of *Disquisitiones* and used it systematically thereafter. The basic idea is simple. The number 27 is congruent to 3 modulo 4,

$$27 \equiv 3 \text{ modulo } 4,$$

because $27 - 3$ is exactly divisible by 4. (The word modulo is often abbreviated to mod.) In general, if $a$, $b$, and $m$ are integers

$$a \equiv b \text{ modulo } m$$

if $a - b$ is (exactly) divisible by $m$ or if $a$ and $b$ have the same remainders on division by $m$. Then $b$ is said to be a residue of $a$ modulo $m$ and $a$ is a residue of $b$ modulo $m$. As Gauss shows, all the residues of $a$ modulo $m$, for fixed $a$ and $m$, are given by $a + km$ where $k = 0, \pm 1, \pm 2, \ldots$.

Congruences with respect to the same modulus can be treated to some extent like equations. Such congruences can be added, subtracted, and multiplied. One can also ask for the solution of congruences involving unknowns. Thus, what values of $x$ satisfy

$$2x \equiv 25 \text{ modulo } 12?$$

This equation has no solutions because $2x$ is even and $2x - 25$ is odd. Hence $2x - 25$ cannot be a multiple of 12. The basic theorem on polynomial congruences, which Gauss re-proves in the second section, had already been established by Lagrange.[2] A congruence of the $n$th degree

$$Ax^n + Bx^{n-1} + \cdots + Mx + N \equiv 0 \text{ modulo } p$$

whose modulus is a prime number $p$ which does not divide $A$ cannot have more than $n$ noncongruent roots.

In the third section Gauss takes up residues of powers. Here he gives a proof in terms of congruences of Fermat's minor theorem, which, stated in terms of congruences, reads: If $p$ is a prime and $a$ is not a multiple of $p$ then

$$a^{p-1} \equiv 1 \text{ modulo } p.$$

The theorem follows from his study of congruences of higher degree, namely,

$$x^n \equiv a \text{ modulo } m$$

where $a$ and $m$ are relatively prime. This subject was continued by many men after Gauss.

The fourth section of *Disquisitiones* treats quadratic residues. If $p$ is a prime and $a$ is not a multiple of $p$ and if there exists an $x$ such that $x^2 \equiv a \bmod p$, then $a$ is a quadratic residue of $p$; otherwise $a$ is a quadratic nonresidue of $p$. After proving some subordinate theorems on quadratic residues Gauss gave the first rigorous proof of the law of quadratic reciprocity (Chap.

2. *Hist. de l'Acad. de Berlin*, 24, 1768, 192 ff., pub. 1770 = *Œuvres*, 2, 655–726.

25, sec. 4). Euler had given a complete statement much like Gauss's in one paper of his *Opuscula Analytica* of 1783 (Chap. 25, sec. 4). Nevertheless in article 151 of his *Disquisitiones* Gauss says that no one had presented the theorem in as simple a form as he had. He refers to other work of Euler including another paper in the *Opuscula* and to Legendre's work of 1785. Of these papers Gauss says rightly that the proofs were incomplete.

Gauss is supposed to have discovered a proof of the law in 1796 when he was nineteen. He gave another proof in the *Disquisitiones* and later published four others. Among his unpublished papers two more were found. Gauss says that he sought many proofs because he wished to find one that could be used to establish the biquadratic reciprocity theorem (see below). The law of quadratic reciprocity, which Gauss called the gem of arithmetic, is a basic result on congruences. After Gauss gave his proofs, more than fifty others were given by later mathematicians.

Gauss also treated congruences of polynomials. If $A$ and $B$ are two polynomials in $x$ with, say, real coefficients then one knows that one can find unique polynomials $Q$ and $R$ such that

$$A = B \cdot Q + R,$$

where the degree of $R$ is less than the degree of $B$. One can then say that two polynomials $A_1$ and $A_2$ are congruent modulo a third polynomial $P$ if they have the same remainder $R$ on division by $P$.

Cauchy used this idea[3] to define complex numbers by polynomial congruences. Thus if $f(x)$ is a polynomial with real coefficients then under division by $x^2 + 1$

$$f(x) \equiv a + bx \bmod x^2 + 1$$

because the remainder is of lower degree than the divisor. Here $a$ and $b$ are necessarily real by virtue of the division process. If $g(x)$ is another such polynomial then

$$g(x) \equiv c + dx \bmod x^2 + 1.$$

Cauchy now points out that if $A_1$, $A_2$, and $B$ are any polynomials and if

$$A_1 = BQ_1 + R_1 \quad \text{and} \quad A_2 = BQ_2 + R_2,$$

then

$$A_1 + A_2 \equiv R_1 + R_2 \bmod B, \quad \text{and} \quad A_1A_2 \equiv R_1R_2 \bmod B.$$

We can now see readily that

$$f(x) + g(x) \equiv (a + c) + (b + d)x \bmod x^2 + 1$$

3. *Exercices d'analyse et de physique mathématique*, 4, 1847, 84 ff. = *Œuvres*, (1), 10, 312–23 and (2), 14, 93–120.

and since $x^2 \equiv -1 \bmod x^2 + 1$ that

$$f(x)g(x) \equiv (ac - bd) + (ad + bc)x \bmod x^2 + 1.$$

Thus the numbers $a + bx$ and $c + dx$ combine like complex numbers; that is, they have the formal properties of complex numbers, $x$ taking the place of $i$. Cauchy also proved that every polynomial $g(x)$ not congruent to 0 modulo $x^2 + 1$ has an inverse, that is, a polynomial $h(x)$ such that $h(x)g(x)$ is congruent to 1 modulo $x^2 + 1$.

Cauchy did introduce $i$ for $x$, $i$ being for him a real indeterminate quantity. He then showed that for any

$$f(i) = a_0 + a_1 i + a_2 i^2 + \cdots$$

that

$$f(i) \equiv a_0 - a_2 + a_4 - \cdots + (a_1 - a_3 + a_5 - \cdots)i \text{ modulo } i^2 + 1.$$

Hence any expression involving complex numbers behaves as one of the form $c + di$ and one has all the apparatus needed to work with complex expressions. For Cauchy, then, the polynomials in $i$, with his understanding about $i$, take the place of complex numbers and one can put into one class all those polynomials having the same residue modulo $i^2 + 1$. These classes are the complex numbers.

It is interesting that in 1847 Cauchy still had misgivings about $\sqrt{-1}$. He says, "In the theory of algebraic equivalences substituted for the theory of imaginary numbers the letter $i$ ceases to represent the symbolic sign $\sqrt{-1}$, which we repudiate completely and which we can abandon without regret since one does not know what this supposed sign signifies nor what sense to attribute to it. On the contrary we represent by the letter $i$ a real quantity but indeterminate and in substituting the sign $\equiv$ for $=$ we transform what has been called an imaginary equation into an algebraic equivalence relative to the variable $i$ and to the divisor $i^2 + 1$. Since this divisor remains the same in all the formulas one can dispense with writing it."

In the second decade of the century Gauss proceeded to search for reciprocity laws applicable to congruences of higher degree. These laws again involve residues of congruences. Thus for the congruence

$$x^4 \equiv q \bmod p$$

one can define $q$ as a biquadratic residue of $p$ if there is an integral value of $x$ satisfying the equation. He did arrive at a law of biquadratic reciprocity (see below) and a law of cubic reciprocity. Much of this work appeared in papers from 1808 to 1817 and the theorem proper on biquadratic residues was given in papers of 1828 and 1832.[4]

4. *Comm. Soc. Gott.*, 6, 1828, and 7, 1832 = *Werke*, 2, 65–92 and 93–148; also pp. 165–78.

To attain elegance and simplicity in his theory of cubic and biquadratic residues Gauss made use of complex integers, that is, numbers of the form $a + bi$ with $a$ and $b$ integral or 0. In Gauss's work on biquadratic residues it was necessary to consider the case where the modulus $p$ is a prime of the form $4n + 1$ and Gauss needed the complex factors into which prime numbers of the form $4n + 1$ can be decomposed. To obtain these Gauss realized that one must go beyond the domain of the ordinary integers to introduce the complex integers. Though Euler and Lagrange had introduced such integers into the theory of numbers it was Gauss who established their importance.

Whereas in the ordinary theory of integers the units are $+1$ and $-1$ in Gauss's theory of complex integers the units are $\pm 1$ and $\pm i$. A complex integer is called composite if it is the product of two such integers neither of which is a unit. If such a decomposition is not possible the integer is called a prime. Thus $5 = (1 + 2i)(1 - 2i)$ and so is composite, whereas 3 is a complex prime.

Gauss showed that complex integers have essentially the same properties as ordinary integers. Euclid had proved (Chap. 4, sec. 7) that every integer is uniquely decomposable into a product of primes. Gauss proved that this unique decomposition, which is often referred to as the fundamental theorem of arithmetic, holds also for complex integers provided we do not regard the four unit numbers as different factors. That is, if $a = bc = (ib)(-ic)$, the two decompositions are the same. Gauss also showed that Euclid's process for finding the greatest common divisor of two integers is applicable to the complex integers.

Many theorems for ordinary primes carry over to the complex primes. Thus Fermat's theorem carries over in the form: If $p$ be a complex prime $a + bi$ and $k$ any complex integer not divisible by $p$ then

$$k^{Np-1} \equiv 1 \text{ modulo } p$$

where $Np$ is the norm $(a^2 + b^2)$ of $p$. There is also a law of quadratic reciprocity for complex integers, which was stated by Gauss in his 1828 paper.

In terms of complex integers Gauss was able to state the law of biquadratic reciprocity rather simply. One defines an uneven integer as one not divisible by $1 + i$. A primary uneven integer is an uneven integer $a + bi$ such that $b$ is even and $a + b - 1$ is even. Thus $-7$ and $-5 + 2i$ are primary uneven numbers. The law of reciprocity for biquadratic residues states that if $\alpha$ and $\beta$ are two primary uneven primes and $A$ and $B$ are their norms, then

$$\left(\frac{\alpha}{\beta}\right)_4 = (-1)^{(1/4)(A-1)(1/4)(B-1)}\left(\frac{\beta}{\alpha}\right)_4.$$