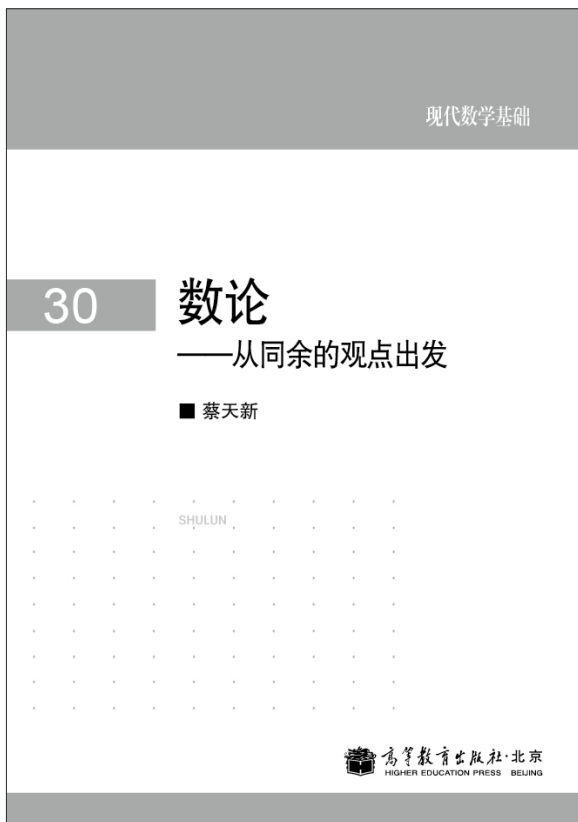


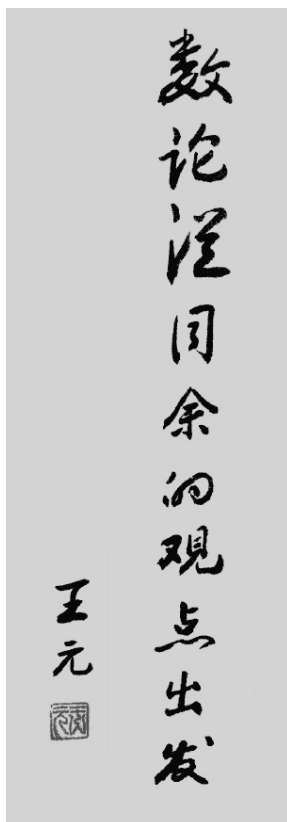
数是我们心灵的产物

蔡天新



《数论——从同余的观点出发》

编者按 本文是蔡天新教授为他新近出版的著作《数论——从同余的观点出发》（高等教育出版社，2012年9月）所作的导言，在这本基础数论教程里，每小节后面都有补充读物，从中介绍了数论研究的新方法，并就若干经典数论问题提出自己大胆新颖的想法或延拓，部分结果发表后引起数论界同行的关注，包括菲尔兹奖得主阿兰·贝克在内的名家都予以褒扬。蔡天新教授认为，他之所以能在近年取得自我突破，部分原因是数学史和数学文化进行了学习和探讨，这提升了他的想象力，促进了他的数论研究。



王元先生扉页题词

将近一个世纪以前，美国出生的英国数学家莫德尔在一篇随笔中写道：“数论是无与伦比的，因为整数和各式各样的结论，因为美丽和论证的丰富性。高等算术（数论）看起来包含了数学的大部分罗曼史。如同高斯给索菲·热尔曼的信中所写的，‘这类纯粹的研究只对那些有勇气探究她的人才会展现最魅人的魔力’。”或许有一天，全世界的黄金和钻石会被挖掘殆尽，可是数论，却是用之不竭的珍宝。

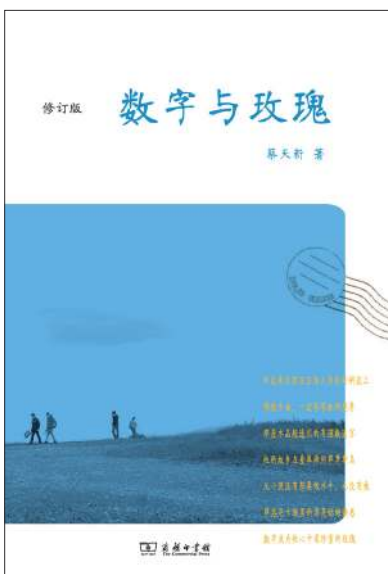
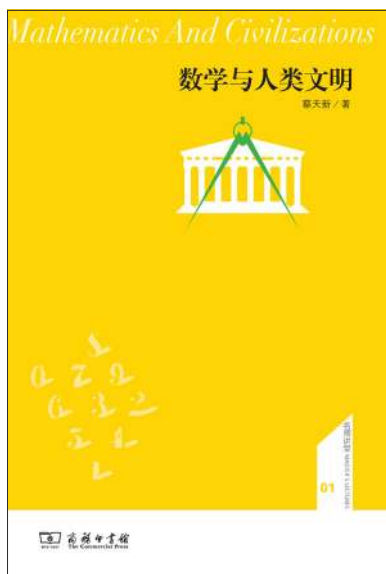
1801年，24岁的德国青年高斯出版了《算术研究》，从而开创了数论研究的新纪元。这部伟大的著作曾投寄到法国科学院而被忽视，但高斯在友人的资助下将它自费出版了。在那个世纪的末端，集合论的创始人康托尔这样评价：

“《算术研究》是数论的宪章……高斯的出版物就是法典，比人类其他法典更高明，因为无论何时何地从未发觉出其中有任何一处错误。”高斯自己则赞叹，“数学是科学的皇后，数论是数学的皇后。”

这部著作的开篇即定义了同余，任意两个整数 a 和 b 被认为是模 n 同余的，假如它们的差 $a - b$ 被 n 整除。高斯首次引进了同余记号，他用符号“ $\equiv$ ”表示同余。于是，上述定义可表示为

$$a \equiv b \pmod{n}$$

有了这个方便的同余记号以后，数论的教科书显得更加简洁美观。今天，基础数论教材的开篇大多介



左:《数学与人类文明》;右:《数字与玫瑰》修订版,两本同是2012年秋冬由商务印书馆出版的数学文化著作,它们与《数论》构成作者的2012数学三部曲

绍整除或可除性。整除与同余式也构成了本书的前两章,实际上,整除拟或带余数除法(在中国、印度和希腊等地有着各自的渊源故事和名称)

$$a \equiv bq + r, 0 \leq r < b$$

也等价于同余式 $a \equiv r \pmod{b}, 0 \leq r < b$ 。

接下来的三章,无论不定方程,还是原根和指标,均与同余有关,更不要说一次、二次和 n 次剩余了。不仅如此,初等数论中最有名的定理,除了算术基本定理以外,均与同余有关。例如,欧拉-费马定理、威尔逊-高斯定理、拉格朗日定理和中国剩余定理,后者的准确名字应为孙子-秦九韶定理,或秦九韶定理(参见第3章第1节)。

进入第3章以后,我们讲述了高斯最得意的、花费许多心血反复论证(共8次)的二次互反律,高斯称其为“算术中的宝石”。设 p 和 q 是不同的奇素数,则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

这里 (p/q) 为勒让德符号,当它取1或-1分别表示二次同余式 $x^2 \equiv p \pmod{q}$ 有解或无解。这个结果是完美无缺的,我们用几何和代数方法给出两个证明。在第6章我们介绍了一个新的同余式,她有着同样美丽的对称性。设 p, q 为不同的奇素数,则

$$\left(\frac{pq-1}{(pq-1)/2}\right) \equiv \left(\frac{p-1}{(p-1)/2}\right) \left(\frac{q-1}{(q-1)/2}\right) \pmod{pq}$$

此处 $()$ 为二项式系数。

除了引进同余符号,高斯还给出了正多边形作图方法和原根存在的充要条件,前者是有着两千多年历史的数学悬案,后者的理论虽较完整仍可以增补(如原根的乘积、求和同余),这些在本书的第4章第5节和第5章均有展示。说到原根的存在性,少不了素幂模同余式,本书的第7章给出了不少素幂模甚或整数幂模的崭新公式,包括拉赫曼同余式的推广,后者在怀尔斯的证明之前一直是研究费马大定理的主要工具。诚如加拿大和爱尔兰两位同行指出,这一推广(指从素幂模到整数幂模)是1906年以来的第一次。又如,设 n 是任意奇数,我们发现并证明了

$$(-1)^{\phi(n)/2} \prod_{d|n} \left(\frac{d-1}{(d-1)/2} \right)^{\mu(n/d)} \equiv 4^{\phi(n)} \begin{cases} \pmod{n^3}, & \text{若 } 3 \nmid n \\ \pmod{n^3/3}, & \text{若 } 3 \mid n \end{cases}$$

其中 $\phi(n)$ 、 $\mu(n)$ 分别为欧拉函数和莫比乌斯函数。当 n 为素数时,此即著名的莫利(Morley)定理。

二次型是高斯著作中的重头戏,尤其是表整数问题,拉格朗日证明了,每一个自然数均可表为4个整数的平方和。本书这方面谈的不多,但对于著名的华林问题,我们却有独到深刻的描述。设 k 和 s 为正整数,考虑丢番图方程

$$n = x_1 + x_2 + \cdots + x_s.$$

其中

$$x_1 x_2 \cdots x_s = x^k$$

由希尔伯特1909年的论证可知,必定存在 $s = s'(k)$, 使对任意的正整数 n , 均可表成不超过 s 个正整数之和,且其乘积是 k 次方。用 $g'(k)(G'(k))$ 分别表示最小的正整数 s , 使对任意(充分大的)正整数 n , 上述方程成立。我们在第7章给出了 $g'(k)$ 的准确值和 $G'(k)$ 的估值,同时猜测 $G'(3) = 3, G'(4) = 4$ 。一个更为精巧的推测是,除了2、5和11,每个素数均可表成3个正整数之和,它们的乘积为立方数。

之所以能提出这类问题,是因为我们把整数的加法和乘法结合起来考虑,这一点受到了 abc 猜想的形式启发,后者可以轻松导出费马大定理等一系列著名