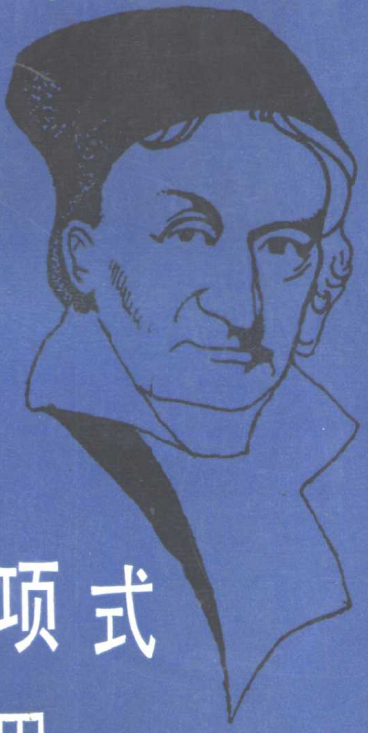
世界数学名题欣赏



置换多项式及其应用

辽宁教育出版社

世界数学名题欣赏丛书

置换多项式及其应用

孙 琦 万大庆 著

辽宁教育出版社
1987年·沈阳

置换多项式及其应用

孙 琦 万大庆 著

辽宁教育出版社出版 辽宁省新华书店发行
（沈阳市南京街6段1里2号） 朝阳新华印刷厂印刷

字数：57,000 开本：787×1092 1/32 印张：4 1/2 插页：4
印数：1—4,500
1987年10月第1版 1987年10月第1次印刷

责任编辑：俞晓群 谭 坚 责任校对：王淑芬
封面设计：安今生 插 图：安 迪

统一书号：7371·499 定价：1.20 元
ISBN 7-5382-0171-X

内 容 简 介

本书是“世界数学名题欣赏丛书”之一。置换多项式就是可表达完全剩余系的多项式。完全剩余系问题是1801年由数学家高斯在他的著作《算术探讨》中首先提出的，这一问题在数论研究中占有非常重要的地位。而置换多项式问题又在完全剩余系研究中占有重要地位。本书系统地介绍了置换多项式的产生、发展和理论，并且着重介绍了它在现代科学中的广泛应用。论述深入浅出，简明生动，读后有益于提高数学修养，开阔知识视野。

Summary

This book is one of A Series of World Famous Mathematics-Appreciation. Permutation polynomial is the polynomial that can express complete residue classes. The problem of complete residue classes was first put forward by mathematician Gauss in his work «Disguisition Arithematicae» in 1801. This problem occupies an important place in the mathematic research. However, the problem of permutation holds an important place in the research of complete residue classes. The book systematically introduces the birth, development and theory of permutation polynomials, and mainly introduces its wide application in modern science. Its exposition explains the profound in simple terms with concise and vivid language. After reading it, we can raise our understanding of mathematics, and widen our knowledge field of vision.

前　言

什么是置换多项式？简单地讲，置换多项式就是表完全剩余系的多项式。历史上，完全剩余系起源于数学王子高斯的工作，早在1801年，在他的名著《算术探讨》中就有对完全剩余系的系统研究。

什么又是完全剩余系呢？设m是一个正整数，我们知道任何一个整数用m去除后其余数均在$\{0,1,\cdots,m-1\}$中。若有m个整数，其余数正好互不相同（因此取$\{0,1,\cdots,m-1\}$中的每个数正好一次），则称这m个数组成的集合为模m的一个完全剩余系。又设a，b是任意整数，$(a,m)=1$，如果x通过模m的一个完全剩余系，则$ax+b$也通过模m的一个完全剩余系，这是数论中一个熟知的性质。注意，$ax+b$是一次整系数多项式。于是自然要问：若$f(x)$是一个n次整系数多项式，那么当x通过模m的一个完全剩余系时，

$f(x)$是否也通过模m的一个完全剩余系？若结论是肯定的，则称$f(x)$是模m的一个置换多项式。

1863年，厄米特首先开创了对模p（p是素数）的置换多项式的研究，得出了判别置换多项式的准则。1866年和1870年，塞利特和约当分别作了进一步的工作。之后，迪克逊于1896年—1897年将置换多项式的概念推广到任意有限域上，对置换多项式作了深入和系统的探讨，这些工作的一个概述可以在他1901年的著作《线性群》中找到。1923年，迪克逊在他的名著《数论史》第三卷中总结了1922年以前有关置换多项式的结果。这一时期的基本工作均是由迪克逊本人完成的。

本世纪五十年代以来，卡里兹及其学生，还有其他一些数学家对置换多项式又开始了新的研究。一些深入的工具，如黎曼曲面的理论，代数数论，算术代数几何等相继用到置换多项式上，得出了许多深刻的结果。模p的单变元置换多项式也开始被推广到剩余类环以至一般环的多变元置换多项式上，这些工作大大丰富了置换多项式的内容，给该领域以极大的推动和发展。1973年，劳斯基和诺鲍尔在其专著《多项式代数》中收入了一百余篇关于置换多项式的论文。到1983年，从利德尔和利德奈特的百科全书式的著作《有限

域》一书中可以看出，研究置换多项式的论文已多达四百余篇！可见，近年来，置换多项式发展相当迅速。

引起置换多项式迅速发展的一个原因是置换多项式已逐渐在数论，组合论，群论，非结合代数，密码系统等领域中得到应用。作为一个有趣的例子，我们在第二章中将给出置换多项式对公开密钥码的一个应用。

应当指出，对置换多项式的研究虽有一百余年的历史，该领域内仍有大量的工作可做，还有许多问题没有得到解决，对于一般环上的置换多项式更是如此。

鉴于上述情况及国内目前尚无介绍这方面工作的读物，我们特将有关置换多项式的基本内容及进展情况整理成册，用尽量简单的形式介绍给我国读者，以促进国内在这方面的研究。在材料的选取上，我们仅限于模m的置换多项式和有限域F_q上的置换多项式，因为这两种情形都是最简单和基本的，都有比较丰富和完善的结果，而且得到了较广泛的应用。所以这种选取并不影响对置换多项式这个课题的了解。对于一般的抽象环上的置换多项式及多变元置换多项式，读者可参考文献〔24〕和〔27〕，后者附有非常完备的参考文献。

另外，对不太复杂的定理，我们都尽量给出其证明，这样，通过本书读者不仅能够了解到置换多项式的一个概貌，而且能学到一些基本的解决问题的方法。我们在书中还提出了一些有待解决的问题，以供有志于在这方面进行研究的读者参考。在附录中，我们还不加证明地介绍了用到的一些预备知识，因此，读者只要具备代数的基础知识，就能读懂本书的绝大部分内容。

最后，由于这本小册子首次将有关置换多项式的基本内容整理成册，限于作者的水平，错误和不妥之处在所难免，敬请读者批评指正。

作　者

1986年9月于成都

世界数学名题欣赏丛书

费马猜想

黎曼猜想

连续统假设

希尔伯特第十问题

欧几里得第五公设

哥德尔不完全性定理

不动点定理

无处可微的连续函数

科克曼女生问题

斐波那契数列

哥德巴赫猜想

置换多项式及其应用

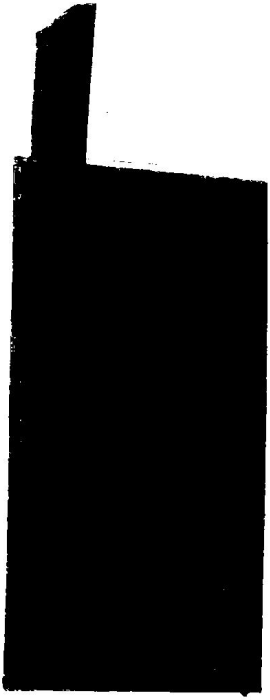
素数判定与大数分解

货郎担问题

作者简介

孙琦（左），1937年生于浙江省吴兴县，1961年毕业于四川大学数学系，现为四川大学数学系教授、数学研究所数论研究室主任、《数学学报》编委、四川省数学会副秘书长。已发表学术论文50余篇，出版著作五种，有：《单位分数》，《谈谈不定方程》，《初等数论100例》，《数论讲义》（上），《快速数论变换》，总共约七十余万字（包括合作）。主要研究方向为数论中的不定方程和应用数论。

万大庆，1964年生于四川重庆，1982年毕业于成都地质学院基础部，1982——1986年在四川大学数学系攻读博士学位，现在美国华盛顿大学数学系学习。已发表论文15篇，主要研究方向是数论。



目　录

Contents

一　剩余类环的置换多项式