

<<素数研究与应用参考手册>>

图书基本信息

书名：<<素数研究与应用参考手册>>

13位ISBN编号：9787030213525

10位ISBN编号：7030213521

出版时间：2008-4

出版时间：科学出版社

作者：高红卫

页数：482

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<素数研究与应用参考手册>>

内容概要

本书是世界上第一本素数研究与应用参考手册，基于数据量为TB级的素数数据库，提供迄今为止较为系统、较为完整的素数序列统计分析资料。

本书所列出的低端素数表和统计分析资料，主要面向基础研究和普及性研究；所列出的高端素数列表和统计分析资料，主要面向加密/解密技术应用研究；尤其是列出的部分连续素因子一阶合数表与特定连续合数完全分解表、部分RSA大合数完全素分割表，对于研究目前世界上比较流行的RSA加密技术中 $p \times q$ 合数之素因子分解问题，具有系统性的参考价值。

本书适合于相关领域研究人员、工程技术人员、软件工程师、大专院校师生、中小学数学教师、数论研究爱好者、信息加密与解密技术工作者与研究爱好者阅读。

<<素数研究与应用参考手册>>

书籍目录

前言第1篇 编例与查阅方法第2篇 部分区间素数统计数据表 $2 \sim (1.26 \times 10^{12} + 1)$ 区间素数统计表 $2 \sim (1.26 \times 10^{12} + 1)$ 区间最大素数间隙与最大间隙率统计表 $2 \sim (1.26 \times 10^{12} + 1)$ 区间素数间隙升序变动表 $2 \sim (1.26 \times 10^{12} + 1)$ 区间衔接区段素数参数统计表 $2 \sim (1.26 \times 10^{12} + 1)$ 区间孪生素数参数统计表 $2 \sim (1.26 \times 10^{12} + 1)$ 区间孪生素数升序变动表 $2 \sim (1.26 \times 10^{12} + 1)$ 区间衔接区段孪生素数统计表 $(6 \times 10^{100} + 2) \sim (6 \times 10^{100} + 1.08 \times 10^{11} + 1)$ 区间素数统计表 $(6 \times 10^{100} + 2) \sim (6 \times 10^{100} + 1.08 \times 10^{11} + 1)$ 区间最大素数间隙与最大间隙率统计表 $(6 \times 10^{100} + 2) \sim (6 \times 10^{100} + 1.08 \times 10^{11} + 1)$ 区间素数间隙升序变动表 $(6 \times 10^{100} + 2) \sim (6 \times 10^{100} + 1.08 \times 10^{11} + 1)$ 区间衔接区段素数参数统计表 $(6 \times 10^{100} + 2) \sim (6 \times 10^{100} + 1.08 \times 10^{11} + 1)$ 区间孪生素数升序变动表 $(6 \times 10^{100} + 2) \sim (6 \times 10^{100} + 1.08 \times 10^{11} + 1)$ 区间衔接区段孪生素数统计表第3篇 低端区间分析数据表 自然数 $6 \times 10^5 + 1$ 以内素数表 3×10^4 个含 5 素数的连续 - 阶合数表 $3 \times 10^4 + 1$ 以内含 7 及以上素因子合数完全分解表第4篇 合数的素分割专题 RSA - 576 素分割数据 RSA - 640 素分割数据 RSA - 704 素分割数据 RSA - 768 素分割数据 RSA - 896 素分割数据 RSA - 1024 素分割数据 RSA - 1536 素分割数据 RSA - 2048 素分割数据附录1 RSA 加密算法简介附录2 Prime Grid 项目简介

<<素数研究与应用参考手册>>

章节摘录

第1篇 编例与查阅方法 1.素数间隙统计数据的使用 需要提请读者注意的是,本手册中的“素数间隙”与其他资料中的“素数间隙”定义是不同。

前者是指:到素数 P 为止,之前有且仅有连续 n 个合数存在;而后者是指:从起点素数 P 开始,之后有且仅有连续 n 个合数存在。

本手册中的“素数间隙率”与其他资料中的“素数间隙度”,定义也是不同的。

前者是指间隙值,2与间隙终点素数 P 之比, p 之比 n/p ,后者则为 $g(p_n) / \lg p_n$:其中 $g(p_n) = p_n - 1 - p_n - a_n$, p_n 和 p_{n+1} 分别指第 n 个及第 $n+1$ 个素数, $\lg p_n$ 为在 p_n 附近的素数之间的平均间隙(理论近似值)。

2.孪生素数族统计数据的使用 孪生素数族的定义是:如果 n 与 $n+1$ 或者 $n+2$ 同为素数,则称 n 及 $n+1$ 或者 $n+2$ 为孪生素数;如果在—组孪生素数之间只存在合数,不存在非孪生素数,称该组孪生素数为孪生素数族。

由于孪生素数族内两对孪生素数之间所跨越的合数数量并不一定相同,因此在孪生素数族中,两对孪生素数之间的距离(所跨越的合数个数)可能很大。

3.统计表的分段数据衔接 为了既保证对原始数据进行统计分析的数据连续性,又适当保证其反映原始数据中蕴含的参数分布特性,本手册采用分段分析统计加衔接区段补充统计的方法对原始数据进行“切块”式分析。

本手册统计表关于素数和孪生素数统计属于无缝衔接(不存在区间内未统计的素数和孪生素数),所以素数和孪生素数的统计数据可以无条件使用。

虽然孪生素数族统计和素数间隙统计不属于无缝衔接(孪生素数族和连续的素数间隙可能跨越不同的切块区间),但是经过理论分析与实际校验,本手册采用的切块方法未实质性损害孪生素数族统计和素数间隙统计数据的科学性——跨越区段的衔接统计数据中没有超过其前后区间最大值的统计参数(即使跨区段连续统计,这些参数也具有不显性),所以素数族统计和素数间隙统计数据在本手册的数据定义下可以安全使用。

为了方便需要详细了解衔接区段数据的读者,本手册专门提供了孪生素数族和素数间隙统计表的区段衔接数据表,需要的读者可直接查阅相关“衔接数据表”。

<<素数研究与应用参考手册>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>