

素数判别法的改进

谭中华

(广东工业大学 应用数学系, 广东 广州 510090)

摘要:在筛法和费尔马小定理的基础上,利用素阶乘及判别数对如何判别一个整数是否是一个素数的算法加以改进.

关键词:素阶乘;同余式;判别数

中图分类号:O156.1

文献标识码:A

文章编号:1007-7162(2002)04-0090-02

1 问题的提出

早在古希腊,著名数学家欧几里德(Euclid 约公元前三世纪)就证明素数有无穷多个,可遗憾的是,至今没有一种简便方法给出素数的一种简便表示.在公元前300年左右爱拉托斯尼(Eratosthenes')给出一种造素数表的方法,人们称为爱拉托斯尼筛法.本文中笔者用 m, n 表示整数, $P_1, P_2, \dots, P_k$ 表示素数, (m, n) 表示求 m, n 的最大公约数.则筛法表示为: n 是一个整数,先求出不大于 $\sqrt{n}$ 的全部素数, $P_1, P_2, \dots, P_k$ 若对任意的 $P_i (i \in \{1, 2, \dots, k\})$ 都有 P_i 不整除 n ,则 n 是素数.本文在筛法和费尔马小定理的基础上加以改进.

2 主要结果

定义 $\overline{P}_k! = P_1 P_2 \cdots P_k$ 为 P_k 的素阶乘.

定理1 设 n 是整数, $P_1, P_2, \dots, P_k$ 是不大于 $\sqrt{n}$ 的全部素数,则 n 是素数的充分必要条件是 $(\overline{P}_k!, n) = 1$.

证明:充分性显然成立.

只须证明必要性成立即可,若 $(\overline{P}_k!, n) = 1$,则有 $(P_i, n) = 1$ 对任意 $i \in \{1, 2, \dots, k\}$ 都成立.由筛法知, n 是素数.

计算 $\overline{P}_k!$ 计算量较大,可利用同余式加以改进.

定理2 若 $\overline{P}_k! \equiv r \pmod{n} (0 \leq r < n)$,则 n 是素数的充分必要条件是 $(r, n) = 1$.

证明:已知 $\overline{P}_k! \equiv r \pmod{n} (0 \leq r < n)$,设 $\overline{P}_k! = nq + r (q \text{ 是整数})$,

若 n 是素数,由定理1知,则 $(nq + r, n) = 1$,故 $(r, n) = 1$ 成立.

若 $(r, n) = 1$,由定理1很容易证明必要性成立.

本文中笔者称 r 为 n 的判数.

法国数学家费尔马(Fermat)在1640年提出一个这样的问题,若 p 是素数,且 p 不整除 a ,则 $a^{p-1} \equiv 1 \pmod{p}$,人们称之费尔马小定理^[1].在此基础上有:

收稿日期:2002-03-12

作者简介:谭中华(1970-),男,助教,主要研究方向为图论.

定理 3 n 是素数的充分必要条件是 $r^{n-1} \equiv 1 \pmod{n}$ ($n > 4$).

证明:若 n 是素数,由定理 2 知, $(r, n) = 1$, 则 n 不整除 r , 由费尔马小定理可知 $r^{n-1} \equiv 1 \pmod{n}$ 成立

若 $r^{n-1} \equiv 1 \pmod{n}$, 可以设 $r^{n-1} = nq' + 1$, 又 $r = \overline{P_k!} - nq$ (q, q' 是整数), 则有 $(\overline{P_k!} - nq)^{n-1} = nq' + 1$. 故 $(\overline{P_k!})^{n-1} \equiv 1 \pmod{n}$, 则易证 P_i 不整除 n ($i \in \{1, 2, \dots, k\}$), 由筛法知 n 是素数.

笔者用此算法同筛法比较, n 比较大时, 计算机确实能节省大量时间.

参考文献:

[1] 戎土奎. 十章数论[M]. 贵阳: 贵州教育出版社, 1994. 12-75.

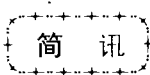
Improvement on the Algorithm of Distinguishing Prime Number

TAN Zhong-hua

(Dept. of Applied Mathematics, GDUT, Guangzhou 510090, China)

Abstract: The algorithm of distinguishing prime number is improved on the basis of Eratosthenes' sieve method and Fermat's minor theorem.

Key words: prime factorial; congruence expression; distinguished number



广东工业大学档案工作上新台阶

2002年9月19日, 广东省档案局组织专家评审组, 对我校档案管理工作进行了评审, 一致同意我校综合档案室为国家二级科技事业档案管理单位, 标志着我校的档案工作上到一个新的台阶.

自1995年合校以来, 校综合档案室积极贯彻落实档案法及其实施办法, 探索合并高校档案管理的办法, 制定了一系列管理制度, 确保了档案的形成、积累、归档工作纳入全校制度化、规范化管理轨道.

通过这次档案升级达标工作, 全校各部门受到了一次深刻的档案法制、档案知识教育, 档案意识明显提高, 主动归档、用档的现象增加, 在征集档案的工作中, 还出现主动将个人珍藏的照片档案上交学校的感人事迹.

在这次活动中, 有15位领导干部、28位专兼职档案员获得为本单位达到科技事业单位“国家二级”档案管理标准做出突出贡献人员荣誉证书.

(校办综合档案室 文燕)