中国剩余定理的两种算法分析

白 宇

(山西大同大学数学与计算机科学学院, 山西大同 037008)

摘 要: 分别采用穷举算法和中国剩余定理(孙子定理)的数学分析算法进行计算机编程求解, 对传统余数问题, 即对‘已知一个正整数被不同的几个正整数除后的余数, 求该数’的问题进行了分析, 并比较了两种算法的特点.

关键词: 中国剩余定理 孙子定理 穷举算法 数学分析算法

中图分类号: O112; TP312 文献标识码: A 文章编号:1674-0874(2008)04-0013-03

谭浩强《Pascal 语言程序设计》(第 2 版)第六章的习题 13 是一个算法类问题, 但书中只给出了结论, 并没有对定理进行详细的分析. 本文用现代数学方法对该问题进行分析, 从而比较使用穷举算法求解和使用数学方法求解的计算机程序的差异.

该问题的内容为:一个正整数分别被 3, 5, 7 除, 余数分别得 k, m, n, 问该数是多少?[1]《孙子算经》中给出的口诀是“三人同行七十稀, 五树梅花二十一, 七子团圆正月半, 除百零五便得知”. 用代数式子表达它的含义为:

$$x = 70k + 21m + 15n - 105R,$$

即对除以 3 的余数(k)乘以 70, 对除以 5 余数(m)乘以 21, 对除以 7 的余数(n)乘以 15, 然后减去一个或多个 105, 如果是求合乎规格的最小的正整数, 则可以直接除以 105, 得到的余数便是[2]. 这实际上是孙子定理的一个特定例子. 孙子定理是数论中最重要的基本定理之一, 实质上刻画了剩余系的结构. 把所求的解表示为一个线性组合, 线性组合中的每一项都满足其中的一个性质, 适当组合起来就是满足要求的解. 这已经不在本文讨论范畴之内, 故不作赘述.

1 穷举算法

对于该问题, 穷举算法可以从最小的正整数 1 开始进行尝试, 逐次增一, 直到找到符合规则的正整数, 显然该数一定是最小的符合规则的正整数. 该算法可以进行一定程度的优化, 即进行一定的约束, 但本文旨在分析两种算法的特点, 故而采用了标准的穷举算法, 不增加任何约束条件.

```
const
    DRTotal = 3;
type
    DRList = array[1..DRTotal] of integer;
function ChinaResEnum (Divisor,  Residue: DRList): int64;
var
    Dividend: int64;
    i: integer;
    FoundFlag: boolean;
begin
    FoundFlag := False;
    Dividend := 0;
    repeat
      Inc(Dividend);
      i := 1;
      while i <= DRTotal do
        if Dividend mod Divisor[i] = Residue[i]
then
          Inc(i)
        else
       break;
     if i = DRTotal + 1 then
```

收稿日期: 2008-01-15

作者简介: 白宇(1976-), 男, 山西大同人, 硕士, 助教, 研究方向: 计算机算法设计与优化.

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

```
    FoundFlag := True;
  until FoundFlag;
  Result := Dividend;
end;
```

该算法将除数和余数的个数定义为常量 DRTotal, 将除数和余数分别放在数组 Divisor 和 Residue 中, 返回符合规则的最小正整数. 程序从 1 开始进行尝试, 只要不能满足任何一条规则, 程序将对下一个数, 即 2 进行尝试, 直到找到为止. 算法 1 的时间复杂度为 $O(n)$[3].

2 数学算法

事实上运用孙子定理解决 3 个数问题的一般形式为: 已知 M_1, M_2, M_3 是两两互质的正整数, 求最小正整数 x, 使它被 M_1, M_2, M_3 除所得余数分别为 C_1, C_2, C_3.

孙子定理的思想便是先分别找出被其中数 M_i 除余 1 而可以被另外二个数整除的数 $W_i(i=1, 2, 3)$, 则所求的数之一便是

$$C_1W_1+C_2W_2+C_3W_3.$$

若欲求的是最小的符合要求的数, 则将上面的得数减去 $M_1\cdot M_2\cdot M_3$ 的整数倍即可. 在《孙子算经》给出的解法中,

$M_1=3$, $M_2=5$, $M_3=7$;

$C_1=2$, $C_2=3$, $C_3=4$;

$W_1=70$, $W_2=21$, $W_3=15$.

其中

$W_1=70=3\times23+1=5\times7\times2$;

$W_2=21=5\times4+1=3\times7\times1$;

$W_3=15=7\times2+1=3\times5\times1$;

而

$C_1W_1+C_2W_2+C_3W_3=$

$2\times70+3\times21+4\times15=263.$

因为

$263-R(3\times5\times7)=263-R\cdot105$

$(R=1, 2, 3, \cdots, n)$

故

$x_1=263-1\times105=158,$

$x_2=263-2\times105=53.$

当 $R\geq3$ 时, x 成为负数, 无意义, 故所求数是 158 或 53.

孙子定理可以推广到对任意 n 个数 M_i 的情形, $n\geq2$, $n\in N$. 孙子定理中较难的部分是求 W_i, 它是在除去 M_i 外的 n-1 个除数的最小公倍数的基础上, 再乘以适当的正整数 a_i 而得到的, 上例中加下划线的数字便是 a_i, 该数字需要试算, 以保证 W_i 被 M_i 除后余 1.下面举例说明.

例 1. 若数 A, 它被 7 除余 1, 8 除余 1, 9 除余 3, 求满足条件的最小正整数 A.

解: 这里 $M_1=7$, $M_2=8$, $M_3=9$;$C_1=1$, $C_2=1$, $C_3=3$. 因为 $8\times9\div7$ 余 2, 所以经过试算可以得到 $a_1=4$, 则

$W_1=8\times9\times\underline{4}=288;$

又由 $7\times9\div8$ 余 7, 故 $a_2=7$, 则

$W_2=7\times9\times\underline{7}=441;$

同理, $7\times8\div9$ 余 2, 故 $a_3=5$, 则

$W_3=7\times8\times\underline{5}=280;$

这里 $W_i(i=1, 2, 3)$是分别被 M_i 除余 1, 而可以被另外两个数整除的数. 因为

$C_1W_1+C_2W_2+C_3W_3=$

$1\times288+1\times441+3\times280=1569.$

而 $1569\div(7\times8\times9)$余数为 57, 故符合条件的最小正整数 A=57.

例 2. 求 3 除余 1, 5 除余 3, 7 除余 1, 8 除余 3 的最小正整数.

解: 这里 $M_1=3$, $M_2=5$, $M_3=7$, $M_4=8$;$C_1=1$, $C_2=3$, $C_3=1$, $C_4=3$. 因 $5\times7\times8\div3$ 余 1, 故 $a_1=1$, 则

$W_1=5\times7\times8\times\underline{1}=280;$

又由 $3\times7\times8\div5$ 余 3, 故可试算 $a_2=2$, 则

$W_2=3\times7\times8\times\underline{2}=336;$

同理, $3\times5\times8\div7$ 余 1, 故 $a_3=1$, 则

$W_3=3\times5\times8\times\underline{1}=120;$

又同理, $3\times5\times7\div8$ 余 1, 故 $a_4=1$, 则

$W_4=3\times5\times7\times\underline{1}=105;$

这里 $W_i(i=1, 2, 3, 4)$是分别被 M_i 除余 1, 而可以被另外 3 个数整除的数. 因为

$C_1W_1+C_2W_2+C_3W_3+C_4W_4=$

$1\times280+3\times336+1\times120+3\times105=1723$

而 $1723\div(3\times5\times7\times8)$余数为 43, 故所求的最小正整数为 43.

《孙子算经》中, 称这里的

M_i $(i=1, 2, 3, \cdots, n)$为定母;

M_i $(i=1, 2, 3, \cdots, n)$的最小公倍 $M_1\cdot M_2\cdot M_3\cdots M_n$ 为衍母;

W_i $(i=1, 2, 3, ..., n)$为用数;

a_i $(i=1, 2, 3, ..., n)$为乘数;

C_i $(i=1, 2, 3, ..., n)$为剩数;

C_iW_i $(i=1, 2, 3, ..., n)$为各总;

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

$\sum_{i=1}^{n} C_i W_i$ 为所求率;

$\sum_{i=1}^{n} C_i W_i \bmod \prod_{i=1}^{n} M_i$

便是最后求得的最小自然数, 称为所求总, 即所求率被衍母除后的余数.

其中, 用数 $W_i = a_i \cdot \prod_{\substack{k=1 \\ k \neq i}}^{n} M_k$, 并称 $\prod_{\substack{k=1 \\ k \neq i}}^{n} M_k$ 为衍数 W_i', 因而 $W_i = a_i W_i'$.

《Pascal 语言程序设计》(第 2 版)第六章习题 13 运用以上公式得到的结果如下:

定母为 3, 5, 7,
衍母为 3×5×7=105,
衍数为 35, 21, 15,
乘数为 2, 1, 1,
用数为 70, 21, 15,
剩数为 2, 3, 4,
各总为 140, 63, 60,
所求率为 140+63+60=263,
所求总为 263 mod 105=53.

通过以上数学分析, 可以设计如下算法.

```
const
    DRTotal = 3;
type
    DRList = array[1..DRTotal] of integer;
function ChinaResMath (Divisor, Residue: DRList): int64;
var
    W: DRList;
    i, j: integer;
    Temp, Product: int64;
begin
    for i := 1 to DRTotal do
    begin
      W[i] := 1;
      for j := 1 to DRTotal do
        if j <> i then
          W[i] := W[i] * Divisor[j];
      Temp := W[i];
      while W[i] mod Divisor[i] <> 1 do
       W[i] := W[i] + Temp;
end;
    Temp := 0;
    for i := 1 to DRTotal do
    begin
      Temp :=  Temp + W[i] * Residue[i];
    end;
    Product := 1;
    for i := 1 to DRTotal do
      Product := Product * Divisor[i];
    Result := Temp mod Product;
end;
```

该算法的时间复杂度为 O (1), 即常量阶, 因为其主要运算均消耗在求解 W_i 上, 而与求解 W_i 相关的除数和余数的个数是很少的, 即内层循环次数很少, 并不耗时[4].

3　结语

穷举算法的时间复杂度明显高于数学算法的时间复杂度, 但穷举算法直观、易于理解, 在问题规模不是很大的情况下使用穷举算法并不会比数学算法耗费更多的时间. 例如以上例题中, 只有 3 到 4 个除数及余数, 并且除数及余数的范围很小, 所以数学算法并不省时. 若将上例中的 3 个除数和余数, 即 M_1, M_2, M_3 和 C_1, C_2, C_3 改为类似 101, 203, 1577 和 97, 134, 15 这样的大范围数字时, 计算结果为 11, 105, 249, 穷举算法需要尝试 11, 105, 249 次, 并且每次尝试可能包含多次运算, 因而数学算法所耗费的时间明显少于穷举算法.

参考文献

[1]谭浩强, 田淑清. Pascal 语言程序设计[M]. 第 2 版. 北京: 高等教育出版社, 1999.
[2]郭书春, 刘钝. 算经十书·卷一 [M]. 辽宁: 沈阳辽宁教育出版社, 1998.
[3]严蔚敏, 吴伟民. 数据结构[M]. 第 2 版. 北京: 清华大学出版社, 1996.
[4]王晓东. 计算机算法设计与分析[M]. 北京: 电子工业出版社, 2001.

(下转第 22 页)

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

[13]Gamaly E G, Rode A V, Davies B L. Ultrafast ablation with high-pulse-rate lasers. Part II: Experiments on laser deposition of amorphous carbon films[J]. J Appl Phys, 1999, 85: 4222-4230.

An Overview of the Pulsed Laser Depsition Technology

WANG Ping, XIE Ting-yue, LI Hai
(School of Physics and Electronic Science, Shanxi Datong University, Datong Shanxi, 037009)

Abstract: Thin film technology is a powerful method to realize the material integration and device fabrication. In this paper, we mainly introduce the basic principle, characters, merits and demerits of the pulsed laser deposition (PLD) technique. The PLD technology is most suitable for the thin film growth of the transition metal oxides with multi-component and complex chemical structure.

Key words: pulsed laser deposition; thin film technology

(上接第 7 页)

On Bernoulli Equation with Periodic Coefficients and Its "Best" Discrete Model

YUAN Hu-ting [1], WANG Quan[2], ZHANG Guang[3]
(1. School of Mathematics and Computer science, Shanxi Datong University, Datong Shanxi, 037009;
2. School of Ccontinuing Education, Shanxi Datong University, Datong Shanxi, 037009)
3 School of Science, Tianjin University of Commerce, Tianjin, 300134)

Abstract: The existence, the uniqueness, and the global asymptotically stable of the Bernoulli equation with periodic coefficients will be considered in this note. The obtained result clearly holds for the Logistic equation because it is the sepcial case of the Bernoulli equation. At the same time, a "best" Bernoulli discrete model is considered and the dynamics behavior of the corresponding diffierential equation will be inherited.

Key words: bernoulli equation; Logistic equation; periodic solution; stability; discrete model

(上接第 15 页)

Two Algorithm Analysis for Chinese Remainder Theorem

BAI Yu
(School of Mathematics and Computer Science, Shanxi Datong University, Datong Shanxi, 037008)

Abstract: This paper first introduces traditional question of remainder: "known remainder of a positive integer to be different positive integer divide, seeking this positive integer", then compares and analyzes exhaustive algorithm and the Chinese remainder theorem (Sunzi theorem) with mathematical analysis algorithm, and with computer programming.

Key words: Chinese remainder theorem; Sunzi theorem; exhaustive algorithm; mathematical analysis algorithms

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net