

判定一般素数的新方法

张 遐

蔡松岳

(无锡轻工业学院基础课部)

(无锡市淡水渔业研究中心)

迄今为止,除特殊形式的素数外,判定某数是否为素数的方法仍以筛法为基础。例如要对数 W 进行判断,就得用不大于 $\sqrt{W}$ 的全部素数去一一试除。随着 W 的增大,这个作为除数的素数列也愈来愈庞大,而且新加进的素数本身还需要事先判定为素数,它们的出现也无章可循。本文提供一种新方法,只用八个素数,经若干次试算就能判定任意数是素数还是合数。

在讨论过程中,我们用到下列诸集合:

$$I = \{\text{自然数(包括0)}\}$$

$$J = \{x | x = 1, 2n, 3n, 5n, n \in I\}$$

$$K = I - J$$

$$P = \{1, 7, 11, 13, 17, 19, 23, 29\}$$

实际上集合 K 是在集合 I 中用筛法删去以2、3、5为因子的数及删去0、1而得到, P 则是选取模 $m=30$ 而得到的“简化剩余系”^[1]。

引理1 对于任意数 $C \in K$,恒可以表示成下列形式:

$$C = 30n + a$$

其中 $n \in I$, $a \in P$, 且 $a=1$ 时 $n \neq 0$ 。

证 略

设 $W \in K$, 若

$$W = UV$$

其中 $U, V \in K$, 则按引理1有

$$W = (30x + a)(30y + b) \quad (1)$$

其中 $x, y \in I$, $a, b \in P$ 。

将(1)式展开得

$$W = 30(30xy + ay + bx) + ab \quad (2)$$

由于 $a, b \in P$, ab 之值只有36种可能。又因 $ab \in K$, 按引理1有

$$ab = 30S + T \quad (3)$$

其中 $S \in I$, $T \in P$ 。因 ab 最大为841, 故 $0 \leq S \leq 28$ 。

当 $T=1$ 时, ab 有六种组合, 其对应的 S 如下表:

ab	1×1	7×13	11×11	19×19	17×23	29×29
S	0	3	4	12	13	28

当 $T=7$ 时, ab 有四种组合, 其对应的 S 如下表:

ab	1×7	11×17	13×19	23×29
S	0	6	8	22

其余 $T=11, 13, 17, 23, 29$ 时各有四种组合, $T=19$ 时有六种组合, 对应 S 值的表从略。

由(2)式得

$$\begin{aligned}\frac{W}{30} &= 30xy + ay + bx + \frac{ab}{30} \\ &= 30xy + ay + bx + \frac{30S + T}{30} \\ &= 30xy + ay + bx + S + \frac{T}{30}\end{aligned}$$

其中整数部分可由下式确定:

$$\frac{W}{30} = Q + \frac{T}{30} \quad (4)$$

Q, T 很容易计算而且是唯一的, 故

$$30xy + ay + bx = Q - S \quad (5)$$

定理 设 $W \in K$, 则 W 是合数的充要条件为:

- ① 对于符合(3)式的 a, b, S 的某个组合, (5)式有正整数解;
- ② $a=1$ 时 $x \neq 0$, $b=1$ 时 $y \neq 0$ 。

证

[必要性] 设 W 是合数, 因而能写成(1)式的形式, 根据前面的论述, (5)式成立。又因 $(30x+a) \in K$, $30x+a \neq 1$, 故在 $a=1$ 时 $x \neq 0$; 同理 $b=1$ 时 $y \neq 0$ 。

[充分性] 设条件①②成立, 因 Q, T 是唯一的, 满足(5)式的 a, b, x, y 必然满足(2)式, 于是(1)式成立, 证实了 W 是合数。

当求得 a, b, x, y 后, 实际上已将 W 分解成两个因数之积, 所以本定理提供了分解合数的途径, 其计算步骤如下:

- ① 将给定的 $W (\in K)$ 按(4)式求出商数 Q 与余数 T ;
- ② 根据 T 值查 ab 与 S 的对照表, 找出 a, b 与 s 的各种组合;
- ③ 将每种组合代入(5)式去求符合条件的 x, y 。

步骤③较复杂, 可对 a, b, S 的每种组合让 x 顺序取 $0, 1, 2, \dots$, 让 y 顺序取 $0, 1, 2, \dots$, 轮流计算 $30xy + ay + bx$ 的值, 直到它等于 $Q - S$ 。我们根据 a, b, S 的 36 种组合编成 36 张表 (见附录一), 这种表很容易利用电子计算机算出。若 W 不大, 易从对应于 T, S 的数在表中检索到所需要的 x, y 值。又由于 x, y 都有上界:

$$W = 900xy + 30ay + 30bx + ab > 900xy$$

$$xy < W/900$$

所以计算的次数是有限的。为了进一步减少计算次数, 需要下面的引理。

引理2 设 R 为任意正实数, 则满足 $xy < R$ 的任意正整数对中, 如不考虑顺序, 取 $y < \sqrt{R}$ 即可。

证 略

按此理, 前述 y 的上界可取 $\sqrt{W/900}$ 。

推论1 如不存在满足条件①、②的 a, b, x, y , 则 W 是素数。

这条推论直接可以从前述定理得出, 在逻辑上不需证明。但这个推论没有提供判定素数的途径, 为此作如下改进:

将(2)式改写成

$$W = 30^2 xy + 30ay + 30bx + ab$$

$$\frac{\frac{W - ab}{30} - ay}{30y + b} = x \quad (6)$$

推论2 设 $W \in K$, $a, b \in P$, $y \in \{0, 1, 2, \dots, [\sqrt{W/900}]\}$, 且 $b=1$ 时 $y \neq 0$, 若对于所有满足上述条件的 a, b, y , 由(6)式计算出的 x 值恒不为正整数, 则 W 是素数。

证

如对应于 a, b, y 的各种情况 x 不为正整数, 则定理中 a, b, x, y 有整数解的条件不能满足, 按推论1, W 是素数。

以推论2为数学模型编制的电子计算机程序比较简单, 但算法是穷举的, 有大量多余的试算。为了避免这一情况, 我们根据 ab 与 T 的关系, 将(6)式的有关形式分写成八条推论, 其中 $R = [\sqrt{W/900}]$ 。

推论2.1 设 $W \in K$ 且 $W \equiv 1 \pmod{30}$, 对于所有 $y \in \{0, 1, 2, \dots, R\}$ 计算下列八个式子 (第一个式子中 $y \neq 0$):

$$\frac{\frac{W-1}{30} - y}{30y+1}, \frac{\frac{W-91}{30} - 7y}{30y+13}, \frac{\frac{W-91}{30} - 13y}{30y+7}, \frac{\frac{W-121}{30} - 11y}{30y+11},$$

$$\frac{\frac{W-361}{30} - 19y}{30y+19}, \frac{\frac{W-391}{30} - 17y}{30y+23}, \frac{\frac{W-391}{30} - 23y}{30y+17}, \frac{\frac{W-841}{30} - 29y}{30y+29}。$$

如果这八个式子所有的值都不是正整数, 则 W 是素数。

这条推论的理由可以由(6)式及前述 ab 与 T, S 的关系罗列出来。

推论2.2 设 $W \in K$ 且 $W \equiv 7 \pmod{30}$, 对于所有 $y \in \{0, 1, 2, \dots, R\}$ 计算下列八个式子 (第一个式子中 $y \neq 0$):

$$\frac{\frac{W-7}{30} - 7y}{30y+1}, \frac{\frac{W-7}{30} - y}{30y+7}, \frac{\frac{W-187}{30} - 11y}{30y+17}, \frac{\frac{W-187}{30} - 17y}{30y+11},$$

$$\frac{\frac{W-247}{30} - 13y}{30y+19}, \frac{\frac{W-247}{30} - 19y}{30y+13}, \frac{\frac{W-667}{30} - 23y}{30y+29}, \frac{\frac{W-667}{30} - 29y}{30y+23},$$

如果这八个式子所有的值都不是正整数, 则 W 是素数。

推论 2.3 到 2.8 分别适用于 $T = 11, 13, 17, 19, 23, 29$ 六种情形, 各有八个式子, 不一一列举。

我们以这八条推论作为数学模型编制的电子计算机程序(见附录二)运行顺利。下列一张表是一批 13 位数的判断结果, 表中各数的前面十位是 $1'000'000'000$, 记号(P)表明该数是素数, 记号/表示前面的数是合数, 后面的数是自动析出的一个因数。

1000'000'000'001/73

'003/61	'007/34519	'009/29	'013/7	'019/1601
'039(P)	'043/11	'049/6337	'051/13	'057/2341
'073/37	'079/23	'081/3929	'087/11	'091(P)
'109/11	'111/7	'117/15079	'121(P)	'123/17
'141/239	'147/37	'151/31	'153/7	'157/17
'177(P)	'181/7	'183/19	'187/41	'189(P)
'211(P)	'213/31	'217/23	'219/11	'223/7
'243/167317	'247/61	'249/53	'253/811	'259/17
'277/189997	'279/7	'283/42979	'289/50273	'291/1279
'309/23	'313/67	'319/1723	'32/7	'327/17
'343/10007	'349/7	'351/11	'357/29	'361/17
'379/173	'381/1151	'387/79	'391/7	'393/59393
'411/19	'417/11	'421/57059	'423/353	'427/30853
'447/7	'451/149	'453/37579	'457/88867	'459(P)
'481/1327	'483/11	'487/19	'489/7	'493/23
'021/11	'027/31	'033/23	'037/59	
'061(P)	'063(P)	'067/29	'069/19	
'093/166063	'097/7	'099/113	'103/13	
'127/265841	'129/13	'133/141359	'139/7	
'159/83	'163(P)	'169(P)	'171/23	
'193(P)	'199/12923	'201/101	'207/13	
'229/79	'231/1181	'237/7	'241/11	
'261/109	'267/823	'271(P)	'273/59	
'297/19	'301/103	'303(P)	'307/11	
'331(P)	'333(P)	'337/13	'339(P)	
'363/13	'367/479	'369/37	'373/11	
'397/787	'399/31	'403/101	'409/43	
'429/17	'433/17	'439/11	'441/13	
'463/17	'469/869179	'471(P)	'477/385223	
'499/199039				

结 束 语

(1) 本文提供的方法理论上是完整的, 取 $m = 30$ 是考虑了实践上的便利。事实上取 $m = 6$ 或 $m = 210$ 等都可以形成相应的体系。

(附录一)

	X	9	10	11	12	13	14	15	16	17
Y	0	63	70	77	84	91	98	105	112	119
	1	346	383	420	457	494	531	568	605	642
	2	629	696	763	830	897	964	1031	1098	1165
	3	912	1009	1106	1203	1300	1397	1494	1591	1688
	4	1195	1322	1449	1576	1703	1830	1957	2084	2211
	5	1478	1635	1792	1949	2106	2263	2420	2577	2734
	6	1761	1948	2135	2322	2509	2696	2883	3070	3257
	7	2044	2261	2478	2695	2912	3129	3346	3563	3780
	8	2327	2574	2821	3068	3315	3562	3809	4056	4303
	9	2610	2887	3164	3441	3718	3995	4272	4549	4826
	10	2893	3200	3507	3814	4121	4428	4735	5042	5349
	11	3176	3513	3850	4187	4524	4861	5198	5535	5872
	12	3459	3826	4193	4560	4927	5294	5661	6028	6395

附录二 程序清单

运行本程序前先建立一个名为 PRIME.DAT 的数据文件,其中包括下列 192 个数:

1	19	91	121	361	391	391	841	7	7	187	187
13	13	133	133	253	253	493	493	17	17	77	77
23	23	143	143	203	203	323	323	29	29	119	119
7	1	11	17	13	19	23	29	11	1	7	23
17	1	7	11	13	29	19	23	19	1	7	13
29	1	7	17	11	19	13	23	1	13	7	11
1	11	23	7	17	13	29	19	1	13	19	7
1	19	7	13	17	29	11	23	1	23	13	11
247	247	667	667	11	11	161	161	221	221	551	551
377	377	437	437	19	19	49	169	289	319	319	529
209	209	299	299	1	7	13	11	19	17	13	29
13	17	19	29	13	1	7	19	11	23	17	29
17	11	29	23	23	1	11	13	7	29	17	19
19	23	17	29	1	7	17	11	19	13	29	23
23	11	29	17	1	17	11	7	29	13	23	19
29	7	19	17	1	29	17	7	19	11	23	13

本程序只检索素数,不对合数分解。

PROGRAM PRIMES

```

var g,i,j,k,q,r,s,w,x,y: integer[35];
    l,z: integer;
    f,a,b: array [1...64] of integer;
    d: file of integer;
    log: boolean;
    procedure sub (m, n: integer);
    begin
        y: = 0;
        repeat
            l: = m;
            repeat
                if (y = 0) and (b[l] = 1) then
                    l: = l + 1;
                q: = w - f[l] - 30 * a[l] * y;
                r: = 900 * y + 30 * b[l];
                x: = q div r;
                if q = r * x then
                    log: = true
                else
                    log: = false;
                l: = l + 1;
            until (l = n + 1) or log;
            y: = y + 1;
        until (y = k + 1) or log;
        if log = false then
            begin
                write(W, ' ');
                z: = z + 1;
            end;
        end;
    end;
begin
    reset (d, 'prime data');
    for l: = 1 to 64 do
        begin
            f[l]: = d^l;
            get(d);
        end;
    for l: = 1 to 64 do

```

```

begin
    a[ 1 ]: = d^;
    get(d);
end;
for l: = 1 to 64 do
begin
    b[ l ]: = d^;
    get(d);
end;
close(d);
z: = 0;
write('    r1(>30) = ');
read(w);
write('    r2 = ');
read(g);
repeat
    k: = 0;
begin
    log: = false;
    y: = w div 2;
    if w = 2 * y then
        log: = true;
    y: = w div 3;
    if w = 3 * y then
        log: = true;
    y: = w div 5;
    if w = 5 * y then
        log: = true;
    if log = false then
begin
        if w >= 900 then
begin
            repeat
                i: = k * k * 900;
                j: = (k + 1) * (k + 1) * 900;
                log: = (i <= w) and (w < j);
                if log = false then
                    k: = k + 1;
            until log;
        end;
    end;
end;

```

```
        end;  
         $q_i = w \text{ div } 30$ ;  
         $s_i = w - 30 \times q_i$ ;  
        if  $s = 1$  then sub(1,8);  
        if  $s = 7$  then sub(9,16);  
        if  $s = 11$  then sub(17,24);  
        if  $s = 13$  then sub(25,32);  
        if  $s = 17$  then sub(33,40);  
        if  $s = 19$  then sub(41,48);  
        if  $s = 23$  then sub(49,56);  
        if  $s = 29$  then sub(57,64);  
    end;  
     $w_i = w + 1$ ;  
end;  
until  $w = g + 1$ ;  
writel('    TOTAL = ', z);  
END.
```

87029

判定一般素数的新方法《无锡轻工业学院学报》1987年,第6卷,

第3期

主题词 素数;合数;计算机

摘要 本文提供了一种判定任意数是素数还是合数的新方法,以该方法为数字模型编制的程序可以对单个自然数作出判断,也可以在一个区间内定出全部素数与合数,程序中断后重新启动也不必重复已做过的工作,这些方面都比筛法好。对该方法进行理论证明,程序运行后取得了很好的成绩。

作者:张遐 蔡松岳

87030

整数和集的渐近密度《无锡轻工业学院学报》1987年,第6卷,第

3期

主题词 渐近的;密度;正整数;集合;基底

摘要 设 A 和 B 都是自然数的集合, C 是它们的和。 A 的渐近密度为 α 。假定 B 是自然数的一个渐近基底, λ 是 B 的渐近平均阶数。 $C = A + B$ 的渐近密度为 γ , 得到了用 α 和 λ 估计 γ 的几个定理。

作者: 孙子常

87031

试论俄语科技语体词汇的特点《无锡轻工业学院学报》1987年,第

6卷,第3期

主题词 俄语;科技;语体;词汇

摘要 根据俄语科技词汇的特点,结合理工院校公共俄语的教学经验,以较丰富的词汇论述了科技词汇的特点,本文对理工院校的学生和科技人员在学习俄语时有较大的实用价值。

作者: 黄洽民

87031

ON SOME CHARACTERISTICS OF RUSSIAN LANGUAGE, ITS
STYLISTIC VOCABULARY OF SCIENCE AND TECHNOLOGY «Journal
of the Wuxi Institute of Light Industry»Vol.6, No.3, 1987
SUBJECTWORDS Russian, Science and technology, Writing style,
Vocabulary

ABSTRACT Based on some stylistic russian vocabularies of science and
technology, and the writer's own experience in teaching. The present arti-
cle takes rich vocabulary to deal with some characteristics of the stylistic
vocabularies of science and technology, so it has certain value in applica-
tion for students and personnel of science and engineering in their reading,
translating, and memorizing new words.

Author: Huang Qiamin

87029

A NEW METHOD for CHACKING a PRIME «Journal of the Wuxi
Institute of Light Industry»Vol.6, No.3, 1987
SUBJECTWORDS Prime, Composite number, Computer

ABSTRACT Until now, sieve of eratosthenes' is still the only method for
deciding a natural number to be a prime. Unfortunately, the checking proce-
dure is too complicate for large numbers. This paper establishes a new me-
thod based on a theory discussed here shows that any natural number can
be decided to be a prime or composite depends only on a set of eight pri-
mitive primes, 1,7,11,13,17,19,23,29. In practice, a PASCAL program
based on the modal of this method shows that the new method is surely
better than the old sieve method.

Author: Zhang Xia Cai Songyue

87030

ON the ASYMPTOTIC DENSITY of SUM of SETS of POSITIVE INTE-
GERS «Journal of the Wuxi Institute of Light Industry»Vol.6, No.3, 1987
SUBJECTWORDS Asymptotic, Density, Basis, Positive integer, set
ABSTRACT Suppose that both A and B are sets of natural numbers, and
C is their sum. Let α denote the asymptotic density of A. Suppose that B
is an asymptotic basis of natural numbers, let λ denote an asymptotic ave-
rage order of B. let I be the asymptotic density of $C=A+B$. Thus several
theorems about estimating I by α and λ are obtained.

Author: Sun Zichang