任意大奇数的“素性”与“合性”判别及“合性奇数”因式分解

王述勋

（新疆生产建设兵团　835200）

A

任意大奇数的“素性”与“合性”判别

摘要：由一元二次方程式求根公式，推导出任意大奇数的“素性”与“合性”的判别式。

关键词：奇数、奇素数、奇合数

引　言：

在自然正整数Z—集合里,对于任意大的奇数m:($m \gg 1-m$),如何判别它是“奇素数”或“奇合数”，至今未有定型的数学表达式来判定。

作者：另辟蹊径，探求有别于现有的诸多种研讨方法。

构建“奇合数”的判别式

（一）基本概念：

1、奇数概念：在自然正整数 Z— 集合里，奇数设定为：m。

即 $m \gg 1-m$ （m不能被2整除）

2、奇合数概念：设定为两个不同等的奇数为p与q，p≠q

p与q可为奇合数或奇素数

将：$m = p \times q$，则m令名为“奇合数”

p与q是m两个不同奇因数的乘积。

3、奇合数的数学表达式：

将 m变形为 $[\sqrt{m}]^2 + n$,将奇合数m分拆为两个不相等的正整数：

$[\sqrt{m}]$ 是m平方根的最大整数部分，n是$[\sqrt{m}]$的余数部分。

设 $[\sqrt{m}] = a$， 得：$m = a^2 + n$ （例如：$123 = 11^2 + 2$）

由：$m = p \times q$

令：$p > a$，则 $p = a + x$ （引入未知量 x）

$q < a$，则 $q = a - y$ （引入未知量 y）

得：$m \Rightarrow p \times q = (a+x)(a-y) \cdots\cdots (A-1)$式

$(A-1)$式引入两个未知量x与y， 设定x≠y，使x与y和 $m \Rightarrow [\sqrt{m}] = a$

构建成未知量x、y，及已知量a的数学关联式：

$m \Rightarrow p \times q = (a+x)(a-y)$

$(A-1)$式，是“奇合数”（$m \gg 1-m$）的数学表达式。

（二）化简$(A-1)$式：$m = (a+x)(a-y)$

在$(A-1)$式中：

x与y的定义域为：

$1 < y < [\sqrt{m}] = a$

$1 < x < \left(\dfrac{m}{a-y} - a\right)$

$$m \Rightarrow p \times q \Rightarrow (a+x)(a-y) \Rightarrow a^2 + n \Rightarrow a^2 + a(x-y) - xy$$
$$\Rightarrow n = a(x-y) - xy$$

$\Rightarrow xy - a(x-y) - n = 0 \cdots\cdots (A-2)$式

（三）$(A-2)$式： $xy - a(x-y) - n = 0$ 在此式中：

设定：$x = y + g$，g为$x-y$的差，即：$x - y = g$

g是两个未知数x与y引入的“参数”

将 $x - y = g$，代入$(A-2)$式中：

得：$y^2 + g \times y - ag - n = 0$

用y的根公式，即一元二次方程的求根公式：

$$y = \frac{-g \pm \sqrt{g^2 + 2ag - n}}{2}$$

在上式中：a与x及y互为奇偶数，x及y同为奇偶数。

可将分母2约去

得：$y = -g \pm \sqrt{g^2 + 2ag - n} \cdots\cdots (A-3)$式

$(A-3)$式是 y 的求解方程式。

由 $m \Rightarrow p \times q \Rightarrow a^2 + n \Rightarrow (a+x)(a-y)$
$\Rightarrow y = -g \pm \sqrt{g^2 + 2ag - n}$

即：$m \gg 1-m$ ，m的求解方程式。

m是否有正整数解

得由根号内代数式“$g^2 + 2ag - n$” 判别：

“$g^2 + 2ag - n$”的数值是大於0的。

则y有两个不相等的实数根：

正整数、有理分数、无理数。

本文约定为“正整数”。

要使y有正整数解，代数式“$g^2 + 2ag - n$”的数值必须为完全平方数，

y才能有正整数解。

代数式 “$g^2 + 2ag - n$” $\cdots\cdots (A-4)$式

（四）引理（1）：

代数式$(A-4)$式 $g^2 + 2ag - n$

当且仅当 $g^2 + 2ag - n = K^2$ （引入未知量K^2）

$$m \gg 1 - m \Rightarrow m \Rightarrow a^2 + n$$

则 m 为奇合数。

证明：由$(A-1)$式 $\Rightarrow (A-2)$式 $\Rightarrow (A-3)$式 $\Rightarrow (A-4)$式

运用算术运算的运算法则、未知量及已知量的设定，推绎而获证。

（五）引理（2）：

代数式$(A-4)$式 “$g^2 + 2ag - n$”

当且仅当 $g^2 + 2ag - n \neq K^2$ 时

$$m \gg 1 - m \Rightarrow m \Rightarrow a^2 + n$$

则 m 为奇素数。

证明：在奇正数Z— 集合里，只有两个元素：“奇合数”和“奇素数”。根据数理逻辑的自然数公理，这两个元素无“后继”，非此即彼。即“奇合数”及“奇素数”二者必居其一，非“合”即“素”。

根据引理（1）证明得代数式：$g^2+2ag-n=K^2$ 为完全平方数时，使 a^2+n 有正整解值，只有一个唯一的解值 K^2。其它的解值是有理分数和无理数，有无穷多个解值。只能是非完全平方数解值。

即：$g^2+2ag-n\neq K^2$ 引理（2）得证。

B

“奇合数”与“奇素数”判别定理

定理：代数式 “$g^2+2ag-n$”

1、当：$g^2+2ag-n=K^2$ 时

则：$m\gg 1-m\Rightarrow m=a^2+n$ m 为“奇合数”。

2、当：$g^2+2ag-n\neq K^2$ 时，

则：$m\gg 1-m\Rightarrow m=a^2+n$，m 为“奇素数”。

证明：$(A-1)$式 $\Rightarrow(A-2)$式 $\Rightarrow(A-3)$式 $\Rightarrow(A-4)$式 $\Rightarrow$引理（1）$\Rightarrow$引理（2）$\Rightarrow$定理。

是将两个引理（1）和引理（2）合并而得证。

此定理是同一个代数式：

“$g^2+2ag-n$”

当：$g^2+2ag-n=K^2$ 时，

则：$m\gg 1-m\Rightarrow m\Rightarrow a^2+n$ m 为“奇合数”。

当：$g^2+2ag-n\neq K^2$ 时

则：$m\gg 1-m\Rightarrow m\Rightarrow a^2+n$，m 为“奇素数”。

根据（B）定理：

代数式 “$g^2+2ag-n$”

当：$g^2+2ag-n=K^2$ 时，

则：$m\gg 1-m\Rightarrow m=a^2+n$ m 为“奇合数”。

得：$g^2+2ag-n=K^2$ ……$(B-1)$式

$(B-1)$式 $g^2+2ag-n=K^2$

此式是一个具有特征数值的“二元二次不定方程式”

它是“m 为奇合数因式分解的求解方程”。

现今的解法有诸多种。

本文旨在求得将 “$m\gg 1-m$”，分解成两个不相等的奇数 p 与 q（p≠q）的乘积为目的，非算术式的因式分解。

在 $(B-1)$式 $g^2+2ag-n=K^2$ 中：

a，n 是工作目标任意选定的 m。

$m\Rightarrow(m\gg 1-m)=a^2+n$ 视为常量（已知量）

$a\Rightarrow(a\gg 1-a)$

a 的数值大小，确定工作目标 m 的长度。

设定 g 是 $(x-y)$ 的差。g 与 K 为未知量（自变量）。

由 a 的数值大小，确定 g 与 K的定义域。

a 是可数，即 g 与 K的定义域亦是可数的，用价数表示 m 的数位：

$m=10^n a$ 其中：a =1，2，3……9

n = 1，2，3……$n\gg 1-n$

$n\gg 1-n$，n 可以任意大，

则 $m=10^n a$ 亦为任意大。

当 n = 6 或 5 时：$g^2+2ag-n=K^2$ 用手工演算较为容易；

当 n = 7，8，9……16 时：$g^2+2ag-n=K^2$ 用手工演算较为困难；

当 n = 17，18…… $(n\gg 1-n)$ 时，$g^2+2ag-n=K^2$

非人工能演算，得用科学技术设备来完成。

人工演算的实例，选择 15 > n 的工作长度。

即在 15 位以内的奇数数值进行数学运算演绎。

C

如何求解$(B-1)$式：$g^2+2ag-n=K^2$

一、$(B-1)$式：$g^2+2ag-n=K^2$

此式为一个“二元二次不定方程式”

其元为“g 与 K”。

根据此式的“数式”特征，是一个“完全平方数式方程式”。

K^2 被 16 整除的余数为：0，1，4，9。

以 16 为模，“mod 16” 构建同余式方程：

$g^2+2ag-n\equiv K^2$ （mod 16）

g 被 16 整除的余数设为g_0 $g_0=1，2，3\cdots\cdots16$。 有 16 个g_0

$2a$被 16 整除的余数设为$2a_0$ $2a_0=2，4，6\cdots\cdots32$。 有 16 个$2a_0$

n 被 16 整除的余数设为n_0 $n_0=0，1，2\cdots\cdots16$。 有 17 个n_0

将 16 个g_0，16 个$2a_0$，17 个n_0，进行三、三组合：

$16\times16\times17=4352$ 个K_0 数值。

在 4352 个K_0 数值中，只有 171 个K_0 数值能匹配成型如

$g_0^2+2a_0g_0-n_0=K_0{}^2$的“初始值完全平方数式方程式”。

其演算过程太冗长，只留成了 171 个“初始值完全平方数式方程式”的数值表，附录於文后，其余的舍去。

二、如何应用“初始值完全平方数式方程式”数值表进行“任意大奇合数

$(m\gg 1-m)$ 的因式分解。

1、任意大奇合数选择在 15 位数左右的奇合数 m

实例设 m =631697288726223

将：631697288726223 分折为a^2+n ：

$m\Rightarrow a^2+n\Rightarrow 25133588^2+42972479$

即：$a=25133588$，$n=42972479$

求得：$2a_0\Rightarrow 2\times25133588\Rightarrow\frac{2\times25133588}{16}\Rightarrow 8\Rightarrow 2a_0$

即：$2a_0=8$，是2×25133588 被 16 整除的余数。

$n_0\Rightarrow\frac{42972479}{16}\Rightarrow 15\Rightarrow n_0$ 是 42972479 被 16 整除的余数。

2、在初始值完全平方数式方程式 数值列表

横序① + ② × ③ – ④ = ⑤ = ⑥中

查寻③$(2a_0)$ – ④(n_0)

同列序号中，如果并列的 ① + ② ⑤ = ⑥ 存在，

则 m 是合数（如果不存在，则m为非合数）。

3、此实例：$2a_0=8$ $n_0=15$

查寻得数值列表（3–1）中

① + ② × ③ – ④ = ⑤ = ⑥

①	②	③	④	⑤	⑥
$g_0{}^2$	g_0	$2a_0$	$-n_0$	$g_0^2+g_0\times2a_0-n_0$	$K_0{}^2$
…	…	…	…		…
12^2	12	8	– 15	144 + 96 – 15	(225)15^2
⋮	⋮	⋮	⋮	⋮	⋮

查得 ③列 $2a_0=8$ ④列 $n_0=-15$

有并列的 ① $g_0{}^2=12^2$ ②$g_0=12$

构成的初始值数列：$12^2+12\times8-15=15^2$

得$(B-1)$式中 $g^2+2ag-n=K^2$

g 被 16 整除的余数为 $g_0=12$

即 $g=16j+12$ j 为 g 被 16 整除的“参数”

构建 m 的“完全平方数式方程式”

$(16j+g_0)^2+2a\times(16j+g_0)-n=K^2$

求解此方程式，求得解值 g 与 K^2。

本文用 j 为正自然数 1，2，3…… $j\gg 1-j$

“逐一取值法”，求得 g 与 K 的解值。

j 的取值域为：$1\le j\le\left[\frac{a}{16}\right]$，$j$是可数的。

经逐一取值 $j=1，2，3\ldots\ldots703$

j 的自然数值在 703 时，得：$g=703\times16+12=11260$

将：$g=11260$　$2a=2\times25133588$　$n=42972479$

代入：$g^2+2ag-n=K^2$ 中：

得数式数值：

$11260^2+2\times25133588\times11260-42972479=K^2$

$\Rightarrow 126787600+566008401760-42972479$

$\Rightarrow 566092216881$

$\Rightarrow\sqrt{566092216881}$

$\Rightarrow 752391$

$\Rightarrow 752391^2\Rightarrow K^2$

即$(B-1)$式：　$g^2+2ag-n=K^2$ 方程式得解。

解值验证：$m\Rightarrow 631697288726223$

$p\Rightarrow(a+g+K)\Rightarrow 25133588+11260+752391\Rightarrow 25897239$

$q\Rightarrow(a+g-K)\Rightarrow 25133588+11260-752391\Rightarrow 24392457$

$m\Rightarrow p\times q\Rightarrow 631697288726223$

$\Rightarrow 25897239\times24392457$

$\Rightarrow 631697288726223$

解值验证：正确。

即：$m=631697288726223$　因数分解过程正确。

（完）

D

附录

数学方程式：$g^2+2ag-n=K^2$ 的应用

在数域较小的自正整数 Z— 集合里奇数 设定为 m，数位设定为 6 位数或小於 6 位数。进行“奇合数因数分解”及其奇数的“合性”与“素性”判别的手工操作方法，是数学方程式“$g^2+2ag-n=K^2$”的应用。

“奇合数”的因数分解，是分解为两个不相等的奇数（或素数）的乘积为目的，非“算术标准式”的因数分解。

操作流程实例

实例（一）：设 6 位数的奇数 $m\Rightarrow$732843

（1）将 m 变型为：$m\Rightarrow 732843=856^2+107$

即：$a=856\Rightarrow 2a=1712$

$n=107\Rightarrow -n=-107$

代入 $g^2+2ag-n=K^2$ 式中：

得：$g^2+g\times1712-107=K^2$

（2）　$g^2+2\times856\times g-107=K^2$　数值演算列表

①+②×③-④=⑤=⑥

①	②	③	④	⑤	⑥
g^2	g	$2a$	$-n$	非K^2数值	K^2数值
1	1	1712	－107	1606	
4	2	3424	－107	3321	
9	3	5136	－107	5038	
16	4	6848	－107	6757	
25	5	8560	－107	8478	
36	6	10272	－107		10201 *
49	7				
64	8				

（3）释表：

① g 可以逐一取值：1，2，3……

g 的取值域为：$\left[\frac{a}{16}\right]>g>1\Rightarrow\left[\frac{856}{16}\right]>g>1$

（*）② g 在逐一取值演算中，取得 K^2 数值时，对应的g值为 6，就是奇合数 m 的解值。此实例 $K^2=10201\Rightarrow 101^2\Rightarrow K=101$

③将取得的解值效验：

由（A）的设定：

$m\Rightarrow p\times q$　$p=a+g+K$　$q=a+g-K$

“g 与 K”是数学方程式 $g^2+2ag-n=K^2$ 的解值“数对”。

在此实例中：$m\Rightarrow p\times q\Rightarrow(a+g+K)(a+g-K)$

$\Rightarrow(856+6+101)(856+6-101)$

$\Rightarrow 732843=963\times761=732843$

（4）按此手工操作，演算证得：$m=732843$ 为“奇合数”。

实例（二）：设 5 位数的奇数 $m\Rightarrow$41333

（1）按实例（一）的工作操作方法

得：$g^2+g\times2\times203-124=K^2$

（2）　$g^2+g\times2\times203-124=K^2$　数值演算列表

①+②×③-④=⑤=⑥

①	②	③	④	⑤	⑥
g^2	g	$2a$	$-n$	非K^2数值	K^2数值
1	1	406	－124	283	
4	2	812	－124	692	
9	3	1218	－124	1103	
16	4	1624	－124	1516	
25	5	2030	－124	1931	
36	6	2436	－124	2348	
49	7	2842	－124	3767	
64	8	3248	－124	3188	
81	9	3654	－124	3611	
100	10	4060	－124	4036	
121	11	4466	－124	4463	
144	12	4872	－124	4892	
169	13	5278	－124	5323	

（3）释表：g 的取值到最大数值：$\frac{a}{16}\Rightarrow\frac{203}{16}\Rightarrow 13$

未取得 K^2 数值。没有对应的 g 值出现。

终止数值演算，逆反证明：

m =41333 为“奇素数”。

诠释：较小数位“6 位或小於 6 位”的奇数是可以用数学方程式：$g^2+2ag-n=K^2$ 的手工数值演算列表，来判别其是“奇合数”或“奇素数”的实用方法。

结束语：

此手工列表演算方法：进行“奇合数因数分解”及“奇素数素性判别”，适用于广大的数论“爱好者”。