數學傳播　39卷3期, pp. 30-41

稀有整數

沈淵源

摘要: 眾所周知, 費馬小定理的逆敘述是不成立的。此文將探討由此所衍生的些許問題, 以及將費馬小定理反逆敘述應用來判斷合成數所牽扯出稱之爲卡麥克數 (Carmichael numbers) 的稀世珍寶。

一、反逆敘述費馬小定理

費馬小定理說: 若 p爲質數, 則

$$a^p \equiv a \pmod{p} \, \forall a \in \mathbb{Z}。$$

將此敘述反逆敘述之, 就變成:

$$若 \ p \in \mathbb{N} \ 且 \ \exists a \in \mathbb{Z} \ 使得 \ a^p \not\equiv a \pmod{p} \ , 則 \ p 是合成數。$$

我們從兩個層面來看擺在面前的這個命題:

(i) 這提供我們一個直截了當、簡單爽快的方法來證明一個數是合成數。表面上看來, 這似乎沒什麼了不起的。然而, 你得想想, 從前你是用最古老的方法, 將一個數 x 除以所有比 $\sqrt{x}$ 小的質數; 末了的時候, 你不是得到 x的一個分解式就是歸結到 x 是一個質數。對小的數如

$$11657\,, \quad 11663 \quad 及 \quad 11677$$

來講, 這沒什麼大不了的; 因其平方根 ≈ 108 , 所以只需除以 108之前的28個質數, 即得 $11663 = 107 \times 109$還有 $11657, 11677$ 都是質數。對大數如

$$m = 113736947625310405231177973028344375862964001$$
$$n = 113736947625310405231177973028344375862953603$$

而言, 執行老方法的計算量可就相當驚人; 因質數定理說: 小於或等於$\sqrt{m}$的質數差不多有 $\sqrt{m}/\ln\sqrt{m} \approx 2 \times 10^{20}$ 個。如果電腦每秒可以處理 10^{10} 個運算, 那要除 2×10^{20}

個質數則要花將近 666年的時間。當下用上述所提直截了當、簡單爽快的方法, 在模 m 計算 2^m; 不需要 666年的時間, 因爲連續平方法計算 $2^m \pmod m$的速度奇快無比, 很快就可得到

$$2^m \equiv 392419708153934990601200436926306159617900 20 \pmod m\,,$$

因而知道 m是合成數。同樣地, 連續平方法計算 $2^n \pmod n$; 這次得到的是

$$2^n \equiv 2 \pmod n\,。$$

費馬小定理可曾告訴我們 n是質數? 答案是絕無此事, 那是費馬小定理的逆敘述所說的, 等下一節再來討論。

(ii) 從應用的層面來看: 通常, $a = 2$ 是我們的首選; 如果 $2^n \neq 2 \pmod n$, 則 n 不可能是質數。因爲連續平方法計算 $2^n \pmod n$ 的速度奇快無比, 這提供了我們一個尋找大質數的方法; 即選取一起始點 n_0, 並連續測試每一個大於 n_0 的奇數 n, 看看是否 $2^n \equiv 2 \pmod n$? 若 n無法通過此測試, 那麼就丟掉此數並進行下一個 n; 若 n 通過此測試時, 再使用更細膩的技巧來測試 n 的不可分解性。這個方法最大的優點就在整個演算過程的連續平方法遠比去分解每個 n要快許多, 尤其是能很快的將許多的 n 剔除。當然, 還有配套辦法可用來加速整個尋找的過程, 譬如說可先將包含有小質數因子的 n 剔除, 然後再進行上述的方法。

二、費馬小定理逆敘述成事否

若將費馬小定理逆敘述之, 則變成:

$$\text{若 } p \in \mathbb{N} \text{ 且 } a^p \equiv a \pmod p, \quad \forall a \in \mathbb{Z} \text{ , 則 } p \text{ 是質數。}$$

理所當然地, 你馬上會問:「這個命題對嗎?」接下來, 我們就好好地探索此命題真乎? 假乎?

持續上一節的 45 位數 n, 此數雖滿足 $2^n \equiv 2 \pmod n$ 卻不足以讓我們推論得到 n 就是質數; 因爲這不是費馬小定理的方向, 而是費馬小定理逆敘述的方向。所以我們就試多一些的 a 值, 直到 $a = 100$ 好了:

$$3^n \equiv 3 \pmod n\,,\ 4^n \equiv 4 \pmod n\,,\ 5^n \equiv 5 \pmod n\,,\ \ldots$$

$$\cdots\cdots\,, \quad 99^n \equiv 99 \pmod n\,, \quad 100^n \equiv 100 \pmod n$$

當下擺在你眼前可是有 99 個 a 滿足 $a^n \equiv a \pmod n$, 你應該認爲 n 就是質數吧! 雖是如此美好, 我們依舊無法用費馬小定理推論得到 n 就是質數; 因爲這不是費馬小定理的方向, 而是費馬小定理逆敘述的方向。因此, 我們現在以謙卑的口氣建議說: n "可能"是質數。

假設我們把一個數 n 當成一個自然現象, 且以實驗科學家的精神來研究探討 n。我們做的實驗就是選取不同的 a 值並算出模 n 之下 a^n 的值

$$a^n \pmod{n};$$

即使只有單一的一個實驗得到不同於輸入之 a 值, 我們即可斬釘截鐵的說 n 是合成數。所以這足以讓我們合理的相信, 每一次做完實驗所得到的確就是輸入之 a 值時; 我們就已經蒐集到一些"證據", 說 n 是質數。

藉著觀察 n 次冪之後不同於 a 的那些 a 值, 我們可以將這樣子的論證放在一個更穩固的根基上。我們擬人化地說這 a 是 n 不是質數的見證人如果 $a^n \neq a \pmod{n}$。這樣的稱呼對 a 來講是挺帥的, 若是 n 想化身充當質數, 那麼起訴律師就請 a 在證人席上作證說 n 實際上是合成數。

若 n是質數, 那麼很明顯的沒有見證人; 這其實就是費馬小定理本身的內容。下面, 我們表列出 ≤ 20的每一個 n不是質數的所有見證人; 看起來, 合成數真是不乏見證人。

n	n 不是質數的見證人	n	n 不是質數的見證人
3	無 (質數)	4	2,3
5	無 (質數)	6	2,5
7	無 (質數)	8	2,3,4,5,6,7
9	2,3,4,5,6,7	10	2,3,4,7,8,9
11	無 (質數)	12	2,3,5,6,7,8,10,11
13	無 (質數)	14	2,3,4,5,6,9,10,11,12,13
15	2,3,7,8,12,13	16	2,3,4,5,6,7,8,9,10,11,12,13,14,15
17	無 (質數)	18	2,3,4,5,6,7,8,11,12,13,14,15,16,17
19	無 (質數)	20	2,3,4,6,7,8,9,10,11,12,13,14,15,17,18,19

爲了更進一步支持『看起來, 合成數真是不乏見證人』的觀點, 我們隨機選幾個介於 100 與 1000 之間的數並數算介於 1與 n 之間見證人的百分比。列表如下:

n	508	783	352	445	176	901
見證總人數	500	774	348	420	164	876
見證百分比	98.4%	98.9%	98.9%	94.4%	93.2%	97.2%
n	282	146	808	425	932	900
見證總人數	274	142	804	380	928	892
見證百分比	97.2%	97.3%	99.5%	89.4%	99.6%	99.1%

似乎是, 只要 n 是合成數; 那麼, 多數的 a值都是見證人。譬如說, 當 $n = 508$ 時, 隨機選一個 a 值; 就有百分之 98.4 的機率是 n 爲合成數的見證人。因此, 不需要太多實驗就可證明 n 是合成數。

所有這些跡象加上普通常識建議我們說, 合成數有著許許多多的見證人。然而, 此話當真? 如果我們繼續製作上上個表格, 將每個數不是質數的見證人一一列出; 接著是 $n = 21, \ldots$ 這樣下去終究會碰上 $n = 561$ 的傷心時刻。這位仁兄是合成數, 因爲 $561 = 3 \times 11 \times 17$; 但很不幸的, 這個數沒有半個見證人。當然你不妨算出所有 561個 a值所對應的 $a^{561} \pmod{561}$之值, 有數學套裝軟體的幫忙, 一轉眼即可完成。不過嗎, 還是讓陪伴在旁的費馬小定理發發威, 我們可以做得更有水準、更有智慧一些。怎麼進行呢? 且看下面的分析: 欲證 $a^{561} \equiv a \pmod{561}$, 僅需證明

$$a^{561} \equiv a \,(\mathrm{mod}\ 3),\ a^{561} \equiv a \,(\mathrm{mod}\ 11) \text{ 及 } a^{561} \equiv a \,(\mathrm{mod}\ 17)\,;$$

因爲被3, 被11, 被17整除的數, 一定可以被其乘積 $3 \times 11 \times 17$整除。首先第一個同餘式, 我們注意到若 3 整除 a 則兩邊都是 0; 否則藉著費馬小定理 $a^2 \equiv 1 \pmod{3}$來計算

$$a^{561} = a^{2\cdot 280+1} = (a^2)^{280} \cdot a \equiv 1 \cdot a \equiv a \pmod{3}\,。$$

依樣畫葫蘆可驗證第二及第三個同餘式。所以當 11 整除 a 則兩邊都是 0; 否則藉著費馬小定理 $a^{10} \equiv 1 \pmod{11}$來計算

$$a^{561} = a^{10\cdot 56+1} = (a^{10})^{56} \cdot a \equiv 1 \cdot a \equiv a \pmod{11}\,。$$

最後, 若17整除 a則兩邊都是 0; 否則藉著費馬小定理 $a^{16} \equiv 1 \pmod{17}$來計算

$$a^{561} = a^{16\cdot 35+1} = (a^{16})^{35} \cdot a \equiv 1 \cdot a \equiv a \pmod{17}\,。$$

因而, 561這個合成數沒有半個見證人; 這也同時告訴了我們, 561這個合成數徹徹底底地粉碎了費馬小定理逆敘述的正確性。

這個例子連同其他的十四個證明了費馬小定理的逆敘述是錯誤的。這15個數在1910年首先被卡麥克[1] 注意到; 因此後人就用他的名字來爲這些數命名, 同時也以此紀念他的貢獻。

三、卡麥克數極稀少

滿足同餘式

$$a^n \equiv a \pmod{n} \quad \forall\, a \in \mathbb{Z}$$

的合成數 n稱之爲卡麥克數 (Carmichael numbers)。換句話說, 卡麥克數乃是那些可以僞裝成質數的合成數, 因爲沒有半個見證人可以爲它們合成數的身分作證。我們剛剛看過 561是一個卡麥克數, 而實際上這是最小的一個。

這種數極其稀少, 在一萬之前只有七個, 而三萬之前只有十個; 前十個卡麥克數的分解式如下:

序	卡麥克數	分解式	序	卡麥克數	分解式
1	561	$3 \times 11 \times 17$	6	6601	$7 \times 23 \times 41$
2	1105	$5 \times 13 \times 17$	7	8911	$7 \times 19 \times 67$
3	1729	$7 \times 13 \times 19$	8	10585	$5 \times 29 \times 73$
4	2465	$5 \times 17 \times 29$	9	15841	$7 \times 31 \times 73$
5	2821	$7 \times 13 \times 31$	10	29341	$13 \times 37 \times 61$

[1]羅伯特·丹尼·卡麥克 (Robert Daniel Carmichael, 1879年生於阿拉巴馬 -1967年逝世), 美國數學家; 1923年擔任美國數學協會 MAA 總裁一年。1898年在 Lineville College 獲學士學位, 1911年在普林斯頓大學獲哲學博士。其論文指導教授是公認爲美國首位對微分方程有顯著貢獻的喬治·大衛·伯克霍夫 (G. David Birkhoff)。卡麥克1911至15年任教印第安那大學, 1915至47年任教伊利諾大學。

聰明的你應該馬上會察覺到, 擺在你眼前這十個卡麥克數都是三個相異奇質數的乘積。所以很有可能這會引導你進一步的猜測說: 卡麥克數都是三個相異奇質數的乘積。

可惜這個猜測沒有好收場, 因爲

$$41041 = 7 \times 11 \times 13 \times 41$$

是一個包含有四個質因子最小的卡麥克數。這並不意味著我們應該捨棄這個猜測, 而是必須做一些修飾。有沒有注意到我們的猜測實際上是三個猜測: 第一個是卡麥克數剛剛好有三個質因子, 其次爲質因子兩兩相異, 最後則說其質因子是奇數。所以我們就割捨錯誤的部分並將其他兩個分別敘述如下:

- 每一個卡麥克數都是奇數。
- 每一個卡麥克數都是相異質數的乘積。

奇數的性質只需從卡麥克同餘式

$$a^n \equiv a \pmod{n} \ \forall\ a \in \mathbb{Z}$$

套入 $a = n - 1 \equiv -1 \pmod{n}$即得

$$(-1)^n \equiv -1 \pmod{n}。$$

然而滿足這個同餘式的偶數只有 $n = 2$ (記否? 在模 2的世界裡, 負的就是正的, 因爲 $1 + 1 = 0 \Rightarrow -1 = 1$), 但卡麥克必須是合成數, 剩下唯一的選項就是 n必須是奇數。

接下來假設 n是卡麥克數。令 p是 n的一個質因子且令

$$p^{k+1} \text{ 是整除 } n \text{ 質數 } p \text{ 的最高次冪。}$$

現在的目標要證明 $k = 0$, 而泉源依舊是卡麥克同餘式

$$a^n \equiv a \pmod{n} \ \forall\ a \in \mathbb{Z}$$

這一次我們套入 $a = p^k$ 可得

$$(p^k)^n \equiv p^k \pmod{n} \implies n \mid (p^{kn} - p^k)。$$

與上面的假設 p^{k+1} 整除 n 合體得到 p^{k+1} 整除 $p^{kn} - p^k$。因此

$$\frac{p^{kn} - p^k}{p^{k+1}} = \frac{p^{k(n-1)} - 1}{p} \in \mathbb{N}。$$

若 $k \neq 0$, 則

$$n-1 \in \mathbb{N} \Longrightarrow k(n-1) \in \mathbb{N} \Longrightarrow \frac{p^{k(n-1)}-1}{p} \notin \mathbb{N};$$

與上面矛盾, 故得證 $k=0$; 這也同時完成了卡麥克數的兩個必要條件的證明。

很自然的你會問, 這兩個必要條件也是充分條件嗎? 感覺上似乎還早呢, 因爲上面證明561是卡麥克的經驗裡好像沒有這兩個條件的影子。但 561提供了我們尋找充分條件的主要線索, 怎麼說呢? 在那兒, 我們沒有正面挑戰卡麥克同餘式 $a^n \equiv a \pmod{n}$; 因爲 n 不是質數, 沒有著力點。所以將 n 取代爲其中的質因子 $p \mid n$, 如此一來費馬小定理順理成章的變成我們的使力點, 也是我們莫大的幫助, 讓我們抵達最後的目標。且回憶一下當中的片段: 若 p 整除 a 則兩邊都是 0; 否則藉著費馬小定理 $a^{p-1} \equiv 1 \pmod{p}$來計算 a^n。如果 $p-1 \mid n-1 \Longrightarrow \frac{n-1}{p-1} \in \mathbb{N}$, 那麼

$$a^n = a^{(p-1)\cdot\frac{n-1}{p-1}+1} = (a^{p-1})^{\frac{n-1}{p-1}} \cdot a \equiv 1 \cdot a \equiv a \pmod{p};$$

這說明了 a是卡麥克數的充分條件是 $p-1 \mid n-1$。其實這個性質也是卡麥克的一個必要條件。證明嗎, 還是回到源頭的同餘式; 若 p 是 n 的一個質因子且 $p \nmid a$, 則

$$a^n \equiv a \pmod{n} \Longrightarrow a^n \equiv a \pmod{p} \Longrightarrow a^{n-1} \equiv 1 \pmod{p}。$$

再來, 取質數 p 的一個原根[2] (primitive root) a ; 我們要證明 $p-1$ 整除 $n-1$。很自然地, 我們將 $n-1$ 除以 $p-1$ 得到 $n-1=(p-1)q+r$, 其中 $0 \leq r < p-1$; 因此得到

$$1 \equiv a^{n-1} \equiv (a^{p-1})^q a^r \equiv 1 \cdot a^r \equiv a^r \pmod{p}。$$

假設 $r > 0$。考慮所有 $a \pmod{p}$ 的次冪即可察覺, 我們頂多就只有 r 個元素。但 $r < p-1$, 因此並非所有模 p 之下的非零元素都是 a 的一個次冪。這與 a 是原根的假設矛盾, 因而剩下來唯一的可能性就是 $r=0$. 所以 $n-1=(p-1)q$, 也就是 $p-1$ 整除 $n-1$。

奇妙的是, 上述三個必要條件合體後就萬事亨通; 三合一, 三個合起來的確變成卡麥克的充分條件。更奇妙的是, 這三個充要條件早在1899年柯謝爾特[3] 就已提出; 當時卡麥克發現的那些數他都沒看過呢。

柯謝爾特判斷法 (Korselt's Criterion): 令 n爲合成數。則 n是卡麥克數若且唯若 n滿足下列三個條件

1. n是奇數

[2]模 p 的原根就是其中的非零元素 a 使得每一個模 p 的非零元素都是 a的一個次冪。

[3]柯謝爾特 (Alwin Reinhold Korselt, 1864-1947), 德國數學家。

2. n是相異質數的乘積

3. n的質因子 p滿足 $p-1\,|\,n-1$

證明: 上面已經證明了這三個條件都是必要條件, 現在證明若合成數 n 滿足這三個條件則 n 是卡麥克數。將 n 寫成質因數的乘積

$$n = p_1 p_2 \cdots p_r \text{。}$$

條件 (2) 告訴我們, 這些質數兩兩互異; 條件 (3) 說每個 i 存在整數 k_i 使得 $n-1=(p_i-1)k_i$。對任意的整數 a, 證明 $a^n \equiv a \pmod{p_i}$如下: 若 p_i整除 a則兩邊都是 0; 否則藉著費馬小定理 $a^{p_i-1}\equiv 1 \pmod{p_i}$來計算

$$a^n = a^{(p_i-1)k_i+1} = \left(a^{p_i-1}\right)^{k_i}\cdot a \equiv 1\cdot a \equiv a \pmod{p_i}\text{。}$$

所以, 對每一個 $i=1,2,\ldots,r$ 我們已經證明了

$$a^n \equiv a \pmod{p_i} \implies p_i\,|\,a^n-a\,;$$

因此 a^n-a 也可以被其乘積 $n=p_1p_2\cdots p_r$ 所整除 (這裡我們用到了這些質數兩兩互異的條件) , 故得證 n 是卡麥克數:

$$a^n \equiv a \pmod{n}\text{。}$$

最後我們舉兩個例子來看看柯謝爾特判斷法的威力, 如下面表格列出的第30及第44個卡麥克數分別爲410041與 1024651: 首先, 柯謝爾特判斷法告訴我們 $410041 = 41\times 73\times 137$ 是卡麥克數; 因爲

$$\frac{410041-1}{41-1}=10251\,,\quad \frac{410041-1}{73-1}=5695\,,\quad \frac{410041-1}{137-1}=3015\text{。}$$

其次, 柯謝爾特判斷法告訴我們 $1024651 = 19\times 199\times 271$ 是卡麥克數; 因爲

$$\frac{1024651-1}{19-1}=56925\,,\quad \frac{1024651-1}{199-1}=5175\,,\quad \frac{1024651-1}{271-1}=3795\text{。}$$

如前面所提到過的, 這種數極其稀少, 下面分佈表告訴我們: 在一萬之前有 7個, 十萬之前有16個, 百萬之前有43個, 千萬之前有105個; 一億之前有 255個, 十億之前有 646個, 百億之前有1547個, 千億之前有3605個; 一兆之前有8241個, 十兆之前有 19279個, 百兆之前有44706個, 千兆之前有105212個; $\cdots$。雖然如此, 卡麥克本人在他1910年的論文[2] 就猜測此種數有無限多個; 過了80多年之後的1994年, 才被沃爾福特 (W.R. Alford) 等三人[4]證明是正確的。

[4]Alford, W. R./Granville, A./Pomerance, C.: "There are Infinitely Many Carmichael Numbers," *Annals of Math.* 140 (1994), 703-722. 網頁:dms.umontreal.ca/ andrew/agpapers.html

$\leq 10^{21}$ 卡麥克數分佈表 (其中 $C(X)$ 乃 $\leq X$ 之卡麥克數個數)

n	$C(10^n)$	n	$C(10^n)$	n	$C(10^n)$	n	$C(10^n)$
2	0	7	105	12	8241	17	585355
3	1	8	255	13	19279	18	1401644
4	7	9	646	14	44706	19	3381806
5	16	10	1547	15	105212	20	8220777
6	43	11	3605	16	246683	21	20138200

前四十四個卡麥克數

序	卡麥克數	序	卡麥克數	序	卡麥克數	序	卡麥克數
1	561	12	46657	23	252601	34	530881
2	1105	13	52633	24	278545	35	552721
3	1729	14	62745	25	294409	36	656601
4	2465	15	63973	26	314821	37	658801
5	2821	16	75361	27	334153	38	670033
6	6601	17	101101	28	340561	39	748657
7	8911	18	115921	29	399001	40	825265
8	10585	19	126217	30	410041	41	838201
9	15841	20	162401	31	449065	42	852265
10	29341	21	172081	32	488881	43	997633
11	41041	22	188461	33	512461	44	1024651

四、合成檢驗有妙方

卡麥克數雖然極其稀少, 但其存在的個數竟然有無限多, 此乃不可爭之事實; 這意味著, 我們必須有一個更好更棒的方法來檢驗合成數。我們先敘述質數基本性質[5] 以及馬上會用到的一個簡單的推論:

質數基本性質: 令 p 爲質數且令 a, b 爲整數。若 $p \mid ab$, 則 $p \mid a$ 或 $p \mid b$.

推論: 令 p 爲質數, 則 $x^2 \equiv 1 \pmod{p}$ 的解只有 $x \equiv \pm 1 \pmod{p}$; 換句話說, 在模 p 下, 1的平方根不是 1就是 -1。

[5]其證明乃高中生耳熟能詳的, 在此省略之。

證明: 因爲

$$x^2 \equiv 1 \pmod{p} \Leftrightarrow p|(x^2-1) = (x-1)(x+1) \Leftrightarrow p|(x-1) \text{ 或 } p\,|\,(x+1),$$

所以 $x \equiv 1 \pmod{p}$ 或 $x \equiv -1 \pmod{p}$, 故得證此推論。

奇質數另一性質: 令 p 爲奇質數並將 $p-1$ 寫成 $2^k\,m$, 其中 m 爲奇數且令 a 爲小於 p的正整數。若在模 p 之下 a^m 與 1 不同餘, 則下列 k個數

$$a^m, \quad a^{2m}, \quad a^{4m}, \quad \ldots, \quad a^{2^{k-1}m}$$

中有一個在模 p之下與 -1 同餘。

證明: 考慮下面 $k+1$個數

$$a^m\,, \quad a^{2m}\,, \quad a^{4m}\,, \ldots, a^{2^{k-1}m}\,, \quad a^{2^k m}\,;$$

費馬小定理告訴我們說: $a^{p-1} \equiv 1 \pmod{p}$; 這意味著, 在模 p之下最後一個數與 1 同餘, 因爲 $2^k\,m = p-1$。再者, 每一個數都是前一個數的平方 (所以一旦出現 $1 \pmod{p}$ 那麼後面就全部都是 $1 \pmod{p}$)。

因此若在模 p 之下 a^m 與 1不同餘, 則令第一個出現 $1 \pmod{p}$ 的是 $a^{2^i m}$, 此處 $0 < i \le k$; 故得一數 $a^{2^{i-1}m}$ 在模 p 之下與 1 不同餘, 但平方之後與 1同餘。上面推論得知: 在模 p 之下, 具此性質的數只有 -1; 所以 $a^{2^{i-1}m} = -1$, 意即最後那個數之前的 k 個數 $a^m, a^{2m}, a^{4m}, \ldots, a^{2^{k-1}m}$ 中有一個就是 $-1 \pmod{p}$。故得證此奇質數的性質。

翻轉上述奇質數的性質, 馬上就得到一個合成數的檢驗法; 稱之爲拉賓-米勒合成數檢驗法 (Rabin-Miller Test for Composite Numbers)。因此, 若 n是奇數但不滿足上述奇質數的性質; 那麼我們就知道 n必定是合成數。如此這般, 我們已經證明了這個合成數的檢驗法。

拉賓 – 米勒合成數檢驗法: 令 n 爲奇數並將 $n-1$ 寫成 $2^k\,m$, 此 m 爲奇數且令 a 爲小於 n的正整數。若在模 n 之下 a^m 與 1 不同餘且若下列 k 個數

$$a^m, \quad a^{2m}, \quad a^{4m}, \quad \ldots, \quad a^{2^{k-1}m}$$

在模 n之下都與 -1 不同餘, 則 n是合成數。

值得在此提出的注意事項有二: 首先, 這個方法非常快而且很容易在電腦上執行; 因爲一旦算完 $a^m \pmod{n}$, 剩下就只有幾個模 n 之下的平方運算而已。其次, 當 $n \equiv 3 \pmod{4}$ 時, 因爲 $k=1$, 所以我們得到 $m = (n-1)/2$; 此時需要計算的僅有 $a^m \pmod{n}$一個數而已, 而其敘述也特別簡單。如下:

特殊情況: 令正整數 $n \equiv 3 \pmod 4$ 且令 a 爲小於 n 的正整數。

若 $a^{(n-1)/2} \not\equiv \pm 1 \pmod n$, 則 n 是合成數。

譬如說, 對正整數 $n = 23590123$ 及 $a = 2$算出 $a^{(n-1)/2} \equiv 3957352 \pmod n$; 因 $a^{(n-1)/2} \not\equiv \pm 1 \pmod n$, 故得 23590123 是合成數。

在第一節時, 我們採用費馬小定理的反逆敘述作爲合成數檢驗法:

若 $n \in \mathbb{N}$ 且 $\exists$ 正整數 $a < n$ 使得 $a^{n-1} \not\equiv 1 \pmod n$, 則 n 是合成數。

另一方面, 在第二節我們擬人化地稱呼這樣的 a爲 n 是合成數的見證人。依樣畫葫蘆, 用拉賓 -米勒合成數檢驗法能成功證明 n 是合成數的 a 值; 不妨稱之爲 n是合成數的拉賓 – 米勒見證人, 而前者就順理成章地改稱爲費馬見證人。

不難證明, 費馬見證人必定是拉賓 – 米勒見證人。因爲如果 a不是拉賓 -米勒見證人, 那麼不是 $a^m \equiv 1 \pmod n$, 就是下列 k個數

$$a^m, \quad a^{2m}, \quad a^{4m}, \quad \ldots, \quad a^{2^{k-1}m}$$

當中有一個在模 n之下與 -1 同餘; 如此一來, $a^{n-1} \equiv 1 \pmod n$, 因而導致 a 不是費馬見證人。聰明的你說那一個演算法好呢?

所以, 可以確定的是: 拉賓 – 米勒見證人的個數必定比費馬見證人的個數多。但到底多多少呢? 上面簡單的推論, 無法提供我們更具體的數據; 而拉賓 – 米勒之所以超級有用乃根基於下面的事實, 其證明可參考更專業的書本。

> 若 n是奇合成數, 則至少有75%介於 1及 $n-1$ 間的 a 值扮演著拉賓 – 米勒見證人。

換句話說, 每一個合成數擁有許許多多的拉賓 – 米勒見證人, 因此在拉賓 – 米勒合成數檢驗法當中不會有"卡麥克"型態的數出現。

譬如說, 如果我們隨機選出 100個不同的 a值; 而且如果沒有半個是 n 的拉賓 – 米勒見證人, 那麼 n 會是合成數的條件機率小於 $0.25^{100} \approx 6 \times 10^{-61}$。況且如果你覺得這樣子還是挺冒險的, 你總可以再試幾百個不同的 a 值。在實作上, 如果 n 是合成數, 那麼僅需幾個拉賓 – 米勒檢驗就會露出其合成數的馬尾來。

舉例說明之, 以 $a = 2$ 對卡麥克數 $n = 561$ 來執行拉賓 -米勒檢驗。我們有 $n - 1 = 560 = 2^4 \times 35$, 接著計算

$$2^{35} \equiv 263 \pmod{561}, \quad 2^{2\times 35} \equiv 263^2 \equiv 166 \pmod{561},$$

$$2^{4\times 35} \equiv 166^2 \equiv 67 \pmod{561}, \quad 2^{8\times 35} \equiv 67^2 \equiv 1 \pmod{561}。$$

第一個數 2^{35} 在模 561之下既不是 1也不是-1, 而且其他的數也都不是-1, 所以 2是561的拉賓 – 米勒見證人。

第二個例子, 我們取大一點的數 $n = 172947529$。我們有

$$n - 1 = 172947528 = 2^3 \times 21618441\,,$$

以 $a = 17$檢驗之; 第一步得 $17^{21618441} \equiv 1 \pmod{172947529}$。所以17不是 172947529的拉賓 – 米勒見證人。下一個試 $a = 3$, 很不幸的我們得

$$3^{21618441} \equiv -1 \pmod{172947529}\,,$$

所以 3也不是 172947529的拉賓 – 米勒見證人。至此碰了兩個釘子, 我們可能會懷疑 n是質數; 但如果再試一個另外的值, 如 $a = 4$, 我們發現

$$4^{21618441} \equiv 2257065\,,\ \ 4^{2\times 21618441} \equiv 1\,,\ \ 4^{4\times 21618441} \equiv 1 \pmod{172947529}\,;$$

所以 4是 172947529的拉賓 – 米勒見證人。實際上, 172947529是一卡麥克數; 但用手算來分解, 並不是那麼容易的。

參考資料

1. Alford, W. R./Granville, A./Pomerance, C. : "There are Infinitely Many Carmichael Numbers," *Annals of Math.* **140** (1994), 703-722.
2. Carmichael, R. D. : "Note on a new number theory function," *Bull. Amer. Math. Soc.*, **16** (1910), pp. 232–238. See also: *Amer. Math. Monthly* **19** (1912), pp. 22–27.
3. Rivest, R.L., Shamir A., and Adleman L. : A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM*, **21**(1978), 120–126.
4. Silverman, Joseph H. : *A Friendly Introduction to Number Theory*, Prentice Hall, Third Edition, 2006.

—本文作者任教東海大學應用數學系—