質數的建造、分佈及檢驗

楊重駿
楊照崑

1.導 言

你看過「數播」七十三年十二月號(32期)上第三十四屆國際科技展數學得獎作品簡介嗎？這類展覽都以「創新」爲作品的評價，而在數學部門中，在「數播」所介紹的八個得獎作品中，就有五個屬於「數論」的領域，佔了得獎作品的一半以上，爲什麼？因爲數論有它特別迷人的地方——那就是在極簡單的規則中，作極複雜的變化，一個類似的例子是下棋。圍棋的規則極簡單而其變化極爲複雜，可以說是最迷人的一種棋類，相反的，海陸空軍棋其規則極繁而變化又小，幾乎沒有人下了。又研究整數論所遭遇的問題及研究對象要比其它各門數學來得簡單明瞭，不外是討論正整數1，2，3，4……的種種特殊性質，其變化之大，一直困惑許許多多的數學家。

以往整數論曾一直被人認爲是最純的純數學，沒想到由于最近美國有人利用找一個大數目的質數因子的困難性及其它質數的一些特有性質，而設計了一種可公開傳遞(即不怕被敵方截獲)且保密性極高的密碼，引起了軍方、工商界的莫大興趣，有關此方的研究經費大爲增加，我們在此簡略地說明一下該密碼的原理(有關較具體的介紹請參閱[1或3])。在收報方甲先找出兩個大的質數 $m=pq$，及取任一與$(p-1)(q-1)$互質的整數a，將此兩數值m，a公開傳遞給發報方乙(甚至登報聲明！)，現假設發報方乙要將一信號(整數形式)拍給甲。設該代號爲整數值x(這是保密的且比p，q小很多)，當然乙不能逕自公開拍發x給甲，而公開拍明碼$c\equiv x^a \pmod m$給甲方，現甲方收到明碼整數c後設法譯回到x，如何做到此一譯碼的工作呢？因甲方有資料a及$\varphi(m)$，φ爲Euler函數，$\varphi(m)$表所有小於m且與m互質的正整數的數目。由假設a，$\varphi(m)$互質，故有正整數d及負整數b使得$ad+\varphi(m)b=1$，這時甲方將收到的明碼c作變換：$y\equiv c^d \pmod m$；注意取y爲小於m的整數，及由於x小於p及q，故x必與m互質，因而由尤拉(Euler)定理我們有$x^{\varphi(m)}\equiv 1 \pmod m$，因此

$$y\equiv c^d\equiv(x^a)^b\equiv x^{ad}\equiv x^{1-\varphi(m)b}$$
$$\equiv x\cdot x^{-\varphi(m)b}\pmod m\equiv x\pmod m$$

現若兩正整數x，y皆小於m且與m爲等模，

故只有 $x = y$，因而甲方就可把密碼收到了。

欲解此密碼勢必要知 d，但要知 d 非要知 $\varphi(m)$（$=(p-1)(q-1)$）也即要知 p 及 q，找不到 p，q 就無法得 $\varphi(m)$ 及 d 而硬要從 c 得出 x 就似乎很困難了。目前分解一個整數 n 的因子仍停留在近似硬試的階段，等下我們知道由“篩法”原理要從 2，3，5，7，……一直試到小於 $\sqrt{n}$ 的質數爲止，由[1]中可知若 n 爲一 50 位數（p，q 皆爲 25 位數），則分解 n 要除 10^{25} 次，以每秒 10^6 次的電腦計算速度則將是一個 10^{11} 年的工作，若用特殊的快速法則來進行也得要 10^{10} 次的運算，約 4 個小時電腦的計算時間，若 n 爲一個 100 位的整數，則用目前最快速的電腦來操作運算也得要 74 年左右（中間還要保證機械沒故障才行），所以目前用這種方法來傳遞需保密的密碼是相當安全的了。

質數可以說是整數的基礎，由上面的應用我們欲充分利用質數必需要能建造很大的質數，要偵破上面密碼的應用，我們也要知道質數的分佈。本文就是針對此兩需求作些淺顯的介紹，希望能引起讀者的更大的興趣，作更進一步的研究（而且可以保證的，任何這方面的突破，將會帶來名利的收獲，古人所謂書中自有黃金屋一點都不錯），光大我們祖先的光輝（因有的密碼是利用“中國人剩餘定理或韓信點兵術原理”造成的）。

具體的講，我們主要將介紹的是 (i) 質數及質數表的製造，(ii) 如何製造任何一串列的大質數，(iii) 質數在整數中的分佈、或密度，(iv) 質數的檢驗。又本文的介紹之參考書[1]，[2]皆是新近出版的。

2. 質數表（篩法）及質數的製造

由于質數是不具有任何異於 1 及其本身的因子，所以早在紀元前 200 年左右古希臘學者 Eratosthenes（以下簡稱愛氏）就爲我們發明一個可找出所有質數的法則，稱爲篩法（Sieve method）。據說愛氏在找質數時，他把整數一一照序寫在一片草質的紙上，凡是非質數者他就用火在那位置燒一個洞，最後整片紙只留下密密麻麻的許多洞，很像一個篩子，故叫做“篩法”。它的原則如下：是將正整數由 1 照大小依次排出一列，或一矩陣（如圖 1 是一正方形矩陣，其由 1 至 100 的整數組成），則頭一個數爲 1，非爲質數刪掉，其下一個爲 2 爲質數留下，則 2 以後刪掉所有 2 的倍數（4，6，8，10，12，14，16，18，…）然後在所剩的數中大於 2 的第一個數 3，其爲一質數，繼 3 以後刪掉 3 的倍數（即 6，9，15，21），3 之後 5 爲第一個未被刪掉的數其爲一質數，刪掉所有 5 的倍數（10，……），如此泡製，所留下的就是所有的質數（若只取 1 至 N 來篩，則如此所得的是 1 與 N 間所有的質數。在沒有一張質數表時，我們怎樣確定一給定的正整數 N 是否爲質數呢？在 N 很大時若是以 2 到 $N-1$ 所有的質數一一來試除 N 會是件很耗時的事的。好在我們只需用 2 到 $\sqrt{N}$ 間所有的質數來試即可，這樣一來就省了許多的除法。這是因爲若 N 非爲質數則 $N=n_1 \times n_2$，n_1 及 n_2 爲兩個大於 1 的正整數，且必有一個數 n_1 或 n_2 不大於 $\sqrt{N}$，利用此一觀察及篩法我們很容易把所有不大於某個正整數 N（N 不是很大時）的質數找出來。譬如我們要列出 100 以下所有的質數，我們只需用小於 $\sqrt{100}=10$ 以下的質數 2，3，5，7 用篩法把所有小於 100 的質數找出如下：

2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53，59，61，67，71，73，79，83，89，97。

目前我們有 10 億（$=10^9$）以內的質數表。而利用大質數的密碼爲了防止敵方利用電腦來偵破，往往是用有 50 位的質數，所以用篩法來建造大質數仍無法合于實用。

又用篩法製造大的質數時的一個缺點是每

圖1 1至100的篩法求質數

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

次要列出或利用許多的正整數來求得，這在實用上很不方便的。我們很想隨意製造一些很大的質數，該如何做呢？最理想的是我們能找出一個公式或一個式子只要把適當的數代入就可得出很大的質數，我們中國人很早有一個有關質數的製造及揀選，認爲一個正整數 n 爲質數的充要（充分及必要）條件是 n 可整除 2^n-2，即 $n \mid (2^n-2)$，例如 $n=5$，$2^n-2=30$，$5 \mid 30$，這個結論當時並沒正式證明，而事實上現今可證明此條件 $n \mid (2^n-2)$ 爲必要的（這可由所謂的小費馬（Fermat）定理來證明，它是說：若 a 與 k 爲兩無公因子的正整數，則 $a^k \equiv a \pmod{k}$），因此 n 爲奇質數時此條件爲必要的立即可見，而當 $n=2$ 時則 $n \mid 2^n-2$ 明顯成立）。但此條件却非充分的，不過至少以當時的計算能力來檢驗，此一眞實性恐怕也不是件很容易的工作，因爲事實上對比小於341的正整數 n，若 n 不是質數則 $n \nmid 2^n-2$，例如 $n=15$，$2^n-2=32{,}766$ 此數不可能被15整除，但 $n=341$（$=11\times 31$）時，用現代的任何小型電子計算機（Programmable Pocket Calculator）可得知341除 $3^{341}-2$ 的剩餘爲0（注意，至於這樣一個具有101位數的商，就不是可由此一類機子可算出了，這也難怪我們的老祖先在只有算盤代勞的劣勢下，更是心有餘而力不足了。）

但很早就有人證明具 $4n+1$ 形式的質數是無窮多的（讀者不妨試證一下！提示：任何一個整數 m 都可表成 $4n$，$4n\pm 1$ 的形式中之一），又對 $f(n)=n^2+n+41$ 對此一二次式而言，在 $n=0$，1，2，……，40連續41個整數的值時皆爲質數，但很明顯 $n=41$ 時，$f(n)$ 有一因子爲41，或許有讀者會問可不可能找到一個多項式 $f(x)=a_0x^k+a_1x^{k-1}+\cdots\cdots+a_k$，係數 a_0，a_1，……（皆爲整數）使得對任何的正整數 n，$f(n)$ 皆爲質數？這個問題的答案不難知是否定的。其證如下：設 $f(n_0)=p$ 爲一質數，則對任何整數 m，$f(n_0+pm)-f(n_0)=\sum_{i=0}^{k}a_i[(n_0+pm)^i-n_0^i]\equiv 0 \pmod{p}$，又方程式 $f(n_0+pm)=0$ 及 $f(n_0+pm)=\pm p$ 至多有 $3k$ 個整數解 m，故當 m 充分大時 $f(n_0+pm)-f(n_0)\neq 0$，$\neq \pm p$，且爲 p 的倍數，故爲非質數。

在上面我們證明了沒有一個多項式 $p(x)=a_0x^n+a_1x^{n-1}+\cdots\cdots+a_n$ 存在使得對所有的整數 m，$f(m)$ 永遠取質數值，但另一方面我們也不難證明對 $p(x)=6x+1$，必有無窮多的質數 $p(m)$（證明參看[1]）。在這方面一個艱深的問題是一個二次或以上的整係數多項式，即 $p(x)=a_0x^n+a_1x^{n-1}+\cdots\cdots+a_n$，$n\geqslant 2$，$a_0\neq 0$，$a_i$（$i=0$，1，2……$n$）皆爲整數，能否證明 $\{p(m)\}_{m=1}^{\infty}$ 必有無窮多個質數？如果讀者中有人能解決此一問題，他的大名一定會記在數學史上。

所以我們知道若要建造一個函數 $f(x)$ 使得 $f(n)$ 在 n 爲正整數時，總爲質數，想由多項式的形式中去尋求，是徒費其勞的。下面我們就介紹密爾史氏（W. H. Mills）的一個建造法（1947年），其基本構想是基於1937年英格翰氏（A. E. Ingham）的一定理：若把所有的質數以大小漸增地排列並以序列 p_1，p_2，……p_n，p_{n+1}，……或 $\{p_n\}_{n=1}^{\infty}$ 表之，即 p_n 表示第 n 個質數，則不等式：$p_{n+1}-p_n<k\,p_n^{5/8}$ 成立，此處 k 爲一定正整數，依據此

定理密爾史氏先證明了下面的一個結果：

輔理1.

設N爲一大於k^8的正整數，則N^3與$(N+1)^3-1$之間必有一質數。

證：設p_n爲小於N^3的最大質數，則

$$N^3<p_{n+1}<p_n+kp_n^{5/8}<N^3+kN^{5/8}$$
$$<N^3+N^2<(N+1)^3-1$$

令q_0爲一大於k^8的質數，則依據上面的輔理我們可找到一無窮多的質數列q_0，q_1，……其滿足

$$q_n^3<p_{n+1}<(q_n+1)^3-1 \quad \cdots\cdots(1)$$

令

$$u_n=q_n^{3^{-n}}，v_n=(q_n+1)^{3^{-n}} \quad \cdots\cdots(2)$$

則由(1)及(2)可得

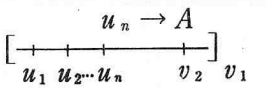
$$v_n>u_n，u_{n+1}>q_{n+1}^{3^{-n-1}}>q_n^{3^{-n}}=u_n \quad (3)$$

及
$$v_{n+1}=(q_{n+1}+1)^{3^{-n-1}}<(q_n+1)^{3^{-n}}$$
$$=v_n \quad \cdots\cdots(4)$$

因此$\{u_{n+1}\}$爲一漸增的數列，且其爲有界的，因而極限

$$\lim_{n\to\infty}u_n=A \quad \cdots(5)$$

存在。



接著密爾史氏證明了下面的定理，先此介紹一個定義及一記號。

定義：稱一個函數$f(x)$爲質數　生成表示函數，若對任何正整數n，$f(n)$爲質數。

$[R]$表示爲一不大於R的最大整數，例如$[3.15]=3$。

定理：設A爲輔理1中所定，則$f(x)=[A^{3^x}]$爲一質數生成表示函數。

證：由式(3)，(4)及(5)可得知

$$u_n<A<v_n$$

或
$$q_n<A^{3^n}<q_{n+1}$$

因而依記號[ ]的意義，立即得

$$[A^{3^n}]=q_n$$

於是我們證得$f(n)=[A^{3^n}]$皆爲質數。

讀完上面定理的結果，有些讀者或許會看出它的一個缺憾，就是這個製造大質數的函數是理論性的一個表示而已，眞正的值仍是無法得出，因爲我們不知A到底是多大？只知道它是$\lim u_n$的極限值（存在且爲有限的），所以要製造大質數仍只有靠硬來的籌法了。但有些具特殊形式的數中，較容易得出一些大的質數（這是下節要談及的）。

我們知當n充分大時n^3與$(n+1)^3-1$兩數之間必有一質數存在，和此現象似乎相衝突的是對任何給定的大的數ℓ我們可以建造一個區間，其長度爲ℓ，且在其間無一整數爲質數。譬如我們想找一百萬個連續的正整數，其皆爲合成數（非質數及1的整數），取$q(n)=(10^6+1)!+n$，則當$n=2$，3，4，……，1,000，0001時　爲合成數，讀者不妨試一下證明此一般性的結果，由前面所提及的英格翰氏定理知一個無質數的區間的大小與兩接連的質數間隔大小有關。值得一提的是由它可推出有名的 Bertrand 臆測：即在任何兩整數n及$2n$之間必有一質數，即

$$p_{k+1}<2p_k$$

另一有關質數分佈的性質是在區間$[n,2n]$內的質數數目，和$[1,n]$間質數數目的大小是同級的（order），此一事實可由質數分佈的漸近函數來說明，今以$\pi(x)$表示小於x的質數數目，則$\pi(x)\sim\dfrac{x}{\log x}$

故

$$\pi(2x)-\pi(x)\approx\frac{2x}{\log x+\log 2}-\frac{x}{\log x}$$
$$=\frac{2x}{\log x}\left(1+\frac{\log 2}{\log x}\right)^{-1}-\frac{x}{\log x}$$
$$\approx\frac{2x}{\log x}\left[1-\frac{\log 2}{\log x}\right]-\frac{x}{\log x}$$
$$=\frac{x}{\log x}-\frac{2x\log 2}{\log^2 x}$$

因而

$$\frac{\pi(2x)-\pi(x)}{\pi(x)}\to 1$$

3.質數的分佈

上節中對質數間的間隔或數目多少我們用到質數數目函數 $\pi(x)\sim\frac{x}{\log x}$ 一事實。我們現對質數此一重要性質作一些討論，今任一正整數在整個正整數集的分佈情況，如它不是質數就是合成數，好像沒什麼機率可言，嚴格講我們將可由質數數目的漸近函數 $\pi(x)$，得知對任一正整數其爲質數的概率爲 0，從我們熟悉的一事實開始：正整數列中每第 2 個數可被 2 整除，每第 3 個數可爲 3 整除等等。如何利用此簡單明瞭的現象去求得出近似 $\pi(x)\sim\frac{x}{\log x}$ 的結果，是我們在下面要探討的。這兒的討論並不嚴謹，但却由直覺的概率來說明，首先我們要求的是對一任意的正整數其可被質數 p_0 整除的概率爲 $1/p_i$，這是因爲由 1 開始每第 p_i 個數可被 p_i 整除，故一個數可被 p_i 整除之概率爲 $1/p_i$，不被 p_i 整除之概率就爲 $1-1/p_i$。我們不妨視被兩個不同質數整除是兩獨立事件（不過對所有的質數視其皆爲獨立是不可能的，但可認爲幾乎是獨立的；例如取一數可被 2 整除，不能幫助你去推測它是否能被 3 整除）。則對任一給定的整數 x 其不爲任何小於其本身的質數整除的概率爲

$$\omega(x)\approx\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdots\cdots$$

$$\approx\prod_{p_i<x}\left(1-\frac{1}{p_i}\right)\cdots\cdots\cdots\cdots\cdots\cdots(6)$$

此時的 x 也都表示一質數。但依據篩法的原則我們只該在上面乘積的式子中取小於 $\sqrt{x}$ 的質數 p_i，但由於如此得出的乘積在分析問題計算中並沒引起多大數值上的差別（x 很大時），所以我們可不計較此改進了。如果對式(6)兩邊取對數可得

$$\log\omega(x)\approx\sum_{p_i<x}\log\left(1-\frac{1}{p_i}\right)$$

這時如果我們同意依據 $\log(1+y)=y-\frac{y^2}{2}+\frac{y^3}{3}+\cdots\cdots$ 的展開式在 y 很小時取 $\log(1+y)\approx y$ 的近似值代入式(6)中就可得下面在 x 很大時的近似表示

$$\log\omega(x)\approx\sum_{p_i<x}\frac{-1}{p_i}\cdots\cdots\cdots\cdots(7)$$

我們仍想把此一表示化成一個更具體而簡潔的形式。參照 $\omega(x)$ 的定義及試想在上面式子(7)中項 $\frac{1}{n}$ 一其出現的概率爲 $\omega(n)$。此一想法使得我們可把式(7)改寫爲

$$\log\omega(x)\approx-\sum_{n=2}^{x}\frac{\omega(n)}{n}\cdots\cdots\cdots\cdots(8)$$

將此式子表成積分形式可得

$$\log\omega(x)\approx-\int_2^x\frac{\omega(n)}{n}dn\cdots\cdots\cdots(9)$$

爲了去掉負號作變換 $A(x)=\frac{1}{w(x)}$ 則由上式可得

$$\log A(x)\approx\int_2^x\frac{dn}{nA(n)}\cdots\cdots\cdots\cdots(10)$$

如果兩邊取微分，得

$$\frac{A'(x)}{A(x)}\approx\frac{1}{xA(x)}$$

即 $$A'(x)\approx\frac{1}{x}$$

因而形式上得

$$A(x)\approx\log x$$

於是

$$\omega(x)\approx\frac{1}{\log x}\cdots\cdots\cdots\cdots\cdots\cdots(11)$$

若視此爲質數密度的平均值，則對於小於或等於 x 的質數數目函數 $\pi(x)$，就可用下面的近似式來表式了：

$$\pi(x)\approx\int_2^x\frac{dx}{\log x}\approx\frac{x}{\log x}$$

4.有關質數檢驗的一些結果

要檢驗一個給定的正整數 n 是否爲質數，簡法是最直接的一法子，但它要用所有小於 $\sqrt{n}$ 的質數來除試（大約有 $2\sqrt{n}/\log n$ 個質數），這對大的 n，即使用電腦來計算也不切實際，我們也知道要建造大的質數也不是件容易的事，但總有些有耐心及聰明的人在那探求找大質數，以下我們就介紹一些有關的嘗試。

和費馬（Fermat，提出有名的費馬臆測的）及笛卡兒特（Descates）爲朋友的法人墨森尼（Mersenne）曾列了一個具形式 $M_n=2^n-1$，但爲質數的一個表，M_n 就稱爲墨森尼數，很明顯若 n 爲合成數，則 M_n 不可能爲質數，所以只有 n 爲質數時 M_n 才可能爲質數，已知的墨森尼質數有

$M_2=2^2-1=3$，$M_3=2^3-1=7$，

$M_5=2^5-1=31$，$M_7=2^7-1=127$，

$M_{13}=2^{13}-1=8191$，$M_{17}=2^{17}-1=131071$，

$M_{19}=2^{19}-1=524287$，

$M_{31}=2^{31}-1=2147483647$

M_{31} 爲質數此一事實是在 1750 年爲尤拉所證明，且爲 1876 年前所知的最大質數，而 $M_{11}=2^{11}-1=2047=23\times 89$，$M_{29}=2^{29}-1=536870911=233\times 1103\times 2089$ 所以不是對所有的質數 p，M_p 亦爲質數。在 1876 年魯克斯（E. Lucas）發現了一個法則間接地證明一個 M_p 數是否爲質數，他主要應用了以 M_p 爲模的整數環（ring），在此環中兩個數的加減乘和往常一樣，只是若結果的值不在 0 到 M_p-1 的範圍內時，以用 M_p 除該數所得的爲非負的剩餘；例如以 M_5 爲模的整數環中，$5\times 7\equiv 3\ (mod\ M_5)$ 的一些基本性質。他的結果被近代的賴莫爾氏（D. H. Lehmer）精簡爲下面的法則：

若 p 爲大於 2 的質數，定義 $L_1, L_2, \cdots$ 如下：

$$L_1=4，及對\ n\geqslant 2$$

$$L_n=L_{n-1}^2-2\ (mod\ M_p)$$

則 M_p 爲質數若且僅若

$$L_{p-1}\equiv 0\ (mod\ M_p)$$

我們看如何用上面法則來檢驗 $M_{11}=2^{11}-1=2041$ 是否爲質數？因 $L_1=4$，$L_2=14$，$L_3=194$，$L_4=788$，$L_5=701$，$L_6=119$，$L_7=1877$，$L_8=240$，$L_9=282$，及 $L_{10}=1736$，于是 $L_{10}\neq 0\ (mod\ 2047)$ 因而 M_{11} 不可能爲質數。

在同年（1876）魯克斯用上法檢驗 M_{127}，他計算了 $L_1, L_2, \cdots\cdots, L_{126}$，發現了 $M_{126}\equiv 0\ (mod\ M_{127})$，因而創下了打破保持了 75 年 M_{31} 爲最大質數的記錄，自從 1950 年開始進入了電腦的紀元後，利用魯克斯法則及二進位的計算原理，很多很大的質數陸續被得出。例如 1952 年證明了有 687 位數的 M_{2281} 爲質數，1971 年證明 M_{19937} 爲質數其有 6002 位數，在 1978 年由兩位 18 歲加州州立大學的學生共同證得具 6533 位的 M_{21701} 爲質數，最近 1983 年有人證得具 39,751 位數的 M_{132049} 爲質數（在證明此一事實中，曾利用 130249 + 1 爲 2 的冪次），如果讀者中有人想能名留千古，不妨試去找出一個比此數更大的質數，這可能比壯烈成仁還來得難些。

用上面敘述的魯克斯的法則來求得證一個數是否爲質數或許較難理解，我們想介紹他的一個較容易爲大家瞭解的定理如下：

定理（魯克斯定理）：設 m 爲大於 1 的整數，a 爲任一與 m 互質之數，若 $a^{m-1}\equiv 1\ (mod\ m)$，且對所有的（$m-1$）的因子 k 而言，$a^k\neq 1\ (mod\ m)$，則 m 必爲一質數。

證明：請參閱［1］，但爲方便讀者起見，我們在此作一概略的證明。假設 m 非爲質數，我們將導出矛盾，由 $\phi(m)$（Euler 函數）定義知 $\phi(m)<m-1$，但由於 a 與 m 互質，故由費馬 - 尤拉定理知

$$a^{\phi(m)}\equiv 1\ \ (mod\ m)$$

另一方面我們可證若 a ，m 互質且 $1<a<m$ ，若 $a^k \equiv 1 \pmod m$ ，則 k 與 $\phi(m)$ 不可能互質，于是 $(m-1)$ 及 $\phi(m)$ 最大公約數爲 $d>1$ ，即 d 爲 $m-1$ 的一因子，並且有兩整數 x ，y 使得 $(m-1)x+\phi(m)y=d$ ，于是

$$a^d \equiv a^{(m-1)x+\phi(m)y} \equiv (a^{m-1})^x (a^{\phi(y)})^y \equiv 1 \pmod m$$

因而 $(m-1)$ 有一因子 d 使得 $a^d \equiv 1 \pmod m$ 與假設不符，故 m 必爲質數。

但這個定理實際用來檢定一已知數 m 是否爲質數並不容易，因爲我們要利用到所有 $(m-1)$ 的因子，這對一個大的 m 而言，並不是件容易的事，但却可利用此定理來建造一些大質數，例如我們令 $m=2^n-1$ ，則 $m-1$ 的眞因子爲 2 ，2^2 ，2^3 ，……，2^{n-1} ，若由其中我們能試找出一個與 m 互質的數 a 像 3 ，5 ，7 ，……之類而且證得

$$a^{m-1} \equiv 1 \pmod m$$

及

$$a^{2^{n-1}} \not\equiv 1 \pmod{\ }$$

（注意因 $m-1=2^n-2=2(2^{n-1}-1)$）

則 m 必爲一質數

今舉一個實際計算探求 $m=257=2^8+1$ 是否爲質數的例子[1 ，119頁]。取 $a=3$ ，我們只要證 $3^{256} \equiv 1 \pmod{251}$ ，但 $3^{2^7}=3^{128} \not\equiv 1 \pmod{251}$ 。

$$3^{128} \equiv (241)^2 \equiv 256 \not\equiv 1 \pmod{257}$$

而 $$3^{256} \equiv (256)^2 \equiv 1 \pmod{257}$$

在[1]中也提到一個有趣的事實：即 m 若不是質數，則至少有一半以上的數從 2 ，3 ，……到 $m-1$ 不能滿足 $a^{m-1} \equiv 1 \pmod m$ ，這點說明若 m 爲質數，則從 2 ，3 ，……，$m-1$ 任取一數 a ，使得 $a^{m-1} \equiv 1 \pmod m$ 成立的機會相當大（至少是 1/2 ），但迄今仍無一簡便的法則找出一個與 m 互質的 a ，這是讀者可以試手腦的問題。

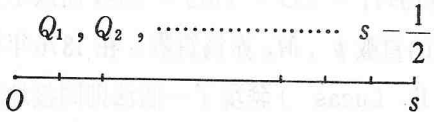
我們提供下面有關質數的一有趣性質，作爲本文之結束。

5.證明 $\sum_{i=1}^{\infty} \frac{1}{p_i} = \infty$（即所有質數級數之和爲發散的）

所有正整數之和：$1+2+\cdots\cdots+n+\cdots$ 顯然是無窮大的（即爲一發散級數），但如問所有正整數之倒數形成之級數 $\sum_{n=1}^{\infty} \frac{1}{n}$ 是否爲發散？解答此問題只要稍用些技巧就可達到，但如可利用級數與積分之關係，則也很容易證明此級數爲發散的，同樣的問題對所有的質數（讀者宜先證明此集合爲一無窮集的事實！），我們也有下面類似的結果，但它的證明就難得多了。它的證明也有幾種，但我們介紹的是一很初等的證明。

定理： 設 p_1 ，p_2 ，……p_k ，…爲所有質數且照遞增秩序排列的數列，則級數 $Q=\sum_{i=1}^{\infty} \frac{1}{p_i}$ 爲發散的，即 Q 的值爲無窮大。

證： 我們將用反證法，即設 Q 爲一收斂的級數並試由此導出矛盾，今假設 Q 收斂于一有限正數 s ，則由收斂值的定義，我們可找到一個整數 n ，使得 Q 的 k 項部分和 $a_{k-1}=\sum_{i=1}^{k-1} \frac{1}{p_i} < s-\frac{1}{2}$ ，而 $Q_k=Q_{k-1}+\frac{1}{p_k} > s-\frac{1}{2}$



（此處 $\frac{1}{2}$ 的選擇並無特別的意義，任何一個小的正數量都可）于是有

$$p_k = Q - Q_k = \frac{1}{p_{k+1}} + \frac{1}{p_{k+2}} + \cdots < \frac{1}{2} \quad (12)$$

就此 k ，我們對任何一正整數 x ，定義

$N(x,k)$ 爲所有不大於 x 的正整數，其不被任何大於 p_k 的質數整除者的集合，我們以 $|N(x,k)|$ 表集合 $N(x,k)$ 中元素的數

目，例如 $k=4$，則所有大於 p_4 的質數集 $=\{p_5, p_6, p_7, \cdots\}=\{11, 13, 17, 19, \cdots\}=T_4$。于是 $N(4, 10)=\{1, 2, 3, \cdots, 10\}$，故 $|N(4, 10)|=10$，而 $N(4, 15)=\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14\}$ 共 13 個元素（這是因爲由 1 到 15 中除了 11，13 外沒有一個正整數可能具有集合 T_4 中任一元素爲因子者。）。

今對任一正整數 z，我們都可先將它表成質因子的冪次的乘積：

$$z=p_1^{a_1}p_2^{a_2}\cdots\cdots p_t^{a_t}$$

其中 $a_1, a_2, \cdots\cdots, a_t$ 爲整數。若將所有具偶數冪次的項與將奇數冪次減 1 的項的乘積以 w^2 表之，其餘項的乘積以 v 表之，則

$$z=w^2v$$

其中 w，v 皆爲整數，v 中的質因子的冪次皆爲 1。

如 $z=2^7 3^4 5^3 7^5$，則 $z=(2^6 3^4 5^2 7^4)\cdot(2\times 7)=(2^3\cdot 3^2\cdot 5\cdot 7)^2(2\times 7)$ 現我們看什麼樣的正整數 y 可能屬於 $N(k, x)$，很顯然它們必須滿足：

(i) $y\leq x$，

(ii)所有 y 的質因子必來自 $\{p_1, p_2, \cdots, p_k\}$ 中。

依據上面兩個條件，我們先來估計一下 $|N(k, x)|$ 的大小。由於對任何 $y\in N(k, x)$，則有 $y=w^2v\leq x$ 及 $v\geq 1$，

故 $w\leq\sqrt{x}$。

而因 v 的因子來自 $\{p_1, p_2, \cdots\cdots, p_k\}$ 且皆爲 1 次冪，故所有可能爲 v 的數至多有 2^k 個，綜合以上的分析，我們得知在符合條件(i)，(ii)下，至多有

$$[(\sqrt{x})]\times 2^k \text{ 個 } y,$$

（其中 $[\alpha]$ 表不大於 α 的最大整數）

可能屬於 $N(k, x)$，于是

$$|N(k, x)|\leq 2^k\sqrt{x} \quad \cdots\cdots(13)$$

故對於任一正整數 x 由 1 到 x 的正整數中，其中 $|N(k, x)|$ 不可能被 $p_{k+1}, p_{k+2}, \cdots\cdots$ 中任一個數整除，剩下的共有 $x-|N(k, x)|$ 個，每個數都可能具有 $p_{k+1}, p_{k+2}, \cdots\cdots$ 中某些數爲因子。現從另一角度來估計 $x-|N(k, x)|$ 的大小，在 $\{1, 2, \cdots\cdots, x-1, x\}$ 中很明顯至多有 x/p_{k+1} 個數可被 p_{k+1} 整除，x/p_{k+2} 個數可被 p_{k+2} 整除，……等等。所以由此及(12)可得

$$\begin{aligned} x-|N(k, x)| &\leq \frac{x}{p_{k+1}}+\frac{x}{p_{k+2}}+\cdots\cdots \\ &\leq x\left\{\frac{1}{p_{k+1}}+\frac{1}{p_{k+2}}+\cdots\right\} \\ &< \frac{x}{2} \end{aligned}$$

因而

$$|N(k, x)|>\frac{x}{2} \quad \cdots\cdots(14)$$

于是由(14)，(13)兩式得

$$\frac{x}{2}<|N(k, x)|<2^k\sqrt{x} \quad \cdots\cdots(15)$$

並注意此不等式的導至與 x 的大小無關，特別取 $x=2^{2n+2}$ 時由(15)將得不等式：

$$2^{2n+1}<|N(k, 2^{2n+2})|<2^{2n+1}$$

此爲不可能。此一矛盾亦證明了 $Q=\sum_{i=1}^{\infty}\frac{1}{p_i}$ 必須爲發散才行。

研究問題：如果我們限制質數的形式結果如何呢？此似乎是個新的問題，具體的我們可以問：設 $\{p_k\}$ 爲具 $4n+1$ 形式的所有質數序列，則 $\sum_{i=1}^{\infty}\frac{1}{p_i}$ 是發散抑或爲收斂？

參考書目

1. 整數論及其應用，楊重駿、楊照崑編著，東華書局，1983。
2. M. R. Schroeder, "Number theory in Science and Communication" Springer-Verlag, 1984。
3. 數論在密碼上的應用（上）及（下），楊重駿、楊照崑，數學傳播第七卷，第三期 26，27，1983 年。