和光同塵

黃文璋
國立高雄大學應用數學系

1 棋盤裡的學問

在某項招生考試中, 有底下一道選擇題: 在一 8×8 的棋盤, 第一格放1個銅板(十元), 第二格放 2 個銅板, 第三格放 2^2 個銅板, 餘類推, 最後一格放 2^{63}個銅板。將這些銅板疊起來, 問下列何者最接近其高度? (A)紐約帝國大廈, (B)玉山, (C)喜馬拉雅山, (D)地球到太陽的距離。考完後, 有些反應是: 沒有計算機, 或不知紐約帝國大廈高度, 或不知一個銅板的厚度, 因此沒有辦法算。當然也有人 4個答案任猜一個。

六個十元銅板其厚度約 1 公分(事實上接近 1.1 公分)。而銅板數總共有

$$1 + 2^1 + 2^2 + \cdots + 2^{63} = 2^{64} - 1 = 18,46,744,073,709,551,615$$

個, 所以疊起來後之高度約爲 $(2^{64} - 1)/6$ 公分。即使你算不出 2^{64}, 但擁有計算機, 立即可得 $2^{64} \doteq 1.84467 \cdot 10^{19}$, 因此 $(2^{64} - 1)/6$ 約爲 $3.07445 \cdot 10^{18}$。即疊起來之高度約爲 $3.07445 \cdot 10^{13}$ 公里, 即約 30.7445 兆公里。而太陽與地球之距離約爲 $1.496 \cdot 10^8$ 公里, 故銅板總高度約爲太陽與地球間距的 20.5 萬倍。

一個銅板並不是太厚, 64 次方也不是太大的次方, 2 也是"合理"情況下的最小正整數底(底取爲 1 就沒什麼好討論的)。但居然這些銅板疊起來, 是如此的高, 超乎我們的想像。如果是將 2^{10} 個銅板疊起來呢? 2^{10} 是 $1,024$, 所以高度僅約 $1,024/6$ 公分 $\doteq 170.6$ 公分, 差不多是一個人的高度。很難相信2^{64} 個銅板(減去的 1 當然是不太重要)疊起來, 就變得這麼高。另外, 就算沒有計算機, 因

$$2^{64} = 2^4 \cdot (2^{10})^6 = 16 \cdot (1,024)^6 > 16 \cdot (10^3)^6 = 1.6 \cdot 10^{19},$$

且就以 10 個銅板高度應超過 1 公分計(這種估計能力總該有吧!), 則銅板總高度大於 $1.6 \cdot 10^{18}$ 公分 $= 1.6 \cdot 10^{13}$ 公里。不必用到計算機仍得到一難以想像的高度。

前述棋盤放銅板, 有一些不同的版本, 底下我們舉一流傳於印度的民間傳說(見Peterson (1990) p.196)。

在印度Shirim 王的時代, 其國師Sissa 發明了西洋棋 (chess) 以供宮廷遊樂。國王覺得怎麼會有這麼好玩的遊戲, 發明者眞是天才, 於是決定好好獎賞Sissa。獎賞方式是在棋盤上的每一空格各放一塊黃金送給Sissa。Sissa 婉謝國王的好意, 他不要黃金, 只要米, 方式是:在棋盤的第一格放一粒米, 第二格放兩粒米, 第三格放 4粒米, 第四格放 8 粒米, $\cdots$, 然後將 64 格中的米都送給他。

國王對Sissa 如此謙遜的要求感到很驚訝, 覺得Sissa 眞有古大臣之風。遂叫一侍衛拿一大袋米來, 依序放進 $1, 2, 2^2, 2^3, \cdots$ 粒米於各格中。到第12 格時, 米便已放不進格子中, 於是將米堆在棋盤旁。到第 20 格時, 袋中米便空了, 於是國王要侍衛去多拿幾袋。最後國王放棄了, 他終於理解到, 即使把皇宮中所有的米搬出來, 均不足以放滿 64 格棋盤。

事實上放滿 64 格的米夠全世界的人吃! 歷經銅板事件, 你大約不會認爲我們言過其實了。

設一碗飯以 $3,000$ 粒米計(要不要數數看?), 又設每人平均每日吃 5 碗飯(不至於低估吧!)。則全世界的 60 億人,一年共吃

$$3,000 \times 5 \times 365 \times 6 \cdot 10^9 = 3.285 \cdot 10^{16}$$

粒米。再以 $2^{64} \doteq 1.84467 \cdot 10^{19}$ 除以 $3.285 \cdot 10^{16}$，得可吃約 561.5 年。夠驚人的吧! 全世界的人吃此棋盤的米(該棋盤必須奇大無比), 可吃五百多年。底下附上一則三十年前的新聞(這是取自 61 年 9 月出版之"活的數學"(一本高中數學參考書)中, 該書作者蔡國琅加一標題"化理論爲實際", 可能是要讓讀者認同數學之重要), 一方面博君一粲(粲剛好是米部), 一方面顯示, 將米不斷加倍, 倒也並非象牙塔裡的遊戲。

數字魔術・駭人聽聞・秤肉粒米・匪夷所思

一粒米十斤肉 算到頭來吃大虧 三十天節節高 幾何級數嚇煞人

【台南訊】住在台南縣柳營鄉的翁圳受和李宗田互相約定, 以白米交換豬肉, 由翁圳受每日拿豬肉十台斤(折合新台幣二百廿元), 向李宗田掉換白米一粒(白米每日以累計倍數計算), 爲期一月。結果卅天下來, 白米累積倍數, 價值十二萬一千二百四十元, 豬肉價只需付出六千六百元。李宗田不甘損失,訴由台南地檢處以詐欺罪嫌提起公訴, 案移地院刑庭推事黃金富審結, 以罪證不足, 判決翁圳受無罪。

這兩個人是在今年六月十四日約定白米換豬肉。李宗田不懂得累計倍數法, 以爲白米換肉會有利可圖, 而於六月十五日在新營鎮環球旅社對面翁代書處, 各邀同保證人簽訂交換契約。第二天李宗田換算結果, 才發現吃了大虧, 於是向台南縣警察局提出告訴。

判決理由中說, 翁圳受與李宗田的約定交換豬肉, 雙方在定契約時有證人蕭明照、楊水勝, 立會人林慶田在座。簽約時李宗田出於自願, 第二天才發現卅日合計豬肉價只有六千六百元, 而白米累積卅日需給付五億三千六百八十七萬零九百十二粒, 折合重量爲三萬二千七百六十八台斤, 按時價每台斤三元七角計算, 達新台幣十二萬一千二百四十一元六角, 相差約廿倍之鉅, 於是拒絕收受豬肉價款,要求解約。

李宗田由他岳父母央託陳永松、楊振基、沈有田出面調解, 以一萬七千五百元賠償給翁圳受, 爲翁所接受, 調解亦因而成立。

判決理由中又說, 雙方口頭約定前, 既經翁圳受加以說明, 亦爲李宗田所同意, 雙方邀同證人, 立會人在翁代書處簽訂交換契約, 應無不愼重核

算後, 再事簽約的道理? 何況李宗田本人是碾米商人, 每日出入米糧不知凡幾, 對累計倍數計算法, 推說不清, 很難相信。當時以一粒米事小, 豬肉十台斤折價二百廿元事大, 而折豬肉以圖近利, 其過在他自己, 因而判決翁圳受無罪。(58 年 11 月 18 日聯合報)

最後, 附帶一提, 在 Chelminski(1999) 一文指出: 在二十世紀初, 英國律師埃德溫・安東尼計算過, 西洋棋頭十步的可能走法一共有 $169,518,829,100,544 \cdot 10^{15}$ 種。據估計, 在一局共走四十步的棋中, 可能的下子法有$25 \cdot 10^{115}$ 種—整個宇宙原子的數量僅是這個數字的一小部分。

小小 8×8 的棋盤, 居然有如此大的變化, 更不要說是通行於亞洲的 19×19 之圍棋盤了。

2 指數函數的威力

大家自中學起便學函數, 利用函數可描述各種複雜的概念。指數函數, 常被拿來作爲描述自然成長的模式。指數函數除了用途廣泛, 其成長之快速, 是極令人驚訝的。

什麼是指數函數呢?諸如

$$g(n) = 2^n, \quad n = 1, 2, 3, \cdots,$$
$$h(x) = e^x, \quad -\infty < x < \infty,$$

皆爲指數函數。一般而言

$$f(x) = a^x, \quad x \in I,$$

其中 a 爲某一正數, I 爲某一實數的集合, 便稱爲指數函數。

指數函數到底成長多快呢? 我們先看表 1 。

由表 1, 即使是 1.01 的 n 次方, 當 $n = 1,000$ 時,便有兩萬多了。如果人口年成長率維持在 1% , 則經 $1,000$ 年, 若無重大天災人禍, 人口將是兩

萬倍以上, 眞是驚人。再以 1.1^n 與 n^{10} 相比, 當 $n = 1,000$ 時, 前者便已較後者大很多了。如果你能找到一平均每年獲利有 10% 以上的投資方式, 則放一單位的錢, 經 30 年後本利和將達17 倍以上。這是家長爲其孩子設立創業基金之一好方式: 在小孩出生時便爲他找一個穩定的投資公司, 放一筆錢, 然後三十年不要去動它。

表1 不同函數增長之近似值

函數	$n = 10$	$n = 30$	$n = 100$	$n = 1,000$
$10n^2$	10^3	$9 \cdot 10^3$	10^5	10^7
n^{10}	10^{10}	$5.90 \cdot 10^{14}$	10^{20}	10^{30}
1.01^n	1.104	1.347	2.704	20959.1
1.05^n	1.628	4.321	131.50	$1.54 \cdot 10^{21}$
1.1^n	2.593	17.449	13780.6	$2.46 \cdot 10^{41}$
1.15^n	4.045	66.211	$1.17 \cdot 10^6$	$4.98 \cdot 10^{60}$
2^n	1024	$1.07 \cdot 10^9$	$1.26 \cdot 10^{30}$	$1.07 \cdot 10^{301}$

在第 1 節裡我們看到 2^{64} 就已是一天文數字, 其實比起我們在其他地方的討論, 這只是一微不足道的數。例如, 目前所知之完全數(perfect number)共有 39 個, 最小的是 $6 = 1 + 2 + 3$, 最大的是在西元 2001 年 12 月所發現的

$$2^{13,466,916}(2^{13,466,917} - 1),$$

其位數達 8,107,892 位(所謂完全數即一數等於其所有眞因數之和, 見黃文璋(1999)第一章)。此數若以 A4 紙來印, 如果一頁可印 4,000 位, 需 2,027 頁, 是一本巨著。諸位看, 是 2的一千三百多萬次方! 而這是不是已經是一夠大的次方呢? 我們曾討論費馬數(Fermat number,見黃文璋(1999)第四章):

$$F_k = 2^{2^k} + 1, \quad k = 0, 1, \cdots \text{。}$$

此數列成長快速。$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65,537$, 但 F_5 就已是$4,294,967,297$ 了。曾有人如此形容: 如果將 F_{73} 這個數印出來, 則全世界沒有一個圖書館容納得下。你可能難以相信。事實上 $F_{73} = 2^{2^{73}} + 1$, 而

$$2^{73} \doteq 9.44 \cdot 10^{21},$$

所以 F_{73} 是比目前所知之最大的完全數大很多。經由取對數, 可得 F_{73} 的位數約有$2.84 \cdot 10^{21}$ 。而一本 $1,000$ 頁的書約可印 $4 \cdot 10^6$ 位(每頁以印$4,000$ 位計)。故將 F_{73} 印出, 約需

$$\frac{2.84 \cdot 10^{21}}{4 \cdot 10^6} = 7.1 \cdot 10^{14}$$

本 $1,000$ 頁厚的書。這些書夠全世界的人每人分十幾萬本。

指數函數與多項函數成長速度之天壤之別, 可以下述微積分中的結果來形容: 對每一正整數 n ,

$$\lim_{x \to \infty} \frac{x^n}{e^x} = 0 \text{。} \tag{1}$$

當 n 很大時, 以 $n = 100$ 爲例, x^n 隨著 x 之增大, 成長很快, 如 $x = 10$ 時, 其值已達10^{100} 。但與 e^x 相比, 只要 x 很大, (1) 式告訴我們 x^n 幾乎可說是微乎其微。例如, $x = 1,000$ 時, $1,000^{100} = 10^{300}$ 有 301 位, 雖很大, 但此時 $e^{1,000}$, 其位數達 435 位。不論 n 多大(但固定), x^n 與 e^x 之比值, 隨著 x 之增大, 而趨近至 0 , 雖 $x \to \infty$ 時, $x^n \to \infty$ 。事實上, 除了 (1) 式, 我們尚有: 對 $\forall a > 1$,

$$\lim_{x \to \infty} \frac{x^n}{a^x} = 0 \text{。}$$

由此立即得對每一多項式 $P(x)$, 只要 $a > 1$,

$$\lim_{x \to \infty} \frac{P(x)}{a^x} = 0 \text{。} \tag{2}$$

不論 $P(x)$ 之次數多高, 而 a 只要比 1 稍大一些, 則 x 夠大後, a^x 均可將$P(x)$ 遠遠拋開。指數函數之威力實在是無以名之的。

由(1)式得, 對每一正整數 n,

$$\lim_{x\to\infty}\frac{e^{-x}}{x^{-n}}=0\text{。} \tag{3}$$

也就是 x 增大時, e^{-x} 下降至 0 的速度亦極快, 快過任一 x^{-n}, $n>0$。

一般多項式微分後, 次數會愈來愈低, 如 $(x^3)'=3x^2$, $(x^2)'=2x$, $(x)'=1$, 而 1 微分後是 0。但 e^x 微分後仍是 e^x, 這也是 e^x 的一特性。曾有個笑話, 有位數學教授因做研究過於投入, 有點神智不清, 遇到人便說"我要微分你"。有次他又說了, 結果對方說"我是 e^x"。自此後那位教授再也不敢微分別人了。

了解指數函數之成長快速的特性後, 要成爲一擁有一億元的富翁, 也非難事。

找到一每年投資報酬率達 15% 的投資方式, 每月固定投資 1 單位的錢, 則經 30 年的複利計算, 本利和將共有 $\sum_{i=1}^{360}a^i$, 其中 $a=1+0.15/12=1.0125$。因

$$\sum_{i=1}^{360}1.0125^i\doteq 7009.82\text{。}$$

而 30 年共投資 360 單位的錢, 故本利和約爲總投資額的 19.47 倍。現若每月投資一萬五千元, 則 30 年後之本利和約爲一億零五百十四萬元。至於共投資之本金, 則是五百四十萬元，差不多只是本利和之零頭而已。

只要持之以恆, 再加上投資正確, 人皆可以爲富翁。當然還要活得夠久。

我們常說上天有眼, 所以多行不義必自斃, 而有志者事竟成。這種上天有眼的想法, 也是基於指數函數之快速成長的原理。

譬如說作壞事, 假設第 i 次被發現的機率爲 p_i, 而每次被發現的事件假設爲相互獨立。則做了 n 次皆未被發現的機率爲 $\prod_{i=1}^{n}(1-p_i)$, 因此至少被發現一次的機率爲 $1-\prod_{i=1}^{n}(1-p_i)$。即使 p_i 都很小, 如果最小的 p_i 大於 0.01, 則

$$1-\prod_{i=1}^{n}(1-p_i)>1-(1-0.01)^n=1-0.99^n\text{。}$$

現若 $n = 100$, 則 $0.99^{100} \doteq 0.36603$, 而 $1 - 0.99^{100} \doteq 0.63396$ 。換句話說, 雖每次被發現的機率不大, 但在 100 次內被發現的機率大於0.63396 。至於若 $n = 1{,}000$, 因 $0.99^{1{,}000} \doteq 0.000043171$, 故被發現的機率大於 0.99995, 已算是很接近 1 了 。

若壞事只做一次可能不易被發現 。只是多半人食髓知味, 一而再再而三, 終有失手的一天 。清朝的一代奇才, 曠世風流的紀曉嵐, 著有"閱微草堂筆記", 是部文言短篇小說集, 多寫神異鬼怪故事 。在該書卷五, 作者藉一害人的故事說明"君子之於小人, 謹備之而已, 無故而觸其鋒, 鮮不敗也 。"對於小人不妨遠遠避開, 並非眞相信上天有眼, 但既然觸其鋒也沒有益處, 也就不用傷神管他 。小人行事往往愈來愈大膽(p_i 愈來愈大), 因此事跡敗壞的日子也不見得會太久(n 不用太大) 。

3 讓東方不敗倒下

武俠世界裡, 代代有高手出現, 在技不如他之下, 聯手以對抗之, 爲一常見的方式 。不世出的奇才張三丰, 似也瞭解指數函數之威力, 並藉此設計出一聯手的陣仗:

在倚天屠龍記中(見金庸 (1996a) pp.383-384), 張三丰在大江之濱, 凝望蛇龜二山, 苦思三晝夜後, 猛地省悟,哈哈大笑, 回到武當山, 將七名弟子叫來, 每人傳了一套武功 。這七套武功分別行使, 固是各有精微奧妙之處, 但若二人合力, 則師兄弟相輔相成, 攻守兼備, 威力立即大增 。若是三人同使, 則比兩人同使的威力又強一倍, 四人相當於八位高手, 五人相當於十六位, 六人相當於三十二位 。到得七人齊施, 猶如六十四位當世一流高手同時出手 。當世之間, 算得上第一流高手的也不過寥寥二三十人, 那有這等機緣, 將這許多高手聚集在一起?

張三丰這套武功由眞武大帝座下龜蛇二將而觸機創制, 是以名之爲"眞武七截陣" 。他當時苦思難解者, 總覺顧得東邊, 西邊便有漏洞, 同時南邊北邊, 均予敵人以可乘之機, 後來想到可命七弟子齊施, 才破解了這個難題 。

聯手, 成爲要對付武功如東方不敗之大高手的好方法。多一人聯手, 威力加倍, 這樣的聯手設計, 可說是極成功的。

我們再看兩個成功的聯手例子。

在神鵰俠侶中(見金庸 (1996b) pp.563-566), 楊過與小龍女, 一使全眞劍法, 一使玉女劍法, 雙劍合璧, 威力立即大得驚人。不但能相互呼應配合, 所有破綻全爲旁邊一人補去, 厲害殺著卻是層出不窮, 打得金輪法王招架不及, 落荒而逃。

在倚天屠龍記中(pp.1460-1576), 少林寺的渡厄、渡劫及渡難, 三僧坐了三十餘年的枯禪, 心意相通, 一人動念, 其餘二人立即意會, 以三根黑索, 組成金剛伏魔圈。張無忌雖身懷九陽神功, 乾坤大挪移及太極拳等三大神功, 卻未能攻破。後邀了明教光明左使楊逍及外公殷天正相助, 亦仍無效, 且殷天正還耗竭身亡。第三次與周芷若以二敵三, 也只能打個平手。

聯手要奏效, 參與的人武功往往也要不錯, 並且要能"相互呼應配合", 或"心意相通"。有些聯手的武功, 威力雖大, 其中卻隱含極大致命傷。例如, 全眞教中最上乘的玄門功夫乃是天罡北斗陣。此陣當敵人來攻時, 正面首當其衝者不用出力招架, 卻由身旁陣友側擊反攻, 猶如一人身兼數人武功, 威不可當。全眞七子本來武功便不低, 即使"劉處玄與王處一同時發掌, 二人掌力合流, 一陰一陽, 相輔相成, 力道竟是大得出奇, 遠非兩人內力相加之可比", 何況七人佈下天罡北斗陣! 此陣對付高手梅超風, 將她牢牢的困在陣中, 對付梅超風的師父東邪黃藥師, 也能打成平手。但西毒歐陽鋒趁他們僵持不下時, 攻擊譚處端, 七人死了一個, 此陣便破了(見射鵰英雄傳, 金庸 (1996c) pp.1022-1033)。可見此陣雖厲害, 號稱"練到爐火純青之時, 七名高手合使, 無敵於天下", 但只要一人被擊潰, 全陣瓦解, 這種陣法的威力未免要大打折扣。甚至若不是由全眞七子主持陣法, 而換成武功較差者, 則只消佔到了北極星位, 便能"以主驅奴, 制得北斗陣縛手縛腳, 施展不得自由"。我們再引一段, 以顯示此陣法是無法對抗眞正的大高手。

郭靖帶著楊過上終南山, 全眞教因誤會, 由一群小道士擺出一天罡北斗陣圍攻他, 卻被郭靖輕易地佔據北極星位, 因而全陣在郭靖控制之下,

七個道士隨著郭靖, 忽而快跑, 忽而緩步, 忽而躍上樹幹。即使後來再以十四個天罡北斗陣共九十八人聯手, 也是被郭靖帶著四五十個人摔入水中, 另數十人踏在別人背上(見神鵰俠侶, 金庸 (1996b) pp.107-121)。

一般而言聯手是要發揮"力道遠非內力相加可比"之效。在碧血劍(金庸(1996d) pp.208-243)中, 溫氏五老的的五行陣本來還算圓轉渾成, 不露絲毫破綻。此陣法令人喪膽之處, 在於敵人入圍之後, 不論如何硬闖巧閃, 五老必能以厲害招數反擊, 一人出手, 其餘四人立即綿綿而上, 不到敵人或死或擒, 永無休止。五老招數互爲守禦, 步法相補空隙, 臨敵之際, 五人猶如一人。不過五人中有一人走錯了腳步, 或是慢得一慢便破了。雖然溫氏五老"是熟的, 包管閉了眼睛也不會走錯", 但碰到高手, 或換年輕的弟子擺陣, 就沒那麼樂觀了。所以與天罡北斗陣有類似的弱點。袁承志由金蛇郎君所寫的金蛇秘笈中, 本已獲知如何破五行陣, 但五老又創一個八卦陣(有 16 人), 置於五行陣外圍, 將所有空隙填得密密實實。袁承志初以爲五行陣外又有八卦陣, 要破此陣,變成難上加難。但他只看了十六人轉幾個圈子, 已了然於胸"敵人若是破不了五行陣,何必再加一個八卦陣? 若是破得了五行陣, 八卦陣徒然自礙手腳。溫氏五老的天資見識, 和金蛇郎君果然差得甚遠。看來這五行陣也是上代傳下來的, 諒五老自己也創不出來。他們自行增添一個陣勢,反成累贅。金蛇郎君當年若知溫氏五老日後有此畫蛇添足之舉, 許多苦心的籌謀反可省去了"。想通後動手,先將五行八卦陣弄得大亂, 溫氏眾人, 陣中不見敵人, 來來去去的盡是自己人。袁承志舉手之間先破八卦陣, 再破五行陣。五老之大哥溫方達見本派這座天下無敵的五行八卦陣, 竟被這小子在片刻之間, 如摧枯拉朽般一番掃蕩, 登時鬧了個全軍覆沒, 一陣心酸, 竟想在柱子上一頭撞死。

畫蛇添足的結局竟是如此, 眞令人心酸。五行陣加八卦陣, 不但沒有發揮"力道遠非兩陣相加可比"之效, 反成作繭自縛。學武之傷心莫過於此, 難怪溫方達想一頭撞死。當天資見識均有限時, 就不要異想天開。這也是爲何在歷史上我們對蕭規曹隨會如此肯定。雄才大略的領導人固然不易得, 即使能審時度勢,信奉蕭規曹隨者亦是罕見。溫氏五老只是在祖宗留下的資產蛇足一番, 就已弄個全軍覆沒。有些庸才一旦掌權, 便迫不

及待地揚棄先人的五行陣, 自創八卦陣, 其後果的不堪實不難預料。這道理人人能懂, 難就難在庸才之所以爲庸才, 就是連自己是庸才都不知道, 讓我們再度向曹參致敬。

完全數愈來愈巨大, 那該如何找尋呢?當然是要藉助計算機, 目前所知的完全數皆爲偶數, 而偶完全數必呈 $2^{n-1}(2^n-1)$ 的型式, 其中 n 爲一正整數, 且 2^n-1 爲一質數, 這種型式的質數, 稱爲梅仙尼質數(Mersenne prime)。找偶完全數便與找梅仙尼質數是等價的。而我們又知道 2^n-1 要爲質數, 則 n 必須爲質數。所以找偶完全數已有了方向, 只要依序對質數n,看 2^n-1 是否爲質數即可。而這工作又只需要交給計算機。那爲何至今只知道39個呢?

目前對一任給的兩百位的數, 若採用試除法, 則即使窮地球的壽命, 往往也極難判定其是否爲質數。你可能覺得我們言過其實, 說明如下:假設計算機平均一秒鐘可做一億次除法, 則一年約可做 $3.1536\cdot 10^{15}$ 次。而檢驗一兩百位的數是否爲質數, 有時要做到近 10^{100} 次試除, 換句話說, 約要 $3.17\cdot 10^{84}$ 年。而估計地球的壽命不過約 50 億$(5\cdot 10^9)$年而已。就算計算機速度增快,一秒鐘可做一兆(10^{12})次除法, 仍要約 $3.17\cdot 18^{80}$ 年。所以要設計發展出較有效的方法, 以大幅減少計算機除的次數, 否則光增快計算機的速度是徒然無功的。

由上討論知, 當質數 n 很大時, 要來驗證 2^n-1 是否爲一質數, 爲一極艱難的工作。處理兩百位的數就已不得了了, 何況是處理數百萬位的數。超級電腦也只能瞠乎其後了, 發揮不了太大的功能。

聯手! 我們看聯手能否發揮功能。

美國的 Woltman ,在西元 1996 年 1 月成立了一 GIMPS(Great Internet Mersenne Prime Search)的組織。他設立了一特別的網站, 免費提供一程式, 以利用個人電腦的剩餘時間, 來尋找梅仙尼質數。他的程式藉助所謂 Lucas-Lehmer 質數測試法, 爲一檢驗一數是否爲質數之有效方法。至西元 1999 年, 全世界已有超過 12,600 人加入他們的組織。經由網際網路, Woltman 將參加者的力量結合起來, 每位參加者, 均可獲得已知結果的資料庫(database), 一旦參加者選定一檢驗的整數區域, 便須告知 Woltman ,

以使其他搜尋者不用重複地找。Woltman 的程式後來被 Kurowski 改進, 使更易使用。經由 Kurowski 的公司 Entropia. Com. Inc. 的 PrimeNet 系統, 將全世界超過 21,500 部個人電腦整合起來, 每秒鐘可做7,200 億以上的計算。若沒有這套系統, 是無法找尋如此巨大的質數。在西元2001年 12 月, 他們第 5 次成功地找到新的梅仙尼質數, 因此一個新的完全數也誕生了。目前最大的 5 個完全數皆是此組織所找到的。

在西元 1999 年初, 電子邊界基金(Electronic Frontier Foundation)提出獎賞: 首位發現百萬位以上之質數者可獲 5 萬美元, 首位發現千萬位以上之質數者可獲10 萬美元, 依此類推,獎金最高至 25 萬美元。歷史上, 一新的梅仙尼質數的產生, 往往也是一最大質數產生的里程碑。讀者諸君不妨加入此一尋找梅仙尼質數的陣容。說不定還可致富呢!

GIMPS 組織, 可說充分發揮"相互呼應配合"及"心意相通"之效, 而且"力道遠非內力相加可比", 而參加者只要有個人電腦, 且僅須利用剩餘時間。因此沒有天罡北斗陣的缺點: 參加者須武功高強, 且一人被擊潰便全軍覆沒。

遇到如東方不敗之類的巨大的數, 結合分散在世界各地, 只需擁有最基本武器(個人電腦)的小兵, 居然可發揮如此大的功能, 這可說是武俠世界裡都見不到的成功聯手情況。但這並非科學界裡唯一的聯手成功的例子。

利用大數之難以分解的特性, 美國麻省理工學院(Massachusetts Institute of Technology, 簡稱 MIT)的幾位數學家 Rivest, Shamir 及 Adleman, 於西元 1977 年提出一所謂公開鑰匙密碼法(Public-Key Cryptography), 又稱 RSA 法, 爲目前最安全的密碼技術。

在提出 RSA 法後, MIT 的研究人員將一個代表一訊息之 128 位數編碼, 欲破此碼, 須先分解一 129 位數。MIT 的研究小組並懸賞 100 美元給第一位破譯者。

這 100 美元看起來是很安全的, MIT 研究小組估計要花 23,000 年才可能分解該129 位數。雖 100 美元似乎不是一筆很大的錢。但你要不要估計經過 23,000 年後, 100 美元成爲多少?若以年利率 6% 的複利計, 爲一

筆有 585 位之鉅款, 夠嚇人的吧! 也許計算機速度的增快, 可使破解的時間降低一兩個位數, 但仍是很安全的 。

可惜人算不如天算, 這個叫陣的 RSA 數經過 17 年, 便敗下陣來, 而將它打下擂台的計算, 全部只花不到一年的時間 。由一批約六百餘位因數分解迷所組成的鬆散組織, 分散在 20 多個國家, 經過 8 個月的努力, 於西元 1994 年 4 月, 成功地將該129 位數, 分解成一 64 位的質數與一 65 位的質數之積, 因而破譯密碼 。

之所以能這麼快便成功, 一方面是靠今日網際網路的發達, 一方面是靠新技術, 所謂二次篩法(Quadratic sieve), 以加速找因數的工作 。而這兩項技術的威力, 都是在西元 1977 年提出 RSA 法時所未想到的 。

有關上述挑戰 RSA 數的過程之報導, 可見 Cipra(1996) pp. 90-99, 倪錄群譯(1997)爲其譯稿 。

除了廣邀志同道合的好漢聯手外, 發展有效率的方法或技術, 爲擊敗科學中的東方不敗之關鍵, 否則就算是參與的人多也不見得就能奏效 。

4 無記憶性質

Cundy(1966)說他曾自收音機中獲知, 知更鳥(robin)平均可再活 1.2 年, 而與牠現在年齡無關 。假設某日你與一朋友相約至海邊垂釣 。朋友的釣魚技術與你相彷 。你抵達約定地點時, 朋友已先到了 30 分鐘, 但尚未釣上魚 。你是否會覺得朋友較你有更大的機會釣上第一條?很可能不會 。原因是: 魚應不至於同情朋友已枯坐了 30 分鐘, 而讓他先釣上一條 。此正如丟一銅板, 直至出現一正面才停止 。如果連丟十次皆得反面, 那就是白丟了, 以後的發展就像重新丟一樣, 而不會是因已丟那麼多次, 所以正面快出現了 。

我們常說歲月催人老 。但如前述釣魚的例子, 有些事物, 歲月不會使其衰老, 此物還會"活"多久, 與一新生代相彷 。此物之"死亡", 似乎都是因爲某一突然的事件發生, 而非逐漸衰退 。亦即若此物已活了 a 單位的時間, 則會再活至少 b 單位的時間之可能性, 與 a 無關 。此物彷彿會忘記它

自己已活了多久。此性質便稱爲無記憶性質(memoryless property)。

年輕人通常不希望壽命有無記憶性質, 老年人一般而言, 就很希望壽命有無記憶性質。不過在戰場上, 對那些在第一線的士兵, 到底還能活多久, 很可能就有無記憶性質了。

正式地說, 一隨機變數 X, 稱爲在某一實數的子集合 S 中有無記憶性質, 若滿足對 $\forall a, b \in S$,

$$P(X > a+b \mid X > a) = P(X > b) \text{。} \tag{4}$$

例1. 連續丟一出現正面機率爲 $p > 0$ 之銅板, 直至得到一正面才停止, 令X表總共的投擲數。則 X 有自 1 開始, 且參數爲 p 之幾何分佈 (geometric distribution), 以 $Ge(p)$ 表之, 即

$$P(X = k) = p(1-p)^{k-1},\ k = 1, 2, 3, \cdots \text{。} \tag{5}$$

則

$$P(X > k) = \sum_{i=k+1}^{\infty} p(1-p)^{i-1} = (1-p)^k \text{。} \tag{6}$$

因此

$$P(X > a+b \mid X > a) = \frac{P(X > a+b)}{P(X > a)} = \frac{(1-p)^{a+b}}{(1-p)^a} = P(X > b) \text{。}$$

即若取 $S = \{1, 2, 3, \cdots\}$,則對 $\forall a, b \in S$,(4)式成立。因此自1 開始之幾何分佈, 有無記憶性質。

有位婦人很想生個女兒, 她已連生 7 個兒子, 朋友都鼓勵她再生, 因爲那有運氣那麼壞的? 你現在知道鼓勵她再生的人是沒有道理的, 因若令 Y 表得到一女兒前, 所生之兒子數, 則 Y 有自 1 開始且參數爲 $1/2$ 之幾何分佈。由於 Y有無記憶性質, 所以 $P(Y > 7+b \mid Y > 7) = P(Y > b)$, 因此那已生的7 個兒子, 並無助於使她更快獲得一女兒。

例2. 指數分佈(exponential distribution)亦有無記憶性質。設 Y 有參數λ之指數分佈, 以 $\mathcal{E}(\lambda)$ 表之, 即 Y 之機率密度函數 (probability density

function,簡稱 p.d.f.)爲

$$f(x) = \lambda e^{-\lambda x},\ x > 0\ 。 \tag{7}$$

則因

$$P(Y > x) = \int_x^\infty \lambda e^{-\lambda u} du = e^{-\lambda x},\ x > 0\ 。 \tag{8}$$

故

$$\begin{aligned} P(Y > a+b \mid Y > a) &= \frac{P(Y > a+b)}{P(Y > a)} \\ &= \frac{e^{-\lambda(a+b)}}{e^{-\lambda a}} = e^{-\lambda b},\ \forall a, b > 0\ 。 \end{aligned} \tag{9}$$

基本上, 幾何分佈及指數分佈爲僅有的兩個具有無記憶性質之分佈。證明見黃文璋(1995)第一章第 6 節。我們發現此二分佈之存活函數(survival function)皆爲指數函數。在此對一隨機變數 X,

$$\overline{F}(x) = 1 - F(x) = P(X > x),\ x \in R,$$

稱爲其存活函數, 其中 $F(x) = P(X \le x)$ 爲 X 之分佈函數(distribution function)。存活函數又稱尾部機率函數(tail probability function)。若 X 表某物之壽命, 則存活函數 $\overline{F}(x)$ 給出此物會存活至少x 單位時間之機率。在諸如機器可靠度(reliability)的探討, 醫學上某種疾病之壽命的探討, 精算學的(actuarial)探討,通常都是對存活函數較有興趣。

指數函數且底小於 1 (幾何分佈底爲$(1-p) < 1$,指數分佈底爲 $e^{-\lambda} < 1$, 分別見 (6) 式及 (9) 式), 表 $k \to \infty$ (或 $x \to \infty$ 時), $P(X > k)$ (或 $P(Y > x)$)趨近至 0 之速度很快。換句話說, 隨著k 之增大(或 x 之增大), X 要大於 k (或 $Y > x$)愈來愈不容易, 其難度, 我們之前以指數函數的威力來形容。但壽命之存活函數若爲指數函數, 則壽命便有無記憶性質, 能再活多久, 不受現有年齡的影響。此物彷彿隨時保持一全新狀態。這眞是一奇特的現象。起初由其存活函數趨近至 0 的速度很大, 我們會以爲此物不易活很久, 沒想到卻隨時像新的一樣。

國內數學界有位資深且爲人敬重的前輩, 一向語多詼諧。他個子不高, 嘗言"身高要看從那裡量, 從天花板量起我最高"。頭頂距天花板的距離, 的確他最遠。年齡亦是如此, 一向我們是量距出生時之歲月長。但距死亡日還多久也是一不錯的比法: 距死亡日較久的便算較年輕。壽命若有幾何分佈或指數分佈, 依此新算法,便永遠像是松柏長青。要知駐顏有術不如青春永駐, 這是恭維人時不可不留意的。

5 波松過程

假設在時間 $t = 0$ 裝了一新燈泡, 用了 X_1 的時間燈泡壞了, 立即換新(更換的時間假設可忽略), 再用了 X_2 的時間, 第二個燈泡又壞了, 於是立即更新, 如此繼續進行下去。若燈泡的壽命$X_1, X_2, \cdots$ 假設爲獨立且有共同分佈(independent and indentically distributed, 簡寫爲 i.i.d.), 且令 $A(t)$ 表至時間 t 所共更換的燈泡數(在 $t = 0$ 裝的那一個不算, 所以 $A(0) = 0$)。則 $\{A(t), t \geq 0\}$ 便稱爲一更新過程 (renewal process)。

更新過程的例子很多, 只要是依序觀察某特定事件, 事件發生之間距設爲 i.i.d. , 則至時間 t 共發生的次數 $A(t), t \geq 0$, 便構成一更新過程。

若事件發生之間距 X_i, $i \geq 1$,以指數爲其共同分佈, 即設存在一$\lambda > 0$,使 $P(X_i \leq x) = 1 - e^{-\lambda x}$, $x > 0$,則 $\{A(t), t \geq 0\}$ 便稱爲一參數爲 λ 之波松過程(Poisson process)。波松過程爲一點過程(point process , 如果發生一事件, 便在時軸上標一點, 在某時區中發生幾個事件, 便是在該時區中有幾個點), 也是一種計數過程(counting process ,計算至時間 t 共發生幾個事件)。

爲何以波松對此過程命名呢?

令 $S_n = X_1 + X_2 + \cdots + X_n$, $n \geq 1$,表第 n 個事件之發生時刻, $S_0 = 0$,若 X_i 以 $\mathcal{E}(\lambda)$ 爲其共同分佈時, 如果你機率論學得夠好, 當知 S_n 有 $\Gamma(n, 1/\lambda)$ 分佈。否則由求 S_n 之拉普拉斯轉換(Laplace transform)

$$\begin{aligned} E(e^{-tS_n}) &= E(e^{-t(X_1+X_2+\cdots+X_n)}) \\ &= (E(e^{-tX_1}))^n \end{aligned}$$

$$= \left(\frac{\lambda}{\lambda+t}\right)^{n} = \left(1+\frac{t}{\lambda}\right)^{-n},$$

亦得 S_n 確有 $\Gamma(n, 1/\lambda)$ 分佈。即 S_n 之 p.d.f. 爲

$$f(x) = \frac{\lambda^n x^{n-1} e^{-\lambda x}}{\Gamma(n)} = \frac{\lambda^n x^{n-1} e^{-\lambda x}}{(n-1)!},\ x > 0\ 。 \tag{10}$$

反覆利用分部積分(integration by parts)可得

$$P(S_n > t) = \int_t^{\infty} f(x)dx = \sum_{i=0}^{n-1} \frac{(\lambda t)^i e^{-\lambda t}}{i!},\ t > 0\ 。 \tag{11}$$

現因事件 $[A(t) = n]$ 與 $[S_n \le t < S_n]$ 等價, 故

$$\begin{aligned} P(A(t) = n) &= P(S_n \le t < S_{n+1}) \\ &= P(S_{n+1} > t) - P(S_n > t) \\ &= \frac{(\lambda t)^n e^{-\lambda t}}{n!},\ \forall t \ge 0,\ n = 0, 1, 2, \cdots\ 。 \end{aligned} \tag{12}$$

即得證對一參數爲 λ 之波松過程, 至時間 t 發生的個數 $A(t)$, 有參數 λt 之波松分佈。這是此過程以波松命名的原因。

對任二 $t,\ s > 0$, $A(t+s) - A(t)$ 表波松過程在區間 $(t, t+s]$ 中所發生的事件個數。可以證明 $A(t+s) - A(t)$ 有參數 λs 之波松分佈。也就是說 $A(t+s) - A(t)$ 之分佈只與區間長度 s 有關, 而與其位置無關。而且 $A(t+s) - A(t)$ 還與 $A(t)$ 獨立呢! 甚至對任意 $n \ge 2$, 及 $0 \le t_0 < t_1 < \cdots < t_n$, $A(t_n) - A(t_{n-1})$, $A(t_{n-1}) - A(t_{n-2}), \cdots, A(t_2) - A(t_1)$, $A(t_1)$, 此 n 個隨機變數相互獨立。即在不相交區間 $[0, t_1], [t_1, t_2], \cdots, [t_{n-1}, t_n]$ 中之事件發生個數相互獨立, 這是波松過程一重要的性質, 稱爲獨立增量(independent increments)性質。

在很多實際的情況中, 如釣魚、交通事故、意外事件及至醫院看病等, 由於至下一事件的等待時間往往有無記憶性質, 因此二事件的間距便有指數分佈, 從而至時間 t 發生的事件數(選一起始點定爲時間 0), 便形成一波松過程。

我們也可以另一方式來說明爲何波松過程處處可見。指數分佈的無記憶性質導致在任一小區間$[t, t+h]$ 中, 會發生一事件之機率爲

$$\begin{aligned} P(X \le h) &= 1 - e^{-\lambda h} \\ &= 1 - (1 - \lambda h + o(h)) \\ &= \lambda h + o(h),\ h \to 0, \end{aligned}$$

其中 X 表一有 $\mathcal{E}(\lambda)$ 分佈之隨機變數, 此處用到當 h 很小時

$$e^{-\lambda h} = 1 - \lambda h + o(h),$$

又 $o(h)$ 爲某一 h 的函數(o 讀爲little-oh), 且滿足

$$\lim_{h \to 0} \frac{o(h)}{h} = 0 \text{。}$$

換句話說, 當 h 很小時, $o(h)$ 與 h 相比更小。很多點過程有這種性質: 在一小區間發生一個點(或說一事件)的機率約與此區間長成正比(除了一更小的誤差), 而與此區間的位置無關。至於會發生兩個以上的點之機率則是極微小, 以$o(h)$表之。注意 $o(h)$ 並非指一特定的函數, 諸如 h^2, $h^{3/2}+h^2$ 皆爲 $o(h)$, $h \to 0$。直觀上來看, 在一區間 $[0, t]$ 中會發生幾個點便有波松分佈(利用二項分佈趨近至波松分佈的結果), 且在不相交區間中各發生幾個點爲相互獨立。波松過程便產生了。

無記憶性質, 事件發生的均勻性(發生機率只與區間長度有關, 且區間較短時, "差不多"是線性的), 此二不少現象之發生會具有的特性, 使得波松過程成爲一出現極頻繁的計數過程。

關於波松過程的討論, 以及更一般的波松過程之定義, 可參考黃文璋(1995)第五章。

6 等待時間之詭論

設有一參數爲 λ 之波松過程 $\{A(t),\ t \ge 0\}$, 譬如說, $A(t)$ 表至時間 t 共換了幾個燈泡。則在時間 t 正在使用的那一燈泡還可用多久呢? 由指數分

佈之無記憶性質, 我們知道該燈泡之剩餘壽命(residual life 或說remaining life), 仍爲有參數 λ 之指數分佈, 與一般正常的間距一樣。至於該燈泡已經用多久了呢? 明顯地, 其已經用的時間(稱做現在壽命(current life)), 不能超過 t 。若以 δ_t 表現在壽命, 則易見只要 $x < t$, 則 $\delta_t > x$, 若且唯若在區間 $(t-x, t]$ 中, 沒有換燈泡, 而此機率爲$1-e^{-\lambda x}$ 。故

$$P(\delta_t \le x) = \begin{cases} 1-e^{-\lambda x} & , \ 0 \le x < t, \\ 1 & , \ x \ge t \text{。} \end{cases} \tag{13}$$

當 $x \ge t$ 時, 由於必有 $\delta_t \le t$, 故 $P(\delta_t \le x) = 1$ 。一般我們用 γ_t 表在時間 t 正在使用的那一燈泡之剩餘壽命。

於時間 t 正在用的那一燈泡之總壽命 $\beta_t = \gamma_t + \delta_t$, 其期望值爲

$$\begin{aligned} E(\beta_t) = E(\gamma_t) + E(\delta_t) &= \frac{1}{\lambda} + \int_0^t x\lambda e^{-\lambda x} dx + tP(\delta_t = t) \\ &= \frac{1}{\lambda} + \frac{1}{\lambda}(1-e^{-\lambda t}) \text{。} \end{aligned} \tag{14}$$

不少人都有下述經驗: 等公車時, 別人的車子總是先到, 自己要搭的卻老不來, 站牌上明明寫15 分鐘一班, 但幾乎每次都差不多要等滿 15 分鐘, 難道每次到站牌, 是公車剛好才開走嗎?

我們先看一所謂"等待時間之詭論"(waiting time paradox)。假設公車依一參數爲λ之波松過程到站, 某人在時間 t 抵達此站。若以 γ_t 表至下一班公車來所需之等待時間(即前面所提的剩餘壽命), 我們想求 γ_t 之期望值$E(\gamma_t)$ 。則可能會有下述二矛盾的答案。

(a) 由指數分佈之無記憶性質, 導出等待時間之分佈應與自己到站牌的時間無關, 因此

$$E(\gamma_t) = E(\gamma_0) = \frac{1}{\lambda} \text{。}$$

(b) 由於某人抵達站牌之時間, 爲前後兩班車到站之區間中任意的一個點, 由對稱性知, 等待時間之期望值, 應大約是相鄰兩班車抵站牌之時間差距期望值之半, 即 $1/(2\lambda)$ 。

這兩種論點看起來似乎皆很合理, 不過由之前所求出的波松過程之剩餘壽命的分佈, 我們知道 (a) 是對的。但 (b) 之錯誤何在?

原因爲雖然對一參數 λ 之波松過程, 每一到達間距 X_i 皆有相同之指數分佈, 且期望值爲 $1/\lambda$, 但若對一固定的 $t > 0$, 找出 X_k 使得

$$\sum_{i=1}^{k-1} X_i < t \leq \sum_{i=1}^{k} X_i,$$

則此 X_k 之期望值, 並不等於 $1/\lambda$ 而是會大於 $1/\lambda$ 。且 $t \to \infty$ 時, 由 (14) 式知, 此期望值趨近至 $2/\lambda$, 而 $2/\lambda$ 之半即爲 $1/\lambda$ 。換句話說, 在 (b) 中我們誤將此一特別的 X_k (即總壽命)之期望值也當做 $1/\lambda$ 。

我們可粗略地這樣想: 較長的區間比較短的區間有更大的機會包含一特定的點 t 。

雖然間距皆有指數分佈, 且參數相同, 但由於是隨機變數, 區間就是有長有短, 假設在一條數線上有一些間距長短不一的點, 你隨機地取一點, 是不是較容易取自一間距較大的區間中? 同樣的道理, 若兩班公車抵站之間距很短, 你的到站時刻, 當然較不易落在其中(等車時間會較短), 而是較易落在一兩班車抵站間距較大的區間(等車時間會較長)。在公車抵站間距爲指數分佈之假設下, 你等車時間之期望值 $1/\lambda$, 差不多等於在你之前與在你之後抵站之二車間距期望值

$$\frac{1}{\lambda} + \frac{1}{\lambda}(1 - e^{-\lambda t})$$

之半, 而不是一般人以爲的 $1/\lambda$ 之半 。

再看另一關於"檢驗的詭論"(inspection paradox)。假設使用某電池, 一旦沒電了便立即換一同廠牌之新電池。電池壽命設爲 i.i.d., 這些換電池的時刻便構成一更新過程 。

某品管人員想檢定電池之壽命, 原先與操作人員約好上午 8 時至工廠,工廠在那時開始運作, 操作人員會在 8 時正啓用30 個新電池。品管人員因故遲到, 但操作人員仍在 8 時正啓用電池。有些電池電耗盡了, 操作人員立即換新,並記錄更換時間, 品管人員來廠後, 先登記正在測試的那些電池分別的啓用時間, 並等到每個電池電耗盡後, 拿到 30 個電池的壽命資料。結果取到的樣本其平均壽命差不多是原先以爲的電池壽命之兩倍, 這是怎麼回事?

假設電池之品質相同, 即壽命之分佈函數皆是某一同樣的 F , 我們以爲這些受測電池之壽命也同樣以 F 爲其分佈函數。其實並不然, 當 F 是指數分佈, 此例本質上與前面等公車的例子相同,即此時正在受測電池的壽命分佈與F 是不同的。這是值得重視的一個問題,我們看到一個明顯偏差的檢驗計畫可能會導致錯誤的結論, 因爲我們所觀察到的樣本並非來自典型的母體(typical population)。

在 Rao(1997)一書的 pp.116-117 , 亦提到一類似的例子。摩洛哥(Morocco, 位於西北非洲之一國家)之國立統計經濟應用研究所曾做一項研究, 目的是估計觀光客在他們國家之平均逗留時間。他們進行了兩種調查, 其一是對住在旅館的觀光客, 其二是對即將離境的旅客。從對 3,000個在旅館的旅客之調查, 得平均逗留時間爲 17.8 日, 而從對 12,321 個離境的旅客之調查, 得平均逗留時間爲 9.0 日。前者差不多是後者的兩倍。你現在該知道何者才是可靠的逗留時間之數據了。

7 和其光同其塵

在老子第四章: 道中, 而用之或不盈, 淵兮似萬物之宗。挫其銳, 解其紛, 和其光, 同其塵, 湛兮似或存, 吾不知誰之子, 象帝之先。

和其光同其塵的意思就是隱藏光耀, 混同塵俗。

不少統計學者均認爲波松分佈與常態分佈爲最重要的兩個分佈。但長久以來, 常態分佈具有獨尊的地位, 不要說波松分佈, 絕大部分的其他分佈, 其重要性往往被低估。

而在隨機過程裡, 波松過程與布朗運動(Brownian motion), 亦爲最重要且最基本的過程, 到處出現, 甚至在許多我們料不到的地方。但再度地, 波松過程的重要性也常被忽略。

忽視波松分佈或波松過程的重要性, 其實是統計學家的損失。因在很多離散的狀態下, 波松分佈或波松過程常是最佳模式。波松分佈及波松過程, 彷彿和光同塵, 明珠卻蒙上灰塵。

雖然萬物有常, 但天下事物不能以常理度量的本就不少, 非常態分佈

之處處存在, 也就不容懷疑。要發現波松分佈之重要, 比當伯樂容易的多, 只要你的眼光, 偶而離開常態分佈 。

習　題

1. 依第 1 節中關於豬肉換米的新聞報導裡, 所給米的重量,估計 2^{64} 粒米的總重量, 並與全世界人口總重(以每人平均 50 公斤重計)相比 。
2. 試估計將 F_{64} 這個數印出來, 約需多少本書?
3. 在第 2 節所述的致富方法中,
   (i) 若每月投資 $15,000$ 元, 40 年後之本利和爲何?
   (ii)若投資報酬率改爲每年 10% , 則 30後之本利和爲多少單位的錢? 40 年後呢?
4. 某工廠宣稱其生產的某型日光燈管可使用 $10,000$ 小時。某辦公室共安裝32 支該型燈管, 使用後才一個月便壞了一支。該辦公室想了解這是否合理。假設燈管壽命爲 i.i.d. 之 $\mathcal{E}(\lambda)$ 分佈, 期望值爲$10,000$ 小時, 又設每月上班 25 天, 每天開燈 8 小時。求
   (i)某特定燈管 1 個月內會壞之機率;
   (ii)辦公室 1 個月內至少會壞一支燈管之機率;
   (iii)辦公室 5 個月內至少會壞二支燈管之機率 。
5. 設 X 有 $\mathcal{E}(\lambda)$ 分佈, Y 爲一非負的隨機變數, 且與 X 獨立。試證 $P(X > Y + t \mid X > Y) = P(X > t)$ 。
6. 設 X 有自 1 開始, 參數 p 之幾何分佈, Y 爲一非負的隨機變數, 且與 X 獨立。試證 $P(X > Y + t \mid X > Y) = P(X > t)$ 。
7. 試證第 5 節中對一更新過程, 事件 $[A(t) = n]$ 與 $[S_n \le t < S_{n+1}]$ 等價, $\forall n \ge 0$ 。
8. 設 X 有 $\mathcal{E}(\lambda)$ 分佈, 又令 $[\cdot]$ 表最大整數函數 。

(i)試證 $[X]$ 與 $X-[X]$ 獨立;

(ii)求 $X-[X]$ 之分佈 。

9. 設 $\{A(t),\, t\geq 0\}$ 爲一參數爲 λ 之波松過程, 求總壽命β_t 之分佈 。

參考文獻

1. 金庸(1996a). 倚天屠龍記, 第三版 。遠流出版社, 台北 。
2. 金庸(1996b). 神鵰俠侶, 第三版 。遠流出版社, 台北 。
3. 金庸(1996c). 射鵰英雄傳, 第三版 。遠流出版社, 台北 。
4. 金庸(1996d). 碧血劍, 第三版 。遠流出版社, 台北 。
5. 倪錄群譯(1997). 大數秘史 。數學譯林, 第16卷第4期, 296-302 。
6. 黃文璋(1995). 隨機過程 。華泰書局, 台北 。
7. 黃文璋(1999). 數學欣賞 。華泰文化事業股份有限公司, 台北 。
8. Chelminski, R. (1999). 西洋棋只是遊戲? 讀者文摘 1999 年三月號, 103-107 。
9. Cipra, B. (1996). 1995-1996 *What's Happening in the Mathematical Sciences.* American Mathematical Society, Providence, Rhode Island.
10. Cundy, H. M.(1966). Birds and atoms. *Math. Gazette* **50**, 294-295.
11. Peterson, I. (1980). *Islands of Truth — A Mathematical Mystery Cruise.* W. H. Freeman and Company, New York.
12. Rao, C. R. (1997). *Statistics and Truth — Putting Chance to Work*, 2nd. ed. World Scientific Publishing Co. Pte. Ltd., Singapore.