數學科讀書心得報告

10338 鄭兆傑

這次我從書單理挑出的兩本書分別是 密碼學 和 愛上數學—悠遊數學世界的 20 個趣味故事 ，這兩本書其實都滿薄的，尤其是密碼學才 130 多頁，不過我還是讀了滿久的，密碼還是很複雜的東西，反倒是愛上數學這本，雖然厚度比較多，可是內容可以說是非常的簡單卻又生活化，越前面的故事又比較簡單，應該是經過編排的結果。裡面是描述一個數學老師在退休之後習慣不改，於是就開始教自己八歲的孫子數學，雖然教給的只是八歲小孩，可是裡面不乏有向圓週率、黃金比例等難度比較高一些的東西，裡面大部分還是很平民化的東西，像第一篇在介紹數字的起源、第三篇討論 0 存在的意義、第四篇討論爲何要先乘除後加減，雖然都是些很簡單的"定理"，幾乎可以說是大家都知道，就像第 13 篇的畢氏定理，說不定"會用"的人會比"了解原理"的人來的多許多，大家都不求甚解。還有我也很訝異的在第 12 篇中的討論，偶數和自然數居然一樣多，這讓人感到很誇張，偶數是自然數的一部分，但是兩個居然一樣多，部分會等於全體！因爲兩個都是無限的，把每個自然數乘二之後都可以對到一個偶數，形成一對一關係，第一次聽到真的還是會決得很離譜，沒辦法，日常生活的所見已成爲基本常識深深印在我們的腦中，只要遇到和常理不同的事物就會轉不過來。每次只要遷扯到無限大都沒有好事，好好的基本常識都會被顛覆，就像上學期的數列級數，根無限大有關係之後就讓人頭痛，在加上複數…之類的東西，就讓人一個頭兩個大，分數就不見啦！還有像有關 0 的計算，所有人應該都知道任何數除 0 無意義，因爲乘法是除法的逆運算，沒有一個數成 0 之後可以不是 0 的，那 0 除 0 呢？還記得我國中學到這個部分的時候，我呆呆的就以爲答案就是 0，0 乘 0 也是 0 啊，你運算也沒問題，當然那題就被扣分了，有講原因嗎？不，大部分老師練爲何不能用 0 除都沒說，書中也有說到，因爲 8 乘 0 也是 0，如此一來就有兩個數符合這答案，甚至無限多個答案，所以不對這種無限多解做討論，而將它一起歸類在無意義。大家都知道圓面積怎麼算，你去問個小學生，他會回答：半徑 X 半徑 X3.14 嘛！問國中生他會回答：拍 r 平方。但是問高中生圓面積爲什麼這樣算，能答出來的人可說是寥寥無幾，在第 17 篇也有這樣的介紹，因爲把圓從半徑剪開可以做出以圓周爲底半徑爲高的三角形，這真的是非常了不起的想法，本書中提到許多的數學家真的都很厲害。

密碼學就是比較近代的東西了，其實早在羅馬的凱薩就有了凱薩密碼，甚至在希臘就有密碼的使用，在偵探小說中密碼更是頻繁，也被偵探們一一破解，像福爾摩斯裡的跳舞人就很有名，到了現代有了電腦，密碼就更複雜了，有了密碼當然也就有人解碼，一種是收到訊息的解碼員，還有一種就是盜取訊息要來破解密碼，當然早期的密碼破解也就比較容易，一開始幾乎都使用頻率分析法就可以了，因爲字母 E 的出現次數一般會較其他字母來得多，在來是 T 還有 A，把握了這些原則要破解也就不是太困難。不管置換法則或甚至用圖形來置換都無法掩飾住這種英文中一直存在的定律，因爲不管被換成哪個英文字母或圖形，只要字

母 E 是最多的，他所對應的密碼文也就會是最多的，依序在分別找出 A 和 T 這兩個次多的字母(英文中 A 單獨出現機率很高但 T 不能單獨存在，所以這兩個字也很好分)，再來除了 A 只有 I 會自己存在，就有四組對應關係了，如果能從這四組找出替換的規律的話就破解成功了，如果沒有規律而只是表對表的一對一置換那就只好再多花一些時間了，這時候只好利用手邊的一些資料來猜，這也不會太難，例如你知道收信人的名字就很有可能出現在裡面，到最後大部分字母出現剩少數單字時，甚至可以一個一個單字放進去，就像填格子遊戲一樣，然後當然從符合單字中找出有意義的選項，通常不會有兩個以上都有意義，一定會有個最合文法語意的單字，單字中未破解的祕文也就破解了，慢慢的就可以將密碼還原，所以在早期的密碼學中和數學的關係並不多，只有在有規律的置換中有使用，解碼員也大都是語言學家。

爲了挽救這種被破解的風險，大家也就當然的開始研究新密碼，畢竟無法保密的密碼就不算是密碼了，果然不久就出現了比較安全的多表代替密碼，關鍵在於加密不同字的密碼不同，例如用一個單字當密鑰依序使用單字各個字母所代表的數字(就是字母的順序 A=1, B=2…)來加密，如此只要加密用的密鑰單字沒有外洩，頻率分析法也就不管用了，因爲同一個 E 可能碰到不同的加密字母成爲不同的單字，大大破壞了原先文字中的出現次數。但是無論如何這種密碼還是被破解了，破解的方法只能說是非常複雜，利用不斷分析頻率來破解密鑰，再用密鑰去解析密文是他的基本方法，詳細就不在多說。到電腦一出現，數學的重要性也提升很多，因爲利用電腦的快速計算可以利用數字做出牢不可破的密碼，到了近代，使用的數字更是一直變大，像有名的 RSA-129 就是一個 129 位數他是由兩個 65 和 64 位數的直數所組成，這也是現代利用單向函數的方式之一，單向函數就像上述，你要用電腦算出這兩個質數的乘積並不會太難，但是要將結果再分解回那兩個質數卻是難上加難，你可能得花上數十甚至數百倍的時間，這個密碼的目的也就達到了，而且現在利用的數字可能還更大，裡面當然有很多利用，都可以說是讓谷人想都沒想到的，最好玩的算是遠程丟硬幣協定，我跟你兩人分隔兩地無法見面，要共同決定一件事的時候，居然可以用丟硬幣決定，重點在你要怎麼確定對方沒說謊。這也是單向函數的利用我很快算出一個數字給你他的函數，你不可能在短時間內逆算回來(單向函數的特性)只好猜他是單數或雙數我再公佈結果，且把答案交給你驗算硬幣就投完了！後來也發展出了公開密鑰這劃時代的發明，這發現使得密碼平民化，密碼保密不再是政府機關的專利品，一般人也可以享用，尤其現在的網路更是無時無刻不受到它的保護，可是政府(研究國)卻也常爲了自身安全處處限制，這也算是密碼學技術限制之外的一個需要解決的大問題吧！