摘要

第一部分先探討各質數本身有無循環個數上關係如有關係，找出敘述其規律之一般式，並加以證明。

第二部分探討單一質數各次方之間有無循環個數上關係如有關係，找出敘述其規律之一般式，並加以證明。

壹、研究動機

本篇的研究動機為，在參加青年程式設計競賽時，有一題目其要求為求解 Fibonacci series 第 N 項對 2 的 k 次方取餘數之值，而此要求之解法必須假定費波納契數列對 2 的 k 次方取餘數之值會循環，而筆者突然萌生了一個想法，既然最小質數之循環規律存在，且已經被證明為正且質數之間時常有類似的性質，那其他質數有無類似的循環規律，即成為了一個值得研究之議題，於是就開始此議題之研究。

貳、 研究目的

本篇之研究目的即為找出各質數之循環個數之規律,再進而找出單一質數各次方間之關係,從而推導出能表示其循環個數狀態之一般式，進而證明其一般式之正確性。

參、 研究設備及器材

本專題使用於編寫程式及撰寫本文之硬體為個人電腦，本專題使用於編寫程式之 IDE(整合式開發環境)為 Dev-C++，本專題所提及之所有程式，使用語言均為 C++語言，語言標準為 C++11。

肆、 背景知識

一、 Fibonacci series

在數學上，Fibonacci series 之定義為

$$\begin{cases} f(0)=0 \\ f(1)=1 \\ f(n)=f(n-1)+f(n-2)\ ,n\geq 2 \end{cases}$$

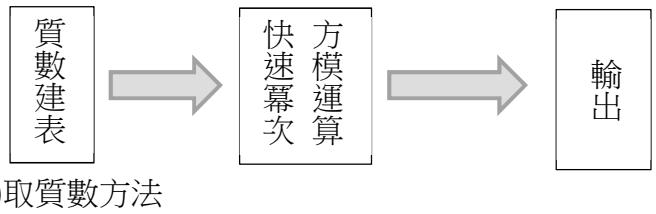
用文字來說，就是 Fibonacci series 由 0 和 1 開始，之後的 Fibonacci series 就是由之前的兩數相加而得出。

二、 模運算

根據培養與鍛鍊程式設計的邏輯腦一書在第 126 頁所述計算除以 m 的餘數又稱為「對 m 取 mod」或「對 m 取模」或「以 m 取模」。下面將一律採用「以 m 取 mod」這種說法。為了讓程式碼更簡潔，以 m 取整數 a 與 b 取餘數若相等則寫成$a \equiv b(\mathrm{mod}\ m)$。另外，以 m 除 a 的餘數要寫成 a mod m。透過簡單的計算，只要$a \equiv c(\mathrm{mod}\ m)$、$b \equiv d(\mathrm{mod}\ m)$，就可以說$a+b \equiv c+d(\mathrm{mod}\ m)$、$a-b \equiv c-d(\mathrm{mod}\ m)$、$a \times b \equiv c \times d(\mathrm{mod}\ m)$是成立的。」

伍、演算法設計說明

(一)演算法流程圖



(二)取質數方法

本節將探討質數建表使用之演算法

1.sieve of Eratosthenes

sieve of Eratosthenes 中文稱埃拉托斯特尼篩法，是目前所知取質數較為快速之演算法，所使用的原理是從 2 開始，將每個質數的各個倍數，標記成合數。

(三)次方運算

1.基礎算法

一般時候我們在計算冪次方時，一般是採用冪次方之基礎算法，即將欲運算之底數連乘欲運算之冪次數 k，而這在冪次極大時可能極慢。使用時間為線性的。

2.快速冪算法

根據培養與鍛鍊程式設計的邏輯腦一書在第 127 頁所述

由於當$\mathbf{n=2^k}$時可將之表示為$x^n=(x^2)^2$……如此便能以連乘 k 次的平方來輕鬆求出冪次方。將這種想法放在心上，並將 n 表示為 2 的冪次方的和就行了。$\mathbf{n=2^{k_1}+2^{k_2}+2^{k_3}}$……這樣一來就會變成$x^n=x^{2^{k_1}}+x^{2^{k_2}}+x^{2^{k_3}}$……只要依序求取$x^{2^i}$並同時進行計算就行了，這樣結果就會變成是以對數時間來求取冪次方了。

可知，此法可以有效降低時間複雜度。

Fibonacci series 對質數 K 次方模運算之循環關係

陸、實驗數據

表一、各質數之循環結果

質數 P	2	3	5	7	11	13	17	19	23
循環個數	3	8	20	16	10	28	36	18	48
質數 P	29	31	37	41	43	47	53	59	61
循環個數	14	30	76	40	88	32	108	58	60
質數 P	67	71	73	79	83	89	97	***101***	103
循環個數	136	70	148	78	168	44	196	***50***	208
質數 P	107	109	***113***	127	131	137	139	149	151
循環個數	72	108	***76***	256	130	276	46	148	150

上表一為將前 36 個質數本身輸入至本文第一段所描述之程式所得之結果整理而得之表格，而由上表一可以推論出以下的規律。令 M=循環個數、P=質數，當 P=2,M=3，當 P=5,M=20

當尾數是 1 時，除 101+60X 外皆遵守 M=P-1。(如表一紅色字)
當尾數是 3 時，除 113+90X 外皆遵守 M=2*P+2。(如表一黃色字)
當尾數是 7 時，除 47+60X 外皆遵守 M=2*P+2。
當尾數是 9 時，除 89+50X 外皆遵守 M=P-1。

表二、各質數及各次方

質數 P / 次方 K	2	3	5	7	11	13	17
1 (M)	3	8	20	16	10	28	36
2 ($M \times P^1$)	6 ($3*2^1$)	24 ($8*3^1$)	100 ($20*5^1$)	112 ($16*7^1$)	110 ($10*11^1$)	364 ($28*13^1$)	612 ($36*17^1$)
3 ($M \times P^2$)	12 ($3*2^2$)	72 ($8*3^2$)	500 ($20*5^2$)	784 ($16*7^2$)	1210 ($10*11^2$)	4732 ($28*13^2$)	10404 ($36*17^2$)
4 ($M \times P^3$)	24 ($3*2^3$)	216 ($8*3^3$)	2500 ($20*5^3$)	5488 ($16*7^3$)	13310 ($10*11^3$)	61516 ($28*13^3$)	176868 ($36*17^3$)
5 ($M \times P^4$)	48 ($3*2^4$)	648 ($8*3^4$)	12500 ($20*5^4$)	38416 ($16*7^4$)	146410 ($10*11^4$)	799708 ($28*13^4$)	3006756 ($36*17^4$)
6 ($M \times P^5$)	96 ($3*2^5$)	1944 ($8*3^5$)	62500 ($20*5^5$)	268912 ($16*7^5$)	1610510 ($10*11^5$)	10396204 ($28*13^5$)	51114852 ($36*17^5$)
7 ($M \times P^6$)	192 ($3*2^6$)	5832 ($8*3^6$)	312500 ($20*5^6$)	1882384 ($16*7^6$)	17715610 ($10*11^6$)	135150652 ($28*13^6$)	868952484 ($36*17^6$)

由以上結果可畫出如上表五，表五之橫軸為質數 P，縱軸為次方 K，由此表可見，結果符合通式$M \times P^{K-1}$。

柒、 結論

一、結論說明

(一) 質數間的關係

在質數間的關係，同樣尾數的質數之間通常會遵守一定的關係式，而且尾數相加等於 10 之質數通常也會遵守一樣的規律。

(二) 單一質數各次方間之關係

在質數各次方間之關係，其循環個數成等比數列，且公比為質數本身。

二、研究過程中所提出之問題

(一) 關於一般式

既然質數之間遵守一定的規律，那有沒有辦法推導出其一般式來表示所有的結果?

(二) 關於證明

那如果有一般式的話，能不能用窮舉法以外之數學方法去證明其一般式之正確性，以及更加推廣。

三、未來值得研究的方向

今天我們發現了質數之間之規律，那可以繼續往合數，正整數，甚至是整數的領域進行推廣。

四、創見

因為其規律以及其循環，以後這可能在密碼學上產生一種加密法，從而成為資訊安全領域中重要的一環。

捌、 參考資料及其他

一、書籍

(一) Sartaj Sahni, Ellis Horowitz(1990)。Fundamental Of Data Structure In C。Computer Science Press。

(二) 吳振奎(2000)。斐波那契數列。九章出版社。

(三) 秋葉拓哉，岩田陽一，北川宜稔(2013)。培養與鍛鍊程式設計的邏輯腦。博碩出版社，2013 年 11 月。

二、期刊

(一) 鄭振牟(2011)。密碼學與模算術。臺大電機系科普系列，2011 年 7 月，取自 https://www.ee.ntu.edu.tw/hischool/doc/2011.07.pdf。

三、網路

(一)維基百科(無日期)。斐波那契數列。2017 年 2 月 24 日，取自 https://zh.wikipedia.org/wiki/斐波那契數列

(二)維基百科(無日期)。黃金分割率。2017 年 2 月 24 日，取自 https://zh.wikipedia.org/wiki/黃金分割率