第十七屆旺宏科學獎

創意說明書

參賽編號：SA17-351

作品名稱：自守數分析及生成演算法之改進

姓名：張志煥

關鍵字：同餘、自守數、原根

摘要

在冪次計算的過程中，我們發現末n位數經過週期後會重複出現。

在第一部分，我們找出了重複出現的週期，以及任意數字重複出現自己的最小次方，以此為契機，我們發現了名為「自守數」的數學定義與我們研究的主題非常相似。

於是在第二部分，我們運用研究結果來找出探討其性質及規律，與週期相仿地定義出了「最小自守」，並找出了導出任意數字最小自守的定理。

並且在最後的第三部分，我們成功地透過「最小自守」的幫助，以及「原根」的性質，透過因倍數關係導出了一套能快速計算出所有「最小自守為k的自守數」所形成集合的演算法，不僅如此，我們還能利用聯集的概念，歸納出一個同樣快速計算「k次方會自守的自守數」所形成集合的演算法，使其從原本的暴力尋找指數時間演算法，晉升為擁有k平方量級時間的優秀演算法。

壹、研究動機

大家都知道我們在計算2的冪次時尾數出現的規律為 2,4,8,6,2,…。

個位數存在著以「2,4,8,6」四個冪次為週期的規律，而4的冪次尾數「4,6,4,…」，是兩個冪次為週期的規律。我們想要了解對於任意數字，這樣的週期規律，是否可以快速的求得。

我們也進一步觀察而若擴展成留下末兩位數的話，又能在$2^{22} = 4194304$時發現其與$2^2 = 4$出現了重複，形成二十個冪次為一週期的規律。這些週期之間似乎有關連存在著？

而我們在網路上發現自守數的數學定義，但是目前的演算法都是暴力搜尋，因此我們希望用數論的方法分析，並且改進目前的演算法。

貳、研究目的

一、找出十進位數字的冪次計算過程中，末n位數重複的規律。

二、探討任意數最小自守之規律，並找出其性質。

三、利用最小自守改進生成k階自守數的演算法。

參、 研究過程

一、定義

$\boldsymbol{P_d(x)}$	滿足$P_d(x)$是最小的正整數，$\exists k < P_d(x) \in \mathbb{N}$， 有$x^{P_d(x)} \equiv x^k (mod\ d)$。
$\boldsymbol{Q_d(x)}$	$Q_d(x) = min(k)$，滿足$x^k \equiv x^{P_d(x)} (mod\ d)$。
$\boldsymbol{ord_d(x)}$	若$(x,d) = 1$， $ord_d(x)$是最小的正整數，滿足$x^{ord_d(x)} \equiv 1 (mod\ d)$。
$\boldsymbol{\delta_d(x)}$	滿足$\delta_d(x)$是> 1的最小正整數，有$x^{\delta_d(x)} \equiv x (mod\ d)$。
$\boldsymbol{A(k,n)}$	滿足$a^k \equiv a (mod\ 10^n)$ 的所有正整數$a < 10^n$所形成的集合。
$\boldsymbol{\Delta(k,n)}$	滿足$\delta_{10^n}(a) = k$的所有正整數$a < 10^n$所形成的集合。
$\boldsymbol{\varphi(n)}$	定義$\varphi(n)$是小於或等於n的正整數中與n互質的正整數個數
$\boldsymbol{\lceil x \rceil}$	滿足$\lceil x \rceil$為大於等於x的最小整數
原根	定義a是p的原根，若且唯若$ord_p(a) = \varphi(p)$
$\boldsymbol{O\big(g(n)\big)}$	定義 $f(n) \in O\big(g(n)\big)$ 若且唯若 $\exists c$、$N \in \mathbb{R}^+$，$\forall n \geq N$ 有 $\lvert f(n) \rvert \leq \lvert cg(n) \rvert$。

二、文獻探討

尤拉函數

定義 $\varphi(n)$是小於或等於n的正整數中與n互質的正整數個數，設

$$n = \prod_{i=1}^{k} p_i^{a_i}, \big(p_i \text{為} n \text{的所有質因數}\big)，\text{則 } \varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

對於任何的正整數a,p，若有$(a,p) = 1$，則$a^{\varphi(p)} \equiv 1 (mod\ p)$

三、原命題之資料分析

2、4、8、16……，2的冪次有種奇妙的魔力，但當指數漸漸變得龐大，計算也逐漸變得困難，為了快速計算，我們試圖尋找一些方法：

$$2,4,8,16,32,64,128,256,512,1024,2408,4096$$

如果只留下末一位數的話，可以發現如下：

$$2,4,8,6,2,4,8,6,2,4,8,6$$

個位數存在著以「2,4,8,6」四個冪次為週期的規律。

而若擴展成留下末兩位數的話，又能在$2^{22} = 4194304$時發現其與$2^2 = 4$出現了重複，形成二十個冪次為一週期的規律。

好奇心驅使之下我們使用 C++程式建表後發現，似乎所有末n位數都存在著固定的週期，為了確認我們猜測的正確性，我們尋求了數學的幫助，列出了以下的尋找目標：

給定一正整數a，尋找最小的正整數p使得

$$a^p \equiv a^q (mod\ 10^n)，其中 q < p，q, n \in \mathbb{N}$$

為了想知道**最早出現重複的**冪次，我們定義了$P_{10^n}(a)$為最小的正數，其末n位數於較小的冪次的末n位數相同，如同上面的例子便可得$P_{10^2}(2) = 22$；相對地欲找出**最早被重複到的**冪次，我們定義出了$Q_{10^n}(a)$，如同上面的例子便可得$Q_{10^2}(2) = 2$，而2的冪次便是一種$a = 2$的特例。

我們另外發現了兩個函數的一個性質：

性質 1

$\forall d, x$
設α表示d的正因數當中，與x互質的最大的正整數，則

$$P_d(x) - Q_d(x) = ord_\alpha(x)$$

Pf:

$x^{P_d(x)} \equiv x^{Q_d(x)} (mod\ d) \iff x^{Q_d(x)}(x^{P_d(x)-Q_d(x)} - 1) \equiv 0 (mod\ d)$

令$x^{Q_d(x)}(x^{P_d(x)-Q_d(x)} - 1) = dk = \alpha Dk$，$D, k \in \mathbb{N}$

$$\iff \begin{cases} x^{P(x)-Q_d(x)} - 1 \equiv 0 (mod\ d) \\ x^{Q_d(x)} \equiv 0 \left(mod \frac{d}{a}\right) \end{cases}$$

根據ord函數的定義與$P_d(x)$、$Q_d(x)$的性質我們有

$\iff P_d(x) - Q_d(x) = ord_\alpha(x)$

因為$P_d(x) = Q_d(x) + ord_\alpha(x)$ ，且$x^{Q_d(x)} \equiv 0 (mod\ \mathrm{d}/\alpha)$，

依照定義必須使$P_d(x)$最小，故我們需要$Q_d(x)$為最小的正整數使得$x^{Q_d(x)} \equiv 0 (mod\ \mathrm{d}/\alpha)$

其中$ord_\alpha(x)$這個值便是我們想尋找的週期大小，以下將用$P_d(x) - Q_d(x)$表示。

從性質 1 可以發現，證明定理需要ord函數的計算，而盲目地窮舉找週期便失去了原本的意義，於是我們試著想找到快速計算ord函數的方法，並先行導出一個方便接下來的研究進行的引理。

引理 1

若d為使得$a^d \equiv 1 (mod\ p)$成立的最小正整數，則

$$\forall d' \text{使得 } a^{d'} \equiv 1 (mod\ p) \ ,\ d | d' \text{皆成立}$$

Pf:

以下使用反證法，假設$d \nmid d'$，令$k, r \in \mathbb{N}$且$r < d$，滿足$d' = kd + r$

則$a^d \equiv 1 \equiv\ a^{d'} \equiv a^{kd+r} \equiv a^{kd} \times a^r \equiv 1 \times a^r\ (mod\ p)$

則我們得到$a^r \equiv 1 (mod\ p)$，但$r < d$，矛盾 ⇒ 假設錯誤，故$d | d'$。

■

引理 1 能幫助我們嚴謹地確定$ord_p(a)$能整除滿足 $a^{d'} \equiv 1(mod\ p)$的任何d'，因為我們考慮末n位數，即考慮同餘10^n，所以我們需要將 Euler 定理進行推廣，於是我們推導出了引理 2。

於是我們推導出了引理 2。

引理 2

取p為一奇質數，且整數$a \neq \pm 1$不被p整除。設$ord_p(a) = r$而k_0是使得$a^r \equiv 1(mod\ p^{k_0})$的最大正整數，則

$$ord_{p^{k_0+n}}(a) = \begin{cases} r, n \leq 0 \\ rp^n, n > 0 \end{cases}$$

Case 1: $n \leq 0$

Pf: 設 $a^r = 1 + p^{k_0}u_o$

$\because n \leq 0\ \therefore p^{k_0+n} | p^{k_0} \Rightarrow a^r \equiv 1(mod\ p^{k_0+n})$

故$ord_{p^{k_0+n}}(a) = r$

■

Case 2: $n > 0$

使用數學歸納法證明$\forall n \geq 0,\ a^r \equiv 1\ (mod\ p^{k_0})$,$\exists u_n$, 且$(u_n, p) = 1$

滿足 $a^{rp^n} = 1 + p^{k_0+n}u_n$

Pf: 設 $a^r = 1 + p^{k_0}u_o$，由於k_0已是滿足的最大正整數，故$(u_0, p) = 1$

假設當$n = l$ 時，有 $a^{rp^l} = 1 + p^{k_0+l}u_l$ 且 $(u_l, p) = 1$

當$n = l + 1$ 時，

$$\left(a^{rp^l}\right)^p = (1 + p^{k_0+l}u_l)^p = 1 + \sum_{i=1}^{p} C_i^p (p^{k_0+l}u_l)^i$$

在$i = 1$ 時，$C_1^p (p^{k_0+l}u_l)^1 = p^{k_0+l+1}u_l$

在$2 \leq i \leq p - 1$ 時，考慮$C_i^p (p^{k_0+l}u_l)^i$，p為質數，故$C_i^p (p^{k_0+l}u_l)^i$中必可提出p^{k_0+l+2}

在$i = p$時$C_p^p (p^{k_0+l}u_l)^p$ 中必可提出 p^{k_0+l+2}

則

$$\left(a^{rp^l}\right)^p = 1 + p^{k_0+l+1}u_l + p^{k_0+l+2}\sum_{i=2}^{p} C_i^p u_l^i p^{i(k_0+l)-k_0-l-2}$$

在這裡我們要使$(u_{l+1}, p) = 1$，因此只提出p^{k_0+l+1}，則

$$\left(a^{rp^l}\right)^p = 1 + p^{k_0+l+1}\left(u_l + p\sum_{i=2}^{p} C_i^p u_l^i p^{i(k_0+l)-k_0-l-2}\right)$$

此時，令

$$u_{l+1} = \left(u_l + p\sum_{i=2}^{p} C_i^p u_l^i p^{i(k_0+l)-k_0-l-2}\right)$$

則$p \nmid u_{l+1}$故

$$\left(a^{rp^l}\right)^p = 1 + p^{k_0+l+1}u_{l+1} \equiv 1\ (mod\ p^{k_0+l+1})$$

故依數學歸納法，$\forall n \in \mathbb{N}$，$a^r \equiv 1\ (mod\ p^{k_0})$，$\exists u_n$ 滿足 $a^{rp^n} = 1 + p^{k_0+n}u_n$

我們將再次使用數學歸納法證明 $rp^n = ord_{p^{k_0+n}}(a)$

當$n = 0$時，由前面的證明可以知道$a^r = 1 + p^{k_0}u_0$，由k_0的定義，$r = ord_{p^{k_0}}(a)$成立

設$n = m$時成立，即$rp^m = ord_{p^{k_0+m}}(a)$

當$n = m + 1$時，

設s為最小的數 $s.t\ a^s \equiv 1\ (mod\ p^{k_0+m+1})$

根據引理 1 $s|rp^{m+1}$ 且由歸納假設 $s \neq rp^m \Rightarrow s = rp^{m+1}$

即得證$ord_{p^{k_0+m+1}}(a) = rp^{m+1}$，也成立，

故由數學歸納法$ord_{p^{k_0+n}}(a) = rp^n$

綜合以上

$$ord_{p^{k_0+n}}(a) = \begin{cases} r, n \leq 0 \\ rp^n, n > 0 \end{cases}$$

■

有了 C++程式建表和引理 2 的輔助，數字的觀察與研究變得方便許多。

如同附錄一，我們可以發現$P_{10}(2)-Q_{10}(2)=4$、$P_{10^2}(2)-Q_{10^2}(2)=20$、$P_{10^3}(2)-Q_{10^3}(2)=100$，表示2在冪次計算過程中不同重複尾數的週期存在著倍數關係，我們導出其一般式，並證明之。

定理 1

週期$P_{10^n}(2)-Q_{10^n}(2)=4\times5^{n-1}$，$P_{10^n}(2)=4\times5^{n-1}+n$

Pf:

在性質 1 中，帶入$d=10^n$，$x=2$，則可以得到$\alpha=5^n$

則$P_{10^n}(2)=Q_{10^n}(2)+ord_{5^n}(2)$

再由引理 2 得出$ord_{5^n}(2)=4\times5^{n-1}$

且需滿足$Q_{10^n}(2)$為最小的正整數使得$2^{Q_{10^n}(2)}\equiv0(mod\ 2^n)$，故取$Q_{10^n}(2)=n$

故$P_{10^n}(2)=4\times5^{n-1}+n$

■

舉例來說，當$n=4$時，我們可以得出$P_{10^4}(2)=4\times5^3+4=504$,

即$2^{504}\equiv2^4(mod\ 10^4)$。而$P_{10^n}(2)-Q_{10^n}(2)=4\times5^{n-1}$，$n=1,2,3$的確有倍數關係。

之後我們針對$a=2^k$的狀況做出了以下了推廣。

定理 2

k為正整數則，週期$P_{10^n}(2^k)-Q_{10^n}(2^k)=\frac{4\times5^{n-1}}{(4\times5^{n-1},k)}$，$P_{10^n}(2^k)=\frac{4\times5^{n-1}}{(4\times5^{n-1},k)}+\left\lceil\frac{n}{k}\right\rceil$

Pf:

在性質 1 中，帶入$d=10^n$，$x=2^k$，則可以得到$\alpha=5^n$

$\Rightarrow P_{10^n}(2^k)=Q_{10^n}(2^k)+ord_{5^n}(2^k)$，再由引理 2 得出$ord_{5^n}(2^k)=\frac{4\times5^{n-1}}{(4\times5^{n-1},k)}$

且$(2^k)^{Q_{10^n}(2^k)}\equiv0(mod\ 2^n)$，故取$Q_{10^n}(2^k)=\left\lceil\frac{n}{k}\right\rceil$

故$P_{10^n}(2^k)=\frac{4\times5^{n-1}}{(4\times5^{n-1},k)}+\left\lceil\frac{n}{k}\right\rceil$

■

舉例來說，當$n=4,k=6$時，我們可以得出$P_{10^4}(2^6)=\frac{4\times5^3}{(4\times5^3,6)}+\left\lceil\frac{4}{6}\right\rceil=\frac{500}{2}+1=251$，即$2^{6\times251}\equiv2^{6\times1}(mod\ 10^4)$。

由於2是10的因數，所以證明時只需考慮模 5 的情況，同是 10 的因數的5在冪次計算過程中應該也存在著類似的規律。

但由於引理 2 並不通用於偶質數冪次的底數，於是我們針對偶質數導出了引理 3 來幫助我們之後的定理推導。

引理 3

若$a=2^ik+1=2^jm-1,i,k,j,m\in\mathbb{N},(k,2)=(m,2)=1,Max(i,j)$表示$i,j$中最大的數。

$$ord_{2^n}(a)=\begin{cases}1,n=1\\1,n\le Max(i,j)=i\\2,n\le Max(i,j)=j\\2^{n-Max(i,j)},n>Max(i,j)\end{cases}$$

Pf:以下先證明$Max(i,j)=1$的情況

$a=2^ik+1=2^jm-1\Leftrightarrow2=2^jm-2^ik$

$Max(i,j)=j\Rightarrow2=2^i(2^{j-i}m-k)$，則$i=1$，又因為$m,k$均為奇數，所以

$2^{j-i}\neq1\Rightarrow j-i>0\Rightarrow j>i\Rightarrow j>1$

同理$Max(i,j)=i\Rightarrow2=2^j(m-2^{i-j}k)$，則$j=1$，且

$2^{i-j}\neq1\Rightarrow i-j>0\Rightarrow i>j\Rightarrow i>1$

顯而易見，若$i=j$時，不論上述何種情況均不成立，故$i\neq j\Rightarrow Max(i,j)\neq1$

根據 Euler 定理 $\because(a,2^n)=1\therefore a^{\varphi(2^n)}\equiv1\ (mod\ 2^n)$

再根據引理 1，若t為最小正整數 s. t. $a^t\equiv1\ (mod\ 2^n)$則 $t|\varphi(2^n)$

故可假設$t=2^L\ \ (L\le n-1)$

先證明$n\le Max(i,j)$的情況，$n=1$，顯然$ord_2(a)=1$，$1<n\le Max(i,j)$時證明如下

$Max(i,j)=i$，時顯然$ord_{2^n}(a)=1$，$Max(i,j)=j$時，由上面的結論可得則$i=1$

又因為$a=2^jm-1,a^2=2^{2j}m^2-2^{j+1}m+1\equiv1\ mod(2^n)$

故 $Max(i,j)=j$，時 $ord_{2^n}(a)=2$，綜合以上$n\le Max(i,j)$時的結論成立

最後用數學歸納法，證明$n>Max(i,j)$且 $Max(i,j)=i$ 時$ord_{2^n}(a)=2^{n-i}$

當$n=i+1$ ， $a^2=\left(2^ik+1\right)^2=2^{i+1}\left(2^{i-1}k^2+k\right)+1\equiv 1\left(mod\ 2^{i+1}\right)$

$$\because Max(i,j)=i,\therefore i>1\ \because 2\nmid\left(2^{i-1}k^2+k\right)\therefore ord_{2^{i+1}}(a)=2^{(i+1)-i}=2$$

設$n=i+r$ ，$ord_{2^{i+r}}(a)=2^r$成立，即$a^{2^r}=2^{i+r}\times l+1$ 且$(l,2)=1$

當$n=i+r+1$，

$$\left(a^{2^r}\right)^2=\left(2^{r+i}\times l+1\right)^2=2^{r+i+1}\left(2^{r+i-1}\times l^2+l\right)+1\equiv 1\left(mod\ 2^{r+i+1}\right)$$

$$\because 2\nmid\left(2^{r+i-1}\times l^2+l\right)\therefore ord_{2^{i+r+1}}(a)=2^{(i+r+1)-i}=2^{r+1}$$

故依數學歸納法 $\forall n>i$ ， $\Rightarrow a^{2^{n-i}}\equiv 1\ (mod\ 2^n)$

而當$n>Max(i,j)$且 $Max(i,j)=j$ 時的情況，則和$Max(i,j)=i$同理

總結以上即得出引理 3。

■

如同附錄二，我們可以發現$P_{10^2}(5)-Q_{10^2}(5)=1$、$P_{10^3}(5)-Q_{10^3}(5)=2$、$P_{10^4}(5)-Q_{10^4}(5)=4$，表示5在冪次計算過程中，重複的週期的確也存在著與2類似的倍數關係，我們一樣導出其一般式，並證明之。

定理 3

週期$P_{10^n}(5)-Q_{10^n}(5)=2^{n-2}$，$P_{10^n}(5)=2^{n-2}+n$

Pf:

在性質 1 中，帶入$d=10^n$，$x=5$，則可以得到$\alpha=2^n$

則$P_{10^n}(5)=Q_{10^n}(5)+ord_{2^n}(5)$

且須滿足$Q_{10^n}(5)$為最小的正數使得$5^{Q_{10^n}(5)}\equiv 0(mod\ 5^n)$，故取$Q_{10^n}(5)=n$

由引理 3 可以得出$ord_{2^n}(5)=2^{n-2}\ \Rightarrow P_{10^n}(5)=2^{n-2}\ +n$

■

同樣地，我們可以推導出5^k的通式。

定理 4

k為一正整數，週期$P_{10^n}(5^k) - Q_{10^n}(5^k) = \frac{2^{n-2}}{(2^{n-2},k)}$， $P_{10^n}(5^k) = \frac{2^{n-2}}{(2^{n-2},k)} + \left\lceil\frac{n}{k}\right\rceil$

Pf:

在性質 1 中，帶入$d = 10^n$，$x = 5$，則可以得到$\alpha = 2^n$

則$P_{10^n}(5^k) = Q_{10^n}(5^k) + ord_{2^n}(5^k)$

由引理 3 得到，$ord_{2^n}(5^k) = \frac{2^{n-2}}{(2^{n-2},k)}$，且$(5^k)^{Q_{10^n}(5^k)} \equiv 0(mod\ 5^n)$，故取$Q_{10^n}(5^k) = \left\lceil\frac{n}{k}\right\rceil$

故$P_{10^n}(5^k) = \frac{2^{n-2}}{(2^{n-2},k)} + \left\lceil\frac{n}{k}\right\rceil$

■

在2,5得出結論後，我們開始想尋求目標數字並非是2或5的冪次的情形，即使數字不完全是2 或 5的冪次，我們同樣可以嘗試用定理 1~4 之結論作歸納。

定理 5

對於正整數a滿足$(a, 10) = 2$，令i為滿足$2^i \mid a$之最大正整數，則 週期$P_{10^n}(a) - Q_{10^n}(a) = ord_{5^n}(a)$， $P_{10^n}(a) = \left\lceil\frac{n}{i}\right\rceil + ord_{5^n}(a)$

Pf:

在性質 1 中，帶入$d = 10^n$，$x = a$，則可以得到$\alpha = 5^n$

則可以得到$P_{10^n}(a) - Q_{10^n}(a) = ord_{5^n}(a)$

且須滿足$Q_{10^n}(a)$為最小的正數使得$a^{Q_{10^n}(a)} \equiv 0(mod\ 2^n)$，故取$Q_{10^n}(a) = \left\lceil\frac{n}{i}\right\rceil$

故$P_{10^n}(a) = \left\lceil\frac{n}{i}\right\rceil + ord_{5^n}(a)$

■

舉例來說，若$a = 12, n = 4$，那麼可得$i = 2$，則 $P_{10^4}(12) = \left\lceil\frac{4}{2}\right\rceil + ord_{5^4}(12) = 502$，即 $12^{502} \equiv 12^2(mod\ 10^4)$。

同樣地我們推得了定理 6。

定理 6

對於正整數a滿足$(a,10)=5$，令i為滿足$5^i|a$之最大正整數，則

$$週期P_{10^n}(a)-\ Q_{10^n}(a)=ord_{2^n}(a)，\ P_{10^n}(a)=\left\lceil\frac{n}{i}\right\rceil+ord_{2^n}(a)$$

Pf:

在性質 1 中，帶入$d=10^n$，$x=a$，則可以得到$\alpha=2^n$

則可以得到$P_{10^n}(a)-\ Q_{10^n}(a)=ord_{2^n}(a)$

且須滿足$Q_{10^n}(a)$為最小的正數使得$a^{Q_{10^n}(a)}\equiv 0(mod\ 5^n)$，故取$Q_{10^n}(a)=\left\lceil\frac{n}{i}\right\rceil$

故$P_{10^n}(a)=\left\lceil\frac{n}{i}\right\rceil+ord_{2^n}(a)$

■

導出$(a,10)=2,5$的情況後，我們想一次把非互質的情況完成，於是我們得出了定理 7。

定理 7

對於正整數a滿足$(a,10)=10$，令i為滿足$10^i|a$之最大正整數，則

$$週期P_{10^n}(a)-\ Q_{10^n}(a)=1，\ P_{10^n}(a)=\left\lceil\frac{n}{i}\right\rceil+1$$

Pf:

在性質 1 中，帶入$d=10^n$，$x=a$，則可以得到$\alpha=1$

則可以得到$P_{10^n}(a)-\ Q_{10^n}(a)=ord_1(a)$

且須滿足$Q_{10^n}(a)$為最小的正數使得$a^{Q_{10^n}(a)}\equiv 0(mod\ 10^n)$，故取$Q_{10^n}(a)=\left\lceil\frac{n}{i}\right\rceil$

得到$P_{10^n}(a)=Q_{10^n}(a)+1$，故$P_{10^n}(a)=\left\lceil\frac{n}{i}\right\rceil+1$

■

若$(a,10)=1$，與10互質的數字存在的最小自守規律較為混亂。

因為不存在因數上的分解，使得提出a^q後得到$a^q(a^{p-q}-1)\equiv 0(mod 10^n)$ 必須要討論$a^{p-q}\equiv 1(mod 10^n)$的問題，而因為 10 並不是質數，我們先前的 Euler 定理與其推廣無法使

用。我們試著找到了ord函數的性質，於是有了引理 4。

引理 4

$\forall p,q \in \mathbb{N}, If(p,q)=1$

$$ord_{pq}(a)=lcm(ord_p(a),ord_q(a))$$

Pf:

設$d=lcm(ord_p(a),ord_q(a))$

$a^{ord_{pq}(a)} \equiv 1(mod\ p)$ ，$a^{ord_{pq}(a)} \equiv 1(mod\ q)$

$\Rightarrow ord_p(a)|ord_{pq}(a), ord_q(a)|ord_{pq}(a)$

$\Rightarrow d|ord_{pq}(a)$

另一方面，顯然有 $a^d \equiv 1(mod\ q),\ a^d \equiv 1(mod\ p)$

由於$(p,q)=1,\ a^d \equiv 1(mod\ pq)$，由引理 1，$ord_{pq}(a)|d \Rightarrow d=ord_{pq}(a)$

■

引理 4 給予了一個因數分解後計算的機會。我們便可以直接使用同樣的結論做結合。

定理 8

對於正整數a滿足$(a,10)=1$，有

$P_{10^n}(a)-\ Q_{10^n}(a)=lcm\big(ord_{2^n}(a),ord_{5^n}(a)\big)$，$P_{10^n}(a)=lcm\big(ord_{2^n}(a),ord_{5^n}(a)\big)+1$

Pf:

在性質 1 中，帶入$d=10^n$，$x=a$，則可以得到$\alpha=10^n$

則可以得到$P_{10^n}(a)-\ Q_{10^n}(a)=ord_{10^n}(a)$

且須滿足$Q_{10^n}(a)$為最小的正數使得$a^{Q_{10^n}(a)} \equiv 0(mod\ 1)$，故取$Q_{10^n}(a)=1$

又根據引理 4，$ord_{10^n}(a)=lcm(ord_{2^n}(a),ord_{5^n}(a))$

即得到$P_{1(a)0^n}=Q_{10^n}(a)+ord_{10^n}(a)=1+lcm\big(ord_{2^n}(a),ord_{5^n}(a)\big)$

■

舉例來說，當$a=17$，$n=4$時，透過定理 8 可以很快地得到：

$P_{10^4}(17)=lcm\big(ord_{2^4}(17),ord_{5^4}(17)\big)+1=501$，即$17^{501} \equiv 17(mod 10^4)$。

四、自守數與命題之關係及資料分析

對於一個自守數a，必滿足以下關係

$$a^2 \equiv a(mod\ 10^n)$$

其中n為滿足$a < 10^n$的最小正整數

於是我們稱原本的自守數為「2 階的自守數」，並推廣到高階的自守數進行探討。

這樣的關係可以對應到原命題 $a^p \equiv a^q(mod\ 10^n)$，在$q = 1$時之情況。

我們前面已經可以知道p的長相，所以我們可以利用p來反推a，可以避免對眾多的a進行高冪次的計算，也才有可能將所有自守數了解清楚。

於是我們將命題修正如下，並賦予其定義：

給定一正整數a，尋找大於 1 的最小的正整數p使得

$$a^p \equiv a(mod\ 10^n)$$，其中$n \in \mathbb{N}$

則我們定義 $p = \delta_{10^n}(a)$，稱其為「n位數下對a的最小自守」

有了最小自守之後，若能找出最小自守為2的a值，亦即找出所有的2階自守數。

我們檢視前面的定理，將$q = 1$的情況推導出來，即可求出最小自守。

性質 2

對於正整數a滿足$(a, 10) = 1$，恆有

$$\delta_{10^n}(a) = P_{10^n}(a)$$

Pf:

$\because a^{P_{10^n}(a)} \equiv a^{Q_{10^n}(a)}(mod\ 10^n)$

又$Q_{10^n}(a) = 1\ \therefore\ a^{P_{10^n}(a)} \equiv a(mod\ 10^n)$

且同時符合$\delta_n(a)$最小正整數之定義，故$\delta_{10^n}(a) = P_{10^n}(a)$

■

舉例來說，我們已知$\delta_{10^4}(17) = P_{10^4}(17) = 501$，則「0017」這個數字是一個 501 階的自守數，即$17^{501} \equiv 17(mod\ 10^4)$。

而對於$(a, 10) \neq 1$的正整數a，出現的結果與先前的研究結果不同，有無解的狀況出現，但依然可以與定理 1~4 的研究方法做連結，並能一起解釋無解的原因。

定理 9

對於正整數a滿足$(a,10)=10$
若$10^n|a$，則$\delta_n(a)=2$，其他狀況無解

Pf:

已知 $a^{\delta_n(a)}\equiv a(mod\ 10^n)\Rightarrow\ a(a^{\delta_n(a)-1}-1)\equiv 0(mod\ 10^n)$

$\because (a,10)=10$，故$10\nmid a^{\delta_n(a)-1}-1\ \therefore a^{\delta_n(a)-1}-1\not\equiv 0(mod\ 10^n)$

所以我們可以推論$a\equiv 0(mod\ 10^n)\ \therefore$ 若 $10^n\nmid a$，無解

若有 $a\equiv 0(mod\ 10^n)$ ，可得$a^2\equiv a\equiv 0(mod\ 10^n)$，滿足$\delta_{10^n}(a)$為最小的定義
$\delta_n(a)=2$

■

定理 10

對於正整數a滿足$(a,10)=2$
若$2^n|a$，則$\delta_{10^n}(a)=ord_{5^n}(a)+1$，其他狀況無解

Pf:

已知 $a^{\delta_n(a)}\equiv a(mod\ 10^n)\Rightarrow\ a(a^{\delta_n(a)-1}-1)\equiv 0(mod\ 10^n)$

$\because (a,10)=2$，故$2\nmid a^{\delta_n(a)-1}-1\ \therefore a^{\delta_n(a)-1}-1\not\equiv 0(mod\ 2^n)$

所以我們可以推論$a\equiv 0(mod\ 2^n)\ \therefore$ 若 $2^n\nmid a$, 無解

若有 $a\equiv 0(mod\ 2^n)$ ，欲使$a^{\delta_{10^n}(a)-1}\equiv 1(mod\ 5^n)$，依$\delta_{10^n}(a)$為最小的定義
則$ord_{5^n}(a)=\delta_{10^n}(a)-1\Rightarrow\delta_{10^n}(a)=ord_{5^n}(a)+1$

■

定理 11

對於正整數a滿足$(a,10)=5$
若$5^n|a$，則$\delta_{10^n}(a)=ord_{2^n}(a)+1$，其他狀況無解

Pf:

已知 $a^{\delta_{10^n}(a)}\equiv a(mod\ 10^n)\Rightarrow\ a(a^{\delta_{10^n}(a)-1}-1)\equiv 0(mod\ 10^n)$

$\because (a,10)=5$ 故 $5\nmid a^{\delta_n(a)-1}-1\because a^{\delta_{10^n}(a)-1}-1\not\equiv 0(mod\ 5^n)\ \therefore a\equiv 0(mod\ 5^n)$

$\therefore$ 若 $5^n\nmid a$, 無解，若有 $a\equiv 0(mod\ 5^n)$，欲使$a^{\delta_{10^n}(a)-1}-1\equiv 0(mod\ 2^n)$
則根據$\delta_{10^n}(a)$定義取最小，即$ord_{2^n}(a)=\delta_{10^n}(a)-1\Rightarrow\delta_{10^n}(a)=ord_{2^n}(a)+1$

■

我們已經有方法得出一個數字屬於「幾階自守」，但卻無法得出「k階自守數」的集合內存在哪些數字，於是我們想用「最小自守」來推導出「k階自守數」的集合。

五、推導自守數

我們在網路上找到了「透視自守數」這篇科展，他們使用二項式展開的方式比對個位數，十位數……等，解決了2~5階自守數的情況，但當尋找高階自守數時會變的很複雜。

於是我們打算分析每個數字最小自守的長相來解決所有自守數的問題。

我們要解決的問題為k階自守數，定義如下：

給定n,k找到 $a \in \mathbb{N}$ 使得 $a^k \equiv a(mod\ 10^n)$

為了求出自守數，我們賦予以下定義：

$A(k,n)$ 表示滿足$a^k \equiv a(mod\ 10^n)$ 的所有正整數$a < 10^n$所形成的解集合。

為了求出自守數的集合，我們進一步定義出以下集合：

$\Delta(k,n)$ 表示滿足$\delta_{10^n}(a) = k$ 的所有正整數$a < 10^n$所形成的集合。

我們求出了兩個集合函數的關係，即定理 12。

定理 12

$$\forall k,n\in\mathbb{N}, A(L,n)=\bigcup_{k-1|L-1}^{L-1}\Delta(k,n)$$

Pf:k

$a\in\Delta(k,n)\Rightarrow a^k\equiv a(mod\ 10^n)$

對任意正整數L我們令$L=b(k-1)+r, 0<r\leq k-1, r\in\mathbb{Z}, b\in\mathbb{N}$

使用數學歸納法證明，$\forall b\in\mathbb{N}\cup\{0\}$，$a^L\equiv a^r$成立

$1^\circ\ b=0\Rightarrow a^L\equiv a^r$

2° 若$a^{b(k-1)+r}\equiv a^r$成立，則$a^{(b+1)(k-1)+r}\equiv a^r$成立

$a^{(b+1)(k-1)+r}\equiv a^{(b+1)(k-1)+r-k}\cdot a^k\equiv a^{(b+1)(k-1)+r-k+1}\equiv a^{b(k-1)+r}\equiv a^r$

由歸納假設，$a^{b(k-1)+r}\equiv a^r$，故$\forall b\in\mathbb{N}\cup\{0\}$，$a^L\equiv a^r$成立

若$k-1|L-1\Rightarrow r=1\Rightarrow a^L\equiv a^r\Rightarrow a^L\equiv a(mod\ 10^n)\Rightarrow a\in A(L,n)$

所以我們有

$$\bigcup_{k-1|L-1}^{L-1}\Delta(k,n)\subset A(L,n)$$

$a\in A(L,n)\Rightarrow$必有$a^k\equiv a(mod\ 10^n)$，依定義$A(L,n)\subset\bigcup_{k-1|L-1}^{L-1}\Delta(k,n)$，故得證。

■

透過定理 12，我們便可以透過求出$\Delta(k,n)$來推得所有的自守數。

舉個例子，若我們欲得出7階自守數的集合$A(7,n)$，那麼可用來聯集的集合便是$\Delta(7,n)$、$\Delta(4,n)$、$\Delta(3,n)$、$\Delta(2,n)$，即$A(7,n)=\Delta(7,n)\cup\Delta(4,n)\cup\Delta(3,n)\cup\Delta(2,n)$。

而因為任何的$\Delta(k,n)$都不存在交集，我們得到了更優秀的結論，所以我們只要找出每一個$\Delta(k,n)$的長相即可完成我們的目標，這點可以清楚地展現出最小自守的用處和意義。

由於以下諸多性質受到$n\geq 3$之限制，我們接下來的定理(定理 13~定理 17)將直接預設所有的$n\geq 3$，而$n<3$之情況由於可直接計算得出，因此不再贅述，可在附錄三、附錄四查詢最小自守表驗證。

對於$\Delta(k,n)$的尋找，我們採取同樣的策略，分成 4 個情況討論。

定理 13

$\forall a \in \Delta(k,n)$且$(a,10)=10$ 時滿足的解不存在

Pf:

$\because a \in \Delta(k,n) \Leftrightarrow a^k \equiv a(mod\ 10^n) \Leftrightarrow a(a^{k-1}-1) \equiv 0(mod\ 10^n)$ 由$(a,10)=10$

和$(a^{k-1}-1,10)=1$，我們可以得到$a \equiv 0(mod\ 10^n)$

$\because a < 10^n \in \mathbb{N}$ ∴無解

■

$(a,10)=10$的情況固然簡單，但對於其他狀況我們卻遇到了瓶頸。

其他情況不存在這種簡易的判斷方法，因為最小自守即觀察$a^k \equiv a(mod\ 10^n)$的最小次方，是利用定理 12 的證明過程與最小自守的定義，等價於觀察$a^{k-1} \equiv 1(mod\ 10^n)$，若能窮舉所有$a < 10^n$的$a$值，便能完成我們的工作。

但是由於這些a的冪次計算太過困難，若能利用單一個數的冪次求得所有10^n下的所有a值，我們的工作就將化為可能——為此我們找到了名叫「原根」的定義。

定義a是p的原根，若且唯若$ord_p(a)=\varphi(p)$

也就是說，不存在兩個正整數$x,y < \varphi(p)$，使得原根a滿足$a^x = a^y$。

這樣的好性質使我們能利用一個數字討論所有可能，並使用冪次的因倍數關係做分析。

又由於5^n有原根3，因此在$(a,10)=2$時我們能就3^x的值來討論所有的解。

為了調整3^x的指數x能嚴謹討論所有可能性，我們引出了新的定理。

定理 14

若給定k欲尋找x滿足$1 \le x \le ord_d(a)$， 且$k-1$為最小的正整數使得$(a^x)^{k-1} \equiv 1\ (mod\ d)$，若且惟若$x=\frac{l}{k-1}ord_d(a)$ 其中l,k滿足$l,k \in \mathbb{N}$，$l \le k-1$，$(l,k-1)=1$，$k-1 \mid ord_d(a)$。

Pf:顯然若$x=\frac{l}{k-1}ord_d(a)$，$(a^x)^{k-1} \equiv 1\ (mod\ d)$必成立，

因此以下證明若$(a^x)^{k-1} \equiv 1\ (mod\ d)$，則$x=\frac{l}{k-1}ord_d(a)$

由引理 1，$ord_d(a) \mid x(k-1)$，令$l \times ord_d(a) = x(k-1) \Leftrightarrow x=\frac{l}{k-1}ord_d(a)$，

接下來說明其中l,k需滿足的條件，由於命題中k是最小正整數，因此若l和$k-1$可約的話，

必存在一數k'小於$k-1$且$(a^x)^{k'} \equiv 1\ (mod\ d)$，因此$(l,k-1)=1$，

注意到x為一個正整數，因此$\frac{l}{k-1} ord_d(a)$必須是整數，又$(l,k-1)=1$，

因此$k-1|ord_d(a)$必須成立，總結以上定理 14 成立。

■

舉個例子，若$k=6$，$a=3,d=5^2$，則$x=\frac{l}{6-1} ord_{5^2}(3)=\frac{l}{5}\times 4\times 5=4l$，

欲滿足$l\le k-1$，$(l,k-1)=1$，則$l=1,2,3,4$，即$x=4,8,12,16$。

但是這樣不夠，由於接下來定理 15 欲滿足的條件有$a\equiv 0(mod\ 2^n)$，為了使數字被2^n整除，我們選擇直接為數字乘上$1-5^{\varphi(2^n)}$，這樣計算出來的數字不會是0，又能保證數字被整除，最重要的是在5^n的同餘系下$1-5^{\varphi(2^n)}$將等價1，恰好滿足了所有性質。

定理 15

$(a,10)=2$ 且$a\in\Delta(k,n)$，若且唯若， a滿足

$$a\equiv 3^x\times\left(1-5^{\varphi(2^n)}\right)(mod\ 10^n),$$

其中$x=\frac{l}{k-1}\cdot 4\times 5^n, l\le k-1, (l,k-1)=1$，且$x\in\mathbb{Z}$

Pf:

首先，由$a\in\Delta(k,n)$我們有$a^k\equiv a\ (mod\ 10^n)$，而我們可以將其分解成下式

$a^k\equiv a\ (mod\ 10^n)\Leftrightarrow a(a^{k-1}-1)\equiv 0(mod\ 10^n)$，注意到$(a,a^{k-1}-1)=1$，因此由

$(a,10)=2$我們推論$a(a^{k-1}-1)\equiv 0(mod\ 10^n)\Leftrightarrow\begin{cases} a\equiv 0(mod\ 2^n)\\ a^{k-1}\equiv 1(mod\ 5^n)\end{cases}$

現在我們考慮右式的條件，先考慮$a^{k-1}\equiv 1(mod\ 5^n)$

首先我們希望由原根來表示a，也就是滿足$ord_{5^n}(g)=\varphi(5^n)$的正整數$g$，此時注意到由

引理 2，$ord_{5^n}(3)=\varphi(5^n)$，因此 3 為原根，我將用$3^x$來表示$a$，故上式改為

$(3^x)^{k-1}\equiv 1(mod\ 5^n)$再根據定理 14，我們可以更加的限制$x$，

即得出$x=\frac{l}{k-1} ord_{5^n}(3)$，其中 $l\le k-1, (l,k-1)=1$，$k-1|ord_d(a)$，

然而這樣的a並不滿足條件$a\equiv 0(mod\ 2^n)$，因此我選擇在同餘下直接乘上

$\left(1-5^{\varphi(2^n)}\right)$，這樣做並不改變$a^{k-1}\equiv 1(mod\ 5^n)$這個條件，而且將滿足

$a\equiv 0(mod\ 2^n)$，故我們得出$a\equiv 3^x\times\left(1-5^{\varphi(2^n)}\right)(mod\ 10^n)$,為我們要的解

■

接下來若$(a,10)=5$，即要考慮同餘2^n的。

在研究過程中，我們注意到2^n並不存在原根，這使研究困難性又再一次增加。

我們目前可以確定的是，根據引理 3，當$n\geq 3$時2^n存在3使得$ord_{2^n}(3)=2^{n-2}=\frac{\varphi(2^n)}{2}$，表示我們依然能以$3^x$枚舉至少一半的可能性。

有沒有辦法透過這一半生成出另一半的可能性呢？最開始我們想尋找一個3^x不能表示的數字r，這樣便能以$r\cdot 3^x$表示剩下的數字，而很幸運地，我們發現$r=-1$時，這樣的結論恰好成立！

引理 5

若 $n\geq 3$, 則$\forall k\in\mathbb{N}, 3^k\not\equiv -1(mod\ 2^n)$

Pf:

設$k,n,m\in\mathbb{N}, n=1$時顯然無解，$n=2$時，$k=1$為唯一解，以下考慮$n\geq 3$

設$3^k\equiv -1(mod\ 2^n)\Rightarrow 3^k=m\cdot 2^n-1\Rightarrow 3^k\equiv -1(mod\ 8)$

但$3^2\equiv 1(mod\ 8)$,$3\equiv 3(mod\ 8)$，因此$3^k\equiv -1(mod\ 8)$不可能成立，引理 5 得證。

■

透過引理 5，我們便可以推論$\pm 3^x$將能夠討論所有的可能解。

定理 16

$(a,10)=5$ 且$a\in\Delta(k,n)$，若且唯若 $(k-1)|2^{n-2}$ ，a滿足

$$a\equiv \mu 3^x\times\left(1-2^{\varphi(5^n)}\right)(mod\ 10^n)$$

其中$x=\frac{i}{k-1}\cdot 2^{n-2}, i\le k-1, \mu=\begin{cases}1 & k=2,(l,k-1)=1\\ 1 or -1 & k\neq 2,(l,k-1)=1\\ -1 & 4|k-3,(l,k-1)=2\end{cases}$

Pf:

由$a\in\Delta(k,n)$我們有$a^k\equiv a\ (mod\ 10^n)\Leftrightarrow a(a^{k-1}-1)\equiv 0\ (mod\ 10^n)$，而由$(a,a^{k-1}-1)=1$，以及$(a,10)=5$，我們可以進一步得出

$a(a^{k-1}-1)\equiv 0\ (mod\ 10^n)\Leftrightarrow\begin{cases}a\equiv 0\ (mod\ 5^n)\\ a^{k-1}\equiv 1\ (mod\ 2^n)\end{cases}$接下來我們將目標放在右式，

考慮條件$a^{k-1}\equiv 1\ (mod\ 2^n)$，我們希望由原根來表示$a$，但和定理 15 不同的地方在於$2^n$並沒有原根，但是我們發現了$3^x$可以表示恰好一半的數，下一步我們希望可以找到一數$t$使得$3^x\not\equiv t(mod\ 2^n)$，而由引理 5，

我們得到$3^x\not\equiv -1(mod\ 2^n)$這件事，達成了我們的目標，

以下證明我們如何辦到利用-1 來表示所有的數。

設$S_{2^n}=\{l\mid 2\nmid l, l<2^n\}$

$S_3=\{l\mid 3^m\equiv l(mod\ 2^n), l<2^n\}, S_3'=\{l\mid -(3^m)\equiv l(mod\ 2^n), l<2^n\}$

根據引理 3，$ord_{2^n}(3)=2^{n-2}$；

又根據引理 5，$3^m\not\equiv -1(mod\ 2^n), m\in\mathbb{N}\Rightarrow$ 故$S_3\cap S_3'=\emptyset$，

而我們知道S_3和S_3'的元素個數一樣多，又這兩個集合的元素個數恰好等於S_{2^n}元素個數，故我們可以推論$S_3\cup S_3'=S_{2^n}$，也就是說，如果$1\le x\le 2^{n-2}$，在同餘2^n的情況下$\pm 3^x$可以出現$1\sim 2^n$的所有情況。

考慮兩個情況，$A\equiv 3^x\ (mod\ 2^n), B\equiv -3^x\ (mod\ 2^n)$

$A\equiv 3^x\ (mod\ 2^n)$，此時直接使用定理 14 即可

1°若$k-1$為偶數

$B\equiv -3^x(mod\ 2^n)$，$\because B^{k-1}\equiv(-1)^{k-1}(3^x)^{k-1}\equiv A^{k-1}(mod\ 2^n)$，同$A$的情況。

但若$4|k-3$，則$B^{\frac{k-1}{2}} \equiv (-1)^{\frac{k-1}{2}}(3^x)^{\frac{k-1}{2}} \equiv -A^{\frac{k-1}{2}} \not\equiv A^{\frac{k-1}{2}}(mod\ 2^n)$

由於$\frac{k-1}{2}$的倍數中，最小的卻又比$\frac{k-1}{2}$大的數字就是$k-1$，並能使負號被消除，形成最小自守，故當$4|k-3$，我們必須針對定理 14 的數對l,k多討論一種$(l,k-1)=2$的情況。

2°若$k-1$為奇數，由定理 14，$k-1|2^{n-2} \Rightarrow k=2$

$B \equiv -3^x(mod\ 2^n)$，$\because B^{k-1} \equiv (-1)^{k-1}(3^x)^{k-1} \equiv -(3^x)^{k-1}(mod\ 2^n)$

根據引理 5，$(3^x)^{k-1} \not\equiv -1(mod\ 2^n) \Leftrightarrow -(3^x)^{k-1} \not\equiv 1(mod\ 2^n)$，故無解。

為了方便描述，我們將解表示為$\mu 3^x$，

其中$\mu = \begin{cases} 1 & ,k=2\ and\ (l,k-1)=1 \\ 1or-1 & ,k\neq 2\ and\ (l,k-1)=1 \\ -1 & ,4|k-3\ and\ (l,k-1)=2 \end{cases}$

所以我們令$a \equiv \mu 3^x \times \left(1-2^{\varphi(5^n)}\right)(mod\ 10^n)$，則可同時滿足$\begin{cases} a \equiv 0(mod\ 5^n) \\ a^{k-1} \equiv 1(mod\ 2^n) \end{cases} \Leftrightarrow$

$\begin{cases} (a,10)=5 \\ a^k \equiv a(mod\ 10^n) \end{cases}$，這樣我們就找出了同餘$10^n$下所有可能的$a$。

■

最棘手的情況回到$(a,10)=1$，有了先前原命題將10分成2,5討論的經驗，我們事先證明出了引理 6：

引理 6

$a^L \equiv 1(mod\ 10^n) \Leftrightarrow a^L \equiv 1(mod\ 2^n)$且$a^L \equiv 1(mod\ 5^n)$

Pf:

1° ⇒

令$a^L = 10^n \cdot m+1, m \in \mathbb{N} \cup \{0\}$，則$a^L \equiv 1(mod\ 2^n) \wedge a^L \equiv 1(mod\ 5^n)$

2° ⇐

令$a^L = 2^n \cdot m+1, m \in \mathbb{N} \cup \{0\}$

$\because (2^n,5^n)=1 \ \therefore 5^n|m \ \therefore 10^n|2^n \cdot m \ \therefore a^L \equiv 1(mod\ 10^n)$

總結以上，即得出引理 6

$$a^L \equiv 1(mod\ 10^n) \Leftrightarrow a^L \equiv 1(mod\ 2^n)\text{且}a^L \equiv 1(mod\ 5^n)$$

■

這樣的性質是非常漂亮的，因為有了這樣的對應關係，我們可以直接把定理 15 和定理 16 的結論做結合。

恰好前兩個定理得出的數字都各自會讓另一個因數整除自己，所以結合後將不會互相影響，又能同時滿足兩個性質。

即$\begin{cases} A \equiv 0(mod\ 2^n) \\ A^x \equiv 1(mod\ 5^n) \end{cases}$、$\begin{cases} B \equiv 0(mod\ 5^n) \\ B^y \equiv 1(mod\ 2^n) \end{cases}$，則令$a = A + B$後，能同時滿足$\begin{cases} a^{k-1} \equiv 1(mod\ 5^n) \\ a^{k-1} \equiv 1(mod\ 2^n) \end{cases}$，我們可以任意調整$x$與$y$以便滿足引理 6 的條件。

但在證明過程中我們發現，還存在一個微小的問題需要解決，不同於先前的定理，定理 17 不能直接在分母擺上$k-1$，我們注意到這樣無法生成出所有的自守數。

透過推導後我們發現，若分母i,j滿足$lcm(i,j) = (k-1)$，同樣能夠生成出最小自守為k的自守數，如此一來問題在細節處理完後便被完整地被解決了。

定理 17

$(a,10) = 1$，$a \in \Delta(k,n)$的所有解為

$$a \equiv 3^x \times \left(1 - 5^{\varphi(2^n)}\right) + \mu 3^y \times \left(1 - 2^{\varphi(5^n)}\right)(mod\ 10^n)$$

其中$x = \frac{\mathrm{i}}{k-1} \cdot 4 \times 5^{n-1}, i \le k-1$，$y = \frac{j}{k-1} \cdot 2^{n-2}, j \le k-1$，$x, y \in \mathbb{N}$

$$\mu = \begin{cases} 1 & ,2 \mid k\ and\ gcd(i,j,k-1) = 1 \\ 1 or -1 & ,2 \nmid k\ and\ gcd(i,j,k-1) = 1 \\ -1 & ,4 \mid k-3\ and\ gcd(i,j,k-1) = 2 \end{cases}$$

Pf:

由$a \in \Delta(k,n)$知$a^k \equiv a(mod\ 10^n) \Longrightarrow a(a^{k-1} - 1) \equiv 0\ (mod\ 10^n)$

且$(a,10) = 1$故$a^{k-1} \equiv 1(mod\ 10^n)$

根據引理 6, $a^{k-1} \equiv 1(mod\ 10^n) \Leftrightarrow \begin{cases} a^{k-1} \equiv 1(mod\ 5^n) \\ a^{k-1} \equiv 1(mod\ 2^n) \end{cases}$

尋找所有$a^{k-1} \equiv 1(mod\ 5^n)$，同定理 15 討論方式，令$A = 3^x$滿足$A^{k-1} \equiv 1\ (mod 5^n)$，由定理 14 有$x = \frac{i}{k-1} \cdot 4 \times 5^{n-1}$，其中$, i \le k-1$

同理尋找所有$a^{k-1} \equiv 1(mod\ 2^n)$，同定理 16 討論方式，令$B = \mu 3^y$滿足$B^{k-1} \equiv 1\ (mod 2^n)$，由定理 14 有$y = \frac{j}{k-1} \cdot 2^{n-2}$，其中$j \le k-1$

在定理 16 中因為有兩類情況的解，當$k-1$為偶數$B=\pm 3^y$，且當$4|k-3$同樣的必須多考慮$gcd(i,j,k-1)=2$

我們一樣利用$\mu 3^y$來描述解的情況，

$$\mu=\begin{cases} 1 & ,2\mid k\ and\ gcd(i,j,k-1)=1 \\ 1 or -1 & ,2\nmid k\ and\ gcd(i,j,k-1)=1 \\ -1 & ,4|k-3\ and\ gcd(i,j,k-1)=2 \end{cases}$$

反之如果我們有$\begin{cases} a^{k-1}\equiv 1(mod\ 5^n) \\ a^{k-1}\equiv 1(mod\ 2^n) \end{cases}\Rightarrow a^L\equiv 1(mod\ 10^n)$

因為k為最小自守，所以必須有$L=k-1$，

令$a\equiv 3^x\times\left(1-5^{\varphi(2^n)}\right)+\mu 3^y\times\left(1-2^{\varphi(5^n)}\right)(mod\ 10^n)$，即滿足$\begin{cases} a^{k-1}\equiv 1(mod\ 5^n) \\ a^{k-1}\equiv 1(mod\ 2^n) \end{cases}$，

擁有上述條件，可知$(a,10)=1$，$a\in\Delta(k,n)$的所有解為定理 16 所述。

■

定理 17 求得自守數的方法比起暴力枚舉在速度上有非常好的進步，由於小於$k-1$的數個數只有$k-2$個，也就是i有$k-2$種可能，$x=\frac{i}{k-1}$，我們有不超過$k-2$個數，而y同理。

故我們只需要枚舉不超過$k\times k=k^2$種組合，便能求出所有定理 17 可得出的自守數，與最原始地暴力窮舉10^n底下的數字顯然有了極大的效率增進。

舉個例子，當$k=3,n=3$，符合條件的數對(i,j)共有$(1,1),(1,2),(2,1),(2,2)$四種，其中：

數對$(2,2)$對應到了$4|k-3$的情況，產生一個三階自守數 751；

數對$(2,1)$使用原本$2\nmid k$的通式，產生兩個三階自守數 251、501；

數對$(1,2)$使用原本$2\nmid k$的通式，產生兩個三階自守數 249、999；

數對$(1,1)$使用原本$2\nmid k$的通式，產生兩個三階自守數 499、749。

現在我們能利用定理 13、定理 15 至 17 生成出$\Delta(k,n)$集合內的多個解，而且因為$(a,10)$只有$1,2,5,10$四種可能，所以我們一定能確定這些定理導出來的數字能涵蓋住整個$\Delta(k,n)$集合。

於是我們最後便能透過定理 12 找到$A(k,n)$之所有解。

接下來我們關注一個問題，有沒有可能找出k階自守數的個數呢？

注意到在定理 15、16 中自守數個數事實上就是找出$gcd(k-1,i)=1$的i的個數，至於定理 17 則是找出$gcd(i,j,k-1)=1$，的數對(i,j)的個數，前者比較容易，因此我們把重點放在後者的研究。

定理 18

給定正整數k滿足$gcd(k-1,i)=1$，i的個數為$\varphi(k-1)$，此處的φ表示尤拉函數
假設給定正整數k滿足$gcd(i,j,k-1)=1$的個數為$f(k-1)$，若$x=p_1^{a_1}p_2^{a_2}\dots p_n^{a_n}$

$$\text{則 } f(x)=\prod_{i=1}^{n}(p_i^2-1)p_i^{2(a_i-1)}$$

Pf:

可以用排列組合算出滿足$gcd(i,j,x)=1$的個數為

$$\sum_{d|x}^{x} d\phi(d)\phi\left(\frac{x}{d}\right)=\prod_{i=1}^{n}(p_i^2-1)p_i^{2(a_i-1)}$$

我們分析生成最小自守集合演算法時間複雜度之改進。

原先暴力法我們將枚舉$O(10^n)$個數字，花費約莫$O(10^n)$的乘法求得最小自守，總時間複雜度將慘至$O(10^{2n})$。

使用定理 9~11 計算最小自守，每個數字可花費$O(logn)$的時間求得最小自守，其總時間複雜度依然只能降至$O(10^n logn)$。

如果改用定理 15~17 生成自守數，首先在定理 15、16 只需要枚舉l，故只需要$O(k)$的時間完成計算，定理 17 即如先前所說，需要$O(k^2)$，故我們總時間複雜度只需要$O(k^2)$便能完成自守數的生成(其n的增長只與機器計算數字的速度相關)！

參考資料及其他

一、簡明數論 潘承洞、潘承彪著（北京大學出版社）

二、MathWorld 自守數的相關資料 埃里克·韋斯坦因著

http://mathworld.wolfram.com/AutomorphicNumber.html