中華民國第 60 屆中小學科學展覽會

作品說明書

高級中等學校組　數學科

探究精神獎

050409

數迴從之

學校名稱：國立臺東高級中學

作者：	指導老師：
高二 張棋鈞 高二 汪承希 高二 林柏辰	簡愷邑

關鍵詞：遞迴數列、同餘、週期性

摘要

本研究在等差數列的基礎上，加入「若a_n為完全平方數，則$a_{n+1}=\sqrt{a_n}$」的遞迴關係，將具有週期性的數列分為「單純週期數列」與「特殊週期數列」，並以單純週期數列為主要研究目標。我們探討單純週期數列的各項性質與充要條件，並透過歐拉準則與費馬小定理討論不同公差與首項是否能形成單純週期，整合與建構「給定公差，尋找可形成週期的首項」之方法，也研究特殊週期數列之性質與充要條件。

壹、 研究動機

在專題課的下課時分，我們在教室書櫃找到數戰數決一書，便被書中的精彩故事深深吸引，同時讓我們對 IMO 國際數學奧林匹亞競賽有更多的認識，也對它的試題產生好奇。上課時，我們上網觀摩幾屆數奧的試題與解析，發現一道結合等差數列與週期性的題目：

問題 1: 對於每個整數 $a_0 > 1$, 用以下方法定義數列 $a_0, a_1, a_2, \ldots$:

$$a_{n+1} = \begin{cases} \sqrt{a_n} & \text{若}\sqrt{a_n}\text{爲整數} \\ a_n + 3 & \text{其他情況} \end{cases} \quad \text{對於所有 } n \geqslant 0\text{皆成立}$$

試求所有可能值 a_0, 滿足存在一個數 A, 使得有無窮多個 n 讓 $a_n = A$。

我們對具有週期性的等差數列(以下稱週期數列)感到相當有趣，決定深入探討週期數列的性質及尋找能形成週期數列的條件，並定義新題目如下：

$a_{n+1}=\begin{cases}\sqrt{a_n} & \text{若}\sqrt{a_n}\text{為正整數}\\ a_n+k & \text{其他情況}\end{cases}$ 對於所有$a_n>1$，$k\in\mathbb{N}$ 且$n\in\mathbb{N}$ 皆成立。尋找一數a_n滿足存在無限多個a_m， $m\in\mathbb{N}$， $m>n$且$a_m=a_n$。

貳、 研究目的

一、尋找單純週期數列形成的條件。

二、討論在公差為一個質數、多個質數相乘，乃至於多質數相乘且存在高次方，如何在給定公差後尋找一數代入a_n使數列形成週期。

三、探討特殊週期數列形成的條件與建構方式。

參、 研究設備及器材

紙、筆、電腦程式(Python,C++)

肆、 研究過程或方法

一、名詞定義

1. k：滿足$k \in \mathbb{N}$，為數列的公差
2. a_n：數列中第n項
3. a：滿足$a \in \mathbb{N}$，$a \leq k$，$a^2 \equiv a(mod\ k)$
4. $A_n = \{2,3,4,\dots\dots,k-1\}$
5. b：滿足$b \in \mathbb{N}$，$b \in A_n$，$b < a$，$b^2 \equiv a(mod\ k)$
6. $\langle a_m \rangle$，$m = 1 \sim n$：週期數列$\langle a, a+k, \dots\dots, a^2, a \rangle$
7. $\langle a_\alpha \rangle$：單純週期數列$\langle a, a+k, \dots\dots, a^2, a \rangle$，滿足$a_i \equiv a(mod\ k)$
8. $\langle a_\beta \rangle$：特殊週期數列$\langle a, a+k, \dots\dots, a^2, a \rangle$，滿足$\exists j \in \mathbb{N}$：$a_j \not\equiv a(mod\ k)$
9. 公差k的列表：分為左右兩欄，左欄由上而下依序為$0 \sim k-1$，右欄為對應左欄的數平方後除以k的餘數。
10. 對稱軸：在某公差k的列表中，若左欄有一數n滿足$n \in \mathbb{Q}$，$0 < n < k-1$ 且$(n+t)^2 \equiv (n-t)^2(mod\ k)$，其中$t \in \mathbb{Q}$且$t < \frac{k}{4}$，則稱$n$為公差$k$的列表的對稱軸。

二、先備知識

(一)費馬小定理

對於$p \in \mathbb{Z}$，k為質數，$p^k \equiv p(mod\ k)$必成立。若$k \nmid p$，此定理亦可表示為$p^{k-1} \equiv 1(mod\ k)$。

(二)歐拉準則

對於$n \in \mathbb{N}$，k為奇質數，n是k的二次剩餘若且唯若$n^{\frac{k-1}{2}} \equiv 1(mod\ k)$。

【定理1】歐拉準則的應用

若p、q皆為大於1之正整數，k為奇質數，滿足$k \nmid pq$、$pq \equiv 1(mod\ k)$，則$p \equiv q^{k-2}(mod\ k)$。

<證明>

1° $\because pq \equiv 1(mod\ k)$，$\therefore pq$為$k$的二次剩餘。

由歐拉準則可知$(pq)^{\frac{k-1}{2}} \equiv 1(mod\ k)$，

$(pq)^{k-1} \equiv 1(mod\ k)$，$(pq)^k \equiv pq(mod\ k)$。

$\because (pq)^2 \equiv pq(mod\ k)$，$\therefore (pq)^k \equiv (pq)^2(mod\ k)$，

$\because k \nmid pq$，$\therefore (pq)^{k-2} \equiv 1(mod\ k)$。

2° 由費馬小定理可知$p^{k-1} \equiv 1(mod\ k)$， $p^{k-2}p \equiv 1(mod\ k)$，

則$p^{k-2}p \equiv (pq)^{k-2}(mod\ k)$，得$p \equiv q^{k-2}(mod\ k)$。■

(三)歐拉定理

對於$p \in \mathbb{N}$，$k \in \mathbb{N}$，$(k,p) = 1$，恆有$p^{\varphi(k)} \equiv 1(mod\ k)$ (其中$\varphi(k)$稱為歐拉函數，表示滿足$n \in \mathbb{N}$、$n \leq k$、$(k,n) = 1$的n的數量)。此定理為費馬小定理的延伸，易知當k為質數時$\varphi(k) = n - 1$，$p^{n-1} \equiv 1(mod\ k)$即費馬小定理。

三、前置研究

我們在「(四)特殊週期數列$\langle a_\beta \rangle$」會討論特殊週期數列的性質與建構，其餘的分析與證明皆以單純週期數列$\langle a_\alpha \rangle$為主。

(一)單純週期數列$\langle a_\alpha \rangle$的性質

觀察一些已知的單純週期數列，例如：

1. $k = 3$，$a_n = 3$，$\langle a_\alpha \rangle$ =3,6,9,3
2. $k = 6$，$a_n = 6$，$\langle a_\alpha \rangle$ =6,12,18,24,30,36,6
3. $k = 39$，$a_n = 13$，$\langle a_\alpha \rangle$ =13,52,91,130,169,13

我們可以發現，$\langle a_\alpha \rangle$形成週期的關鍵在於數列遞增時某項出現完全平方數，下一項開根號後形成週期。

【性質1-1】a^2的存在性

對於所有$\langle a_\alpha \rangle$皆滿足：$a_n = a$、$a \leq k$，形成$\langle a_\alpha \rangle$的必要條件為$\exists i \in \mathbb{N}$、$i > n$：$a_i = a^2$。

<證明>

設$\nexists i \in \mathbb{N}$、$i > n$：$a_i = a^2$，

1° 若$\langle a_\alpha\rangle$任一項皆不是完全平方數，則對於$j\in\mathbb{N}、j>n$皆滿足$a_{j+1}=a_j+k>a(\because a\le k)$。

2° 若$\langle a_\alpha\rangle$中，$\exists \ell\in\mathbb{N}、\ell>n:\sqrt{a_\ell}\in\mathbb{N}$，

則$\sqrt{a_\ell}\neq a$必成立$(\because \nexists i\in\mathbb{N}、i>n:a_i=a^2)$，且$\sqrt{a_\ell}+k\neq a$亦成立$(\because a\le k)$。■

【性質1-2】a為k的二次剩餘

對於所有$\langle a_\alpha\rangle$皆存在：$a^2\equiv a(mod\ k)$。

<證明>

$\because$對於所有$\langle a_\alpha\rangle$皆滿足：$a_j\equiv a(mod\ k)$，$\therefore$恆有$a^2\equiv a(mod\ k)$。■

【性質1-3】無限多個a_m的存在性

對於所有$\langle a_\alpha\rangle$皆滿足：若$\exists m\in\mathbb{N}、\ m>n:a_m=a_n$，則存在無限多個$a_m$。

<證明>

$\because\exists m\in\mathbb{N}、m>n:a_m=a_n$，$\therefore\exists 2m-n\in\mathbb{N}:a_{2m-n}=a_n$。

顯然$\exists x\in\mathbb{N}、m\in\mathbb{N}、m-n\in\mathbb{N}:a_{n+x(m-n)}=a_n$。■

我們同時發現：對於單純週期數列$\langle a_\alpha\rangle$，其他條件相同時，數列中任意一數作為a_n皆可以使數列進入週期。為了簡化形成單純週期數列$\langle a_\alpha\rangle$的條件，我們未來的研究將以尋找數列中最小的數為目標。

【引理1-4-1】

$b_{j+1}=\begin{cases}\frac{b_j}{2}&，若b_j是偶數\\ \frac{b_j+1}{2}&，若b_j是奇數\end{cases}$ 對於所有$j\in\mathbb{N}$，b_1為偶數皆滿足$\exists \ell\in\mathbb{N}、\ell>j:b_\ell=1$。

<證明>

1° 若b_j是偶數，設$b_j=2t(t\in\mathbb{N})$，則$b_{j+1}=t$，

$\because t<2t=b_j$，$\therefore b_{j+1}<b_j$。

因此當b_j是偶數時，$\exists r\in\mathbb{N}、r>j:b_r<b_j$。

2° 若b_j是奇數，設$b_j=2t'+1(t'\in\mathbb{Z}、t'\ge 0)$，則$b_{j+1}=t'+1$，

$\because\forall t'\in\mathbb{N}:t'+1<2t'+1$，$\therefore\exists!\, t'=0:t'+1=2t'+1$，

此時$b_j = b_\ell = 1$。■

【性質1-4】a的最小性

當$k \geq 3$，$\langle a_\alpha \rangle$滿足$\exists i \in \mathbb{N}：a_i = a$且$\nexists j \in \mathbb{N}：a_j < a$。

<證明>

已知存在有限個b_i滿足${b_i}^2 \equiv a(mod\ k)$，不失一般性設$b_i = b_1, b_2, b_3, \dots\dots, b_n$，

且$b_1 < b_2 < b_3 < \cdots < b_n$。在不遇到${b_i}^2$的條件下(顯然$k < 3$時不合)，

$\exists m \in \mathbb{N}、s \in \mathbb{N}、m > n：a_m = a^{2s}$。由**【引理1-4-1】**可知，數列在$a^{2s}$後恆存在一項$a$。

$\because a_i \equiv a(mod\ k)$，$\therefore$對於所有$\langle a_\alpha \rangle$皆滿足$\nexists j \in \mathbb{N}：a_j < a$。■

(二)尋找$\langle a_\alpha \rangle$的形成條件

我們寫出k的列表，藉此尋找k的二次剩餘，如表 1：

表 1

0	$0^2(mod\ k)$
1	$1^2(mod\ k)$
2	$2^2(mod\ k)$
⋮	⋮
$k-2$	$(k-2)^2(mod\ k)$
$k-1$	$(k-1)^2(mod\ k)$

以$k = 6$為例，如表 2：

表 2

0	0
1	1
2	4
3	3
4	4
5	1

從k的列表中除了可找出k的二次剩餘外，我們也發現一些性質：右欄除了最上方的0外，呈現上下對稱，我們稱為二分對稱性。

【性質2-1】列表右欄的二分對稱性與二分對稱軸

k的列表右欄除了最上方的 0 外，呈現上下對稱，且對稱軸為$\frac{k}{2}$。

<證明>

1° 當$2 \mid k$，設$(\frac{k}{2}+t)^2 \not\equiv (\frac{k}{2}-t)^2 (mod\ k)$(其中$t \in \mathbb{N}$)，

則$\frac{k^2}{4}+kt+t^2 \not\equiv \frac{k^2}{4}-kt+t^2 (mod\ k)$，$2kt \not\equiv 0(mod\ k)$，矛盾。

因此恆有$(\frac{k}{2}+t)^2 \equiv (\frac{k}{2}-t)^2 (mod\ k)$。

2° 當$2 \nmid k$，設$(\frac{k+1}{2}+t')^2 \not\equiv (\frac{k-1}{2}-t')^2 (mod\ k)$(其中$t' \in \mathbb{N}$)，

$\frac{k^2+2k+1}{4}+t'(k+1)+t'^2 \not\equiv \frac{k^2-2k+1}{4}-t'(k-1)+t'^2 (mod\ k)$，

$\frac{k^2+2k+1}{4}+kt' \not\equiv \frac{k^2-2k+1}{4}-kt' (mod\ k)$，

$k^2+2k+1+4kt' \not\equiv k^2-2k+1-4kt' (mod\ k)$，

$4k(1+2t') \not\equiv 0(mod\ k)$，矛盾。

故恆有$(\frac{k+1}{2}+t')^2 \equiv \left(\frac{k-1}{2}-t'\right)^2 (mod\ k)$。■

我們觀察其他k的列表，發現有時會出現兩條以上的對稱軸。以$k=8$為例，如表 3：

表 3

0	0
1	1
2	4
3	1
4	0
5	1
6	4
7	1

由表 3 可以發現右欄不僅以$\frac{k}{2}$為對稱軸，$\frac{k}{4}$和$\frac{3k}{4}$也是對稱軸。對於$\frac{k}{4}$和$\frac{3k}{4}$的上下對稱性，我們稱為四分對稱性，$\frac{k}{4}$和$\frac{3k}{4}$兩數稱為四分對稱軸。此外，我們也好奇$\frac{nk}{2^s}$($s \in \mathbb{N}$，n為奇數且$n<2^s$)是否皆為對稱軸？但是觀察$k=8$的例子(表 3)中並不存在對應左欄$\frac{k}{8}$為對稱

軸的性質。我們討論**【性質2-2】**、**【性質2-3】**及**【性質2-4】**：

【性質2-2】列表的四分對稱性與四分對稱軸

當k滿足 $4 \mid k$：列表除了以 $\frac{k}{2}$ 為對稱軸外，$\frac{k}{4}$ 和 $\frac{3k}{4}$ 亦為對稱軸。

<證明>

設$(\frac{k}{4}+t)^2 \not\equiv (\frac{k}{4}-t)^2 (mod\ k)$，$(\frac{k^2}{16}+\frac{k}{2}+1) \not\equiv (\frac{k^2}{16}-\frac{k}{2}+1) (mod\ k)$，

則$-\frac{k}{2} \not\equiv \frac{k}{2} (mod\ k)$，$k \not\equiv 0 (mod\ k)$，矛盾。

故恆有$\left(\frac{k}{4}+t\right)^2 \equiv \left(\frac{k}{4}-t\right)^2 (mod\ k)$，顯然亦恆有$\left(\frac{3k}{4}+t\right)^2 \equiv \left(\frac{3k}{4}-t\right)^2 (mod\ k)$。■

【性質2-3】四分對稱性的必要條件

若列表存在 $\frac{k}{4}$ 與 $\frac{3k}{4}$ 兩對稱軸，則$4 \mid k$。

<證明>

設$\frac{k}{4}+t \in \mathbb{N}$、$\frac{k}{4}-t \in \mathbb{N}$，$t \in \mathbb{R}$，$(\frac{k}{4}+t)^2 \equiv (\frac{k}{4}-t)^2 (mod\ k)$，

則 $\frac{kt}{2} \equiv -\frac{kt}{2} (mod\ k)$，$kt \equiv 0 (mod\ k)$，得 $t \in \mathbb{Z}$。

$\because \frac{k}{4}+t \in \mathbb{N}$，$\therefore \frac{k}{4} \in \mathbb{N}$，因此$4 \mid k$。■

【性質2-4】對稱軸的有限性

當$k = t2^s$，t、n為奇數，$s \in \mathbb{N}$、$s \geq 3$ 時 $\frac{nk}{2^s}$ 不為對稱軸。

<證明>

設r為奇數，若滿足$(\frac{n}{2^s}k+r)^2 \equiv (\frac{n}{2^s}k-r)^2 (mod\ k)$，

則 $\frac{n}{2^{s-1}}kr \equiv -\frac{n}{2^{s-1}}kr (mod\ k)$，$\frac{n}{2^{s-2}}kr \equiv 0 (mod\ k)$，

$\because k = t2^s$，$\therefore \frac{n}{2^{s-2}}kr = \frac{n}{2^{s-2}}t2^s r = 2^2 ntr$，

$\because s \geq 3$且n、t、r皆為奇數，$\therefore 2^2 ntr \not\equiv 0 (mod\ k)$，矛盾。

因此$(\frac{n}{2^s}k+r)^2 \not\equiv (\frac{n}{2^s}k-r)^2 (mod\ k)$。■

同時我們也發現：有些滿足$a^2 \equiv a(mod\ k)$的a代入a_n後卻無法形成週期。以$k = 10$為例，如表 4：

表 4

0	0
1	1
2	4
3	9
4	6
5	5
6	6
7	9
8	4
9	1

由表 4 可以發現：6 滿足$6^2 \equiv 6(mod\ 10)$，但$k = 10$、$a_n = 6$代入數列，形成$\langle 6,16,4,2,\dots\dots\rangle$不存在週期性(2不是10的二次剩餘)，將成為嚴格遞增數列。我們歸納不存在週期性的原因為存在b，且觀察表 4 可知存在$4 < 6$ 滿足$4^2 \equiv 6(mod\ 10)$。

【引理2-5-1】

已知$b < a \leq k$，則b^2、b^4、b^8、……、$b^{2^n}(n \in \mathbb{N})$必有一數介於$a$和$a^2$間。

<證明>

設$b^2 > a$，$\because b < a$，$\therefore b^2 < a^2$，$a < b^2 < a^2$。

設$b^2 < a$，$b^4 > a$，$\because b^2 < a$，$b^4 < a^2$，$\therefore a < b^4 < a^2$。

顯然b^2、b^4、b^8、……、b^{2^n}必有一數介於a和a^2間。■

【性質2-5】$\langle a_\alpha \rangle$成立的必要條件

以公差k、$a_n = a$形成$\langle a_\alpha \rangle$時，不存在b。

<證明>

由**【引理2-5-1】**可知：

若存在b，數列$\langle a, a+k, \ldots\ldots, b^{2^n}, \ldots\ldots, b\rangle$存在$b \not\equiv a(mod\ k)$，

與$\langle a_\alpha\rangle$必要條件$a_i \equiv a(mod\ k)$矛盾。■

【性質2-6】$\langle a_\alpha\rangle$成立的充要條件

$\langle a_\alpha\rangle$成立的充要條件為存在a且不存在b。

<證明>

設存在a且不存在b，$a_n = a$代入數列後，

∵不存在b，∴必有$m > n$滿足$a_m = a^2$，則$a_{m+1} = a$，

由**【性質1-3】**可知存在週期性。■

因為$\langle a_\alpha\rangle$成立的充要條件為存在a且不存在b，由列表的二分對稱性與四分對稱性可知：

在構造a滿足$a^2 \equiv a(mod\ k)$時，除了$a = k$(將在**【性質2-9】**討論)外僅需考慮$a \le \frac{k}{2}$(當$4 \nmid k$)

或$a \le \frac{k}{4}$(當$4 \mid k$)。

【性質2-7】構造a的相關條件

當$k = \prod_{i=1}^{n} p_i$ ，p_i為任意相異質數，$j \in \{1,2, \ldots\ldots, n-1\}$，對於$a \ge 2$恆有$(k, a) = \prod_{i=1}^{j} p_i$。

<證明>

若$p_s \nmid a (s \in \mathbb{N})$，∵$a^2 \equiv a(mod\ \prod_{i=1}^{n} p_i)$，∴$a(a-1) \equiv 0(mod\ \prod_{i=1}^{n} p_i)$，$\prod_{i=1}^{n} p_i \mid a-1$；

∵$a-1 < a \le \frac{k}{2} = \frac{\prod_{i=1}^{n} p_i}{2}$(因**【性質2-1】**僅考慮$a \le \frac{k}{2}$)且$a \ge 2$，∴$\prod_{i=1}^{n} p_i \nmid a-1$，矛盾。■

【引理2-8-1】

當$k = \prod_{i=1}^{n} {p_i}^{\alpha_i}\ (n \in \mathbb{N})$，$p_i$為任意相異質數，$j \in \{1,2, \ldots\ldots, n-1\}$，對於$a \ge 2$恆有$(k, a) = \prod_{1}^{j} p_i$。

<證明>

若$(k, a) = 1$，∵$a^2 \equiv a(mod\ \prod_{i=1}^{n} {p_i}^{\alpha_i})$，∴$a(a-1) \equiv 0(mod\ \prod_{i=1}^{n} {p_i}^{\alpha_i})$，

$\prod_{i=1}^{n} {p_i}^{\alpha_i} \mid (a-1)$，但$a-1 < a \le \frac{k}{2} = \frac{\prod_{i=1}^{n} {p_i}^{\alpha_i}}{2}$，當$a \ge 2$時$\prod_{i=1}^{n} {p_i}^{\alpha_i} \nmid (a-1)$，矛盾。■

【引理2-8-2】

當$k=\prod_{i=1}^{n}{p_i}^{\alpha_i}\ (n\in\mathbb{N}、\alpha_i\in\mathbb{N})$，$p_i$為任意相異質數，$j\in\{1,2,\dots\dots,n\}$，對於$a\geq 2$若滿足$p_j\mid a$，即恆有${p_j}^{\alpha_j}\mid a$。

<證明>

不失一般性設$j=n$且$a=tp_n(t\in\mathbb{N})$，

$\because a^2\equiv a(mod\ \prod_{i=1}^{n}{p_i}^{\alpha_i})$，$\therefore a(a-1)\equiv 0(mod\ \prod_{i=1}^{n}{p_i}^{\alpha_i})$，

$a=tp_n$代入得$tp_n(tp_n-1)\equiv 0(mod\ \prod_{i=1}^{n}{p_i}^{\alpha_i})$，

顯然當$a=tp_n\geq 2$時${p_n}^{\alpha_n-1}\nmid(tp_n-1)$，因此${p_n}^{\alpha_n}\mid tp_n$。■

【性質2-8】構造a的相關條件

當$k=\prod_{i=1}^{n}{p_i}^{\alpha_i}\ (n\in\mathbb{N})$，$p_i$為任意相異質數，$j\in\{1,2,\dots\dots,n-1\}$，恆有$(k,a)=\prod_{i=1}^{j}{p_i}^{\alpha_i}$。

<證明>

由**【引理2-8-1】**可知$(k,a)\neq 1$，

由**【引理2-8-2】**可知當a和k有一共同質因數p_j，${p_j}^{\alpha_j}$必為a和k的公因數。■

【性質2-9】$a\equiv 0(mod\ k)$與$a\equiv 1(mod\ k)$

對於$k\geq 3$：當$a\equiv 0(mod\ k)$，若$k=\prod_{i=1}^{n}p_i\ (n\in\mathbb{N}$，$p_i$為任意相異質數)能形成週期，反之亦然；當$a\equiv 1(mod\ k)$時皆不能形成週期。

<證明>

由**【性質1-4】**可知當$k\geq 3$，$a\equiv c(mod\ k)$時$\langle a_\alpha\rangle$必須存在$a_m=c$，但由題目之$a_n>1$可知a_n必不為0或1。以下兩點分別討論：

1° 當$a\equiv 0(mod\ k)$，此時存在$a=k$滿足$a_n=a>1$。

考慮當$k=\prod_{i=1}^{n}p_i$時，

$\nexists b\in\mathbb{N}、b<n:b^2\equiv 0(mod\ k)$，由**【性質2-5】**可知存在$\langle a_\alpha\rangle$。

若$\prod_{i=1}^{n}\alpha_i\neq 1$，設$k=\prod_{i=1}^{n-1}p_i\,{p_n}^{\alpha_n}(\alpha_n\in\mathbb{N}、\alpha_n\geq 2)$，

則$\exists b=\prod_{i=1}^{n-1}p_i\,{p_n}^{\alpha_n'}、\alpha_n'\geq\frac{\alpha_n}{2}:b^2\equiv 0(mod\ k)$，由**【性質2-5】**可知不存在$\langle a_\alpha\rangle$。

2° 當$a\equiv 1(mod\ k)$，$\nexists c\leq k、c\neq 1:c\equiv 1(mod\ k)$，由**【性質1-4】**可知不存在$\langle a_\alpha\rangle$。■

根據【**性質2-9**】，我們構造a時將優先觀察k質因數分解的結果。

【性質2-10】$k=1$

當$k=1$，$a_n \in \mathbb{N}$皆能使數列形成$\langle a_\alpha \rangle = \langle \dots,2,3,4,2,3,4,2,\dots \rangle$。

<證明>

若存在$\langle a_\alpha \rangle = \langle x, x+1, \dots\dots, x^2, x \rangle$，

考慮$(x-1)^2 - x = x^2 - 3x + 1 > 0$的解為$x > \frac{3+\sqrt{5}}{2}$或$x < \frac{3-\sqrt{5}}{2}$(不合)，

可知當$x \geq 3$時存在$a_i = x - 1 < x$，因此數列終將進入$\langle a_\alpha \rangle = \langle \dots,2,3,4,2,3,4,2,\dots \rangle$。■

【性質2-11】k為質數

若k為奇質數，形成$\langle a_\alpha \rangle$若且唯若$a_n \equiv 0 (mod\ k)$。若$k=2$，形成$\langle a_\alpha \rangle$若且唯若$a_n \in \mathbb{N}$：
當$a_n = 2n (n \in \mathbb{N})$時數列終將進入$\langle a_\alpha \rangle = \langle \dots,2,4,2,4,2,\dots \rangle$；
當$a_n = 2n'+1 (n' \in \mathbb{N})$時數列終將進入$\langle a_\alpha \rangle = \langle \dots,3,5,7,9,3,\dots \rangle$。

<證明>

當k為質數，由費馬小定理可知$\forall a \in \mathbb{Z}$：$a^k \equiv a (mod\ k)$。

考慮$a \in \mathbb{N}$，分為兩種情況：

1° 當k為奇質數，考慮$a^k \equiv a (mod\ k)$顯然不合$\langle a_\alpha \rangle$的充要條件；

考慮若a同時滿足$a^2 \equiv a (mod\ k)$，

$\because a^2 \equiv a (mod\ k)$，$\therefore a(a-1) \equiv 0 (mod\ k)$，

則$k \mid a \vee k \mid (a-1)$，

因此$a \equiv 0 (mod\ k) \vee a \equiv 1 (mod\ k)$，

由【**性質2-9**】可知$a \equiv 1 (mod\ k)$無法形成$\langle a_\alpha \rangle$； $a \equiv 0 (mod\ k)$必能形成$\langle a_\alpha \rangle$。

因此存在$\langle a_\alpha \rangle$若且唯若$a \equiv 0 (mod\ k)$。

2° 當$k=2$時，對所有$a \in \mathbb{N}$必能滿足$a^2 \equiv a (mod\ 2)$，因此必能形成週期。

且由奇偶性可知$\forall x = 2n$：$x^2 \equiv 0 (mod\ 2)$，$\forall x = 2n'+1$：$x^2 \equiv 1 (mod\ 2)$。

當$a_n = 2n$，考慮等差數列$\langle 2n, 2n+2, \dots\dots, \rangle$中存在$a_m = (2n-2)^2$，

則$(2n-2)^2 - 2n = 4n^2 - 10n + 4 > 0$的解為$n > 2$ 或$n < \frac{1}{2}$ (不合)，

因此所有$a_n = 2n$代入數列後都將形成$\langle a_\alpha \rangle = \langle \dots, 2, 4, 2, 4, \dots \rangle$。

當$a_n = 2n' + 1$，考慮等差數列$\langle 2n' + 1, 2n' + 3, \dots\dots, \rangle$中存在$a_m = (2n' - 1)^2$，

則$(2n' - 1)^2 - (2n' + 1) = 4n'^2 - 6n' > 0$的解為$n' > \frac{3}{2}$或$n' < 0$(不合)，

因此所有$a_n = 2n' + 1$代入數列後都將形成$\langle a_\alpha \rangle = \langle \dots, 3, 5, 7, 9, 3, \dots \rangle$。■

【性質2-12】k為單一質數多次方

當$k = p^n$，p為任意質數，$n \in \mathbb{N}$且$n \geq 2$，則$\nexists a \neq 0$、$a \neq 1$：$a^2 \equiv a (mod\ k)$，且必不存在$a_n \equiv a$可形成週期。

<證明>

由**【性質2-8】**可知：若存在a，則$(k, a) = p^n$，但由**【性質2-1】**可知$a \leq \frac{p^n}{2}$，矛盾。

由**【性質2-9】**可知$a \equiv 0 (mod\ k)$或$a \equiv 1 (mod\ k)$在$k = p^n$，$a_n \equiv a$皆無法形成週期。■

(三)對k分類討論

我們將k按質因數分解後的形式分類，分別討論「構造a」與「考慮b的存在」兩部分：

1. **$k = pq$，其中p和q為任意相異質數，因【性質2-1】僅考慮$a \leq \frac{k}{2}$。**

(1) 構造a：

由**【性質2-6】**可知$p \mid a \vee q \mid a$。以下不失一般性討論$(k, a) = p$：

【性質3-1】

$k = pq$，若$(k, a) = p$：當$q \neq 2$，$a = p(p^{q-2} - mq)(m \in \mathbb{Z})$；當$q = 2$，則$a = p$即為所求。

<證明>

設$a = tp (t \in \mathbb{N})$，則$(tp)^2 \equiv tp (mod\ pq)$，$tp \equiv 1 (mod\ q)$。分為兩種情況：

1° 當$q \neq 2$，由**【定理1】**可知$t \equiv p^{q-2} (mod\ q)$，

設$t = p^{q-2} - mq$，得$a = p(p^{q-2} - mq)$，

計算$mq \equiv x (mod\ p)(x \in \mathbb{N})$後代回求得$a$值即完成構造。

2° 當$q = 2$，$k = 2p$，

考慮當$a = tp$時應滿足$2 \mid tp - 1$與$tp \leq \frac{k}{2} = \frac{2p}{2} = p$，因此 $a = p$即為所求。■

(2) 考慮b的存在：

【性質3-2】

當$k=pq$，若存在a則不存在b。

<證明>

不失一般性考慮$(k,a)=p$，設$a=tp(t\in\mathbb{N})$，$\because a\le\frac{pq}{2}$，$\therefore t\le\frac{q}{2}$。

若存在b，$\because b^2\equiv a^2(mod\ pq)$，$\therefore(a+b)(a-b)\equiv 0(mod\ pq)$，

得$pq\mid(a+b)(a-b)$。

$\because p\mid(a+b)\vee p\mid(a-b)$，$p\mid a$，$\therefore(k,b)=p$。

設$b=t'p(t'\in\mathbb{N})$，代入$a^2-b^2\equiv 0(mod\ pq)$，

得 $(tp)^2-(t'p)^2\equiv 0(mod\ pq)$，$(t+t')(t-t')p^2\equiv 0(mod\ pq)$，

則$q\mid(t+t')\vee q\mid(t-t')$。

但$\because b<a$，且$a=tp$，$b=t'p$，$\therefore b<a\le\frac{k}{2}$，$t'<t\le\frac{q}{2}$，

故$t+t'<q$、$t-t'<q$，得$q\nmid t+t'$、$q\nmid t-t'$，矛盾。■

2. $k=pqr$，其中p、q、r為任意相異質數，因【性質2-1】僅考慮$a\le\frac{k}{2}$。

(1) 構造a：

由**【性質2-6】**可知$p\mid a\vee q\mid a\vee r\mid a$。以下不失一般性討論$(k,a)=pq$與$(k,a)=p$：

【性質3-3】

$k=pqr$，若$(k,a)=pq$：當$r\neq 2$，$a=pq[(pq)^{r-2}-mr](m\in\mathbb{Z})$；當$r=2$，$a=pq$即為所求。

<證明>

1° 當$r\neq 2$，設$a=tpq(t\in\mathbb{N})$，

由**【定理1】**可知$t=(pq)^{r-2}-mr$，$a=pq[(pq)^{r-2}-mr]$，

計算$(pq)^{r-2}\equiv x(mod\ r)$代回求得$a$值即可。

2° 當$r=2$：考慮$a=tpq$須滿足$2\mid tpq-1$與$tpq\le\frac{k}{2}=\frac{2pq}{2}=pq$，因此$a=pq$即為所求。■

【性質3-4】

$k=pqr$，若$(k,a)=p$，則符合所求的a須同時滿足對q構造與對r構造的結果。

<證明>

當$(k,a)=p$、$q\neq 2$且$r\neq 2$：設$a=tp(t\in\mathbb{N})$，

則$(tp)^2\equiv tp(mod\ pqr)$，$tp\equiv 1(mod\ qr)$，考慮以下情況：

1° 對q構造：$tp\equiv 1(mod\ q)$，

由**【定理1】**知$t=p^{q-2}-m_1q(m_1\in\mathbb{Z})$，

計算$p^{q-2}\equiv x(mod\ q)$，將x代回$p(p^{q-2}-m_1q)$求值，

並將所有正整數值寫成數列$\langle q_n\rangle$：$\langle q_1,q_2,q_3,\dots\rangle$。

2° 對r構造：$tp\equiv 1(mod\ r)$，

由**【定理1】**知$t=p^{r-2}-m_2r(m_2\in\mathbb{Z})$，

計算$p^{r-2}\equiv x(mod\ r)$，將x代回$p(p^{r-2}-m_2r)$求值，

並將所有正整數值寫成數列$\langle r_n\rangle$：$\langle r_1,r_2,r_3,\dots\rangle$。

3° ∵a必須滿足$pqr\mid a(a-1)$，∴符合所求的a必須同時滿足$a\in\langle q_n\rangle$與$a\in\langle r_n\rangle$。

當$2\mid qr$，不失一般性設$r=2$，考慮以下情況：

1° 對q構造：同$\langle q_n\rangle$：$\langle q_1,q_2,q_3,\dots\rangle$。

2° 對r構造：考慮$2\mid tp-1$且$t\leq q(\because tp\leq\frac{2pq}{2}=pq)$，

將符合上述性質的tp寫成$\langle s_n\rangle$：$\langle s_1,s_2,s_3,\dots\rangle$。

3° ∵a必須滿足$pqr\mid a(a-1)$，∴符合所求的a必須同時滿足$a\in\langle q_n\rangle$與$a\in\langle s_n\rangle$。■

(2) 考慮b的存在：

【引理3-5-1】

當$k=pqr$，滿足$(k,a)=pq$，若存在b則$(k,b)=pq$。

<證明>

若$(k,b)\neq pq$，設$a=tpq(t\in\mathbb{N})$，$b=n(n\in\mathbb{N})$，

$\because (a+b)(a-b) \equiv 0 (mod\ pqr)$，$\therefore pqr \mid (a+b)(a-b)$。

$\because pqr \mid (a+b)(a-b)$，$\therefore pq \mid (a+b)(a-b)$。

又$\because (k,b) \neq pq$、$(k,a) = pq$，$\therefore pq \nmid (a+b)(a-b)$，矛盾。■

【性質3-5】

當$k = pqr$，滿足 $(k,a) = pq$則不存在b。

<證明>

設$a = tpq(t \in \mathbb{N})$且存在$b$，

$\because a^2 \equiv b^2 (mod\ pqr)$，$(a+b)(a-b) \equiv 0 (mod\ pqr\ )$，$\therefore pqr \mid (a+b)(a-b)$。

由**【引理3-5-1】**可知$(k,b) = pq$，設$b = t'pq(t' \in \mathbb{N})$，

$\because pqr \mid (a+b)(a-b)$， $\therefore pqr \mid (t+t')(t-t')(pq)^2$。

則$r \mid (t+t') \vee r \mid (t-t')$。$\because b < a \leq \frac{k}{2}$，$\therefore t' < t \leq \frac{r}{2}$，

則$t - t' < t + t' < r$，因此$r \nmid (t-t')$、$r \nmid (t+t')$，矛盾。■

【性質3-6】

當$k = pqr$，滿足 $(k,a) = p$則有條件存在b。

<證明>

設$a = tp(t \in \mathbb{N})$，由$(a+b)(a-b) \equiv 0 (mod\ pqr)$可知$(k,b) = p$。

設$b = t'p(t' \in \mathbb{N})$，則$pqr \mid (t+t')(t-t')p^2$，$qr \mid (t+t')(t-t')$。分為兩種情況：

1° $qr \mid (t+t') \vee qr \mid (t-t')$，

$\because t' < t \leq \frac{qr}{2}$，$\therefore t - t' < t + t' < qr$，$qr \nmid (t-t')$、$qr \nmid (t+t')$，矛盾。

2° $q \mid (t+t')$、$r \mid (t-t')$或$r \mid (t+t')$、$q \mid (t-t')$，

不失一般性設$t + t' = m_1 q$，$t - t' = m_2 r$(其中m_1 、$m_2 \in \mathbb{R}$)，

兩式相加得$2t = m_1 q + m_2 r$，則$m_1 q \equiv 2t (mod\ r)$，

求出$m_1 \equiv x (mod\ r)$，將$m_1 = x$代回$2t = m_1 q + m_2 r$求出m_2，

若存在m_1 、$m_2 \in \mathbb{N}$則存在b。■

3. $\boldsymbol{k=\prod_{i=1}^{n}p_i\,(n\in\mathbb{N})}$，$\boldsymbol{p_i}$**為任意相異質數，因【性質2-1】僅考慮**$\boldsymbol{a\le\frac{k}{2}}$。

(1) 構造a：

由【**性質2-6**】可知恆有$(k,a)=\prod_{i=1}^{j}p_i$。以下不失一般性討論$(k,a)=\prod_{i=1}^{n-1}p_i$與$(k,a)=\prod_{i=1}^{r}p_i\,(r\in\mathbb{N}，1\le r<n-1)$。

【性質3-7】

$k=\prod_{i=1}^{n}p_i$，若$(k,a)=\prod_{i=1}^{n-1}p_i$：當$p_n\neq 2$， $a=\prod_{i=1}^{n-1}p_i\,[(\prod_{i=1}^{n-1}p_i)^{p_n-2}-mp_n](m\in\mathbb{Z})$；當$p_n=2$，$a=\prod_{i=1}^{n-1}p_i$。

<證明>

1° 當$p_n\neq 2$，由【**定理1**】得$a=\prod_{i=1}^{n-1}p_i\,[(\prod_{i=1}^{n-1}p_i)^{p_n-2}-mp_n]$……式1

計算$\prod_{i=1}^{n-1}{p_i}^{p_n-2}\equiv x(mod\ p_n)$的值後代回式1求出$a$值即可。

2° 當$p_n=2$，考慮$a=t\prod_{i=1}^{n-1}p_i\,(t\in\mathbb{N})$須滿足$2\mid a-1$、$a\le\frac{k}{2}=\prod_{i=1}^{n-1}p_i$，

因此$a=\prod_{i=1}^{n-1}p_i$即為所求。■

【性質3-8】

$k=\prod_{i=1}^{n}p_i$，若$(k,a)=\prod_{i=1}^{r}p_i\,(r\in\mathbb{N}，1<r<n-1)$，符合所求的$a$必須滿足對所有$p_j(r+1<j\le n)$構造的結果。

<證明>

1° 若$p_j\neq 2$，由【**定理1**】對每個p_j可得$\prod_{i=1}^{r}p_i\left[(\prod_{i=1}^{r}p_i)^{p_j-2}-mp_j\right](m\in\mathbb{Z})$……式2

計算$(\prod_{i=1}^{r}p_i)^{p_j-2}\equiv x\left(mod\ p_j\right)$的值後代回式2求值，

將不同p_j求出的正整數值分別寫成數列$\langle c_n\rangle$、$\langle d_n\rangle$、$\langle e_n\rangle$、……，

符合所求的a必須同時存在於$\langle c_n\rangle$、$\langle d_n\rangle$、$\langle e_n\rangle$、……。

2° 若$p_j=2$，不失一般性設$p_n=2$，

對p_n構造時考慮$2\mid t\prod_{i=1}^{r}p_i-1(t\in\mathbb{N})$與$t\prod_{i=1}^{r}p_i\le\frac{k}{2}=\prod_{i=r+1}^{n-1}p_i$，

將符合性質的$t\prod_{i=1}^{r}p_i$寫成數列$\langle f_n\rangle$，

符合所求的a必須同時存在於$\langle c_n\rangle$、$\langle d_n\rangle$、$\langle e_n\rangle$、$\langle f_n\rangle$、……。

(2) 考慮b的存在：

【引理3-9-1】

當$k=\prod_{i=1}^{n}p_i\ (n\in\mathbb{N})$，滿足$(k,a)=\prod_{i=1}^{n-1}p_i$，若存在$b$則$(k,b)=\prod_{i=1}^{n-1}p_i$。

<證明>

若$(k,b)=\prod_{i=1}^{m}p_i\ (m\in\{1,2,\ldots\ldots,n-2\})$，

令$a=t\prod_{i=1}^{n-1}p_i\ (t\in\mathbb{N})$，$b=r\prod_{i=1}^{m}p_i\ (r\in\mathbb{N})$，代回$(a+b)(a-b)$：

$(a+b)(a-b)=(t\prod_{i=1}^{n-1}p_i+r\prod_{i=1}^{m}p_i)(t\prod_{i=1}^{n-1}p_i-r\prod_{i=1}^{m}p_i)$

$=(\prod_{i=1}^{m}p_i)^2(t\prod_{i=m+1}^{n-1}p_i+r)(t\prod_{i=m+1}^{n-1}p_i-r)$。

$\because(a+b)(a-b)\equiv 0(mod\ \prod_{i=1}^{n}p_i)$，$\therefore\prod_{i=1}^{n}p_i\mid(a+b)(a-b)$，

則$\prod_{i=1}^{n}p_i\mid(\prod_{i=1}^{m}p_i)^2(t\prod_{i=m+1}^{n-1}p_i+r)(t\prod_{i=m+1}^{n-1}p_i-r)$，

$\prod_{i=m+1}^{n-1}p_i\mid(t\prod_{i=m+1}^{n-1}p_i+r)(t\prod_{i=m+1}^{n-1}p_i-r)$，此式成立唯若$\prod_{i=m+1}^{n-1}p_i\mid r$。■

【性質3-9】

當$k=\prod_{i=1}^{n}p_i\ (n\in\mathbb{N})$，滿足$(k,a)=\prod_{i=1}^{n-1}p_i$則不存在$b$。

<證明>

由**【引理3-9-1】**可知$(k,b)=\prod_{i=1}^{n-1}p_i$。

設$b=t'\prod_{i=1}^{n-1}p_i\ (t'\in\mathbb{N})$，

$\because\prod_{i=1}^{n}p_i\mid(a+b)(a-b)$，$\therefore\prod_{i=1}^{n}p_i\mid(t+t')(t-t')(\prod_{i=1}^{n-1}p_i)^2$，

則$p_n\mid(t+t')\vee p_n\mid(t-t')$。

又$\because t'<t\leq\frac{p_n}{2}$，$\therefore t-t'<t+t'<p_n$，

得$p_n\nmid(t+t')\wedge p_n\nmid(t-t')$，矛盾。■

【性質3-10】

當$k=\prod_{i=1}^{n}p_i\ (n\in\mathbb{N})$，滿足$(k,a)=\prod_{i=1}^{m}p_i\ (m\in\mathbb{N}，m<n-1)$則有條件存在$b$。

<證明>

設$a=t\prod_{i=1}^{m}p_i\ (t\in\mathbb{N})$，

$\because(a+b)(a-b)\equiv 0(mod\ k)$，$\therefore(k,b)=\prod_{i=1}^{m}p_i$。

設$b = t'\prod_{i=1}^{m} p_i\,(t' \in \mathbb{N})$，

代入$\prod_{i=1}^{n} p_i \mid (a+b)(a-b)$得$\prod_{i=1}^{n} p_i \mid (t+t')(t-t')(\prod_{i=1}^{m} p_i)^2$，

則$\prod_{i=m+1}^{n} p_i \mid (t+t')(t-t')$。分為兩種情況：

1° $\prod_{i=m+1}^{n} p_i \mid (t+t') \vee \prod_{i=m+1}^{n} p_i \mid (t-t')$，

$\because t' < t \leq \frac{\prod_{i=m+1}^{n} p_i}{2}$，$\therefore \prod_{i=m+1}^{n} p_i \nmid (t+t') \wedge \prod_{i=m+1}^{n} p_i \nmid (t-t')$，矛盾。

2° $\prod_{i=m+1}^{r} p_i \mid (t+t') \wedge \prod_{i=r+1}^{n} p_i \mid (t-t')$或$\prod_{i=m+1}^{r} p_i \mid (t-t') \wedge \prod_{i=r+1}^{n} p_i \mid (t+t')$

(其中$r \in \mathbb{N}$且$r < n$)，

不失一般性設$t+t' = m_1\prod_{i=m+1}^{r} p_i$、$t-t' = m_2\prod_{i=r+1}^{n} p_i$(其中$m_1$、$m_2 \in \mathbb{R}$)，

兩式相加得$2t = m_1\prod_{i=m+1}^{r} p_i + m_2\prod_{i=r+1}^{n} p_i$……式3

則$m_1\prod_{i=m+1}^{r} p_i \equiv 2t(mod\ \prod_{i=r+1}^{n} p_i)$，

計算$m_1 \equiv x(mod\ \prod_{i=r+1}^{n} p_i)$代回式3求出$m_2$，

若存在$m_1 \in \mathbb{N}$、$m_2 \in \mathbb{N}$則存在b。■

4. **$k = p^n q$，p、q為任意相異質數，$n \in \mathbb{N}$、$n \geq 2$，若$p \neq 2$：因【性質2-1】僅考慮$a \leq \frac{k}{2}$；若$p = 2$：因【性質2-2】僅考慮$a \leq \frac{k}{4}$。**

(1) 構造a：

由【性質2-7】可知$p^n \mid a \vee q \mid a$，以下分別討論$(k,a) = p^n$與$(k,a) = q$的情況：

【性質3-11】

若$(k,a) = p^n$：當$q \neq 2$，$a = p^n\left(p^{n(q-2)} - mq\right)(m \in \mathbb{Z})$；當$q = 2$，$a = p^n$。

<證明>

1° 當$q \neq 2$，由【定理1】可知$a = p^n(p^{n(q-2)} - mq)(m \in \mathbb{Z})$……式4

計算$p^{n(q-2)} \equiv x(mod\ q)$的值後代回式4求得$a$值即可。

2° 當$q = 2$，設$a = tp^n(t \in \mathbb{N})$，

$\because 2 \mid a(a-1)$，$\therefore 2 \mid tp^n - 1$；

由【性質2-1】可知$a = tp^n \leq \frac{k}{2} = p^n$，

因此$a = p^n$即為所求。■

【性質3-12】

$k=p^nq\left(n\in\mathbb{N}、n\geq 2\right)$，若$(k,a)=q$：
當$p\neq 2$，若存在$m\in\mathbb{Z}$滿足$q(q^{p-2}-mp)>0$且$p^n \mid q(q^{p-2}-mp)$，則$a=\ q(q^{p-2}-mp)$；
當$p=2$(即$k=2^nq$)，若存在$t\in\mathbb{N}$，$t\leq 2^{n-2}$滿足$2^n \mid tq-1$，則$a=tq$。

<證明>

1° 當$p\neq 2$，由**【定理1】**得$q(q^{p-2}-mp)(m\in\mathbb{Z})$……式5

計算$q^{p-2}\equiv x(mod\ p)$的值後代回式5求值，

由於**【定理1】**構造的結果僅滿足$p \mid [q(q^{p-2}-mp)-1]$，

因此仍須檢驗$p^n \mid [q(q^{p-2}-mp)-1]$是否成立，

若是則$a=\ q(q^{p-2}-mp)$即為所求。

2° 當$p=2$，$k=2^nq$，設$a=tq(t\in\mathbb{N})$，

$\because 2^n \mid a-1$，$\therefore 2^n \mid tq-1$，

由**【性質2-2】**可知，$a=tq\leq\frac{k}{4}=2^{n-2}q$，因此$t\leq 2^{n-2}$。

若存在t滿足上述性質，則$a=tq$即為所求。■

(2) 考慮b的存在：

【性質3-13】

當$k=p^nq$，滿足$(k,a)=q$且$p\neq 2$時不存在b； $p=2$時有條件存在b。

<證明>

設$a=tq(t\in\mathbb{N})$且存在b，$\because p^nq \mid (a+b)(a-b)$，$\therefore (k,b)=q$。

令$b=t'q(t'\in\mathbb{N})$，則$p^nq \mid (t+t')(t-t')q^2$，分為兩種情況：

1° 若$p^n \mid (t+t')\vee p^n \mid (t-t')$，

$\because t'<t\leq\frac{p^n}{2}$，$\therefore t-t'<t+t'<p^n$，故$p^n\nmid(t+t')\wedge p^n\nmid(t-t')$，矛盾。

2° 若$p^m \mid (t+t')$且$p^{n-m} \mid (t-t')$(其中$m\in\mathbb{N}$且不失一般性設$n>m$)，

則$(t+t',t-t')=p^{n-m}$，又$(t+t')-(t-t')=2t'$，因此若$p\neq 2$時矛盾；

當$p=2$時需檢驗$p^{n-m} \mid 2t'$是否成立，若是則存在b。■

【性質3-14】

當$k=p^nq$，滿足$(k,a)=p^n$則有條件存在b。

<證明>

設$a=tp^n(t\in\mathbb{N})$且存在b，

$\because p^nq\mid(a+b)(a-b)$，$\therefore(k,b)=p^m\ (m\in\mathbb{N}、m\geq\frac{n}{2})$。

令$b=t'p^m\left(t'\in\mathbb{N}\text{ 且不失一般性設}n>m\right)$，

代入$p^nq\mid(a+b)(a-b)$得$p^nq\mid(p^m)^2(tp^{n-m}+t')(tp^{n-m}-t')$，

則$q\mid(tp^{n-m}+t')\vee q\mid(tp^{n-m}-t')$，$q\mid t'(\frac{a}{b}+1)\vee q\mid t'(\frac{a}{b}-1)$，

若存在$b\in\mathbb{N}$則存在b。■

5. **$k=p^nq^m$，p、q為任意相異質數，$n\in\mathbb{N}$、$m\in\mathbb{N}$且$n\geq2$、$m\geq2$，若$p\neq2$、$q\neq2$：**

   因【性質2-1】僅考慮$a\leq\frac{k}{2}$；若$p=2\vee q=2$：因【性質2-2】僅考慮$a\leq\frac{k}{4}$。

   (1) 構造a：

   由**【性質2-7】**可知$p^n\mid a\vee q^m\mid a$。以下不失一般性討論$(k,a)=p^n$：

【性質3-15】

當$k=p^nq^m$，若$(k,a)=p^n$：當$q\neq2$，若存在$m\in\mathbb{Z}$滿足$p^n(p^{n(q-2)}-mq)>0$且 $q^m\mid\left[p^n(p^{n(q-2)}-mq)-1\right]$，則$a=p^n(p^{n(q-2)}-mq)$； 當$q=2$，若存在$t\in\mathbb{N}$，$t\leq2^{m-2}$滿足$2^m\mid(tp^n-1)$，則$a=tp^n$。

<證明>

1° 當$q\neq2$，由**【定理1】**得$p^n(p^{n(q-2)}-mq)(m\in\mathbb{Z})$……式6

求出$p^{n(q-2)}\equiv x(mod\ q)$後代回式6求值，

$\because$**【定理1】**構造的值僅滿足$q\mid[p^n(p^{n(q-2)}-mq)-1]$，

$\therefore$仍須檢驗$q^m\mid[p^n(p^{n(q-2)}-mq)-1]$是否成立，

若是則$a=p^n(p^{n(q-2)}-mq)$即為所求。

2° 當$q=2$，$a=tp^n(t\in\mathbb{N})$，$\because2^m\mid(a-1)$，$\therefore2^m\mid(tp^n-1)$，

由【**性質2-2**】可知，$a = tp^n \le \frac{k}{4} = 2^{m-2}p^n$，因此$t \le 2^{m-2}$。

若存在t滿足上述性質，則$a = tp^n$即為所求。■

(2) 考慮b的存在：

【性質3-16】

當$k = p^n q^m$，滿足$(k, a) = p^n$則有條件存在b。

<證明>

設$a = tp^n (t \in \mathbb{N})$，$\because p^n q^m | (a+b)(a-b)$，$\therefore (k, a) = p^r (r \ge \frac{n}{2})$。

令$b = t'p^r (t' \in \mathbb{N})$(不失一般性設$n > r$)，

則$p^n q^m \mid (p^r)^2 (tp^{n-r} + t')(tp^{n-r} - t')$，

$q^m \mid (tp^{n-r} + t')(tp^{n-r} - t')$，分為兩種情況：

1° 若$q^s \mid (tp^{n-r} + t') \wedge q^{m-s} \mid (tp^{n-r} - t')$(其中 $s \in \mathbb{N}$且$s < m$)，

則$tp^{n-r} + t' \equiv tp^{n-r} - t' (mod\ q)$，$2t' \equiv 0 (mod\ q)$，

此式成立若且唯若$q = 2$，因此當q為奇質數時不合；

而$q = 2$時，檢驗$q^s \mid (tp^{n-r} + t') \wedge q^{m-s} \mid (tp^{n-r} - t')$成立即存在$b = t'p^r$，

2° 當$q^m \mid (tp^{n-r} + t') \vee q^m \mid (tp^{n-r} - t')$，則$q^m | t'(\frac{a}{b} + 1) \vee q^m | t'(\frac{a}{b} - 1)$成立即存在$b$。■

6. $\boldsymbol{k = \prod_{i=1}^{n} p_i^{\alpha_i}}$，$\boldsymbol{p_i}$**為任意相異質數，**$\boldsymbol{n}$、$\boldsymbol{\alpha_i} \in \mathbb{N}$。

(1) 構造a：

由【**性質2-7**】可知對於$j \in \mathbb{N}$，$j < n$恆有$(k, a) = \prod_1^j {p_i}^{\alpha_i}$。

【性質3-17】

當$(k, a) = \prod_{i=1}^{n-1} {p_i}^{\alpha_i}$： 若 $p_n \ne 2$ ， $m \in \mathbb{Z}$ 滿足 $\prod_{i=1}^{n-1} ({p_i}^{\alpha_i})^{p_n - 2} - mp_n > 0$ 且 ${p_n}^{\alpha_n} \mid \left\{ \prod_{i=1}^{n-1} {p_i}^{\alpha_i} \left[\prod_{i=1}^{n-1} ({p_i}^{\alpha_i})^{p_n - 2} - mp_n \right] - 1 \right\}$，則$a = \prod_{i=1}^{n-1} {p_i}^{\alpha_i} \left[\prod_{i=1}^{n-1} ({p_i}^{\alpha_i})^{p_n - 2} - mp_n \right]$即為所求；若$p_n = 2$，若存在$t \in \mathbb{N}$且$t \le 2^{\alpha_n - 2}$(若$\alpha_n = 1$ 則 $t = 1$)滿足$2^{\alpha_n} \mid (t \prod_{i=1}^{n-1} {p_i}^{\alpha_i} - 1)$，則$a = t \prod_{i=1}^{n-1} {p_i}^{\alpha_i}$。

<證明>

1° 當$p_n \neq 2$，由【**定理 1**】可得$\prod_{i=1}^{n-1} {p_i}^{\alpha_i}\left[\prod_{i=1}^{n-1}({p_i}^{\alpha_i})^{p_n-2} - mp_n\right]$……式7

計算$\prod_{i=1}^{n-1}({p_i}^{\alpha_i})^{p_n-2} \equiv x(mod\ p_n)$，代回式 7 求值；

∵【**定理1**】構造的值僅滿足$p_n \mid \left\{\prod_{i=1}^{n-1} {p_i}^{\alpha_i}\left[\prod_{i=1}^{n-1}({p_i}^{\alpha_i})^{p_n-2} - mp_n\right] - 1\right\}$，

∴仍須檢驗${p_n}^{\alpha_n} \mid \left\{\prod_{i=1}^{n-1} {p_i}^{\alpha_i}\left[\prod_{i=1}^{n-1}({p_i}^{\alpha_i})^{p_n-2} - mp_n\right] - 1\right\}$是否成立，

若是則$a = \prod_{i=1}^{n-1} {p_i}^{\alpha_i}\left[\prod_{i=1}^{n-1}({p_i}^{\alpha_i})^{p_n-2} - mp_n\right]$即為所求。

2° 當$p = 2$，設$a = t\prod_{i=1}^{n-1} {p_i}^{\alpha_i}\ (t \in \mathbb{N})$，

∵$\prod_{i=1}^{n} {p_i}^{\alpha_i} \mid a(a-1)$，∴$2^{\alpha_n} \mid (a-1)$，即$2^{\alpha_n} \mid (t\prod_{i=1}^{n-1} {p_i}^{\alpha_i} - 1)$。

由【**性質2-1**】可知當$\alpha_n = 1$時$a = t\prod_{i=1}^{n-1} {p_i}^{\alpha_i} \leq \frac{k}{2} = \prod_{i=1}^{n-1} {p_i}^{\alpha_i}$，因此$t = 1$；

由【**性質2-2**】可知當$\alpha_n \geq 2$時$a = t\prod_{i=1}^{n-1} {p_i}^{\alpha_i} \leq \frac{k}{4} = \prod_{i=1}^{n-1} {p_i}^{\alpha_i}\, 2^{\alpha_n-2}$，因此$t \leq 2^{\alpha_n-2}$。

若存在t滿足上述性質，則$a = t\prod_{i=1}^{n-1} {p_i}^{\alpha_i}$即為所求。

【性質3-18】

$k = \prod_{i=1}^{n} {p_i}^{\alpha_i}$，若$(k, a) = \prod_{i=1}^{r} {p_i}^{\alpha_i}\ \left(r \in \mathbb{N}\text{ 且 } 1 \leq r < n-1\right)$：

當$p_\ell \neq 2$(其中 $\ell \in \{r+1, r+2, \ldots\ldots, n\}$)，符合所求的$a$必須滿足對所有${p_j}^{\alpha_j}(r+1 < j \leq n)$構造的結果。

當$p_\ell = 2$，$t' \in \mathbb{N}$滿足$t' \leq \prod_{i=r+1}^{n-1} {p_i}^{\alpha_i}$ (當$\alpha_\ell = 1$時)或$t' \leq 2^{\alpha_n-2}\prod_{i=r+1}^{n-1} {p_i}^{\alpha_i}$ (當$\alpha_\ell \geq 2$時)，且滿足$2^{\alpha_\ell} \mid (t'\prod_{i=1}^{r} {p_i}^{\alpha_i} - 1)$，則$a = t'\prod_{i=1}^{r} {p_i}^{\alpha_i}$即為所求。

<證明>

1° 當$p_\ell \neq 2$，由【**定理 1**】得$\prod_{i=1}^{r} {p_i}^{\alpha_i}\,[(\prod_{i=1}^{r} {p_i}^{\alpha_i})^{(p_j-2)} - mp_j]$……式8

計算$\prod_{i=1}^{r}({p_i}^{\alpha_i})^{(p_j-2)} \equiv x\left(mod\ p_j\right)$，

代回式 8 求值，並將不同所有正整數值寫成數列$\langle c_n\rangle$、$\langle d_n\rangle$、$\langle e_n\rangle$、 ……。

由於應用【**定理 1**】時會使模從${p_j}^{\alpha_j}$變成p_j，

因此找到一數y同時存在於$\langle c_n\rangle$、$\langle d_n\rangle$、$\langle e_n\rangle$、 ……後，

仍需檢查$\prod_{i=1}^{n} {p_i}^{\alpha_i} \mid y(y-1)$是否成立，若是則$a=y$即為所求。

2° 當$p_\ell = 2$，設$a = t' \prod_{i=1}^{r} {p_i}^{\alpha_i}\ (t' \in \mathbb{N})$並不失一般性設$p_\ell = p_n$，

$\because \prod_{i=1}^{n} {p_i}^{\alpha_i} \mid a(a-1)$，$\therefore 2^{\alpha_n} \mid (a-1)$，即$2^{\alpha_n} \mid (t' \prod_{i=1}^{r} {p_i}^{\alpha_i} - 1)$。

由**【性質2-1】**可知，當$\alpha_n = 1$時$a \le \frac{k}{2} = \prod_{i=1}^{n-1} {p_i}^{\alpha_i}$，因此$t' \le \prod_{i=r+1}^{n-1} {p_i}^{\alpha_i}$；

由**【性質2-2】**可知，當$\alpha_n \ge 2$時$a \le \frac{k}{4} = \prod_{i=1}^{n-1} {p_i}^{\alpha_i}\, 2^{\alpha_n - 2}$，因此$t' \le 2^{\alpha_n - 2} \prod_{i=r+1}^{n-1} {p_i}^{\alpha_i}$。

若存在t'符合上述性質，則$a = t' \prod_{i=1}^{r} {p_i}^{\alpha_i}$即為所求。

(2) 考慮b的存在：

【性質3-19】

當$k = \prod_{i=1}^{n} {p_i}^{\alpha_i}$，滿足$(k, a) = \prod_{i=1}^{n-1} {p_i}^{\alpha_i}$且$\alpha_i = 1$，$p_n \ne 2$時不存在$b$；若$p_n = 2$則有條件存在$b$。

<證明>

設$a = t \prod_{i=1}^{n-1} {p_i}^{\alpha_i}\ (t \in \mathbb{N})$且存在$b$，

$\because \prod_{i=1}^{n} {p_i}^{\alpha_i} \mid (a+b)(a-b)$，$\therefore (k, b) = \prod_{i=1}^{n-1} {p_i}^{\alpha_i}$。

令$b = t' \prod_{i=1}^{n-1} {p_i}^{\alpha_i}\ (t' \in \mathbb{N})$，則$\prod_{i=1}^{n} {p_i}^{\alpha_i} \mid (t+t')(t-t')(\prod_{i=1}^{n-1} {p_i}^{\alpha_i})^2$，分為兩種情況：

1° 若${p_n}^{\alpha_n} \mid (t+t')$ ∨ ${p_n}^{\alpha_n} \mid (t-t')$ 成立，

$\because t' < t \le \frac{{p_n}^{\alpha_n}}{2}$，$\therefore t - t' < t + t' < {p_n}^{\alpha_n}$，

故${p_n}^{\alpha_n} \nmid (t+t') \wedge {p_n}^{\alpha_n} \nmid (t-t')$，矛盾。

2° 若${p_n}^{m} \mid (t+t')$且${p_n}^{\alpha_n - m} \mid (t-t')$(其中$m \in \mathbb{N}$ 且$m < \alpha_n$)，

則$(t+t', t-t') = {p_n}^{\alpha_n - m}$(不失一般性設$m \ge \frac{\alpha_n}{2}$)，

又$(t+t') - (t-t') = 2t'$，當$p_n \ne 2$時$p_n \nmid 2t'$，矛盾；

若$p_n = 2$，則檢驗${p_n}^{\alpha_n - m} \mid 2t'$是否成立，若是則存在$b$。■

【性質3-20】

當$k = \prod_{i=1}^{n} {p_i}^{\alpha_i}$，滿足$(k, a) = \prod_{i=1}^{m} {p_i}^{\alpha_i}$ $(m \in \mathbb{N}$ 且 $1 \le m \le n-1)$，則有條件存在b。

<證明>

當$(k,a)=\prod_{i=1}^{m}{p_i}^{\alpha_i}$，設$a=t\prod_{i=1}^{m}{p_i}^{\alpha_i}\ (t\in\mathbb{N})$，

$\because \prod_{i=1}^{n}{p_i}^{\alpha_i}\mid(a+b)(a-b)$，$\therefore(k,b)=\prod_{i=1}^{m}{p_i}^{\alpha_i'}\ (\alpha_i'\in\mathbb{N},\alpha_i'\geq\frac{\alpha_i}{2})$。

設$b=t'\prod_{i=1}^{m}{p_i}^{\alpha_i'}\ (t'\in\mathbb{N})$，

$\because \prod_{i=1}^{n}{p_i}^{\alpha_i}\mid(a+b)(a-b)$且不失一般性設$\sum_{i=1}^{m}\alpha_i\geq\sum_{i=1}^{m}\alpha_i'$，

$\therefore \prod_{i=1}^{n}{p_i}^{\alpha_i}\mid(\prod_{i=1}^{m}{p_i}^{\alpha_i'})^2\ (t\prod_{i=1}^{m}{p_i}^{(\alpha_i-\alpha_i')}+t')(t\prod_{i=1}^{m}{p_i}^{(\alpha_i-\alpha_i')}-t')$，

分為兩種情況：

1° 若$\prod_{i=m+1}^{n}{p_i}^{\alpha_i}\mid(t\prod_{i=1}^{m}{p_i}^{(\alpha_i-\alpha_i')}+t')\ \vee\prod_{i=m+1}^{n}{p_i}^{\alpha_i}\mid(t\prod_{i=1}^{m}{p_i}^{(\alpha_i-\alpha_i')}-t')$，

則$\prod_{i=m+1}^{n}{p_i}^{\alpha_i}\mid t\left(\frac{b}{a}+1\right)\vee\prod_{i=m+1}^{n}{p_i}^{\alpha_i}\mid t(\frac{b}{a}-1)$，如果存在$b\in\mathbb{N}$則存在$b$。

2° 若$\prod_{i=m+1}^{r}{p_i}^{\alpha_i}\mid(t\prod_{i=1}^{m}{p_i}^{(\alpha_i-\alpha_i')}+t')\wedge\prod_{i=r+1}^{n}{p_i}^{\alpha_i}\mid(t\prod_{i=1}^{m}{p_i}^{(\alpha_i-\alpha_i')}-t')$ (其中$m+1\leq r\leq n-1$)：

設$\left(t\prod_{i=1}^{m}{p_i}^{(\alpha_i-\alpha_i')}+t'\right)=m_1\prod_{i=m+1}^{r}{p_i}^{\alpha_i}$，

$(t\prod_{i=1}^{m}{p_i}^{(\alpha_i-\alpha_i')}-t')=m_2\prod_{i=r+1}^{n}{p_i}^{\alpha_i}\ (m_1、m_2\in\mathbb{R})$，

兩式相加得$2t\prod_{i=1}^{m}{p_i}^{(\alpha_i-\alpha_i')}=m_1\prod_{i=m+1}^{r}{p_i}^{\alpha_i}+m_2\prod_{i=r+1}^{n}{p_i}^{\alpha_i}$……式9

$m_1\prod_{i=m+1}^{r}{p_i}^{\alpha_i}\equiv 2t\prod_{i=1}^{m}{p_i}^{(\alpha_i-\alpha_i')}\ (mod\ \prod_{i=r+1}^{n}{p_i}^{\alpha_i})$，

求出$m_1\equiv x(mod\ \prod_{i=r+1}^{n}{p_i}^{\alpha_i})$，代回式 9求出$m_2$，若存在$m_1$、$m_2\in\mathbb{N}$則存在$b$。■

(四)特殊週期數列$\langle a_\beta\rangle$

觀察所有週期數列$\langle a_m\rangle$，可以發現有些$\langle a_m\rangle$並不滿足任意項$a_i\equiv a(mod\ k)$。例如$k=14$，$a_n=a=2$，$\langle a_m\rangle=\langle 2,16,4,2,\dots\rangle$，但$4\not\equiv 2(mod\ k)$。我們稱這些發生餘數轉換的數列為「特殊週期數列$\langle a_\beta\rangle$」，滿足$\exists j\in\mathbb{N}：a_j\not\equiv a(mod\ k)$。我們發現它們在餘數的轉換時會產生一些性質。以$k=55$，$a_n=a=5$為例，餘數將依序出現$5\to 15\to 20\to 25\to 5$，我們同時發現$5^{16}\equiv 5(mod\ 55)$。對此，我們提出**【性質4−1】**：

【性質4−1】形成$\langle a_\beta\rangle$的必要條件

若$a_n=c_1$且數列在轉換s次$(s\in\mathbb{N}、s\geq 2)$餘數後形成$\langle a_\beta\rangle$，則恆有${c_1}^{2^s}\equiv c_1(mod\ k)$。

<證明>

設$\langle a_\beta \rangle = \langle c_1, \dots, c_2, \dots, c_{s-1}, \dots, c_s, \dots, c_1 \rangle$且$a_m = c_2$，

滿足$a_n = c_1$，$\nexists i \in \mathbb{N}、j \in \mathbb{N}、i < j \leq s : c_i \equiv c_j (mod\ k)$，

且$\nexists \ell \in \mathbb{N}、\ell \leq s、a_\ell \neq c_j : \sqrt{a_{\ell-1}} \in \mathbb{N}$，

$\because \forall x \in \mathbb{N}、n \leq x < m : a_x \equiv c_1 (mod\ k)$，$\therefore {c_2}^2 \equiv c_1 (mod\ k)$，

顯然${c_3}^2 \equiv c_2 (mod\ k)$、${c_4}^2 \equiv c_3 (mod\ k)$、……、${c_s}^2 \equiv c_{s-1} (mod\ k)$、${c_1}^2 \equiv c_s (mod\ k)$。

將${c_1}^2 \equiv c_s (mod\ k)$代回${c_s}^2 \equiv c_{s-1} (mod\ k)$得${c_1}^4 \equiv c_{s-1} (mod\ k)$，

逐項代回至${c_2}^2 \equiv c_1 (mod\ k)$可得${c_1}^{2^s} \equiv c_1 (mod\ k)$。■

【引理4-2-1】

對於$\langle a_\beta \rangle$，${c_1}^{2^s} \equiv c_1 (mod\ k)$與$\{c_n\} : \{c_1、c_2、\dots\dots、c_s\}$，$c_i$必存在於數列中。

<證明>

設$a_n = x$滿足$x \equiv c_i (mod\ k)$且$x^{2^s} \equiv x (mod\ k)$，

$\because c_i < x$，$\therefore \exists s \in \mathbb{N} :\ x < {c_i}^{2^s} < x^2$(若否，則${c_i}^{2^s} < x$且${c_i}^{2^{s+1}} > x^2$，矛盾)，

故存在$m > n$滿足$a_m = c_i$。■

【性質4-2】形成$\langle a_\beta \rangle$的充要條件

$\exists c_1、s \in \mathbb{N}、c_1 \geq 2 : {c_1}^{2^s} \equiv c_1 (mod\ k)$，$\{c_n\} : \{c_1、c_2、\dots\dots、c_s\}$必存在${c_2}^2 \equiv c_1 (mod\ k)$、${c_3}^2 \equiv c_2 (mod\ k)$、……、${c_s}^2 \equiv c_{s-1} (mod\ k)$、${c_1}^2 \equiv c_s (mod\ k)$； 若同時滿足$\nexists n \in \mathbb{N}、n < c_i : n^2 \equiv c_i (mod\ k)$即存在$\langle a_\beta \rangle$。

<證明>

令${c_1}^2 \equiv c_2 (mod\ k)$、${c_1}^{2^2} \equiv c_3 (mod\ k)$、……、${c_1}^{2^{s-1}} \equiv c_s (mod\ k)$且滿足$c_i \leq k$，

顯然c_i必滿足${c_2}^2 \equiv c_1 (mod\ k)$、${c_3}^2 \equiv c_2 (mod\ k)$、……、${c_s}^2 \equiv c_{s-1} (mod\ k)$、${c_1}^2 \equiv c_s (mod\ k)$。

由**【引理4-2-1】**可知c_i必在數列中，若$\exists n \in \mathbb{N}、n < c_i : n^2 \equiv c_i (mod\ k)$，

$\because n < c_i$，$\therefore n^2 < {c_{i-1}}^2$，因此數列將出現$a_\ell = n$破壞原本週期。■

(五)補充說明

即使已確知$a_n = a$代入數列可形成週期，並不保證任意正整數x滿足$x \equiv a (mod\ k)$即可以

$a_n = x$代入數列形成週期。根據k的列表之對稱性，可知當$a \neq \frac{k}{2}$且$a \neq k$時必然有一數i滿足$a < i < k$且$i^2 \equiv a(mod\ k)$，此時若令$x = i^2$，$a_n = x$代入數列將使$a_{n+1} = i$破壞週期。

伍、 研究結果

一、對於週期數列$\langle a_m \rangle$，存在無限多個$a_m = a_n$若且唯若$\exists m \in \mathbb{N}$、 $m > n$：$a_m = a_n$。

二、k的列表右欄存在二分對稱性若且唯若$k \in \mathbb{N}$；存在四分對稱性若且唯若$4 \mid k$。任意k的列表均不存在其他對稱性。

三、形成單純週期數列$\langle a_\alpha \rangle$的充要條件為數列中存在a且不存在b。

四、對於$k \geq 3$，$\langle a_\alpha \rangle$滿足$\exists i \in \mathbb{N}$：$a_i = a$且$\nexists j \in \mathbb{N}$：$a_j < a$。

五、當$k = 1$，形成$\langle a_\alpha \rangle$若且唯若$a_n = c$滿足$c \in \mathbb{N}$，且數列終將進入$\langle a_\alpha \rangle = \langle \dots,2,3,4,2, \dots \rangle$。

六、當k為奇質數，形成$\langle a_\alpha \rangle$若且唯若$a_n = c$滿足$c \equiv 0(mod\ k)$，因此第 58 屆 IMO 競賽第一題的答案是「a_0為所有3的倍數」；當$k = 2$，形成$\langle a_\alpha \rangle$若且唯若$a_n = c'$滿足$c' \in \mathbb{N}$，且當$a_n = 2n(n \in \mathbb{N})$時數列終將進入$\langle a_\alpha \rangle = \langle \dots,2,4,2,4, \dots \rangle$；當$a_n = 2n' + 1(n' \in \mathbb{N})$時數列終將進入$\langle a_\alpha \rangle = \langle \dots,3,5,7,9,3, \dots \rangle$。

七、對任意$k \geq 3$：當$a \equiv 0(mod\ k)$，若$k = \prod_{i=1}^{n} p_i$ ($n \in \mathbb{N}$，p_i為任意相異質數)能形成週期，反之亦然；當$a \equiv 1(mod\ k)$時皆不能形成週期。

八、當$k = \prod_{i=1}^{n} {p_i}^{\alpha_i}$ ($n \in \mathbb{N}$，p_i為任意相異質數且$j \in \{1,2, \dots \dots, n-1\}$)，恆有$(k, a) = \prod_{1}^{j} {p_i}^{\alpha_i}$。

九、構造a：

(一) $k = \prod_{i=1}^{n} {p_i}^{\alpha_i}$，當$(k, a) = \prod_{i=1}^{n-1} {p_i}^{\alpha_i}$，分為兩種情況(以下$m \in \mathbb{Z}$)：

1° $p_n \neq 2$， $\prod_{i=1}^{n-1} ({p_i}^{\alpha_i})^{p_n - 2} - mp_n > 0$、${p_n}^{\alpha_n} \mid \left\{ \prod_{i=1}^{n-1} {p_i}^{\alpha_i} \left[\prod_{i=1}^{n-1} ({p_i}^{\alpha_i})^{p_n - 2} - mp_n \right] - 1 \right\}$ 皆成立時，$a = \prod_{i=1}^{n-1} {p_i}^{\alpha_i} \left[\prod_{i=1}^{n-1} ({p_i}^{\alpha_i})^{p_n - 2} - mp_n \right]$即為所求。

2° $p_n = 2$，若存在$t \in \mathbb{N}$且$t \leq 2^{\alpha_n - 2}$(若$\alpha_n = 1$則$t = 1$)滿足$2^{\alpha_n} \mid (t \prod_{i=1}^{n-1} {p_i}^{\alpha_i} - 1)$，則$a = t \prod_{i=1}^{n-1} {p_i}^{\alpha_i}$即為所求。

(二) 當$(k, a) = \prod_{i=1}^{r} {p_i}^{\alpha_i}$ $\left(r \in \mathbb{N} \text{ 且 } 1 \leq r < n-1\right)$：

1° 當$p_\ell \neq 2$(其中 $\ell \in \{r+1, r+2, \dots \dots, n\}$)，符合所求的$a$必須滿足對所有${p_j}^{\alpha_j}(r + 1 <$

$j \le n$)構造的結果。

2° 當$p_\ell = 2$，$t' \in \mathbb{N}$滿足$t' \le \prod_{i=r+1}^{n-1} {p_i}^{\alpha_i}$ (當$\alpha_\ell = 1$時)或$t' \le 2^{\alpha_n - 2} \prod_{i=r+1}^{n-1} {p_i}^{\alpha_i}$ (當$\alpha_\ell \ge 2$時)，且滿足$2^{\alpha_\ell} \mid (t' \prod_{i=1}^{r} {p_i}^{\alpha_i} - 1)$，則$a = t' \prod_{i=1}^{r} {p_i}^{\alpha_i}$即為所求。

十、考慮b存在：

當$k = \prod_{i=1}^{n} {p_i}^{\alpha_i}$：

若$(k, a) = \prod_{i=1}^{n-1} {p_i}^{\alpha_i}$且$\alpha_i = 1$，$p_n \ne 2$時不存在$b$；若$p_n = 2$，檢查${p_n}^{\alpha_n - m} \mid 2t'$是否成立(其中$m$、$t' \in \mathbb{N}$且不失一般性設$m \ge \frac{\alpha_n}{2}$)，若是則存在$b$。

若$(k, a) = \prod_{i=1}^{m} {p_i}^{\alpha_i}\ (m \in \mathbb{N}$ 且 $1 \le m \le n-1)$，設$b = t' \prod_{i=1}^{m} {p_i}^{\alpha_i'}$ ($t' \in \mathbb{N}$且不失一般性設$\sum_{i=1}^{m} \alpha_i \ge \sum_{i=1}^{m} \alpha_i'$)，分為兩種情況：

(一)當$\prod_{i=m+1}^{n} {p_i}^{\alpha_i} \mid t\left(\frac{b}{a} + 1\right) \vee \prod_{i=m+1}^{n} {p_i}^{\alpha_i} \mid t(\frac{b}{a} - 1)$成立時即存在$b$。

(二)存在m_1、$m_2 \in \mathbb{N}$滿足$\left(t \prod_{i=1}^{m} {p_i}^{(\alpha_i - \alpha_i')} + t'\right) = m_1 \prod_{i=m+1}^{r} {p_i}^{\alpha_i}$與$(t \prod_{i=1}^{m} {p_i}^{(\alpha_i - \alpha_i')} - t') = m_2 \prod_{i=r+1}^{n} {p_i}^{\alpha_i}$即存在$b$。

十一、不必考慮「b存在」的a(僅存在於$k = \prod_{i=1}^{n-1} p_i {p_n}^{\alpha_n}$，而此處以$k = \prod_{i=1}^{n} p_i$說明)：

當$p_n \ne 2$， $a = \prod_{i=1}^{n-1} p_i\, [(\prod_{i=1}^{n-1} p_i)^{p_n - 2} - m p_n] (m \in \mathbb{Z})$；

當$p_n = 2$，$a = \prod_{i=1}^{n-1} p_i$。

對於其他的a皆有條件存在b。

十二、給定k後，尋找可形成週期的a的方式：

1° 觀察k的列表(適用於k值較小時，如表 5)：

表 5

⋮	⋮
a	a
⋮	⋮

列表中若存在某列左右欄的數相同(如表 5 中的a)，且右欄的a滿足「所有位在它上方的數皆不是a」，則$a_n = a$代入數列可形成$\langle a_\alpha \rangle$。對於特殊週期數列中k的列表，如表 6：

表 6

⋮	⋮
c_1	c_2
⋮	⋮
c_2	c_3
⋮	⋮
c_n	c_1
⋮	⋮

設表 6 中存在「若左欄為c_i，則對應右欄為c_{i+1}(當左欄為c_n時對應右欄為c_1)」的關係，且右欄對應之c_j都滿足「所有位在它上方的數皆不是c_j」，則$a_n = c_i$代入數列即可形成$\langle a_\beta \rangle$。

2° 一般尋找(較耗時但較完整)：將k質因數分解為$\prod_{i=1}^{n} {p_i}^{\alpha_i}$ →構造a →排除b存在的情況。

3° 有效構造(僅適用於$k = \prod_{i=1}^{n-1} p_i \, {p_n}^{\alpha_n}$，較快速但可能有遺漏)：將$k$質因數分解→考慮$(k, a) = \prod_{i=1}^{n-1} p_i$之所有情況，而$a$構造完成後不須考慮$b$即可代入數列形成週期。

十三、形成特殊週期數列$\langle a_\beta \rangle$的充要條件：對於c、$s \in \mathbb{N}$ 且c、$s \geq 2$滿足$c^{2^s} \equiv c(mod\ k)$，且$\nexists n \in \mathbb{N}$、$n < c_i$：$n^2 \equiv c_i(mod\ k)$即存在$\langle a_\beta \rangle$。

十四、即使已確知$a_n = a$代入數列可形成週期，並不保證任意正整數x滿足$x \equiv a(mod\ k)$即可以$a_n = x$代入數列形成週期。

十五、舉例 $(k = 30)$：

因為質因數分解為$2 \times 3 \times 5$，故採用「有效構造」分別討論幾種常見情況與$a = 6t$、$a = 10t$、$a = 15t$(其中$t \in \mathbb{N}$)。

1° 因為質因數分解為$2 \times 3 \times 5$，故$a = 30$ 即為所求。

2° 設$a = 6t$，$a = 6[6^3 - 5m]$，由歐拉定理可知$6^4 \equiv 1(mod\ 5)$，則$6^3 \equiv 1(mod\ 5)$，因此$a = 6$、36(大於$\frac{30}{2}$因此不合)。

3° 設$a = 10t$，$a = 10[10^1 - 3m]$，因此$a = 10$、40(大於$\frac{30}{2}$因此不合)。

4° 設$a = 15t$，因為30質因數分解後2只有一次方，因此$a = 15$即為所求。

使用程式檢驗$k = 30$所有可形成週期的a：6、10、15、30。

陸、討論

一、誠如詩經 蒹葭篇所言：「溯洄從之，道阻且長。」對於質因數分解後有多質因數連乘且有高次方的k，構造a的速度較緩慢。

二、尚未歸納出$\langle a_\beta \rangle$較快的構造方法，值得未來努力探究。

柒、參考資料及其他

一、傅承德、劉啟昌(2014)・*數戰數決：台灣數學資優生出國比賽記*・臺北市：商業週刊

二、游森棚(2019)・*普通高級中學數學課本* (2 乙版)・臺南市：翰林。

三、高竹嵐(2017)・*2017 年第 58 屆國際數學奧林匹亞競賽試題解答*・**數學傳播 41 卷 3 期**。

【評語】050409

1. 作者利用接近窮舉的方式討論特殊遞迴數列，有得到一些成果，不過整體來說並不具創意。

2. 本作品所研究一個等差數列，處理完全平方數時則將該項開根號，所形成數列的週期性質。這個問題並不容易，但是卻是一個數論上已經研究數百年的二次剩餘(quadratic residue)理論的應用。也因為研究成果眾多，作者在整份作品裏，列出整整 46 個性質或定理並加以證明，但在參考文獻裏，卻只有含高中教科書在內的三個中文文獻。因此，本研究需交待到底那些性質是已知，那些是作者自行處理。建議作者在作品的呈現上，應該聚焦在自己的研究成果，並對於已知的性質，適當地加以引用文獻上的已知結果。

3. 本研究宜作文獻探討，尤其須說明定理 1 歐拉準則的應用是否為本研究的發現。

4. 本研究方法的構想是否有參考資料？何以如此探討其建構週期數列？

作品海報

摘要

本研究在等差數列的基礎上，加入「若a_n為完全平方數，則$a_{n+1}=\sqrt{a_n}$」遞迴關係，將具有週期性的數列分為「單純週期數列」與「特殊週期數列」，並以單純週期數列為主要研究目標。我們探討單純週期數列的各項性質與充要條件，並透過歐拉準則與費馬小定理討論不同公差與首項是否能形成單純週期，整合與建構「給定公差，尋找可形成週期的首項」之方法，也研究特殊週期數列之性質與充要條件。

研究動機

在專題課的下課時分，我們在教室書櫃找到數戰數決一書，便被書中的精彩故事深深吸引，同時讓我們對IMO國際數學奧林匹亞競賽有更多的認識，也對它的試題產生好奇。上課時，我們上網觀摩幾屆數奧的試題與解析，發現一道結合等差數列與週期性的題目：

問題 1: 對於每個整數 $a_0 > 1$, 用以下方法定義數列 $a_0, a_1, a_2, \ldots$:

$$a_{n+1} = \begin{cases} \sqrt{a_n} & \text{若} \sqrt{a_n} \text{爲整數} \\ a_n + 3 & \text{其他情況} \end{cases} \quad \text{對於所有 } n \geqslant 0 \text{皆成立}$$

試求所有可能值 a_0, 滿足存在一個數 A, 使得有無窮多個 n 讓 $a_n = A$。

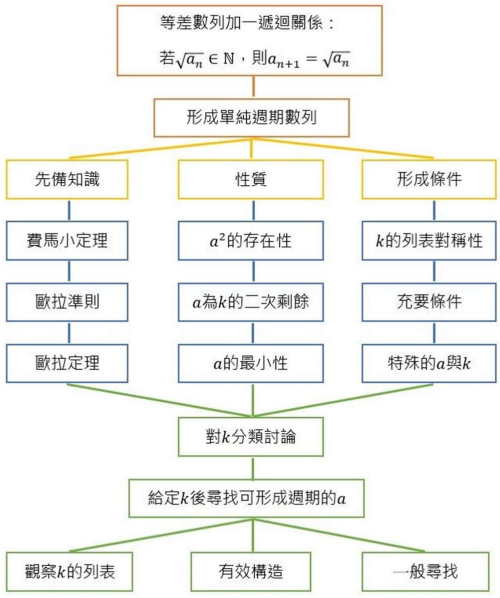
我們對具有週期性的等差數列(以下稱週期數列)感到相當有趣，決定深入探討週期數列的性質及尋找能形成週期數列的條件，並定義新題目如下：

$$a_{n+1} = \begin{cases} \sqrt{a_n} & \text{若} \sqrt{a_n} \in \mathbb{N} \\ a_n + k & \text{其他情況} \end{cases}$$ 對於所有$a_n > 1$，$k \in \mathbb{N}$且$n \in \mathbb{N}$皆成立。尋找一數a_n滿足存在無限多個a_m，$m \in \mathbb{N}$，$m > n$且$a_m = a_n$。

研究目的

一、尋找單純週期數列形成的條件。
二、討論在公差為一個質數、多個質數相乘，乃至於多質數相乘且存在高次方，如何在給定公差後尋找一數代入a_n使數列形成週期。
三、探討特殊週期數列形成的條件與建構方式。

研究流程



圖一、研究流程圖

研究過程與結果

一、名詞定義

1. k：滿足$k \in \mathbb{N}$，為數列的公差
2. a_n：數列中第n項
3. a：滿足$a \in \mathbb{N}$，$a \leq k$，$a^2 \equiv a(mod\ k)$
4. $A_n = \{2, 3, 4, \ldots\ldots, k-1\}$
5. b：滿足$b \in \mathbb{N}$，$b \in A_n$，$b < a$，$b^2 \equiv a(mod\ k)$
6. $\langle a_m \rangle$，$m = 1 \sim n$：週期數列$\langle a, a+k, \ldots\ldots, a^2, a \rangle$
7. $\langle a_\alpha \rangle$：單純週期數列$\langle a, a+k, \ldots\ldots, a^2, a \rangle$，滿足$a_i \equiv a(mod\ k)$
8. $\langle a_\beta \rangle$：特殊週期數列$\langle a, a+k, \ldots\ldots, a^2, a \rangle$，滿足$\exists j \in \mathbb{N}$：$a_j \not\equiv a(mod\ k)$
9. 公差k的列表：分為左右兩欄，左欄由上而下依序為$0 \sim k-1$，右欄為對應左欄的數平方後除以k的餘數
10. 對稱軸：k的列表中，若左欄有一數n滿足$n \in \mathbb{Q}$，$0 < n < k-1$且$(n+t)^2 \equiv (n-t)^2 (mod\ k)$，其中$t \in \mathbb{Q}$且$0 < t < \frac{k}{4}$，則$n$為公差$k$的列表的對稱軸

二、性質討論

（一）尋找形成單純週期數列的充要條件：存在a且不存在b。

（二）觀察k的列表：

表1：k的列表

0	$0^2(mod\ k)$
1	$1^2(mod\ k)$
2	$2^2(mod\ k)$
$\vdots$	$\vdots$
$\vdots$	$\vdots$
$k-2$	$(k-2)^2(mod\ k)$
$k-1$	$(k-1)^2(mod\ k)$

表2：k=7的列表

0	0
1	1
2	2
3	4
4	4
5	2
6	1

由k的列表可以觀察出對稱軸與對稱性的存在。我們據此歸納：

任意k的列表皆存在二分對稱性；當$4 \mid k$時k的列表存在四分對稱性。

（三）討論特殊的a：

$k \geq 3$時：當$a \equiv 0(mod\ k)$，若$k=\prod_{i=1}^{n} p_i$ $(n \in \mathbb{N}$，p_i為任意相異質數)能形成週期，反之亦然；當$a \equiv 1(mod\ k)$時皆不能形成週期。

（四）討論特殊的k：

當$k=1$，$a_n \in \mathbb{N}$皆能使數列形成$\langle a_\alpha \rangle = \langle \dots, 2, 3, 4, 2, 3, 4, 2, \dots \rangle$。

當k為奇質數，形成$\langle a_\alpha \rangle$若且唯若$a_n \equiv 0(mod\ k)$。

當$k=2$，形成$\langle a_\alpha \rangle$若且唯若$a_n \in \mathbb{N}$，而$a_n = 2n(n \in \mathbb{N})$時數列終將進入$\langle a_\alpha \rangle = \langle \dots, 2, 4, 2, 4, \dots \rangle$；若$a_n = 2n'+1(n' \in \mathbb{N})$時數列終將進入$\langle a_\alpha \rangle = \langle \dots, 3, 5, 7, 9, 3, \dots \rangle$。

當k為單一質數多次方，$\nexists a \neq 0$、$a \neq 1 : a^2 \equiv a(mod\ k)$，且不存在$a_n \in \mathbb{N}$可形成週期。

三、對k討論

當$k=\prod_{i=1}^{n} {p_i}^{\alpha_i}$，$p_i$為任意相異質數，$n$、$\alpha_I \in \mathbb{N}$：

（一）構造a：

當$(k,a)=\prod_{i=1}^{n-1} {p_i}^{\alpha_i}$且$\alpha_i = 1$：

當$p_n \neq 2$，$a = p_n\left[\left(\prod_{i=1}^{n-1} p_i\right)^{p_n-2} - mp_n\right](m \in \mathbb{Z})$；當$p_n = 2$，$a=\prod_{i=1}^{n-1} p_i$。

當$(k,a)=\prod_{i=1}^{n-1} {p_i}^{\alpha_i}$：

1. 若$p_n \neq 2$，存在$m \in \mathbb{Z}$滿足$\prod_{i=1}^{n-1}({p_i}^{\alpha_i})^{p_n-2} - mp_n > 0$且${p_n}^{\alpha_n} \mid \left\{\left[\prod_{i=1}^{n-1}({p_i}^{\alpha_i})^{p_n-2} - mp_n\right]-1\right\}$，

   則$a=\prod_{i=1}^{n-1} {p_i}^{\alpha_i}\left[\prod_{i=1}^{n-1}({p_i}^{\alpha_i})^{p_n-2} - mp_n\right]$即為所求。

2. 若$p_n = 2$，若存在$t \in \mathbb{N}$且$t \leq 2^{\alpha_n-2}$(若$\alpha_n = 1$則$t=1$)滿足$2^{\alpha_n} \mid (t\prod_{i=1}^{n-1} {p_i}^{\alpha_i} - 1)$，

   則$a = t\prod_{i=1}^{n-1} {p_i}^{\alpha_i}$。

當$(k,a)=\prod_{i=1}^{r} {p_i}^{\alpha_i}$ $(r \in \mathbb{N}$且$1 \leq r < n-1)$：

1. 當$p_\ell \neq 2$(其中$\ell \in \{r+1, r+2, \dots\dots, n\}$)，符合所求的$a$必須滿足對所有${p_j}^{\alpha_j}(r+1 < j \leq n)$構造的結果。

2. 當$p_\ell = 2$，$t' \in \mathbb{N}$滿足$t' \leq \prod_{i=r+1}^{n-1} {p_i}^{\alpha_i}$(當$\alpha_\ell = 1$時)或$t' \leq 2^{\alpha_n-2}\prod_{i=r+1}^{n-1} {p_i}^{\alpha_i}$(當$\alpha_\ell \geq 2$時)，且滿足$2^{\alpha_\ell} \mid (t'\prod_{i=1}^{r} {p_i}^{\alpha_i} - 1)$，則$a = t'\prod_{i=1}^{r} {p_i}^{\alpha_i}$即為所求。

（二）考慮b的存在：

當$k=\prod_{i=1}^{n} {p_i}^{\alpha_i}$，滿足$(k,a)=\prod_{i=1}^{n-1} {p_i}^{\alpha_i}$且$\prod_{i=1}^{n-1} \alpha_i = 1$，$p_n \neq 2$時不存在$b$；若$p_n = 2$則有條件存在$b$。

當$k=\prod_{i=1}^{n} {p_i}^{\alpha_i}$，滿足$(k,a)=\prod_{i=1}^{m} {p_i}^{\alpha_i}$ $(m \in \mathbb{N}$且$1 \leq m < n-1)$，則有條件存在b。

四、特殊週期數列

形成$\langle a_\beta \rangle$的充要條件:

$\exists c_1、s \in \mathbb{N}、c_1 \geq 2：{c_1}^{2^s} \equiv c_1 (mod\ k)$，集合$\{c_n\}：\{c_1、c_2、\ \ldots\ldots、c_s\}$恆有${c_2}^2 \equiv c_1 (mod\ k)$、${c_3}^2 \equiv c_2 (mod\ k)$、$\cdots\cdots$、${c_s}^2 \equiv c_{s-1} (mod\ k)$、${c_1}^2 \equiv c_s (mod\ k)$，若同時滿足$\nexists n \in \mathbb{N}、n < c_i：n^2 \equiv c_i (mod\ k)$即存在$\langle a_\beta \rangle$。

五、補充說明

即使已確定$a_n = a$代入數列可形成週期，並不保證任意正整數x滿足$x \equiv a (mod\ k)$即可以使$a_n = x$代入數列形成週期。根據k的列表之對稱性可知當$a \neq \frac{k}{2}$且$a \neq k$時恆有一數i滿足$a < i < k$且$i^2 \equiv a (mod\ k)$，此時若令$a_n = i^2$代入數列將使$a_{n+1} = i$破壞週期。

六、實際尋找

(一) 觀察k的列表(k值較小時適用)：

表5

⋮
⋮
a
⋮
⋮

表6

⋮	⋮
c_1	c_2
⋮	⋮
c_2	c_3
⋮	⋮
c_n	c_1
⋮	⋮

1. 列表中若存在某列左右欄的數相同(如表5中的a)，且右欄的a滿足「所有位在它上方的數皆不是a」，則$a_n = a$代入數列可形成$\langle a_\alpha \rangle$。
2. 設表6中存在「若左欄為c_i，則對應右欄為c_{i+1}(當左欄為c_n時對應右欄為c_1)」的關係，且右欄對應之c_j都滿足「所有位在它上方的數皆不是c_j」，則$a_n = c_i$代入數列即可形成$\langle a_\beta \rangle$。

(二) 一般尋找(較耗時但較完整)：將k質因數分解為$\prod_{i=1}^{n} {p_i}^{\alpha_i}$ →構造a →排除b存在的情況。

(三) 有效構造(僅適用於$k = \prod_{i=1}^{n-1} p_i {p_n}^{\alpha_n}$，較快速但可能有遺漏)：將$k$質因數分解→考慮$(k, a) = \prod_{i=1}^{n-1} p_i$之所有情況，而$a$構造完成後不須考慮$b$即可代入數列形成週期。

舉例 $(k = 30)$：

因為質因數分解為$2 \times 3 \times 5$，故採用「有效構造」分別討論幾種常見情況與$a = 6t$、$a = 10t$、$a = 15t$(其中$t \in \mathbb{N}$)。

1. 因為質因數分解為$2 \times 3 \times 5$，故$a = 30$即為所求。
2. 設$a = 6t$，$a = 6\left[6^3 - 5m\right]$，由歐拉定理可知$6^4 \equiv 1 (mod\ 5)$，則$6^3 \equiv 1 (mod\ 5)$，因此$a = 6$、$36$(大於$\frac{30}{2}$因此不合)。
3. 設$a = 10t$，$a = 10\left[10^1 - 3m\right]$，因此$a = 10$、$40$(大於$\frac{30}{2}$因此不合)。
4. 設$a = 15t$，因為30質因數分解後2只有一次方，因此$a = 15$即為所求。

使用程式檢驗$k = 30$所有可形成週期的a：6、10、15、30。

討論

一、誠如詩經蒹葭篇所言：「溯洄從之，道阻且長。」對於質因數分解後有多質因數連乘且有高次方的k，構造a的速度較緩慢。

二、尚未歸納出$\langle a_\beta \rangle$較快的構造方法，值得未來努力探究。

參考資料

一、傅承德、劉啟昌(2014)。*數戰數決：台灣數學資優生出國比賽記*。臺北市：商業週刊

二、游森棚(2019)。*普通高級中學數學課本*（2乙版）。臺南市：翰林

三、高竹嵐(2017)。*2017年第58屆國際數學奧林匹亞競賽試題解答*。數學傳播41卷3期