中華民國第 65 屆中小學科學展覽會
作品說明書

國小組　數學科

探究精神獎

080414

數列 DNA—等差數列的質與合

學校名稱： 康橋學校財團法人新北市康橋高級中學

作者：	指導老師：
小六 陳立洋	楊錦花
小六 詹軒亦	林東岳
小六 葉蔡叡	
小六 李丞祐	

關鍵詞： 質項、合項、模冪

摘　要

本研究取材自科學研習期刊的數學專欄題。

給定一個正整數數列，如果數列元素可以寫成這個數列的某些項的乘積，就稱該元素為這個數列的合項，否則稱該元素為這個數列的質項。

我們將研究聚焦於等差數列，並成功發展出首項為 1，以及首項=公差-1 之等差數列的合項快速篩檢模式，更進一步發現「**首項的冪次模公差的週期性**」，對於判斷任何等差數列的合項性質都具有關鍵作用。

我們證實存在「**完全由質項構成的等差數列**」，也觀察到梅森質數在特定的等差數列中可以作為其質項。

最後，我們修改質數定理，成功預估了首項為 1、不同公差等差數列的質項密度。本研究為為理解數列的結構與性質提供了全新的工具與視角。。

本作品說明書中所有圖形與表格均由作者或指導老師親自繪製。

壹、前言

一、研究動機

2024 年 8 月份科學研習期刊「森棚教官數學題—質項與合項」(游森棚[1])

給定一個正整數數列$a_1, a_2, \ldots$，如果a_n可以寫成這個數列的某些項(≥ 2 項，可重複)的乘積(1 除外)，就稱a_n為這個數列的合項，否則稱a_n為這個數列的質項，1 不列入質項也不列入合項。

例如偶數的正整數數列

$\langle a_n \rangle_{n\geq 1} = 2, 4, 6, 8, \ldots, 2n, \ldots$ 之中，2,6 都是質項；4,8 是合項。

這與我們學到的質數與合數的概念，有些相關又無法完全套用，它提供我們重新思考整數數列的內部結構，也引起了我們深入探討的興趣。

二、研究目的

（一）探討特殊等差數列的質項與合項檢核模式。

（二）以首項與公差的質因數集合探討等差數列的質項與合項。

（三）將等差數列的質項與質數研究做聯結性的探討。

三、文獻探討

由數列中尋找合項與質項是一個新的概念，故無法從歷屆科展中找到相關的研究。

四、本作品的特色

(一) 重新定義數列元素的分解模式

以數列元素當因數的單位去做項數元素的分解。

(二) 快速簡易的合項篩選機制

提出首項為 1 及首項=公差−1 的等差數列合項快速篩選法，大幅降低計算複雜度。

(三) 模冪規律性的應用

發現首項冪次模公差的週期規律，可以成為等差數列判別合項的基準。

(四) 全質項數列的發現

證實存在完全由質項構成的質項等差數列，挑戰傳統數列結構認知。

(五) 連結梅森質數

找出梅森質數在特定等差數列中必為質項，建立與經典質數的深刻關聯。

(六)質項密度

推導出廣義質項密度估計式，擴展質數定理的應用範疇。

五、名詞定義與符號說明

(一) 數列與數列中的元素

數列指由一系列數組成的序列，本研究以$\langle a_n\rangle_{n\geq1}$表示數列。

數列元素指數列中的項，數列$\langle a_n\rangle_{n\geq1}$的元素以$a_1$、$a_2$、…、$a_n$表示。

(二) 質數與質項：

質數：當一個正整數不能寫成比本身還小的兩個正整數相乘，我們稱此數為「質數」。

質項：指數列中的元素，**無法**寫成這個數列中的某些項(至少 2 項，可重複)的乘積(1 除外)，我們稱這個元素為「質項」。

(三) 合數與合項：

合數：當一個正整數可以寫成兩個正整數相乘(1 除外)，我們稱此數為「合數」。

合項：指數列中的項**可以**寫成這個數列中的某些項(至少 2 項，可重複)的乘積(1 除外)，我們稱這個元素為「合項」。

(四) 質因項：數列元素為質項且為合項因數分解中的元素，稱為該合項的質因項。

(五) 質項等差數列：指數列中每項皆無法分解成某些項的乘積，例$\langle a_n\rangle_{n\geq1}=$ 2,6,10,14,18 … ,如 18=2· 9，9 非數列元素

(六) 符號說明

1. $\mathbf{P}_{\boldsymbol{k}}$表$k$的質因數所成的集合。

   例：$a_1=18=2\cdot3^2$，則P_{a_1}={2, 3}；$d=21=3\cdot7$，則$\mathrm{P}_d=\{3,7\}$。

2. $\boldsymbol{v}_{\boldsymbol{p}}(\boldsymbol{x})$表示質因數$p$在$x$的標準分解式中的指數

六、研究架構

數列DNA—等差數列的質與合

研究過程

- a_1=1
- a_1 ≠1→d=a_1+1

特殊化

一般化

- $P_{a_1} \cap P_d = \emptyset$
- $P_{a_1} = P_d$
- $P_d \subsetneq P_{a_1}$
- $P_{a_1} \subsetneq P_d$
- $P_{a_1} \cap P_d \neq \emptyset$

合項條件

質項等差數列

討論

- 埃氏篩應用
- 梅森質數與等差數列數列的質項
- 質項密度探討

未來展望

- 二次方程式數列
- 不同形式數列
- 密碼學應用

參、研究過程或方法

1. 同餘與模算術(許介彥[3])

   $a \equiv b\ (mod\ m)$ 且 $c \equiv d\ (mod\ m)$，那麼

$$a + c \equiv b + d\ (mod\ m)$$
$$a - c \equiv b - d\ (mod\ m)$$
$$ac \equiv bd(modm)$$
$$a^n \equiv b^n(modm)$$
$$ak \equiv bk(modm)$$

2. 中國剩餘定理(許志農[4])

   設m, n是互質的正整數，a, b為整數，則同餘式

$$x \equiv a\ \ (mod\ m)$$
$$x \equiv b\ \ (mod\ n)$$

   有共同的整數解x_0，且所有共同的整數解x也構成一個同餘式為

$$x \equiv x_0\ \ (mod\ mn)$$

3. 歐拉函數$\varphi(n)$是不大於n的正整數中與n互質的數的個數。若n為質數，$\varphi(n) = n - 1$。(維基百科[5])

4. 歐拉定理：若a, d為正整數，且a, d互質，則

$$a^{\varphi(d)} \equiv 1(mod\ d)$$

5. 模冪運算是指求整數b的次方b^e被正整數m所除得到的餘數c的過程，可用數學符號表示為$c = b^e(modm)$。由c的定義可得 $0 \le c \le m-1$。(維基百科[6])
6. 埃拉托斯特尼篩法：從最小的質數 2 開始，將該質數的所有倍數標記成合數，而下一個尚未被標記的最小自然數 3 即是下一個質數。如此重複這一過程，將各個質數的倍數標記為合數並找出下一個質數，最終便可找出一定範圍內所有質數。

   尋找小於等於n的質數時，若找到了一個大於$\sqrt{n}$的質數，則剩餘的所有尚未標記的數也都是質數。(Stein[2])

肆、研究結果

一、首項為 1，公差>2 的等差數列

(一) 公差= 3，首項=1 的等差數列。$\langle a_n\rangle_{n\geq 1}=1,4,7,10,13,\ldots,3(n-1)+1\ldots$

表 1-1：首項 1 公差 3 的等差數列 $m+a_m$的值與合項的關係

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a_m	1	4	7	10	13	16	19	22	25	28	31	34	37	40	43
$m+a_m$	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58

n	6	10	14	17	18	22	24	26	30	31	34	38	42	44	45	46	50
a_n	16	28	40	49	52	64	70	76	88	91	100	112	124	130	133	136	148
因數分解	4^2	$4\cdot 7$	$4\cdot 10$	7^2	$4\cdot 13$	4^3	$7\cdot 10$	$4\cdot 19$	$4\cdot 22$	$7\cdot 13$	$4\cdot 25$	$4^2\cdot 7$	$4\cdot 31$	$10\cdot 13$	$7\cdot 19$	$4\cdot 34$	$4\cdot 37$
質因項分解	${a_2}^2$	a_2a_3	a_2a_4	${a_3}^2$	a_2a_5	${a_2}^3$	a_3a_4	a_2a_7	a_2a_8	a_3a_5	a_2a_9	${a_2}^2a_3$	a_2a_{11}	a_4a_5	a_3a_7	a_2a_{12}	a_2a_{13}

1. **當$n=m+a_m$時，則a_n為合項。**

(1)對照表 1-1 上、下表發現：大部分的合項都有一個有趣的現象(如底框藍色部分)

當 $n=m+a_m(m\geq 2)$時，則a_n為合項。

例 $n=2+a_2=2+4=6$，$a_6=16={a_2}^2$

$n=3+a_3=3+7=10$，$a_{10}=28={a_2}^2a_3$

$n=4+a_4=4+10=14$，$a_{14}=40={a_2}^2a_4$

(2) 當$n=m+a_m(m\geq 2)$，則a_n 都包含第二項$a_2=4$ 的質因項。

證明：

首項為1，公差為3，$\langle a_n\rangle_{n\geq 1}=1,4,7,10,13,\ldots,3(n-1)+1$

$a_m=1+3(m-1)=3m-2$

$n=m+a_m=m+(3m-2)=4m-2$

$a_n=3(4m-2)-2=12m-8=4(3m-2)=a_2a_m$ ■

(3) 當$n\neq m+a_m$ 且a_n為合項時，如 a_{17}、a_{24}、a_{31}、a_{44}、a_{45}、a_{52}、a_{57} 這些合項都不包含 a_2的質因項。換句話說，若合項的質因項不包含a_2，該合項的項次無法從 $n=m+a_m(m\geq 2)$求得，需另作分析。

表 1-2：合項中含因項「$a_3=7$」的條件分析

$n=3+a_3k$	10=3+7	17=3+7×2	24=3+7×3	31=3+7×4	38=3+7×5	45=3+7×6
a_n	$a_{10}=28$	$a_{17}=49$	$a_{24}=70$	$a_{31}=91$	$a_{38}=112$	$a_{45}=133$
因數分解	$4\cdot 7$	$7\cdot 7$	$7\cdot 10$	$7\cdot 13$	$4^2\cdot 7$	$7\cdot 19$
質因項分解	a_2a_3	${a_3}^2$	a_3a_4	a_3a_5	${a_2}^2a_3$	a_3a_7

2. $\boxed{\text{當}\boldsymbol{n=3+a_3k}\text{，則}\boldsymbol{a_n}\text{為含有質因項}\boldsymbol{a_3}\text{=7 的合項。}}$

由表 1-2 發現：若 $n=3+a_3k$，如a_{10}、a_{17}、a_{24}、a_{31}、a_{38}、a_{45}、...，則a_n為含有因數a_3=7 的合項。

3. 類似的狀況也出現在含有$\boldsymbol{a_4}$=10 的質因項與$\boldsymbol{a_5}$=13 質因項的合項。

(1) $\boxed{\boldsymbol{n=4+a_4k}\text{，則}\boldsymbol{a_n}\text{為含有質因項}\boldsymbol{a_4}\text{=10 的合項}}$。例：

① 14=4+10×1；$a_{14}=40=4\times10=a_2\times a_4$。

② 24=4+10×2，$a_{24}=70=7\times10=a_3\times a_4$。

③ 34=4+10×3；$a_{34}=100=10\times10=a_4\times a_4$。

④44=4+10×4，$a_{44}=130=10\times13=a_4\times a_5$、....。

(2) $\boxed{\boldsymbol{n=5+a_5k}\text{，則}\mathbf{a_n}\text{為含有質因項}\boldsymbol{a_5}\text{=13 的合項}}$。例：

①18=5+13×1；$a_{18}=52=4\times13=a_2\times a_5$。

②31=5+13×2；$a_{31}=91=7\times13=a_3\times a_5$。

③44=5+13×3；$a_{44}=130=10\times13=a_4\times a_5$。

④57=5+13×4；$a_{57}=169=13\times13=a_5\times a_5$、....。

(3) **$\boldsymbol{a_n}$為含有$\boldsymbol{a_2}$=4 的質因項的合項也適用$\boldsymbol{n=2+a_2k}$**

即$\boxed{\boldsymbol{n=2+a_2k}\text{，則}\boldsymbol{a_n}\text{為含有質因項}\boldsymbol{a_2}\text{=4 的合項。}}$

①6=2+4×1；$a_6=16=4\times4=a_2\times a_2$。

②10=2+4×2；$a_{10}=28=4\times7=a_2\times a_3$。

③14=2+4×3；$a_{14}=40=4\times10=a_2\times a_4$。

④18=2+4×4；$a_{18}=52=4\times13=a_2\times a_5$....。

4. 故合項篩檢模式我們可修正

首項為 1，公差為 3 的等差數列，當$\boldsymbol{n=m+a_mk}$且$\mathbf{m\geq2}$，$\boldsymbol{k}$為正整數時，$\boldsymbol{a_n}$為合項。

證明：當 $\boldsymbol{n=m+a_mk}$且$\mathbf{m\geq2}$，$\boldsymbol{k}$為正整數時，$\boldsymbol{a_n}$為合項。

$$n=m+a_mk=m+(3m-2)k=m+3mk-2k$$

$$\begin{aligned}a_n&=3(m+3mk-2k)-2=3m+9mk-6k-2\\&=3k(3m-2)+(3m-2)=(3m-2)(3k+1)\\&=a_ma_{k+1}\end{aligned}$$

$a_n=a_ma_{k+1}$，故當 $n=m+a_mk$ 且$m\geq2$，k為正整數時，a_n為合項。■

(二) 檢核公差為 4，首項為 1 的等差數列是否適用當$\boldsymbol{n = m + a_m k}$且$\boldsymbol{m \geq 2}$，$\boldsymbol{k}$為正整數時，$\boldsymbol{a_n}$為合項。

1. d =4，a_1=1，$a_n = 4(n-1)+1 = 4n-3$；$\langle a_n \rangle_{n\geq 1} = 1,5,9,13,17,\ldots 4n-3\ldots,$，

表 1-3：首項 1，公差 4 的等差數列前 18 項合項分析

n	7	12	17	21	22	27	30	32	37	39	42	43	47	48	52	56	57	62
a_n	25	45	65	81	85	105	117	125	145	153	165	169	185	189	205	221	225	245
因數分解	5^2	5×9	5×13	9^2	5×17	5×21	9×13	5^3	5×29	9×17	5×33	13^2	5×37	9×21	5×41	13×17	5×45	5×49
質因項分解	${a_2}^2$	a_2a_3	a_2a_4	${a_3}^2$	a_2a_5	a_2a_6	a_3a_4	${a_2}^3$	a_2a_8	a_3a_5	a_2a_9	${a_4}^2$	a_2a_{10}	a_3a_6	a_2a_{11}	a_4a_5	a_2a_{12}	a_2a_{13}

2. 檢核表 1-3 中數列的合項是否符合$n = m + a_m k$

(1) 含a_2=5 質因項的合項包括a_7、a_{12}、a_{17}、a_{22}、a_{27}、a_{32}、a_{37}、a_{42}、…

其項次皆符合 $n = 2 + a_2 k = 2 + 5k$

例： 7=2+5，12=2+5×2，17=2+5×3，22=2+5×4，27=2+5×5….。

(2) 含a_3=9 質因項的合項包括a_{12}、a_{21}、a_{30}、a_{39}、a_{48}、a_{57}、a_{66}、…

其項次皆符合 $n = 3 + a_3 k = 3 + 9k$

例： 12=3+9，21=3+9×2，30=3+9×3，39=3+9×4，48=3+9×5…。

(3) 含a_4=13 質因項的合項包括a_{17}、a_{30}、a_{43}、a_{56}、…

其項次皆符合 $n = 4 + a_4 \times k = 4 + 13k$

例：17=4+13，30=4+13×2，43=4+13×3，56=4+13×4，…

3. 依此推論：首項為 1，公差為 4 的等差數列，當 $\boldsymbol{n = m + a_m k}$且$\mathbf{m} \geq \mathbf{2}$，$\boldsymbol{k}$為正整數時，則 $\boldsymbol{a_n}$為合項。

證明：

$$n = m + a_m k = m + (4m-3)k = m + 4mk - 3k$$

$$a_n = 4(m + 4mk - 3k) - 3 = 4m + 16mk - 12k - 3 = (4m-3) + 4k(4m-3)$$

$$= (4m-3)(4k+1) = a_m a_{k+1}$$ 。

$n = m + a_m k$，$a_n = a_m a_{k+1}$，故當 $n = m + a_m k$ 時，a_n為合項。 ■

4. 故我們推測當$n = m + a_m k (m \geq 2)$ 且 $m \geq 2$，k為正整數 時， a_n為合項。適用在所有首項為 1 的等差數列。

定理 1：首項為 1 的等差數列，當 $n = m + a_m k$ 且$m \geq 2$，k為正整數時，a_n為合項，

$a_n = a_m a_{k+1}$。

證明：

設首項為 1，公差為d，等差數列 $\langle a_n \rangle_{n\geq1} = 1,1+d, 1+2d, ..., 1+(n\text{-}1)d,...$，

$$n = m + a_m k = m + (1 + md - d)k = m + k + mdk - dk$$

$$\begin{aligned} a_n &= 1 + [(m + k + mdk - dk) - 1]d \\ &= 1 + dm + dk + \mathrm{d}^2 mk - d^2 k - d \\ &= (dm - d + 1) + dk(dm - d + 1) \\ &= (dm - d + 1)(dk + 1) = a_m a_{k+1} \end{aligned}$$ ■

二、首項大於 1 且 $d > a_1$ 的等差數列

(一)$a_1 = 2$，公差$d = 3$的等差數列：$\langle a_n \rangle_{n\geq1} = 2, 5, 8, 11, 14, \ldots, 3n - 1 \ldots$

1. 是否可沿用首項 1等差數列的合項篩檢模式($n = m + a_m k$時，a_n為合項)檢核合項？

表 1-4：首項 2，公差 3 的等差數列$m + a_m$的值與合項的關係

n	3	7	11	15	17	19	23	27	31	35	37	39	42	43	47
a_n	8	20	32	44	50	56	68	80	92	104	110	116	125	128	140
因數分解	2^3	$2^2 \cdot 5$	2^5	$2^2 \cdot 8$	$2 \cdot 5^2$	$2^2 \cdot 14$	$2^2 \cdot 17$	$2^4 \cdot 7$	$2^2 \cdot 23$	$2^2 \cdot 26$	$2 \cdot 5 \cdot 11$	$2^2 \cdot 29$	5^3	2^7	$2 \cdot 5 \cdot 14$
質因項分解	${a_1}^3$	${a_1}^2 a_2$	${a_1}^5$	${a_1}^2 a_3$	$a_1 {a_2}^2$	${a_1}^2 a_5$	${a_1}^2 a_6$	${a_1}^4 a_2$	${a_1}^2 a_8$	${a_1}^2 a_9$	$a_1 a_2 a_4$	${a_1}^2 a_{10}$	${a_2}^3$	${a_1}^7$	$a_1 a_2 a_5$

2. 當首項a_1=2 時，包含質因項a_1 =2 的合項，能否適用$n = 1 + 2k$檢核合項？

(2.1) 包含質因項a_1 =2 的合項有a_3、a_7、a_{11}、a_{15}、a_{17}、a_{19}、a_{23}、a_{27}、a_{31}、...

3=1+2×1，7=1+2×3，11=1+2×5，15=1+2×7，17=1+2×8，

19=1+2×9，23=1+2×11，27=1+2×13，31=1+2×15，35=1+2×17，

37=1+2×18，39=1+2×19，43=1+2×21，47=1+2×23，...

(2.2) $\boxed{1,3,5,7,... ⇨ 2k - 1；3,8, 13,18, 23,28,... ⇨ 5k - 2}$

(2.3) 由以上紀錄可看出含質因項a_1 =2 的合項項次的篩檢需修正為

① n=1+a_1($2k - 1$) ② n=1+a_1($5k - 2$)

3. 當第二項a_2=5 時，包含質因項 5 的合項，能否適用$n = 2 + a_2 \times k$ 篩檢？

(1) 包含質因項 5 的合項有a_7、a_{17}、a_{27}、a_{37}、a_{42}、a_{47}、a_{57}、a_{67}、a_{77}、a_{87}、a_{92}、...

7=2+5×1，17=2+5×3，27=2+5×5，37=2+5×7，42=2+5×8，47=2+5×9，

57=2+5×11，67=2+5×13，77=2+5×15，87=2+5×17，92=2+5×18，...

(2) 由以上紀錄可看出含質因項a_2=5 的合項項次的篩檢需修正為

① n=2+a_2($2k - 1$) ② n=2+a_2($5k - 2$)。

4. 當首項a_4=11 時，包含質因項 11 的合項，我們也發現合項項次的篩檢需修正為

① n=4+$a_4(2k-1)$ ② n=4+$a_4(5k-2)$

例：a_{15}→15=4+11×1，a_{59}→59=4+11×5，a_{81}→81=4+11×7，...

a_{37}→37=4+11×3，a_{92}→92=4+11×8，a_{202}→202=4+11×18，...

5. 由含質因項 2、5、11 的合項我們推測 $a_1=2$，$d=3$的等差數列合項應該包括兩種模式：① $n=m+a_m(2k-1)$ ② $n=m+a_m(5k-2)$

證明：

① 若 $n=m+a_m(2k-1)$，則a_n為合項。

$n=m+a_m\times(2k-1)=m+(3m-1)(2k-1)=6km-2k-2m+1$

$a_n=3(6km-2k-2m+1)-1=18km-6k-6m+2=(6m-2)(3k-1)$

$=2(3m-1)(3k-1)=2\cdot a_m\cdot a_k=a_1a_ma_k$ ■

② 若 $n=m+a_m(5k-2)$，則a_n為合項。

$n=m+a_m(5k-2)=m+(3m-1)(5k-2)$

$=m+15km-5k-6m+2=15km-5k-5m+2$

$a_n=3n-1=3(15km-5k-5m+2)-1=45km-15k-15m+5$

$=15k(3m-1)-5(3m-1)=5(3k-1)(3m-1)=a_2a_ka_m$ ■

6. 首項為 2，公差為 3 的等差數列，以 $n=m+a_m(2k-1)$或 $n=m+a_m(5k-2)$，兩種合項檢核模式都只能篩選出含有a_1與a_2，那針對未含有a_1或a_2的合項的篩檢模式應如何修正？

(1) $n=m+a_m(2k-1)\Rightarrow a_n=a_1a_ma_k$；$a_1=2$，$n=1$。

$n=m+a_m(5k-2)\Rightarrow a_n=a_2a_ka_m$；$a_2=5$，$n=2$。

是否存在$n=m+a_m(a_sk-s)\Rightarrow a_n=a_sa_ma_k$；$a_s$，$n=s$。

(2) 將$a_4=11$，$n=m+a_m(a_sk-s)$的算式中

m=1，k=2，則$n=m+a_m(a_sk-s)=1+2(11\cdot 2-4)=37$

$a_{37}=2+3(37-1)=110=2\cdot 5\cdot 11=a_1a_2a_4$

(3) 將$a_5=14$，$n=m+a_m(a_sk-s)$的算式中

m=1，k=2，則$n=m+a_m(a_sk-s)=1+2(14\cdot 2-5)=47$

$a_{47}=2+3(47-1)=140=2\cdot 5\cdot 14=a_1a_2a_5$

7、因此我們猜測：

$a_1=2$，公差d=3 的等差數列，若$n=m+a_m\times(a_sk-s)$，則a_n為合項。

證明：

設首項為 2，公差為 3，等差數列 $\langle a_n\rangle_{n\geq1}=2,5,8,11,\ldots$；$a_n=2+3(n-1)$

$$n=m+a_m(a_sk-s)=m+(3m-1)(3sk-k-s)$$
$$=m+9msk-3mk-3ms-3sk+k+s$$
$$a_n=2+3(m+9msk-3mk-3ms-3sk+k+s-1)$$
$$=27msk-9ms-9mk+3m-9sk+3s+3k-1$$
$$=9ms(3k-1)-3m(3k-1)-3s(3k-1)+(3k-1)$$
$$=[3m(3s-1)-(3s-1)](3k-1)$$
$$=(3m-1)(3s-1)(3k-1)=a_m\cdot a_s\cdot a_k$$

當 $n=m+a_m\times(a_sk-s)$時，$a_n=a_ma_sa_k$，為合項 ■

(二) $n=m+a_m\times(a_sk-s)$，則a_n為合項，是否適用所有首項不為 1 的等差數列？

(1) 以公差$=4$，首項$=2$，$\langle a_n\rangle_{n\geq1}=2,6,10,14,18,22,\ldots$的條件檢核

發現公差$=4$，首項$=2$的等差數列是質項等差數列無法適用。

(2) 以公差$=4$，首項$=3$，$\langle a_n\rangle_{n\geq1}=3,7,11,15,19,23,\ldots$的條件檢核

m=1，s=2，k=3 代入$n=m+a_m\times(a_sk-s)=1+3(7\cdot3-2)=58$

$a_{58}=3+4(58-1)=231=3\cdot7\cdot11=a_1a_2a_3$(適用)

(3) 以公差$=5$，首項$=2$，$\langle a_n\rangle_{n\geq1}=2,7,12,17,22,27,\ldots$的條件檢核

m=1，s=2，k=3 代入$n=m+a_m\times(a_sk-s)=1+2(7\cdot3-2)=39$

$a_{39}=2+5(39-1)=192=2^4\cdot12\neq a_1a_2a_3$(不適用)

(4) 以公差$=5$，首項$=3$，$\langle a_n\rangle_{n\geq1}=3,8,13,18,23,28,\ldots$的條件檢核

m=1，s=2，k=3 代入$n=m+a_m\times(a_sk-s)=1+3(8\cdot3-2)=67$

$a_{67}=3+5(67-1)=333\neq a_1a_2a_3$(不適用)

(5) 以公差$=5$，首項$=4$，$\langle a_n\rangle_{n\geq1}=4,9,14,19,24,29,\ldots$的條件檢核

m=1，s=2，k=3 代入$n=m+a_m\times(a_sk-s)=1+4(9\cdot3-2)=101$

$a_{101}=4+5(101-1)=504=4\cdot9\cdot14=a_1a_2a_3$(適用)

9、綜合以上推論，$n=m+a_m\times(a_sk-s)$，則a_n為合項的推論可能只適用在公差=首項+1 的特例，因此我們有了定理 2 的推論。

定理 2： $d = a_1 + 1$的等差數列，當$n = m + a_m(a_s k - s)$時，$a_n = a_m a_s a_k$，a_n為合項。

證明：

$$d = a_1 + 1 \Rightarrow a_1 = d - 1$$

$$a_n = a_1 + (n-1)d = d - 1 + nd - d = nd - 1$$

$$n = m + a_m \times (a_s k - s) = m + (dm-1)(dsk - k - s)$$

$$= m + d^2msk - dmk - dms - dsk + k + s$$

$$a_n = d(m + d^2msk - dmk - dms - dsk + k + s) - 1$$

$$= dm + d^3msk - \mathrm{d}^2mk - d^2ms - d^2sk + dk + ds - 1$$

$$= d^2sk(dm-1) - dk(dm-1) - ds(dm-1) + (dm-1)$$

$$= (dm-1)[dk(ds-1) - (ds-1)]$$

$$= (dm-1)(ds-1)(dk-1) = a_m a_s a_k$$

當$n = m + a_m(a_s k - s)$時，$a_n = a_m a_s a_k$，a_n為合項。■

三、從首項與公差的質因數集合探討首項大於 1 的等差數列

(一) 等差數列的合項條件

引理 1：a_n為首項大於 1 的等差數列中元素，若存在$k \geq 2$，

滿足$a_n = {a_1}^k \equiv a_1 \pmod d$，則$a_n$為合項。

證明：

依合項定義，a_n若為合項，則a_n可以寫成數列中其他項的乘積(1 除外)，即

若$a_n = {a_1}^k$為合項，依合項定義需符合兩個條件：

(1) ${a_1}^k$為等差數列中的元素

(2) ${a_1}^k$可以寫成數列中其他項的乘積

(1) ${a_1}^k$為等差數列中的元素

設等差數列首項 $a_1 > 1$，公差為d，則

$\langle a_n \rangle_{n\geq 1} = a_1, a_1{+}d, a_1{+}2d, a_1{+}3d, \ldots, a_1{+}(\mathrm{n}-1)d, \ldots$

因首項不為 1，故數列中的元素 $a_1 \equiv a_2 \equiv a_3 \equiv \cdots \equiv a_n (mod d)$

由引理 1 條件：**若存在$k \geq 2$，滿足$a_n = {a_1}^k \equiv a_1 \pmod d$**

已明確定義$a_n \equiv a_1 \pmod d$ 故${a_1}^k$為數列元素。

(2) $a_n = {a_1}^k$顯然a_n可以寫成k個a_1的乘積■

引理 2：若$a_1{}^k$為合項，則在數列中任取k個元素(可重複)的乘積皆為合項。

證明：

令$x = a_{s_1} \cdot a_{s_2} \cdot \ldots \cdot a_{s_k}$

則因$a_{s_1} \equiv a_{s_2} \equiv \cdots \equiv a_{s_k} \equiv a_1 \ (mod\ d)$，

得$x \equiv a_1{}^k \equiv a_1 \ (mod\ d)$ 可知x為此數列中的某項，

又由定義，x為此數列數個項的乘積，故x為此數列之合項。■

1. 由引理1可知，首項大於 1 的等差數列，若我們找到$a_1{}^k \equiv a_1 \ (mod\ d)$，即找到該數列的合項。

2. 以首項2，公差3的等差數列為例說明：

   首項2，公差3的等差數列雖為首項大於1等差數列的特例，但亦符合引理1的條件，故我們以這個數列為例，說明「引理1」和「引理2」的存在與應用。

(1) 尋找$a_1{}^k \equiv a_1(modd)$的k值。

$\langle a_n \rangle_{n\geq 1} = 2,5,8,11,14, \ldots.,3n-1 \ldots$

$a_1 \equiv 2(modd)$

$2^2 = 4 \equiv 1(mod3)$，$\boxed{2^3 = 8 \equiv 2(mod\ 3)}$，即當$k$等於3時，即能滿足

$a_n = a_1{}^3 \equiv 2(modd)$，$a_n$為合項。

(2) 又 $a_1 \equiv a_2 \equiv a_3 \equiv \cdots \equiv a_n(mod3)$

且$a_1{}^3 \equiv 2 \ (mod\ 3)$，因為是同餘關係，

可知 $a_1{}^3 \equiv a_1{}^2 a_2 \equiv a_1{}^2 a_3 \equiv a_1 a_2 a_3 \equiv 2 \ldots (mod\ 3)$

(3) 以$a_1{}^3 \equiv a_1{}^2 a_2 \equiv a_1 \ldots (mod\ 3)$為例，

取$a_n = a_1{}^2 a_2 = 2^2 \cdot 5 = 20$，

20=$2 + 3(n-1)$⇒n=7，即$a_n = a_7$為合項，符合引理2。

(4) 以$a_1{}^3 \equiv a_1 a_2 a_3 \equiv a_1 \ldots (mod\ 3)$為例

$a_n = a_1 a_2 a_3 = 2 \cdot 5 \cdot 8 = 80$，

80=$2 + 3(n-1)$⇒n=27，即$a_n = a_{27}$為合項，符合引理2。

4. 故我們在尋找合項的過程，只要能找到$k \geq 2$且滿足$a_n = a_1{}^k \equiv a_1 \ (mod\ d)$，

   則a_n為合項，就能鎖定合項的範圍：只要k個數列中的元素乘積，皆為此數列的合項。

(二) 首項與公差的質因數關係

1. 給定等差數列$\langle a_n\rangle_{n\geq 1}$，設公差為$d$，$P_{a_1}$表$a_1$質因數的集合，$P_d$表$d$質因數的集合

2. 依據公差與首項的質因數關係，我們將首項大於1的等差數列，分以下幾種狀況討論：

   (1)$P_{a_1}\cap P_d=\emptyset$ (2)$P_{a_1}=P_d$ (3) $P_{a_1}\supsetneq P_d$ (4)$P_{a_1}\subsetneq P_d$

   (5) $P_{a_1}\cap P_d\neq\emptyset$且不符合上面分類

(三) 首項與公差互質的等差數列($P_{a_1}\cap P_d=\emptyset$)

1. 以首項2，公差 7，$\langle a_n\rangle_{n\geq 1}$ = 2, 9, 16, 23, … 7(n − 1)+2為例觀察。

(1)根據引理 1，尋找$k\geq 2$滿足$a_n=a_1{}^k\equiv a_1\ (mod\ d)$的$k$值，即可找到合項。

$2^2\equiv 4(mod7)$，$\boxed{2^3=8\equiv 1(mod7)}$，$\boxed{2^4=16\equiv 2(mod7)，}$

$2^5=32\equiv 4(mod7)$，$\boxed{2^6=64\equiv 1(mod7)}$，$\boxed{2^7=128\equiv 2(mod7)}$

$2^8=256\equiv 4(mod7)$，$\boxed{2^9=512\equiv 1(mod7)}$，$\boxed{2^{10}=1024\equiv 2(mod7)\cdots}$

(2) 即當k=4、7、11、…，都滿足$a_n=a_1{}^k\equiv a_1\ (mod\ d)$，$a_n$為合項。

k=4,7,11⇒3k+1，「3」為滿足$2^3\equiv 1\ (mod\ 7)$的最小整數

即首項 2，公差 7 的等差數列當$a_n=a_1{}^{3k+1}$時，a_n為合項。

(3) 故我們猜測首項與公差互質的等差數列，需先找到一個滿足$a_1{}^m\equiv 1\ (mod\ d)$的$m$值，才可找到合項，合項$a_n=a_1{}^{mk+1}$。

定理 3：首項大於1且與公差互質的等差數列，必存在 m 滿足$a_1{}^m\equiv 1\ (mod\ d)$的最小整數，則對於任意正整數$k$，$a_1{}^{mk+1}\equiv a_1\ (mod\ d)$，

當$a_n=a_1{}^{mk+1}$時，a_n為合項。

證明：

首項大於1的等差數列：$a_1\equiv a_2\equiv a_3\equiv\cdots\equiv a_n(mod d)$

$gcd(a_1,d)=1$，根據歐拉定理得$a_1{}^{\varphi(d)}\equiv 1\ (mod\ d)$

故我們定可找到$1\leq m\leq\varphi(d)$的整數m，m為滿足$a_1{}^m\equiv 1\ (mod\ d)$的最小整數。

則$a_1{}^m\equiv 1\ (mod\ d)\Rightarrow a_1{}^{mk}\equiv 1\ (mod\ d)$，

將$a_1{}^{mk}\equiv 1\ (mod\ d)$左、右兩邊各乘$a_1$，得 $a_1{}^{mk+1}\equiv a_1\ (mod\ d)$

根據引理1，$mk+1$ 滿足$a_1{}^{mk+1}\equiv a_1\ (mod\ d)$，$a_1{}^{mk+1}$為合項，

故當$a_n=a_1{}^{mk+1}$時，a_n為合項。■

(四) 首項與公差質因數相同的等差數列($\boldsymbol{P_{a_1} = P_d}$)

1. 由引理1得知：當$a_n = a_1^k \equiv a_1 \pmod{d}$時，$a_n$為合項。故可以觀察$a_1^k \pmod{d}$不同 k 值的變化，尋找合項的條件。

表2-1：不同a_1與d值滿足$P_{a_1} = P_d$的等差數列與$a_1^x \pmod{d}$的關係示例

	a_1	d	$\langle a_n\rangle_{n\ge 1}$	$a_1^x \pmod{d}$			
				a_1	a_1^2	a_1^3	a_1^3
1	$12=2^2\cdot 3$	$6=2\cdot 3$	12,18,24,30,...	0	0	0	0
2	$6=2\cdot 3$	$6=2\cdot 3$	6,12,18,24,30	0	0	0	0
3	2	$8=2^3$	2,10,18,26	2	4	0	0
4	$6=2\cdot 3$	$12=2^2\cdot 3$	6,18,30,42,...	6	0	0	0

1. 由表 2-1 我們可發現，雖然質因數相同，但$a_1^k \pmod{d}$卻分成兩種模式：

(1) $a_1 \equiv a_1^2 \equiv a_1^3 \equiv a_1^4 \equiv 0 \pmod{d}$……數列1與數列2

(2) 存在一個$a_1^k \equiv 0 \pmod{d}$，

當$x \ge k$，則$a_1^k \equiv 0$，當$x < k$，a_1^x皆不同餘……數列3與數列4

2. 針對這兩種狀況，我們做以下的分析。

性質 1：若 $\boldsymbol{gcd(a_1, d) = d}$，則 $\boldsymbol{a_1 \equiv a_1^2 \equiv a_1^3 \equiv \cdots \equiv a_1^k \equiv 0 \pmod{d}}$。

證明：

若 $gcd(a_1, d) = d$，表示$d \mid a_1$，即 $a_1 \equiv 0 \pmod{d}$

$a_1 \equiv 0 \pmod{d}$

$\Rightarrow a_1 \equiv a_1^2 \equiv a_1^3 \equiv \cdots \equiv a_1^k \equiv 0 \pmod{d}$。 ■

性質 2：若$\boldsymbol{P_d \subseteq P_{a_1}}$且 $\boldsymbol{gcd(a_1, d) \ne d \pmod{d}}$，則必存在一個 $\boldsymbol{k}$，$\boldsymbol{k \ge 2}$，使得

$\boldsymbol{a_1^k \equiv 0 \pmod{d}}$，$\boldsymbol{a_1^k \equiv a_1^{k+1} \equiv a_1^{k+2} \equiv \cdots \equiv 0 \pmod{d}}$

證明：

$P_d \subseteq P_{a_1}$，令$a_1 = mp_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$，$d = p_1^{\beta_1}p_2^{\beta_2}\dots p_s^{\beta_s}$，$(p_1, p_2, \dots, p_s$為質數$)$

$gcd(a_1, d) \ne d$，代表$d \nmid a_1$，$a_1 \not\equiv 0 \pmod{d}$

依阿基米德公理必可找到最小的$l_1, l_2, \dots, l_s$

使得 $\alpha_1 l_1 \ge \beta_1$，$\alpha_2 l_2 \ge \beta_2$，…，$\alpha_s l_s \ge \beta_s$，

取 $k = Max(l_1, l_2, \dots, l_s)$，保證$d \mid a_1^k$，則$a_1^k \equiv 0 \pmod{d}$

$a_1^k \equiv 0 \pmod{d} \Rightarrow a_1^k \equiv a_1^{k+1} \equiv a_1^{k+2} \equiv \cdots \equiv 0 \pmod{d}$ ■

性質 3：若 k為使$a_1^{k} \equiv 0 \ (mod\ d)$的最小整數，則

不存在 $1 \le i < j \le k$，使得$a_1^{j} \equiv a_1^{i} \ (modd)$

證明：

假設存在$1 \le i < j \le k$，使得 $a_1^{i} \equiv a_1^{j} \quad (modd)$，兩邊同乘以 a_1^{k-j}，

則$a_1^{i+(k-j)} \equiv a_1^{j+(k-j)} \ (mod\ d) \Rightarrow a_1^{k+i-j} \equiv a_1^{k} \equiv 0 \ (mod\ d)$

$i < j$，故$(k+i-j) < k$，即存在一個比k小的數使$a_1^{k+i-j} \equiv 0\ (mod\ d)$

與k為使$a_1^{k} \equiv 0 \ (mod\ d)$的最小整數相互矛盾。

故$a_1^{j} \equiv a_1^{i} \quad (mod\ d)$的假設不成立。 ■

3. 根據以上性質，我們整理成定理 4.1

定理 4.1：首項質因數集合與公差質因數集合相同的等差數列，若

$gcd(a_1, d) = d$，則最小合項$a_n = a_1^{2}$；

$gcd(a_1, d) \neq d$，則該數列為質項等差數列。

證明：

(1) $P_{a_1} = P_d$，若$v_p(a_1) \ge v_p(d)$

即a_1中所有質因數的指數皆大於在d中所有質因數，則$d \mid a_1 \Rightarrow gcd(a_1, d) = d$。

根據性質1：若$gcd(a_1, d) = d$，則 $a_1 \equiv a_1^{2} \equiv a_1^{3} \equiv \cdots \equiv a_1^{k} \equiv 0 \ (mod\ d)$。

a_1為最小質項，故$gcd(a_1, d) = d$，最小合項為a_1^{2}。 ■

(2) 若$v_p(a_1) \le v_p(d)$，則$gcd(a_1, d) \neq d$，即 $d \nmid a_1 \Rightarrow a_1 \not\equiv 0\ (mod\ d)$

根據性質2： $P_d \subseteq P_{a_1}$且 $d \nmid a_1$必存在一個k，使得$a_1^{k} \equiv a_1^{k+1} \equiv \cdots \equiv 0\ (mod\ d)$

根據性質3：若k為使$a_1^{k} \equiv 0 \ (mod\ d)$的最小整數，則不存在 $1 \le i < j \le k$，使得$a_1^{j} \equiv a_1^{i} \ (modd)$，即$a_1 \not\equiv a_1^{2} \not\equiv \cdots \not\equiv a_1^{k}$

根據性質4： $gcd(a_1, d) \neq d$不存在任何k，使得$a_1^{k} \equiv a_1\ (mod\ d)$即不存在合項。

故當$P_{a_1} = P_d$且$gcd(a_1, d) \neq d$的數列，為質項等差數列。 ■

(五) 公差質因數集合包含於首項質因數集合的等差數列($P_{a_1} \supsetneq P_d$)

1. 尋找滿足$a_1^{k} \equiv a_1 \ (mod\ d)$的$k$值

表 2-2：不同a_1與d值滿足 $P_{a_1} \supsetneq P_d$ 的等差數列與${a_1}^x (mod\ d)$的關係示例

	a_1	d	$\langle a_n \rangle_{n\geq 1}$	${a_1}^x(\mathrm{mod}\ \ d)$						
				a_1	${a_1}^2$	${a_1}^3$	${a_1}^4$	${a_1}^5$	${a_1}^6$	${a_1}^7$
1	$12=2^2\cdot 3$	$4=2^2$	12,16,20,24,28,...	0	0	0	0	0	0	0
2	$24=2^3\cdot 3$	$8=2^3$	24,32,40,48,56,...	0	0	0	0	0	0	0
3	$6=2\cdot 3$	$9=3^2$	6,15,24,33,42,51,...	6	0	0	0	0	0	0
4	$6=2\cdot 3$	$16=2^4$	6,22,38,54,70,86,...	6	4	8	0	0	0	0

2. 由表 2-1 我們可發現，$P_{a_1} \supsetneq P_d$ 的等差數列，${a_1}^k \quad (mod\ \ d)$跟$P_{a_1} = P_d$的等差數列相同一樣分成兩種模式：

(1) $a_1 \equiv {a_1}^2 \equiv {a_1}^3 \equiv {a_1}^4 \equiv 0\ \ (mod\ d)$……數列1與數列2

(2) 存在一個${a_1}^k \equiv 0 \quad (mod\ \ d)$，

當$x \geq k$，則${a_1}^k \equiv 0$，當$x < k$，${a_1}^x$皆不同餘……數列3與數列4

3. 故我們可仿造定理4.1模式描述$P_{a_1} \supsetneq P_d$ 的等差數列的合項模式

定理 4.2：公差質因數集合包含於首項質因數集合的等差數列，若

$\gcd(a_1, d) = d$，則最小合項$a_n = {a_1}^2$；

$\gcd(a_1, d) \neq d$，則該數列為質項等差數列。

證明：

(1) $P_d \subset P_{a_1}$表示公差的質因數全都出現在P_{a_1}中，故當$v_p(a_1) \geq v_p(d)$，則$gcd(a_1, d) = d$成立。

根據性質 1：若$gcd(a_1, d) = d$，則$a_1 \equiv {a_1}^2 \equiv \cdots \equiv {a_1}^k \equiv 0\ (mod\ d)$

故$P_d \subset P_{a_1}$，若$gcd(a_1, d) = d$，則最小合項$a_n = {a_1}^2$。■

(2) $P_d \subset P_{a_1}$的等差數列，若$v_p(a_1) \geq v_p(d)$，則 $d \nmid a_1$，$gcd(a_1, d) \neq d$。

根據性質 2：若$P_d \subseteq P_{a_1}$且 $gcd(a_1, d) \neq d$，即 $d \nmid a_1 \Rightarrow a_1 \not\equiv 0\ (mod\ d)$，

必存在一個≥2 的k，使得${a_1}^k \equiv\ 0\ (mod\ d)$。

根據性質 3，當$a_1 \not\equiv\ 0\ (mod\ d)$且${a_1}^k \equiv\ 0\ (mod\ d)$，則

$a_1 \not\equiv {a_1}^2 \not\equiv {a_1}^3 \not\equiv \cdots \not\equiv {a_1}^k\ \ (mod\ d)$，即該數列無合項，為質項等差數列。■

(六) 首項質因數集合包含於公差質因數集合的等差數列($P_{a_1} \subsetneq P_d$)

1. 尋找滿足${a_1}^k \equiv a_1\ \ (mod\ d)$的$k$值

表 2-3：不同a_1與d值滿足 $P_{a_1} \subsetneq P_d$的等差數列與$a_1{}^x(mod\ d)$的關係示例

	a_1	d	$\langle a_n \rangle_{n\geq1}$	$a_1{}^x(\mathrm{mod}\ d)$						
				a_1	$a_1{}^2$	$a_1{}^3$	$a_1{}^4$	$a_1{}^5$	$a_1{}^6$	$a_1{}^7$
1	$18=2\cdot 3^2$	$30=2\cdot3\cdot5$	18,48,78,108,138,…	18	24	12	6	18	24	12
2	$18=2\cdot 3^2$	$42=2\cdot3\cdot7$	18,60,102,144,186,…	18	30	36	18	30	36	18
3	$4=2^2$	$56=2^3\cdot7$	14,70,126,182,238,…	4	16	8	32	16	8	32
4	$6=2\cdot3$	$90=2\cdot3^2\cdot5$	6,96,186,276,366,…	6	36	36	36	36	36	36

1. 觀察 $P_{a_1} \subsetneq P_d$ **的等差數列**$a_1{}^x(mod\ d)$的規律，發現也粗略分成兩種：
   (1) 從首項開始呈現有規律的循環，如數列 1、2。
   (2) 從首項之後開始呈現有規律的循環，如數列 3、4。

2. 首先我們來研究 $P_{a_1} \subsetneq P_d$等差數列第一種性質

性質 4：若 $P_{a_1} \subsetneq P_d$且若對於所有同時是a_1和d的質因數 p，都有$v_p(a_1) \geq v_p(d)$，則存在一個最小的整數k，滿足 1≤ $k-1 \leq \varphi\left(\frac{d}{\gcd(a_1,d)}\right)$使得 $a_1{}^k \equiv a_1\ (mod\ d)$。

證明：

$P_{a_1} \subsetneq P_d$ ，表示首項a_1的質因數全都出現在公差d中。

設$a_1 = p_1{}^{\alpha_1}p_2{}^{\alpha_2} \dots p_s{}^{\alpha_s}$，$d = p_1{}^{\beta_1}p_2{}^{\beta_2} \dots p_s{}^{\gamma_s}q_1{}^{\gamma_1}q_2{}^{\gamma_2} \dots q_t{}^{\gamma_t}$；

($p_1, p_2, \dots, p_s$，$q_1, q_2, \dots, q_t$為質數)

將d的分解式中$p_1{}^{\alpha_1}p_2{}^{\alpha_2} \dots p_s{}^{\alpha_s}$以$d_p$表示 ，$q_1{}^{\gamma_1}q_2{}^{\gamma_2} \dots q_t{}^{\gamma_t}$ 以d_q表示，即$d = d_p d_q$

若所有$1 \leq i \leq s$，$\alpha_i \geq \beta_i$ 則$gcd(a_1, d) = p_1{}^{\beta_1}p_2{}^{\beta_2} \dots p_s{}^{\beta_s} = d_p$

利用中國剩餘定理將模d分解成模d_p與模d_q，找出同時滿足兩條件的k值。

$$\begin{cases} \text{模}d_p：gcd(a_1, d_p) = d_p\text{，即}d_p \mid a_1\text{，故}a_1 \equiv a_1{}^k \equiv a_1{}^{\varphi(d_q)} \equiv 0\ (mod\ d_p) \\ \text{模}d_q：gcd(a_1, d_q) = 1\text{，利用歐拉定理得}a_1{}^{\varphi(d_q)} \equiv 1\ (mod\ d_q)\text{ 可知} \end{cases}$$

存在一個最小的整數k，滿足$2 \leq k \leq \varphi\left(\frac{d}{\gcd(a_1,d)}\right) + 1$，使得 $a_1{}^k \equiv a_1\ (mod\ d)$

依據中國剩餘定理整合兩者關係求模數 d 時，因為模d_p：$a_1 \equiv a_1{}^k \equiv 0\ (mod\ d_p)$

固定為0，此可知其一般式必可寫成$0\cdot d_p{}^{-1} + r \cdot a_1{}^{k-1} = r \cdot a_1{}^{k-1}$ (mod d)

其中$\begin{cases} d_p{}^{-1} \equiv 1(mod\ d_p) \\ d_p{}^{-1} \equiv 0(mod\ d_q) \end{cases}$， r為模d_q之餘數。得$a_1{}^k = a_1 a_1{}^{k-1} \equiv a_1\ (mod\ d)$

$$gcd(a_1, d) = d_p\text{，}d = d_p d_q\text{，}$$

$d_q = \frac{d}{gcd(a_1,d)}$，$\varphi(d_q) = \varphi\left(\frac{d}{gcd(a_1,d)}\right)$，

所以可找到 k 滿足$1 \leq k-1 \leq \varphi(d_q)$ ⇒滿足$1\leq k-1 \leq \varphi\left(\frac{d}{\gcd(a_1,d)}\right)$■

3. 以實際的例子，第一個數列$a_1=18$，$d=30$驗證性質4的推論：

$a_1=18=2\cdot 3^2$，$d=30=2\cdot 3\cdot 5$，共同質因數 2,3 皆$v_p(a_1)\geq v_p(d)$

存在一個最小的整數 k，滿足$1\leq \mathrm{k}-1\leq \varphi\left(\frac{d}{\gcd(a_1,d)}\right)\Rightarrow 1\leq \mathrm{k}-1\leq \varphi\left(\frac{30}{\gcd(18,30)}\right)$

$\Rightarrow 1\leq \mathrm{k}-1\leq 5\Rightarrow 2\leq \mathrm{k}\leq 6$

實際尋找滿足${a_1}^k\equiv a_1(mod\ d)$的最小值。

$18^2=324\equiv 24\ (mod\ 30)$　　$18^3=5832\equiv 12\ (mod\ 30)$

$18^4=104976\equiv 6\ (mod\ 30)$　　$18^5=1889568\equiv 18\ (mod\ 30)$

我們找到 $k=5$，滿足$18^5\equiv 18\ (mod\ 30)$，合乎$2\leq \mathrm{k}\leq 6$的範圍。

4. $P_{a_1}\subsetneq P_d$等差數列第二種性質

性質 5：若$P_{a_1}\subsetneq P_d$且若對於所有同時是a_1和d的質因數p，都有$v_p(a_1)\leq v_p(d)$，則不存在$k\geq 2$使得 ${a_1}^k\equiv a_1\ (mod\ d)$。

證明：

$P_{a_1}\subsetneq P_d$，表示首項a_1的質因數全都出現在公差d中。

設$a_1={p_1}^{\alpha_1}{p_2}^{\alpha_2}\ldots{p_s}^{\alpha_s}$，$d={p_1}^{\beta_1}{p_2}^{\beta_2}\ldots{p_s}^{\gamma_s}{q_1}^{\gamma_1}{q_2}^{\gamma_2}\ldots{q_t}^{\gamma_t}$；

($p_1,p_2,\ldots,p_s$，$q_1,q_2,\ldots,q_t$為質數)

將d的分解式中${p_1}^{\alpha_1}{p_2}^{\alpha_2}\ldots{p_s}^{\alpha_s}$以$d_p$表示，${q_1}^{\gamma_1}{q_2}^{\gamma_2}\ldots{q_t}^{\gamma_t}$ 以d_q表示，即$d=d_pd_q$

若所有$1\leq i\leq \mathrm{s}$，$\alpha_i\leq\beta_i$則$gcd(a_1,d)\neq d_p\Rightarrow gcd(a_1,d_p)\neq d_p$

利用中國剩餘定理將模d分解成模d_p與模d_q，找出同時滿足兩條件的k值。

模d_q：$gcd(a_1,d_q)=1$，利用歐拉定理得${a_1}^{\varphi(d_q)}\equiv 1\ (mod\ d_q)$

我們可找到一個比${a_1}^{\varphi(d_q)}$小的 $k-1$ 值滿足${a_1}^k\equiv a_1(mod\ d)$

模d_p：因 $gcd(a_1,d_p)\neq d_p$，$d_p\nmid a_1$，但 $P_{a_1}=P_d$，

依據性質3會出現${a_1}^k\equiv 0(mod\ d_p)$；性質4會出現$a_1\not\equiv {a_1}^2\not\equiv\cdots\not\equiv {a_1}^{k-1}$

因此找不到任何 k 值可以滿足${a_1}^k\equiv a_1(mod\ d_p)$

依據中國剩餘定理整合兩者關係時，${a_1}^k\equiv a_1(mod\ d)$時，需模$d_p$與模$d_q$同時滿足，

但模d_p無法滿足，故 $k\geq 2$ 時，${a_1}^k\equiv a_1(mod\ d)$ 也不存在■

5. 以實際的例子，第一個數列 $a_1=18$，$d=30$驗證性質5的推論：

$a_1=4=2^2$，$d=56=2^3\cdot 7$，共同質因數2，$2^2<2^3$

實際尋找滿足${a_1}^k\equiv a_1(mod\ d)$的最小值。

$a_1=4\ (mod\ 4)$　　$4^2=16\equiv 16\ (mod\ 56)$　　$4^3=64\equiv 8\ (mod\ 56)$

$4^4=256\equiv 32\ (mod\ 56)$　　$4^5=1024\equiv 16\ (mod\ 56)$　　$4^6=4096\equiv 8\ (mod\ 56)$

故4^x $(mod\ 56)$的模冪序列為4,16,8,32,16,8,32,16，從 x ≥ 2 才開始出現同餘的循環，即無法找不到任何 k ≥ 2，能滿足$a_1 \equiv {a_1}^k$的 k 值。

我們找到$k = 5$，滿足$18^5 \equiv 18$ $(mod\ 30)$，合乎 2≤ k ≤ 6 的範圍。

定理 5.1：首項質因數集合包含於公差質因數集合的等差數列，

若對於所有同時是a_1和d的質因數p，都有$v_p(a_1) \geq v_p(d)$，則存在一個最小的整數k，滿足$2 \leq k \leq \varphi\left(\frac{d}{\gcd(a_1,d)}\right) + 1$，使得 ${a_1}^k \equiv a_1$ $(mod\ d)$。

若對於所有同時是a_1和d的質因數p，都有$v_p(a_1) \leq v_p(d)$，則該數列為質項等差數列。

證明：

定理5.1描述$P_{a_1} \subsetneq P_d$的等差數列會因為同時存在 a_1 和 d 的質因數 p 的指數，而出現兩種現象：

(1) 若對於所有同時是 a_1 和 d 的質因數p，都有$v_p(a_1) \geq v_p(d)$，則存在一個最小的整數k，滿足$2 \leq \mathrm{k} \leq \varphi\left(\frac{d}{\gcd(a_1,d)}\right) + 1$，使得 ${a_1}^k \equiv a_1$ $(mod\ d)$。

這點我們可從性質4得知。

(2) 若對於所有同時是a_1和d的質因數p，都有$v_p(a_1) \leq v_p(d)$，則該數列為質項等差數列。這點我們可從性質5得知。

故定理5.1成立。■

(六)首項質因數集合與公差質因數集合有相同質因數，又各有不同質因數的等差數列。

表 2-4：不同a_1與d值滿足$P_{a_1} \cap P_d \neq \emptyset$的等差數列與模冪關係示例

	a_1	d	$\langle a_n \rangle_{n\geq1}$	${a_1}^x(\mathrm{mod}\ d)$						
				a_1	${a_1}^2$	${a_1}^3$	${a_1}^4$	${a_1}^5$	${a_1}^6$	${a_1}^7$
1	$18=2\cdot 3^2$	$21=3\cdot 7$	18,39,60,81,102,...	18	9	15	18	9	15	18
2	$14=2\cdot 7$	$21=3\cdot 7$	14,35,56,77,98,119,...	14	7	14	7	14	7	14
3	$14=2\cdot 7$	$147=3\cdot 7^2$	14,161,308,455,602,...	14	49	98	49	98	49	98
4	$18=2\cdot 3^2$	$20=2^2\cdot 5$	18,38,58,78,98,118,...	18	4	12	16	8	4	12

發現 ${a_1}^x(\mathrm{mod}\ d)$ 的序列變化與 $P_{a_1} \subsetneq P_d$的等差數列相似，故我們猜測他們合項成立的條件應該相同。

定理 5.2：首項質因數集合與公差質因數集合有相同質因數

，又各有不同質因數的等差數列若對於所有同時是a_1和d的質因數p，都有$v_p(a_1) \geq v_p(d)$，則存在一個最小的整數k，滿足$2 \leq k \leq \varphi\left(\frac{d}{\gcd(a_1,d)}\right)+1$，使得 $a_1{}^k \equiv a_1 \pmod d$。

若對於所有同時是a_1和d的質因數p，都有$v_p(a_1) \leq v_p(d)$，則該數列為質項等差數列。

證明：

定理5.1描述首項質因數集合與公差質因數集合有相同質因數，又各有不同質因數的等差數列會因為同時存在a_1和d的質因數p的指數，而出現兩種現象：

設$a_1 = p_1{}^{\alpha_1} p_2{}^{\alpha_2} \dots p_s{}^{\alpha_s} w_1{}^{\delta_1} w_2{}^{\delta_2} \dots w_v{}^{\delta_v}$，$d = p_1{}^{\beta_1} p_2{}^{\beta_2} \dots p_s{}^{\beta_s} q_1{}^{\gamma_1} q_2{}^{\gamma_2} \dots q_t{}^{\gamma_t}$

($p_1, p_2, \dots, p_s$，$w_1, w_2, \dots, w_v$，$q_1, q_2, \dots, q_t$為質數)

將d的分解式中$p_1{}^{\alpha_1} p_2{}^{\alpha_2} \dots p_s{}^{\alpha_s}$以$d_p$表示，$q_1{}^{\gamma_1} q_2{}^{\gamma_2} \dots q_t{}^{\gamma_t}$ 以d_q表示，即$d = d_p d_q$

因為a_1與d不互質，我們無法直接套用歐拉定裡去尋找合數，又因為a_1與d各有不同的質因數，所以$d \nmid a_1$，因此我們還是引用中國剩餘定理將d的分解有共同質因數的d_p和與a_1不同因數的d_q來處理$a_1 (mod\ d)$的情形。

若對於所有同時是a_1和d的質因數p，都有$v_p(a_1) \geq v_p(d)$，則存在一個最小的整數k，滿足$2 \leq k \leq \varphi\left(\frac{d}{\gcd(a_1,d)}\right)+1$，使得 $a_1{}^k \equiv a_1 \pmod d$。這點我們套用性質4證明成立。

若對於所有同時是a_1和d的質因數p，都有$v_p(a_1) \leq v_p(d)$，則該數列為質項等差數列。這點我們可套用性質5證明該種狀況成立。

故定理5.2成立。■

1. 以$a_1 = 14$，$d = 21$，為例說明

$a_1 = 14 = 2 \cdot 7$，$d = 21 = 3 \cdot 7$，共同質因數7，指數相等。屬於第種狀況1

$$\varphi\left(\frac{d}{\gcd(a_1,d)}\right)+1 = \varphi\left(\frac{21}{\gcd(14,21)}\right)+1 = \varphi\left(\frac{21}{7}\right)+1 = \varphi(3)+1 = 3$$

a_1的k次方列舉如下

$14 \equiv 14 \pmod{21}$

$14^2 \equiv 196 \equiv 7 \pmod{21}$

$\boxed{14^3 \equiv 2744 \equiv 14 \pmod{21}}$

$a_1=14$，$d=21$，最小合項 $a^k=14^3=2744\equiv 14\ (mod\ 21)$， $2\le k\le 3$ 。

2. 以 $a_1=14$，$d=147$，為例說明

$a_1=14=2\cdot 7$，$d=147=3\cdot 7^2$，…相同質因數7，$7\le 7^2$，屬於第2種狀況，無法依此找到合項。

實際尋找k值

$14\equiv 14\quad(mod\ 147)$

$14^2\ \equiv 196\equiv 49\ (mod\ 147)$ $\qquad 14^3\ \equiv 2744\equiv 98(mod\ 147)$

$14^4\ \equiv 38416\equiv 49\ (mod\ 147)$ $\qquad 14^5\ \equiv 537824\equiv 98(mod\ 147)$

$a_1=14$，$d=21$數列中的元素中在模 147 的情況都需同餘 14，而$14^k\ (mod\ 147)$，模冪的序列為 14,49,98,49,98,...，會出現循環，不過出現循環的數都與$a_1=14$，$d=21$數列中的元素不同餘，皆不屬於$a_1=14$，$d=21$數列中的元素。

(七) 相似定理合併

1. 定理4.1與定理4.2，即$P_{a_1}=P_d$與$P_d\subsetneq P_{a_1}$的等差數列，對合項的篩選模式相同，故我們將兩個定理合併為定理4，即將$P_{a_1}=P_d$與$P_d\subsetneq P_{a_1}$合併為$P_d\subseteq P_{a_1}$的等差數列。

定理 4：公差質因數集合包含等於首項質因數集合的等差數列，若

$\gcd(a_1,d)=d$，則最小合項$a_n=a_1{}^2$；

$\gcd(a_1,d)\ne d$，則該數列為質項等差數列。

2. 定理5.1與定理5.2，即$P_{a_1}\subset P_d$與$P_{a_1}\cap P_d\ne\emptyset$又各有不同質因數的等差數列，對合項的篩選模式相同，可整合為範圍較寬的$P_{a_1}\cap P_d\ne\emptyset$的等差數列。

定理 5：首項質因數集合與公差質因數集合有相同質因數的等差數列 ($P_{a_1}\cap P_d\ne\emptyset$)

若對於所有同時是a_1和d的質因數p，都有$v_p(a_1)\ge v_p(d)$，則存在一個最小的整數k，滿足$2\le k\le\varphi\left(\frac{d}{\gcd(a_1,d)}\right)+1$，使得$a_1{}^k\equiv a_1\ \ (mod\ d)$。

若對於所有同時是a_1和d的質因數p，都有$v_p(a_1)\le v_p(d)$，則該數列為質項等差數列。

伍、討論

一、仿照「埃氏篩法」找出等差數列的質項與合項。

(一)仿照埃氏篩法找出首項為 1，公差 3 的等差數列 100 項內的合項和質項。

1、埃氏篩法提到尋找n以內的質數時，若找到了一個大於$\sqrt{n}$的質數，則剩餘的所有尚未標記的數也都是質數。

2、首項為 1，公差 3 的等差數列$(a_n)_{n\geq1} = 1,4,7,10,13,\ldots,a_{100}$，我們要找出$a_{100}$以內的所有質項與合項；$a_{100} = 1+3(100-1) = 298$。$17^2 < 298 < 18^2$，故我們只要找到$a_n$最接近 17的極大值質項即可。

3、公差為 3 的等差數列 $a_2 = 4$、$a_3 = 7$、$a_4 = 10$、$a_5 = 13$、$a_6 = 16$、$a_7 = 19$、其中a_7>17(超過，不合)，$a_6 = 16 = 4^2$(為合項，不合)，故最接近 17的極大值質項為a_5。

(二) 等差數列合項檢核公式 $n = m + a_m k$ $(x \geq 2$，k為整數$)$，化為同餘模式。

1、$n = m + a_m k$，即 $n_1 = m + a_m \times 1$，$n_2 = m + a_m \times 2$，$n_3 = m + a_m \times 3$，....，

2、即符合$n = m + a_m k$ 條件的n_k都是a_m的倍數加 m，所以我們可以將篩揀的對象由等差數列的元素a_n，簡化為數值較小的項次n；即若 $n \equiv m(mod\ a_m)$，則a_n為合項。

(**仿照「埃氏篩法」是個找出 a_1=1，d=3 等差數列，n=100 以內所有質項。**(如圖 5-1)

1. 以$n \equiv 2(mod 4)$篩出含有質項a_2因數的合項項次，並標記底色。
2. 以$n \equiv 3(mod 4)$篩出含有質項a_3因數的合項項次，並標記底色。
3. 以$n \equiv 4\ (mod\ 10)$找出含有$a_4 = 10$因數的合項項次，並標記底色
4. 以$n \equiv 5\ (mod\ 13)$找出含有$a_5 = 13$因數的合項項次，並標記底色

等差數列質項、合項項次(a_1=1，d=3)									
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

圖 5-1：埃氏篩法示例

5. 圖 5-1，塗色的項次如 6、10、14、17、...，代表等差數列中該項次的元素$a_6 = 16$、a_{10}=28、$a_{14} = 40$、$a_{17} = 49$、...，為合項。
6. 圖 5-1，未塗色的項次如2、3、4、5、 .... 、97、99、100，代表等差數列中該項次的元素a_2、a_3、a_4、a_5、...、a_{97}、a_{99}、a_{100}，為質項。

二、梅森質數與等差數列的質項

(一)關於梅森質數

1. 梅森數是形如2^n-1的數(n是正整數)，記為M_n；如果梅森數是質數就稱梅森質數，
   目前已發現的最大梅森質數是$2^{136279841}-1$。
2. 當n是合數時，梅森數一定是合數，但當n是質數時，梅森數不一定是質數；
   除了 2 以外，所有的質數階為奇數，故我們可說梅森質數中2 的指數一定是奇數，即梅森質數應該是$2^{2k+1}-1$。

(二) 梅森質數與公差為2^k的等差數列關係

1. 梅森質數模$(d=2^k)$的餘數

$$2^k \mid 2^{2K+1} \Rightarrow 2^{2k+1} \equiv 0\ (mod\ 2^k)$$

$$2^{2k+1} \equiv 0\ (mod\ 2^k) \Rightarrow 2^{2k+1}-1 \equiv -1\ (mod\ 2^k)$$

$$2^{2k+1}-1 \equiv -1\ (mod\ 2^k) \Rightarrow 2^{2k+1}-1 \equiv 2^k-1\ (mod\ 2^k)$$

由以上推論我們發現梅森質數模$(d=2^k)$的餘數為2^k-1，因此我們只要找出數列元素模$(d=2^k)$都同餘2^k-1，即代表梅森質數為該數列元素。

2. 公差是2^k，首項是多少才會與梅森數模$(d=2^k)$同餘

(1) 設等差數列首項 $a_1>1$，公差為d，則

$\langle a_n\rangle_{n\geq1}=a_1, a_1+d, a_1+2d, a_1+3d, \ldots, a_1+(\mathrm{n}-1)d, \ldots$

故首項不為 1 的數列的元素 $a_1 \equiv a_2 \equiv a_3 \equiv \cdots \equiv a_n\ \ (mod\ d)$

(2) 當d=2^k時，數列元素要同餘2^k-1，代表首項$a_1=2^k-1$。

(3) 首項為2^k-1，公差為2^k，數列元素皆與梅森質數同餘2^k-1，即梅森質數也是該數列的元素。

3. 以首項$2^k-1=15$，公差為2^k=16 為例驗證我們的推論

(1) $\langle a_n\rangle_{n\geq1}=15,31,47,63,79,95,111,\ldots$；

$15\equiv31\equiv47\equiv63\equiv\cdots\equiv15\ \ (mod\ 16)$

即a_1 =15= 2^4-1，$d=16=2^4$；$a_n=15+16(n-1)$

(2) 檢驗 2024 年 10 月已知最大的梅森質數$2^{136279841}-1$是否為其數列元素，

$$2^4 \mid 2^{136279841} \Rightarrow 2^{34069960\times4+1} \equiv 0\ \ (mod\ 16)$$

$$2^{136279841}-1 \equiv -1 \quad \equiv 15\ \ (\mathrm{mod}\ 16)$$

故梅森質數$2^{136279841}-1$是$a_1=15$，d=16 數列中的元素。

$2^{136279841}-1$ 是首項 15，公差 16 等差數列中已知的最大質項。

(三) 梅森質數與公差為$3 \cdot 2^k$的等差數列關係

1. 由上一節我們已知：只要找出數列元素模(d)都與梅森質數同餘，即代表梅森質數為該數列元素。

2. 我們將所有梅森質數$(2^{2k+1}-1)$都設定為數列元素，將這些數列元素模d(公差)若出現同餘，代表這些梅森質數都是數列元素。

3. 觀察梅森質數$(2^{2k+1}-1)$模$(d=3\cdot 2^m)$的餘數(r)

表 5-1：$2^{2k+1}-1$ 模$(d=3\cdot 2^m)$的餘數

$2^{2k+1}-1$ / r / $d=3\cdot 2^m$	7	31	127	511	2047	8191	32767	131071
3	1	1	1	1	1	1	1	1
6	1	1	1	1	1	1	1	1
12	7	7	7	7	7	7	7	7
24	7	7	7	7	7	7	7	7
48	~~7~~	31	31	31	31	31	31	31
96	~~7~~	31	31	31	31	31	31	31
192	~~7~~	~~31~~	127	127	127	127	127	127
384	~~7~~	~~31~~	127	127	127	127	127	127

4. 由表 5-1 我們可以觀察到當$2^{2k+1}-1$的值從7開始都與$d=3$ 或 6 同餘1，

(1) 故我們可設定首項$a_1=1$，公差為 3 或 6，則梅森質數定為數列元素。

$a_1=1$，$d=3$，$\langle a_n\rangle_{n\geq 1}=1,4,7,10,13,16,19,22,\ldots$

$a_1=1$，$d=6$，$\langle a_n\rangle_{n\geq 1}=1,713,19,25,31,37,\ldots$

(2) 故我們可設定首項$a_1=7$，公差為 12 或 24，則梅森質數定為數列元素。

$a_1=7$，$d=12$，$\langle a_n\rangle_{n\geq 1}=7,19,31,43,55,67,79,\ldots$

$a_1=7$，$d=24$，$\langle a_n\rangle_{n\geq 1}=7,31,55,79,103,127,151,\ldots$

(3) 以此類推首項$a_1=31$，公差為 48 或 96，首項 $a_1=127$，公差為 192 或384…。

模數$3\cdot 2^m$，m為偶數時，首項為$2^{m+1}-1$；m為奇數時，首項為2^m-1，故我們可整理為模數為$3\cdot 2^m$時，首項為$2^{\lfloor\frac{m}{2}\rfloor\cdot 2+1}-1$即$2^{2K+1}-1\equiv 2^{\lfloor\frac{m}{2}\rfloor\cdot 2+1}-1 \pmod{3\cdot 2^m}$

(4) 依此推論$2^{2k+1}-1$存在首項為$2^{\lfloor\frac{m}{2}\rfloor\cdot 2+1}-1$，公差為$3\cdot 2^m$的數列中。

即最大梅森質數$2^{136279841}-1$ 是數列中的最大質項。

5. 以$m=4$，首項$=2^{\left\lfloor\frac{m}{2}\right\rfloor\cdot 2+1}-1\ =31$，公差$=3\cdot 2^m=48$為例：

$\langle a_n\rangle_{n\geq 1}=31,79,127,175,223\ldots$；$31\equiv 79\equiv 127\equiv 175\equiv 223\equiv 7\ (mod\ 48)$；

將公差 48，分解為$48=3\cdot 2^4$，觀察最大梅森質數$2^{136279841}-1$，模 3 和模2^4的情形。

模 2^4：已知 $2^{136279841}-1\equiv 15\ (\mathrm{mod}\ 16)$

模 3：$2^2=4\equiv 1\ (mod\ 3)\Rightarrow 2^{2k}\equiv 1\ (mod\ 3)$

$$2^{2k}\cdot 2\equiv 1\cdot 2\ (mod\ 3)\Rightarrow 2^{2k+1}\equiv 2(mod\ 3)\Rightarrow 2^{136279841}-1\equiv 1(mod\ 3)$$

依中國剩餘定理得 $\begin{cases}2^{136279841}-1\equiv 15\ \ (\mathrm{mod}\ 16)\\ 2^{136279841}-1\equiv 1\qquad (mod\ 3)\end{cases}\Rightarrow 2^{136279841}-1\equiv 31\ \ (mod\ 48)$

故梅森質數$2^{136279841}-1$存在$a_1=31$，d=48 的等差數列中。

三、等差數列的質項密度探討

一、由質數定理[8]，我們知道 $\pi(x)\approx\frac{x}{\ln(x)}$ ，其中，$\pi(x)$ 定義為不大於 x 的質數個數。而本作中的質項和質數有許多性質是很類似的，所以我們推測質項的個數應該也可以使用類似的方式進行估計。

二、為了估計質項的密度，我們需先把$\pi(x)$重新定義：

定義[質項計數函數]：$\pi(x)$為不大於x的質項個數，

若x為質項則$\pi(x)$定義等同「x是第$\pi(x)$個質項」。

例：在 $\langle a_n\rangle=\langle 3n+1\rangle$ 中，$a_{12}=37$為此數列的第10個質項，故$\pi(37)=10$。

三、回顧此近似函數的歷史，可知最早是由 $\pi(x)\approx\frac{x}{A\ln(x)+B}$ 演變而來，把此式稍作整理後可得$\frac{x}{\pi(x)}\approx A\ln(x)+B$。我們可以猜測：

等差數列中$\frac{a_n}{\pi(a_n)}$的近似函數應為$\ln(a_n)$的一次函數。而$\frac{a_n}{\pi(a_n)}$即為質項密度函數的倒數。

四、以 $\langle a_n\rangle=\langle 3n+1\rangle$ 為例，我們用程式計算前 5000 個質項後，對於每個質項a_n標示座標 $\left(\ln(a_n),\frac{a_n}{\pi(a_n)}\right)$ 繪製於座標圖後如圖 5-2：

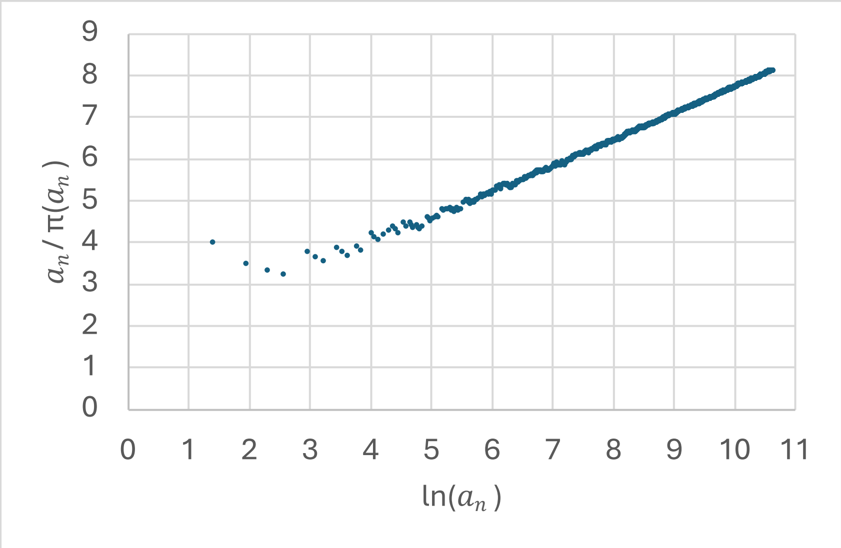


圖 5-2：當 $\langle a_n\rangle = \langle 3n+1\rangle$ 時，以 $\left(\ln(a_n), \frac{a_n}{\pi(a_n)}\right)$ 所繪製之散佈圖

五、圖 5-2 很明顯地顯示除了前面數個資料點外，近似一條斜率為正的直線。由試算表計算第50個至 5000個資料點所得到的迴歸直線方程式為 $y = 1.375 + 0.637x$ 其中橫軸為 $\ln(a_n)$ ，縱軸為 $\frac{a_n}{\pi(a_n)}$；而由相關係數 $r \approx 0.9998$ 為高度正相關。

六、表 5-2 為不同公差 d 中，$\langle a_n\rangle = \langle n\cdot d+1\rangle$ 時利用第 50 筆至 5000 筆資料點計算迴歸直線求得的近似函數 $\frac{a_n}{\pi(a_n)} \approx A\ln(a_n) + B$ 的係數與相關係數 r 的列表，圖 5-3 為公差與回歸直線斜率(A) 的折線圖。

表 5-2：不同公差下的迴歸直線係數與相關係數列表(取第 50 至 5000 筆資料)

a_n	$n+1$	$2n+1$	$3n+1$	$4n+1$	$5n+1$	$6n+1$
A	0.977077	0.969137	0.636690	0.676262	0.497814	0.693208
B	−0.841054	−0.757359	1.375457	1.891853	3.685644	3.223657
r	0.999829	0.999769	0.999793	0.999783	0.999611	0.999616
a_n	$7n+1$	$8n+1$	$9n+1$	$10n+1$	$11n+1$	$12n+1$
A	0.485039	0.563185	0.507765	0.570098	0.478229	0.573015
B	5.443822	5.737285	7.027194	7.460410	9.016607	9.211589
r	0.999486	0.999590	0.999496	0.999594	0.999232	0.999274

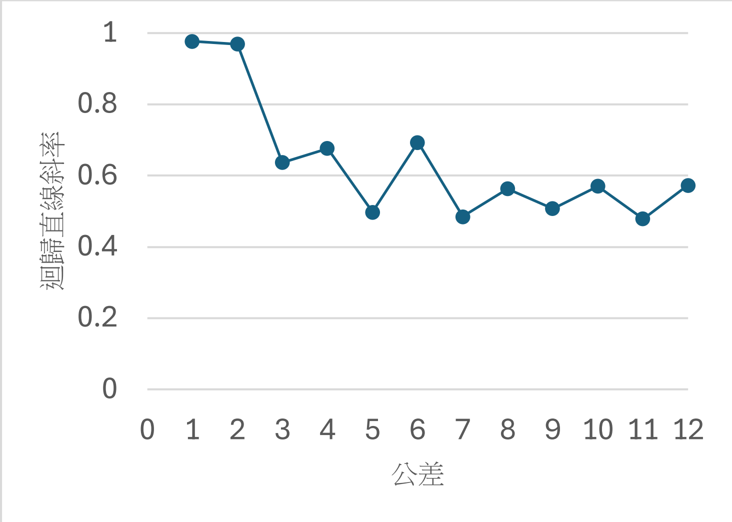


圖 5-3：公差與迴歸直線斜率之關係折線圖

七、由表 5-2 可知不同公差下，相關係數 r 皆非常接近 1，雖然 A 與 B 不同，但都可用 $ln(a_n)$ 估計 $\pi(a_n)$，進而推估出質項密度。

四、未來展望

數列 DNA—等差數列的質與合是以嶄新的角度去解析數列的結構與性質，我們僅以等差數列去做研究，就發現其中蘊藏著許多數學最基本的理論，其中a_1的冪次模d的週期性，可以幫助我們分析合項的成立條件，居然是密碼學的重要研究工具之一。

而數列元素完全是質項的質項等差數列，是我們驚喜的發現，它打破了過去數學家一直苦尋不著的全質數數列的思考，目前我們不知道它存在著什麼價值性，但它讓我們理解到一個事實，換個角度去思考迷人的「質數」，也許就開啟了一扇窗，讓我們進入一個更寬闊的領域。

數列 DNA 開啟了一個嶄新的視界，還有許多值得探討的問題：二次方程式的數列、各種不同形式的數列、質項在密碼學的應用，...，希望大家與我們繼續發掘屬於這新視界的秘密。

陸、結論

一、首項為 1，且公差大於 2 的等差數列

首項為 1 的等差數列，當 $\boldsymbol{n = m + a_m k}$ 且 $\boldsymbol{m \geq 2}$，$\boldsymbol{k}$為正整數時，$\boldsymbol{a_n = a_m a_{k+1}}$，$\boldsymbol{a_n}$ 為合項。

二、首項與公差的質因數的關係

性質 1：$\boldsymbol{k \geq 2}$，等差數列$\boldsymbol{\langle a_n \rangle_{n\geq 1}}$中元素$\boldsymbol{a_n}$，當$\boldsymbol{a_n \equiv {a_1}^k \equiv a_1 \ (mod\ d)}$時，$\boldsymbol{a_n}$為合項。

性質 2：若 $\boldsymbol{gcd(a_1, d) = d}$，則 $\boldsymbol{a_1 \equiv {a_1}^2 \equiv {a_1}^3 \equiv \cdots \equiv {a_1}^k \equiv 0\ (mod\ d)}$。

性質 3：若$\boldsymbol{P_d \subseteq P_{a_1}}$ 且 $\boldsymbol{\gcd(a_1, d) \neq d\ (mod\ d)}$，則必存在一個不小於 2 的$\boldsymbol{k}$，使得 $\boldsymbol{{a_1}^k \equiv 0\ (mod\ d)}$。

性質 4：若 $\boldsymbol{k}$為使$\boldsymbol{{a_1}^k \equiv 0\ (mod\ d)}$的最小整數，則不存在$\boldsymbol{1 \leq i < j \leq k}$，使得$\boldsymbol{{a_1}^j \equiv {a_1}^i}$ $\boldsymbol{(modd)}$

性質 5：若$\boldsymbol{P_{a_1} \subsetneq P_d}$且若對於所有同時是$\boldsymbol{a_1}$和$\boldsymbol{d}$的質因數$\boldsymbol{p}$，都有$\boldsymbol{v_p(a_1) \leq v_p(d)}$，則不存在 $\boldsymbol{{a_1}^k \equiv a_1\ (mod\ d)}$的 $\boldsymbol{k}$ 值。

三、首項大於1的等差數列

(一) $\boldsymbol{d = a_1 + 1}$的等差數列，當$\boldsymbol{n = m + a_m(a_s k - s)}$時，$\boldsymbol{a_n = a_m a_s a_k}$，$\boldsymbol{a_n}$為合項。

(二) 公差與首項互質的等差數列

$\gcd(a_1, d) = 1$，且m是滿足${a_1}^m \equiv 1(mod\ d)$的最小整數，則對於任意正整數 k，有 ${a_1}^{mk+1} \equiv a_1(mod\ d)$，即若$a_n = a^{mk+1}$，$a_n$為合項。

(三) 公差質因數集合包含等於首項質因數集合的等差數列

若 $gcd(a_1, d) = d$，則最小合項$= {a_1}^2$；若$gcd(a_1, d) \neq d$，則該數列為質項等差數列。

(四) 首項與公差有公因數的等差數列

若對於所有同時是 a_1 和 d 的質因數 p，都有 $v_p(a_1) \geq v_p(d)$，

則存在一個最小的整數k，滿足$2 \leq k \leq \varphi\left(\frac{d}{\gcd(a_1,d)}\right) + 1$，使得 ${a_1}^k \equiv a_1\ (mod\ d)$。

若對於所有同時是a_1和d的質因數p，都有$v_p(a_1) \leq v_p(d)$，則該數列為質項等差數列。

四、梅森質數與等差數列的質項關係

首項為2^k-1，公差為2^k的等差數列與首項為$2^{\left\lfloor \frac{m}{2} \right\rfloor \cdot 2+1}-1$，公差為$3 \cdot 2^m$的等差數列最大梅森質數$2^{136279841}-1$同時也是這兩類等差數列的已知最大質項。

五、等差數列的質項密度估計

等差數列質項密度倒數$\frac{a_n}{\pi(a_n)}$近似於$ln(a_n)$的一次函數。

柒、參考資料

[1] 游森棚. (2024). 質項與合項. 科學研習月期刊. *63*(4), 100.

[2] Stein, S. K. (2008). 數學是啥玩意 (葉偉文 譯.). 天下遠見出版股份有限公司.

[3] 許介彥. (2011). 數學悠哉遊. 台北市。三民書局.

[4] 許志農. (2013, October). 算術講義. 非想非非想數學網. http://pisa.math.ntnu.edu.tw/math-education/2013-10-03-02-39-03/2013-10-03-02-59-03

[5] 歐拉定理. (2024) 維基百科. https://zh.wikipedia.org/zh-tw/%E6%AC%A7%E6%8B%89%E5%AE%9A%E7%90%86_(%E6%95%B0%E8%AE%BA)

[6] 模冪. (2024). 維基百科. https://zh.wikipedia.org/zh-tw/%E6%A8%A1%E5%B9%82

[7] Weisstein, Eric W. "Mersenne Prime." From MathWorld--A Wolfram Web Resource. https://mathworld.wolfram.com/MersennePrime.html

[8] 質數定理. (2025). 維基百科.https://zh.wikipedia.org/zh-tw/%E8%B3%AA%E6%95%B8%E5%AE%9A%E7%90%86

【評語】080414

該研究取材於科學月刊數學專欄,探討特定等差數列中合項與質項的篩檢模式與其延伸的相關研究。整體而言，本研究為理解數列的結構與性質提供了一種不同的視角,唯在整體研究成果呈現上著重於理論型定理的陳述與證明過程所用定理的說明,建議強化研究問題的背景與動機,突顯該階段情境下解決問題過程的技巧，並進一步陳述理論結果的意涵。

作品海報

數列DNA

–等差數列的質與合

前　言

研究動機

2024 年 8 月份科學研習期刊「森棚教官數學題—質項與合項」[1]

給定一個正整數數列$a_1, a_2, a_3, \dots, a_n$，如果 a_n可以寫成這個數列的某些項的乘積(1 除外)，就稱為這個數列的合項，否則稱為這個數列的質項，1 不列入質項也不列入合項。

這與我們學到的質數與合數的概念，有些相關又無法完全套用，因此引起了我們深入探討的興趣。

研究目的

(一) 探討特殊等差數列的質項與合項檢核模式。

(二) 以首項與公差的質因數集合探討等差數列的質項與合項。

(三) 聯結等差數列的質項與質數研究。

名詞定義與符號說明

質項：數列中的元素，**無法**寫成這個數列中的某些項的乘積(1 除外)，我們稱該項為「質項」。
若數列某一項是質數，則該項必為質項。

$v_p(x)$：表示質因數 p 在 x 的標準分解式中的指數。

例 $a_1 = 18 = \boxed{2 \cdot 3^2}$， $d = 30 = \boxed{2 \cdot 3} \cdot 5$，若 p
表 a_1 與 d 共同質因數 2 與 3，則 $v_p(a_1) \ge v_p(d)$

數列DNA–等差數列的質與合

研究過程	討論	未來展望
■ a_1=1 ■ $a_1 > 1$ • d=a_1+1 特殊化 一般化 ● $P_{a_1} \cap P_d = \emptyset$ ● $P_{a_1} \cap P_d \neq \emptyset$ • $P_{a_1} = P_d$, • $P_d \subsetneq P_{a_1}$ } ➢ $P_d \subseteq P_{a_1}$ • $P_{a_1} \subsetneq P_d$, • 其他 } ➢ $P_d \not\subseteq P_{a_1}$	• 埃氏篩應用 • 梅森質數與等差數列數列的質項 • 質項密度探討	• 二次方程式數列 • 不同形式數列 • 密碼學應用

研究範疇：首項與公差為正整數的等差數列

研 究 過 程 與 結 果

一、首項為 1 的等差數列

表 1 ：首項 1 公差 3 的等差數列$m + a_m$的值與合項的關係

m	1	2	3	4	5	6	7	8	9	10	11	12
a_m	1	4	7	10	13	16	19	22	25	28	31	34
$m + a_m$	2	6	10	14	18	22	26	30	34	38	42	46

n	6	10	14	17	18	22	24	26	30	31	34	38	42	44
a_n	16	28	40	49	52	64	70	76	88	91	100	112	124	130
因數分解	4^2	$4 \cdot 7$	$4 \cdot 10$	7^2	$4 \cdot 13$	4^3	$7 \cdot 10$	$4 \cdot 19$	$4 \cdot 22$	$7 \cdot 13$	$4 \cdot 25$	$4^2 \cdot 7$	$4 \cdot 31$	$10 \cdot 13$
質因項分解	${a_2}^2$	$a_2 a_3$	$a_2 a_4$	${a_3}^2$	$a_2 a_5$	${a_2}^3$	$a_3 a_4$	$a_2 a_7$	$a_2 a_8$	$a_3 a_5$	$a_2 a_9$	${a_2}^2 a_3$	$a_2 a_{11}$	$a_4 a_5$

上表為 1~12 項的數列元素

下表為 44 項之前出現的合項

發現：

當 $n = m + a_m$時，a_n為合項。

這些合項都含a_2這個質因項。如：

$a_6 = {a_2}^2$， $a_{10} = a_2 a_3$， $a_{14} = a_2 a_4$

表 2 ：首項 1 公差 3 的等差數列含質因項 a_3, a_4, a_5 的合項

$n = 3 + a_3 k \Rightarrow a_n = a_3 a_{k+1}$	$n = 4 + a_4 k \Rightarrow a_n = a_4 a_{k+1}$	$n = 5 + a_5 k \Rightarrow a_n = a_5 a_{k+1}$
10=3+7 ； $a_{10} = 28 = a_2 \times a_3$	14=4+10·1 ； $a_{14} = 40 = a_2 \times a_4$	18=5+13·1 ； $a_{18} = 52 = a_2 \times a_5$
17=3+7·2 ； $a_{17} = 49 = a_3 \times a_3$	24=4+10·2 ； $a_{24} = 70 = a_3 \times a_4$	31=5+13·2 ； $a_{31} = 91 = a_3 \times a_5$

發現：

當 $n = m + a_m k$ 時

$a_n = a_m a_{k+1}$

定理 1 ：首項為 1 的等差數列，當 $n = m + a_m k$ 且 $m \ge 2$ 時，$a_n = a_m a_{k+1}$；a_n為合項。

證明：

設首項為 1，公差為d，等差數列$\langle a_n \rangle_{n \ge 1} = 1, 1+d, 1+2d, \dots, 1+(n-1)d$

$n = m + a_m k = m + (1 + md - d)k = m + k + mdk - dk$

$$a_n = 1 + [(m + k + mdk - dk) - 1]d = 1 + dm + dk + d^2mk - d^2k - d = (dm - d + 1) + dk(dm - d + 1)$$
$$= (dm - d + 1)(dk + 1) = [1 + (m-1)d][1 + (k + 1 - 1)d] = a_m a_{k+1} \quad ■$$

二、公差比首項多 1 的等差數列

表 3 ：首項 2 公差 3 的等差數列前 15 項合項($\langle a_n \rangle_{n \ge 1} = 2,5,8,11,14,17,20,\dots$)

n	3	7	11	15	17	19	23	27	31	35	37
a_n	8	20	32	44	50	56	68	80	92	104	110
因數分解	2^3	$2^2 \cdot 5$	2^5	$2^2 \cdot 11$	$2 \cdot 5^2$	$2^2 \cdot 14$	$2^2 \cdot 17$	$2^4 \cdot 5$	$2^2 \cdot 23$	$2^2 \cdot 26$	$2 \cdot 5 \cdot 11$
質因項分解	${a_1}^3$	${a_1}^2 a_2$	${a_1}^5$	${a_1}^2 a_4$	$a_1 {a_2}^2$	${a_1}^2 a_5$	${a_1}^2 a_6$	${a_1}^4 a_2$	${a_1}^2 a_8$	${a_1}^2 a_9$	$a_1 a_2 a_4$

發現：

當$n = m + a_m(a_s k - s)$ 時

$a_n = a_m a_s a_k$

表 4 ：首項 1 公差 3 的等差數列含質因項 a_1, a_2, a_4 的合項 (以 $m = 1$，$a_m = 2$ 為例)

$n = m + a_m(a_1 k - 1) \Rightarrow a_n = a_1 a_1 a_k$	$n = m + a_m(a_2 k - 2) \Rightarrow a_n = a_1 a_2 a_k$	$n = m + a_m(a_4 k - 4) \Rightarrow a_n = a_1 a_4 a_k$
15=1+2(2·4−1)；$a_{15} = 44 = a_1 a_1 a_4$	17=1+2(5·2−2)；$a_{17} = 50 = a_1 a_2 a_2$	15=1+2(11·1−4)； $a_{15} = 44 = a_1 a_4 a_1$
23=1+2(2·6−1)；$a_{23} = 68 = a_1 a_1 a_6$	27=1+2(5·3−2)；$a_{27} = 80 = a_1 a_2 a_3$	37=1+2(11·2−4)； $a_{37} = 110 = a_1 a_4 a_2$

定理 2 ：首項大於 1 且公差比首項多 1 的等差數列，當 $n = m + a_m(a_s k - s)$時，$a_n = a_m a_s a_k$，a_n 為合項。

證明：

$d = a_1 + 1 \Rightarrow a_1 = d - 1$；$a_n = a_1 + (n-1)d = dn - 1$

$n = m + a_m \times (a_s k - s) = m + (dm - 1)(dsk - k - s) = m + d^2msk - dmk - dms - dsk + k + s$

$$a_n = d(m + d^2msk - dmk - dms - dsk + k + s) - 1 = dm + d^3msk - d^2mk - d^2ms - d^2sk + dk + ds - 1$$
$$= d^2sk(dm - 1) - dk(dm - 1) - ds(dm - 1) + (dm - 1) = (dm - 1)(ds - 1)(dk - 1) = a_m a_s a_k \ ■$$

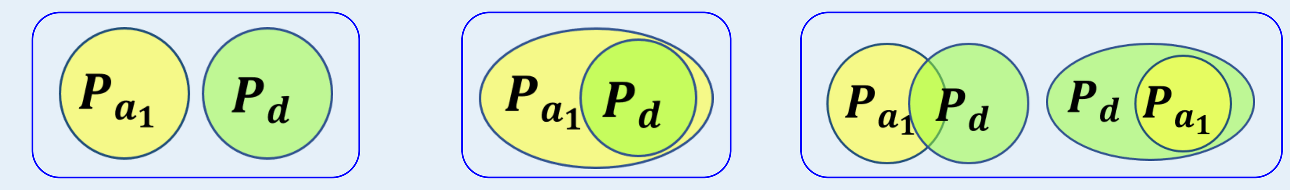
三、從首項與公差的質因數，探討首項大於 1 等差數列的質項與合項。

(一) 首項大於 1 的等差數列合項條件

引理 1 ：a_n 為首項大於 1 的等差數列中元素，若存在 $k \geq 2$，滿足 $a_n \equiv {a_1}^k \equiv a_1 \pmod{d}$，則 a_n 為合項。

引理 2 ：若 ${a_1}^k$ 為合項，則在數列中任取 k 個元素相乘(可重複)皆為合項。

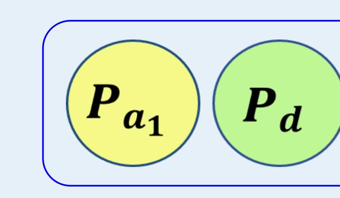
(二) 首項與公差質因數的關係



1. 給定等差數列，設 P_{a_1} 表示 a_1 質因數的集合，P_d 表示 d 質因數的集合。
2. 依首項與公差質因數關係，我們將首項大於 1 的等差數列整合成以下三種模式(1) $P_d \cap P_{a_1} = \emptyset$ (2) $P_d \subseteq P_{a_1}$ (3) $P_d \not\subseteq P_{a_1}$

(三) 首項與公差互質的等差數列 ($P_d \cap P_{a_1} = \emptyset$)

定理 3 ：首項大於 1 且與公差互質的等差數列，若存在 m，滿足 ${a_1}^m \equiv 1 \pmod{d}$ 的最小整數，則對於任意正整數 k，${a_1}^{mk+1} \equiv a_1 \pmod{d}$，當 $a_n = {a_1}^{mk+1}$ 時， a_n 為合項。



以首項 2，公差 7，$\langle a_n \rangle_{n\geq 1} = 2,9,16,23,30,\ldots$ 為例說明

gcd(2,7)=1，根據歐拉定理得 $2^{\varphi(7)} \equiv 2 \pmod 7$，尋找不大於 $\varphi(7)$ 又能滿足 $2^m \equiv 1 \pmod 7$的最小整數。

$2^2 \equiv 4 \pmod 7$，$2^3 = 8 \equiv 1 \pmod 7$，得最小整數 $m = 3$， 即$2^{3k+1} \equiv 4 \pmod 7$ ，為合項。

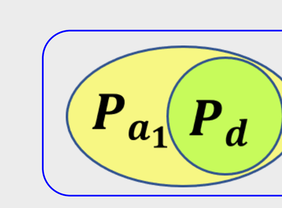
例 $a_{47} = 324 = 2^2 \cdot 9^2 \equiv 2^4 \equiv 2 \pmod 7$ ；a_{47} 為合項。

(四) 公差的質因數包含於首項的等差數列 ($P_d \subseteq P_{a_1}$)

性質 1 ：若 $\gcd(a_1, d) = d$ 則 $a_1 \equiv {a_1}^2 \equiv \cdots \equiv {a_1}^k \equiv 0 \pmod{d}$

性質 2 ：若 $P_d \subseteq P_{a_1}$且 $\gcd(a_1, d) \neq d$ 則必存在一個 k， $k \geq 2$，使得 ${a_1}^k \equiv {a_1}^{k+1} \equiv {a_1}^{k+2} \equiv \cdots \equiv 0 \pmod{d}$。

證明：



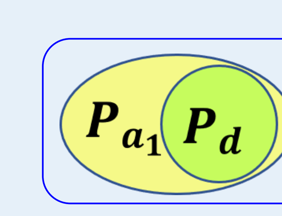
$P_d \subseteq P_{a_1}$，令 $a_1 = m{p_1}^{\alpha_1}{p_2}^{\alpha_2}\ldots{p_s}^{\alpha_s}$， $d = {p_1}^{\beta_1}{p_2}^{\beta_2}\ldots{p_s}^{\beta_s}$，$\gcd(a_1,d) \neq d$，代表$d \nmid a_1$，$a_1 \not\equiv 0 \pmod{d}$。

依阿基米德公理必可找到最小的 $l_1, l_2, \ldots, l_s$ 使得 $\alpha_1 l_1 \geq \beta_1$，$\alpha_2 l_2 \geq \beta_2$，…，$\alpha_s l_s \geq \beta_s$，

取 $k = Max(l_1, l_2, \ldots, l_s)$保證$d \mid {a_1}^k$，則 ${a_1}^k \equiv 0 \pmod{d} \Rightarrow {a_1}^k \equiv {a_1}^{k+1} \equiv {a_1}^{k+2} \equiv \cdots \equiv 0 \pmod{d}$ ■

性質 3 ：若 k 為使 ${a_1}^k \equiv 0 \pmod{d}$ 的最小整數，則不存在 $1 \leq i < j \leq k$ 使得 ${a_1}^j \equiv {a_1}^i \pmod{d}$。

定理 4 ：公差的質因數包含於首項的等差數列，若 $\gcd(a_1, d) = d$，則最小合項 $a_n = {a_1}^2$ ；$\gcd(a_1, d) \neq d$ ，則該數列為質項等差數列。



以首項為 12，公差 4 為例，$\langle a_n \rangle_{n\geq 1}$ =12,16,20,24,28,...

gcd(12,4)=4，最小合項=$12^2 = 144 = a_{34}$

以首項為 6，公差 8 為例， $\langle a_n \rangle_{n\geq 1} = 6,14,22,30,38,\ldots$

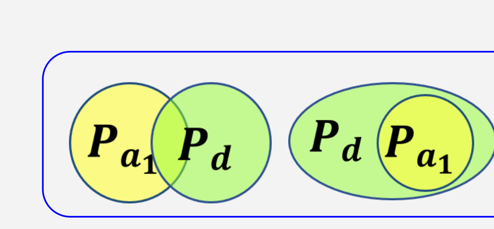
gcd(6,8)=2≠8，a_1= 6 (mod 8) ， 6^2 =36$\equiv$ 4 (mod 8)，6^3=216 $\equiv$0 (mod 8)，$6 \not\equiv 6^2 \not\equiv 6^3 \equiv 0 \pmod 8$。

找不到任何與a_1 同餘的合項，故該數列為$\boxed{\text{質項等差數列}}$。

(五) 首項與公差有共同的質因數，也各擁有不同質因數的等差數列。($P_d \not\subseteq P_{a_1}$)

性質 4 ：若對於所有同時是 a_1 和 d 的質因數 p，都有 $v_p(a_1) \geq v_p(d)$，則存在一個最小整數 k，滿足 $1 \leq k - 1 \leq \varphi\left(\frac{d}{\gcd(a_1,d)}\right)$，使得 ${a_1}^k \equiv a_1 \pmod{d}$

證明：



設 $a_1 = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\ldots{p_s}^{\alpha_s}w$，$d = {p_1}^{\beta_1}{p_2}^{\beta_2}\ldots{p_s}^{\beta_s}{q_1}^{\gamma_1}{q_2}^{\gamma_2}\ldots{q_t}^{\gamma_t}$。

將 d 的分解式中與a_1有共同質因數的分解式以d_p表示，與a_1不同質因數的分解式以d_q表示，$d = d_p d_q$。

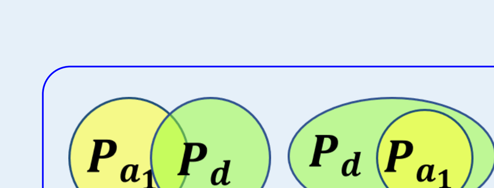
模 d_p： $v_p(a_1) \geq v_p(d) \Rightarrow \gcd(a_1, d_p) = d_p \Rightarrow d_p \mid a_1 \Rightarrow a_1 \equiv {a_1}^k \equiv 0 \pmod{d_p}$

模 d_q ：$\gcd(a_1, d_q) = 1 \Rightarrow {a_1}^{\varphi(d_q)} \equiv 1 \pmod{d_q} \Rightarrow {a_1}^{k-1} \equiv 1 \pmod{d_q} \Rightarrow {a_1}^k \equiv a_1 \pmod{d_q}$

$\begin{cases} {a_1}^k \equiv a_1 \pmod{d_p} \\ {a_1}^k \equiv a_1 \pmod{d_q} \end{cases}$ 由 CRT 得${a_1}^k \equiv a_1 \pmod{d}$ ■

性質 5 ：若對於所有同時是a_1 和d 的質因數 p，都有 $v_p(a_1) \leq v_p(d)$，則不存在 $k \geq 2$，使得 ${a_1}^k \equiv a_1 \pmod{d}$。

定理 5 ：首項質因數集合與公差質因數集合有相同質因數的等差數列，若對於所有同時是a_1和 d 的質因數 p，都有 $v_p(a_1) \geq v_p(d)$，則存在一個最小的整數 k，滿足 $2 \leq k \leq \varphi\left(\frac{d}{\gcd(a_1,d)}\right) + 1$，使得 ${a_1}^k \equiv a_1 \pmod{d}$；若對於所有同時是$a_1$和 d的質因數 p，都有 $v_p(a_1) \leq v_p(d)$，則該數列為質項等差數列。



$a_1 = 18 = \boxed{2 \cdot 3^2}$ ，$d = 30 = \boxed{2 \cdot 3} \cdot 5$ 為例，$\langle a_n \rangle_{n\geq 1}$ =18,48,78,108,138,...

共同質因數 2,3 皆 $v_p(a_1) \geq v_p(d)$，$\gcd(18,6) = 6$，$18 \equiv 18^k \equiv 0 \pmod 6$

$\gcd(18,5) = 1$，$18^{\varphi(5)} \equiv 1 \pmod 5$ ，尋找 $\varphi(5)$ 又能滿足 $18^{k-1} \equiv 1 \pmod 5$ 即 $18^k \equiv 18 \pmod 5$

$18^2 = 324 \equiv 4 \pmod 5$，$18^3 = 5832 \equiv 2 \pmod 5$，$18^4 = 104976 \equiv 1 \pmod 5$，$18^5 = 1889568 \equiv 18 \equiv 3 \pmod 5$，

$\begin{cases} 18 \equiv 18^5 \pmod 6 \\ 18 \equiv 18^5 \pmod 5 \end{cases}$ 由 CRT 得 $18 \equiv 18^5 \pmod{30}$ 即最小合項為$18^5 = 1889568 = a_{62986} = {a_1}^5$。

以 $a_1 = 4 = \boxed{2^2}$， $d = 56 = \boxed{2^3} \cdot 7$ 為例， $\langle a_n \rangle_{n\geq 1}$ = 4,60,116,172,228,...

共同質因數 2，$2^2 < 2^3$，$4^2 = 16 \equiv 16 \pmod{56}$，$4^3 = 64 = 8 \pmod{56}$，$4^4 = 256 = 32 \pmod{56}$，$4^5 = 1024 = 16 \pmod{56}$，...

故$4^x \pmod{56}$ 的模冪序列為 4,16,8,32,16,8,32,16，從$x \geq 2$ 才開始出現同餘的循環，即不存在$4^k \equiv 4 \pmod{56}$，為$\boxed{\text{質項等差數列。}}$

討　論

一、仿照「埃氏篩法」找出等差數列的質項與合項。

(一) 找出首項為 1，公差為 3 的等差數列 100 項以內的所有質項。

1. $\langle a_n\rangle_{n\geq 1}=1,4,7,10,13,16,19,\ldots$
2. $a_{100}=298$，$17^2<298<18^2$，故不大於$\sqrt{a_{100}}$ 的最大質項為 $a_5=13$。

(二) 將等差數列的合項檢核式，簡化為合項項次檢核式

1. $n=m+a_m k$，即 $n_1=m+a_m\times 1$，$n_2=m+a_m\times 2$ ，$n_3=m+a_m\times 3$
   $n_1\equiv n_2\equiv n_3\equiv\cdots\equiv m \pmod{a_m}$
2. 將 1 與含有質因項 a_2,a_3,a_4,a_5 的合項項次著色，未著色的即為質項。

等差數列的質項、合項項次(a_1=1，$d=3$)

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

圖 1：首項 1 公差 3，100 項內的質項

a_2　a_3　a_4　a_5

二、梅森質數與等差數列的質項

(一) 已知最大梅森質數 $2^{136279841}-1$ 是首項2^{k-1} 公差2^k 的最大質項。

1. 梅森數M_n 是形如 2^n-1 的數，為避免梅森數中的n 與等差數列中的項次n 混淆，本作將梅森數記為2^{m-1} 。
2. 設 $k\leq m\Rightarrow 2^k\mid 2^m\Rightarrow 2^m\equiv 0 \pmod{2^k}\Rightarrow 2^m-1\equiv -1\equiv 2^k-1 \pmod{2^k}$
   梅森數是首項2^k-1 公差2^k 的等差數列元素，即已知最大梅森數$2^{136279841}-1$ 是該數列的最大質項。

(二) 已知最大梅森質數$2^{136279841}-1$是首項$2^{\left\lfloor\frac{k}{2}\right\rfloor\cdot 2+1}-1$ 公差$3\cdot 2k$ 等差數列的最大質項。

1. 當梅森數M_n ，n 是奇數時，我們記為$2^{2m+1}-1$ 。
2. 當k 為偶數時，$2^{2m+1}-1\equiv 2^{k+1}-1 \pmod{3\cdot 2^k}$；
3. 當k 為奇數時，$2^{2m+1}-1\equiv 2^k-1 \pmod{3\cdot 2^k}$。
   即$2^{2m+1}-1$ 型的梅森數是首項 $2^{\left\lfloor\frac{k}{2}\right\rfloor\cdot 2+1}-1$，公差 $3\cdot 2^k$ 的數列元素。

表 5：$2^{2m+1}-1 \pmod{3\cdot 2^k}$的餘數 r

d \ $2^{2m+1}-1$ (r)	7	31	127	511	2047	8191
3	1	1	1	1	1	1
6	1	1	1	1	1	1
12	7	7	7	7	7	7
24	7	7	7	7	7	7
48	7	31	31	31	31	31

三、等差數列的質項密度探討

(一) 定義[質項計數函數]

π(x)為不大於x 的質項個數，若x 為質項則π(x) 等價於「x 是第π(x) 個質項。」

(二) 參考質項定理，我們可以猜測$\dfrac{a_n}{\pi(a_n)}\approx A\ln(a_n)+B$

將資料點$\left(\ln(a_n),\dfrac{a_n}{\pi(a_n)}\right)$佈於二維座標平面上，並嘗試利用迴歸直線找出 $\ln(a_n)$ 與$\dfrac{a_n}{\pi(a_n)}$之間的關係。(取第 50 至 5000 筆資料)

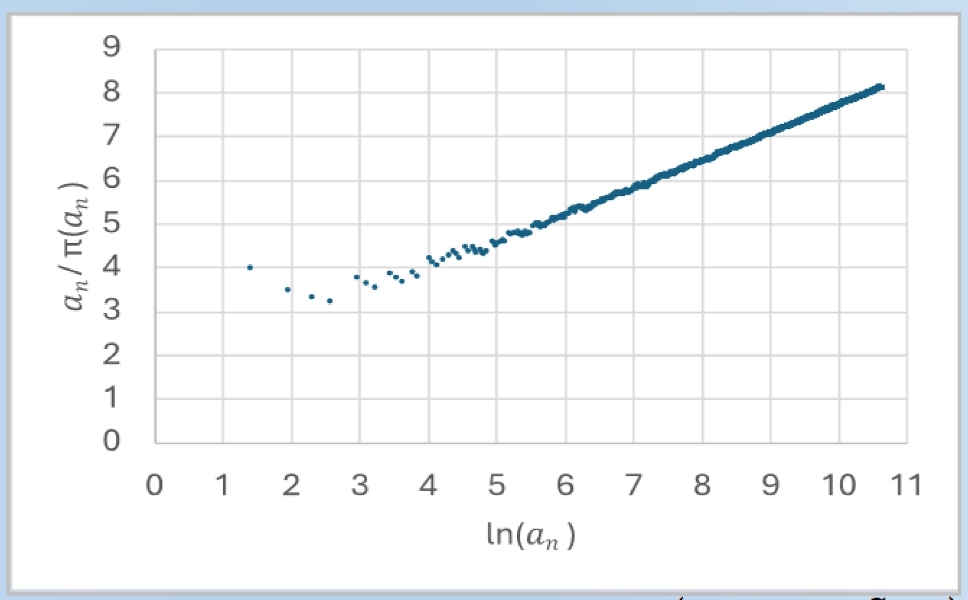


圖 2：$\langle a_n\rangle=\langle 3n+1\rangle$，以$\left(\ln(a_n),\dfrac{a_n}{\pi(a_n)}\right)$所繪製之散佈圖

(三)$\langle a_n\rangle=\langle 3n+1\rangle$，$x=\ln(a_n)$ 與 $y=\dfrac{a_n}{\pi(a_n)}$ 的迴歸直線方程式 $y=1.375+0.637x$

由相關係數$r\approx 0.9998$可知其為高度正相關。

(四) 相關係數接近 1，故可用$\ln(a_n)$與$\dfrac{a_n}{\pi(a_n)}$推估質項密度。

表 6：不同公差下的迴歸直線係數與相關係數列表

a_n	$n+1$	$2n+1$	$3n+1$	$4n+1$	$5n+1$	$6n+1$
A	0.977077	0.969137	0.636690	0.676262	0.497814	0.693208
B	−0.841054	−0.757359	1.375457	1.891853	3.685644	3.223657
r	0.999829	0.999769	0.999793	0.999783	0.999611	0.999616

結　論

一、首項為 1 的等差數列，當 $n=m+a_m k$ 且 $m\geq 2$ 時，$a_n=a_m a_{k+1}$ ，a_n 為合項。

二、公差比首項多 1 的等差數列，當 $n=m+a_m(a_s k-s)$ 時， $a_n=a_m a_s a_k$，a_n 為合項。

三、公差與首項互質的等差數列，m 是滿足 $a_1{}^m\equiv 1 \pmod{d}$的最小整數，則對於任意正整數k，有 $a_1{}^{mk+1}\equiv a_1 \pmod{d}$，即若$a_n=a_1{}^{mk+1}$，$a_n$為合項。

四、公差質因數集合包含於首項質因數集合的等差數列

若 $\gcd(a_1,d)=d$ ，則最小合項$=a_1{}^2$；若 $\gcd(a_1,d)\neq d$ 則該數列為質項等差數列。

五、首項與公差有共同質因數，也各擁有不同質因數的等差數列

若對於所有同時是 a_1和 d 的質因數p，都有 $v_p(a_1)\geq v_p(d)$，則存在一個最小的整數k，滿足 $2\leq k\leq\varphi\left(\dfrac{d}{\gcd(a_1,d)}\right)+1$ 使得$a_1{}^k\equiv a_1 \pmod{d}$；

若對於所有同時是 a_1和 d 的質因數 p，都有 $v_p(a_1)\leq v_p(d)$，則該數列為質項等差數列。

六、已知最大梅森質數 $2^{136279841}-1$ 是首項為2^k-1 公差為2^k 與首項為$2^{\left\lfloor\frac{m}{2}\right\rfloor\cdot 2+1}-1$公差為$3\cdot 2^k$ 等差數列的已知最大質項。

七、等差數列質項密度倒數$\dfrac{a_n}{\pi(a_n)}\approx A\ln(a_n)+B$ (A,B為常數) 。

未 來 展 望

質項研究開啟了嶄新的視界，還有許多值得深入探討的問題：二次方程式的數列、各種不同形式的數列、質項在密碼學的應用...等，希望大家與我們繼續發掘屬於這新視界的秘密。

參 考 資 料

[1] 游森棚(2024)。質項與合項。《科學研習月期刊》63(4)，100。

[2] Stein, S. K. (2008)。數學是啥玩意(葉偉文譯)。台北市：天下遠見出版股份有限公司。

[3] 許介彥(2011)。數學悠哉遊。台北市：三民書局。