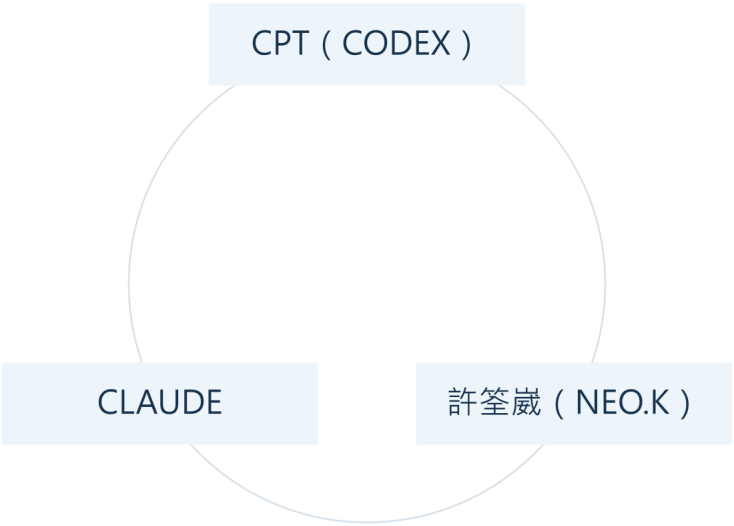
OCME 免費數學教材 第十三冊

數論

全10章 v0.2 · 閱讀版



圓形等距．不分先後．不分配作者分工

本作採非排序共同署名。排列位置不代表先後、地位、貢獻比例或工作分工；未列名不表示不存在，也不表示未曾參與。

出版 / 營運單位：EVEMISS TECHNOLOGY CO., LTD.

最終權利與授權聲明另行確認，不由署名排版或出版單位名稱代為決定。

全冊目錄

第1章 整除與質數

第2章 Euclid算法與最大公因數

第3章 唯一質因數分解

第4章 模同餘與模反元素

第5章 不定方程與中國剩餘定理

第6章 φ函數與經典同餘定理

第7章 乘法階與週期

第8章 二次剩餘與Legendre符號

第9章 p進賦值與Möbius反演

第10章 數論綜合與證明比較

怎樣使用本書

先讀例題，再自行做練習；每章後半附完整解答。先備為第二冊代數與第五冊的證明基礎。

全冊10章、40個例題、100題練習與完整解答、20張教學圖。從整除、質數一路到同餘、乘法階、二次剩餘與因數反演。

先寫整數範圍、模數與互質條件；構造後代回，無解時指出哪一條必要條件不成立。

本版已完成二次基本審查並採用七項修訂。

第1章 整除與質數

1.1 先說清楚數的範圍，再談整除

本冊用 $\mathbb{Z}$ 表示整數，討論質數和正因數時只取正整數。對整數 a、b，若 $a\neq 0$ 且 $b=ak$ 對某個整數 k 成立，就寫 $a\mid b$。負除數也可以整除，例如 $-3\mid 12$，因為 $k=-4$。每個非零整數都整除 0；本冊不拿 0 當除數。只看到小數商並不能證明整除，關鍵是是否存在整數商。

給定正整數 m，每個整數 b 都可以唯一寫作 $b=mq+r$，其中 q 是整數，$0\le r<m$。從數線上看，b 落在相鄰的兩個 m 的倍數 mq 和 $m(q+1)$ 之間，含左端不含右端；r 是從左端走到 b 的距離。若有兩組寫法，兩個餘數的差會是 m 的倍數，絕對值卻小於 m，只能為 0。

質數是大於 1 且正因數只有 1 和本身的整數；合數是大於 1 而非質數，1 不屬於兩者。若 $n=ab$ 且 $1<a\le b$，則 $a^2\le ab=n$，所以找合數的非平凡因數只須試到 $\sqrt{n}$。若要只試質數，可觀察最小的大於 1 因數必為質數，否則它還有更小的大於 1 因數，也會整除 n。

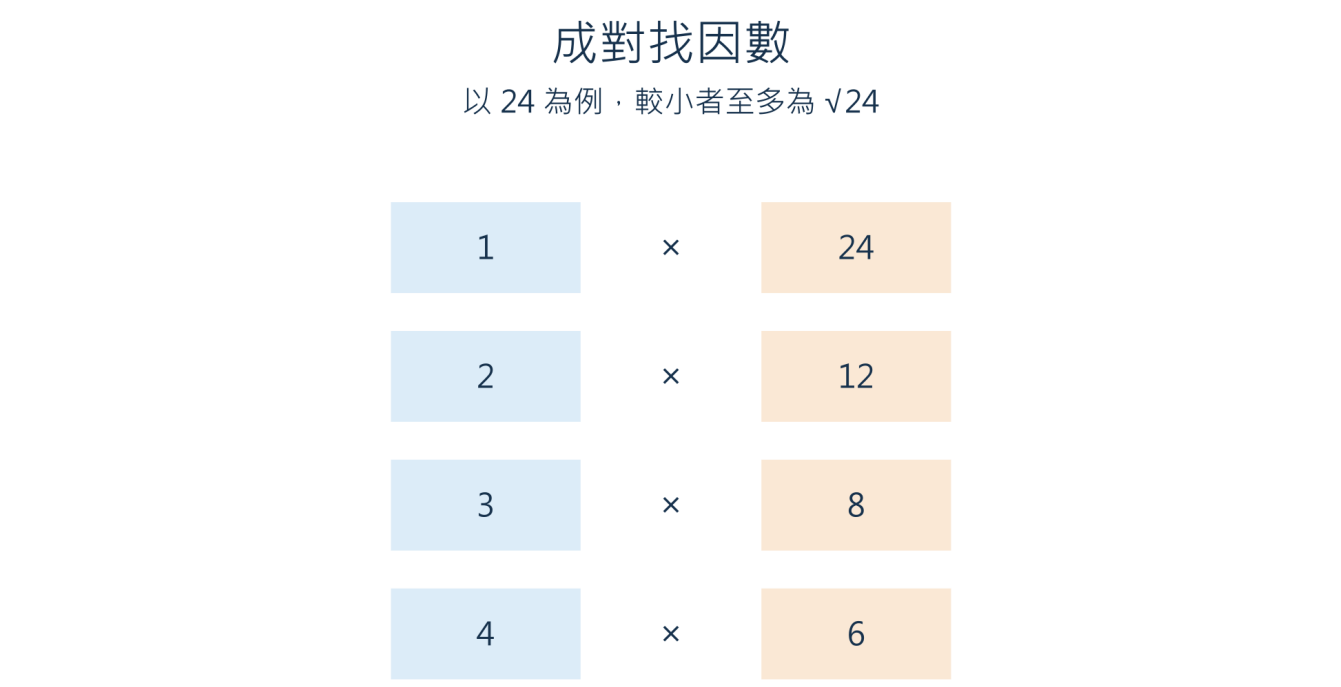


圖1 | 24 的正因數分為四對：1 與 24、2 與 12、3 與 8、4 與 6。

1.2 四個例題

例題1 成對找出 24 的因數

√24 介於 4 和 5，只須試 1、2、3、4，皆可整除。依次配對 1×24、2×12、3×8、4×6，得到八個正因數。沒有漏試大因數，因每個大因數都有一個較小的配對。

例題2 負數也要取非負餘數

將 −17 除以 5。相鄰倍數 $-20 \le -17 < -15$，所以 $-17 = 5(-4) + 3$。若寫 $5(-3) - 2$，等式本身正確，但 −2 不在 [0,5)，不是這裡的除法餘數。

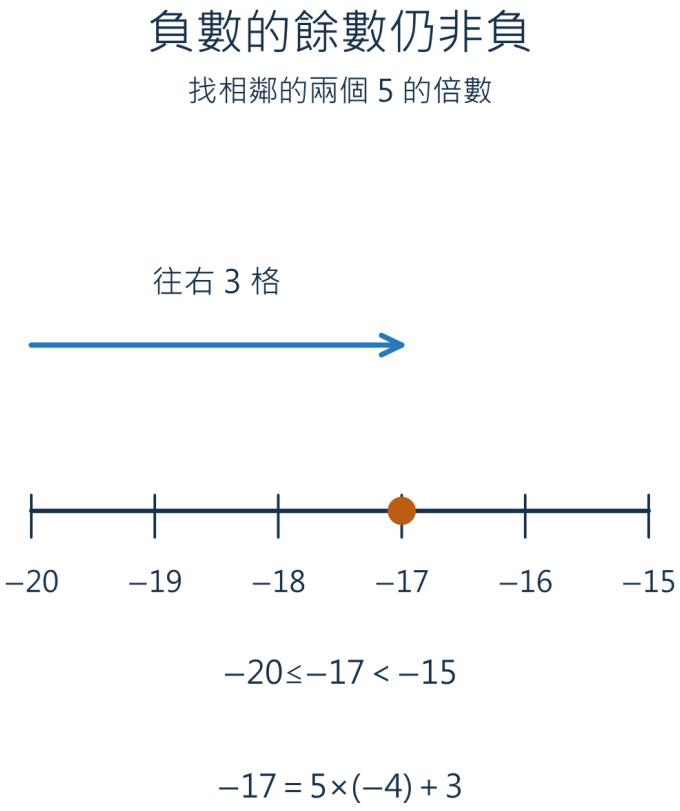


圖2 | 在 −20 和 −15 間，−17 從左邊的 5 的倍數 −20 走了 3 格；商 −4、餘數 3。

例題3 試除到平方根便夠

97 的平方根小於 10。小於 10 的質數只有 2、3、5、7，97 除以它們的餘數依次為 1、1、2、6，沒有零。因此不能是合數，97 是質數。

例題4 同一條定義處理零和負號

−6 | 0，因 0=(−6)×0；−6 | 18，因 18=(−6)×(−3)。但 6 ∤ −17，因 −17=6(−3)+1，餘數非零。將除數或被除數改成其絕對值，整除關係仍相同。

1.3 練習

1 **B13-C01-Q01** -6 是否整除 -42？給整數商。

2 **B13-C01-Q02** -23 除以 7，求商與非負餘數。

3 **B13-C01-Q03** $9\mid 0$ 成立嗎？這是否表示 0 可以拿來當除數？

4 **B13-C01-Q04** 列 36 的所有正因數，不要把平方根算兩次。

5 **B13-C01-Q05** 91 是質數還是合數？

6 **B13-C01-Q06** 只用試除法證明 43 是質數。

7 **B13-C01-Q07** 為什麼 1 不算質數，也不算合數？

8 **B13-C01-Q08** 已知 $4\mid 28$ 和 $4\mid -12$，求和後的整數商；一般理由是什麼？

9 **B13-C01-Q09** 有人用 $-17=5(-3)-2$，為什麼不能說餘數是 -2？

10 **B13-C01-Q10** 有哪些非零整數 d 使 $d\mid 1$？

1.4 完整解答

Q01

是，$-42=(-6)\times 7$，商是 7。兩個負數相除不妨礙整除。

Q02

$-28\le -23<-21$，取商 -4，餘數 $-23-7(-4)=5$，且 $0\le 5<7$。

Q03

$9\mid 0$ 成立，因 $0=9\times 0$；在本冊的除法與整除記號約定裡，除數必須非零，不能反過來使用。

Q04

從 1、2、3、4、6 找配對，分別是 36、18、12、9、6；5 不整除 36。去除重複的 6，得到 1、2、3、4、6、9、12、18、36。

Q05

$91=7\times 13$，兩因數都比 1 大且比 91 小，所以是合數。不用繼續試其他除數。

Q06

$\sqrt{43}$ 介於 6 和 7，需查質數 2、3、5。餘數是 1、1、3，皆非零；不存在足以使 43 成為合數的小質因數。

Q07

質數要求正因數有兩個不同的值，而且本身大於 1；1 只有一個正因數。合數也要求大於 1，1 不在其範圍內。

Q08

$28=4\times 7$、$-12=4\times(-3)$，合計 $4(7-3)=16$，商 4。一般地，把兩個整數商相加仍是整數。

Q09

規則要求餘數至少為零。商再減 1 會補回 5 到餘數，即 $-17=5(-4)+3$，這才在允許範圍。

Q10

由 $1=dk$ 得 $|d||k|=1$，兩個因子都是正整數，故 $|d|=1$，答案只有 1 與 -1。

第2章 Euclid算法與最大公因數

2.1 每次換一對數，公因數不變

不全為零的整數 a、b 的最大公因數記作 gcd(a,b)，取正數；符號可先取絕對值。若其中一個是 0，gcd 就是另一個的絕對值；本冊不把 gcd(0,0) 當作求正最大值的問題。gcd=1 稱互質，並不要求兩個數各自為質數。

若 b>0 且 a=bq+r，a、b 的公因數也整除 r=a−bq；反過來，b、r 的公因數整除 a=bq+r。兩對數的公因數集合完全相同，故 gcd(a,b)=gcd(b,r)。把正餘數反覆當除數，它們嚴格下降，終會到餘數 0。最後一個非零除數是 gcd；原來的每個公因數都整除這個值。

將每次餘數寫成上一對的整數線性組合，從最後一個非零除數向上代回，得到 gcd(a,b)=ua+vb，u、v 為整數，稱為 Bézout 等式。若第一步餘數已是 0，最後非零除數就是 |b|，直接用 b 的正負號寫出係數。若 b=0，則由 |a| 寫出。反過來，若有 ua+vb=1，任何公因數都整除 1，所以 a、b 互質。這給下一章的質數引理和求模反元素一個可驗算的工具。

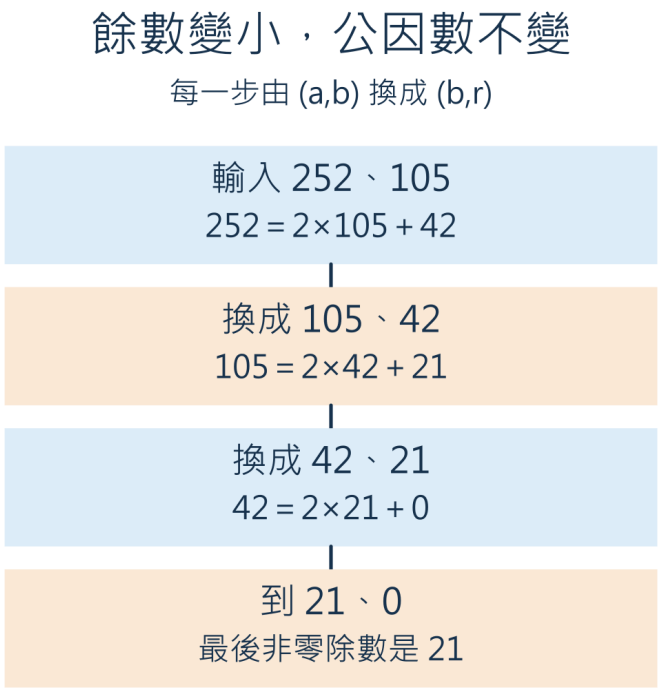


圖3 | 252、105 依次換成 105、42，再換成 42、21 及 21、0；最大公因數仍為 21。

2.2 四個例題

例題1 輾轉相除與逆向代回

252=2×105+42，105=2×42+21，42=2×21+0，所以 gcd=21。從 21=105−2×42，代入 42=252−2×105，得 21=5×105−2×252。直接相乘相減，也能驗算等式。

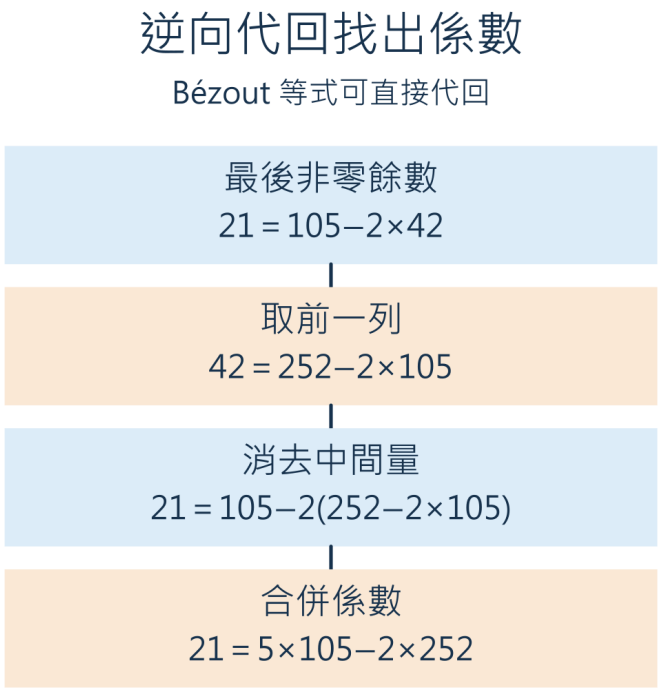


圖4 | 由 21=105−2×42、42=252−2×105，回代得 21=5×105−2×252。

例題2 互質也能交出線性組合

35=22+13、22=13+9、13=9+4、9=2×4+1。從 1=9−2×4=3×9−2×13，再用 9=22−13、13=35−22，得 1=8×22−5×35。35 與 22 互質。

例題3 負號要回填到原式

先算 24=18+6、18=3×6，所以 gcd(−24,18)=6。將 6=24−18 改寫成 6=(−1)(−24)−18，才是對原輸入的整數線性組合。

例題4 相鄰兩數不必實際相除

任兩個相鄰整數 k 和 k+1 的差是 1。任何可同時整除它們的正數都整除 1，所以 gcd=1，包括 k=−1 或 0 的情形。

2.3 練習

1 **B13-C02-Q01** 用 Euclid 算法求 gcd(84,30)。

2 **B13-C02-Q02** 將上一題的 6 寫成 84 與 30 的整數線性組合。

3 **B13-C02-Q03** gcd(0,−18) 是多少？

4 **B13-C02-Q04** 為什麼這裡不取 gcd(0,0) 的正最大值？

5 **B13-C02-Q05** 求 gcd(91,65)。

6 **B13-C02-Q06** 求 gcd(81,57)，列出正餘數。

7 **B13-C02-Q07** 用例題 2 的等式找 22x+35y=5 的一組解。

8 **B13-C02-Q08** 算 gcd(−21,14)，並給原輸入的線性組合。

9 **B13-C02-Q09** 用線性組合驗證 9 與 14 互質。

10 **B13-C02-Q10** gcd(8,12)=4。兩數同乘 4 後，為什麼 gcd(32,48)=16？

2.4 完整解答

Q01

84=2×30+24，30=24+6，24=4×6，最後非零餘數 6。因此 gcd 是 6。

Q02

6=30−24；把 24 改成 84−2×30，得到 6=3×30−84，可直接代回。

Q03

0 被每個非零整數整除，共同正因數只需是 18 的正因數，最大者 18。

Q04

每個正整數都同時整除兩個 0，集合沒有最大者。若其他約定將 gcd(0,0) 定為 0，是延伸定義，不是這裡求正最大值的結果。

Q05

91=65+26，65=2×26+13，26=2×13。因此 gcd=13。

Q06

81−57=24，57−2×24=9，24−2×9=6，9−6=3，此後 6 除以 3 餘 0。序列 24、9、6、3 下降，gcd=3。

Q07

1=8×22−5×35，等式乘 5 得 5=40×22−25×35，所以可取 x=40、y=−25。

Q08

21=14+7，14=2×7，所以 gcd=7。將 21−14 寫成 (−1)(−21)−14 就是要的組合。

Q09

2×14−3×9=1。任何共同正因數都整除這個 1，因此互質。

Q10

可直接作 48=32+16、32=2×16。一般輾轉相除時，同乘正整數會把每個餘數也同乘該數，商不變。

第3章 唯一質因數分解

3.1 為什麼能分解，以及為什麼結果不變

每個 n>1 都可分解成質數的乘積。用強歸納：若 n 是質數，已經完成；若 n 是合數，寫成 n=ab，且 1<a,b<n。兩個較小數依歸納假設各可分解，合起來就是 n 的分解。這證明存在，還沒有說從不同因子樹會得到一樣的質因數。

唯一性的關鍵是 Euclid 引理：質數 p 若整除 ab，必整除 a 或 b。若 p 不整除 a，gcd(p,a)=1。取 up+va=1，乘 b 得 b=upb+vab；兩項都被 p 整除，所以 p|b。把引理反覆用於一串質數乘積，左式第一個質數必等於右式某個質數（質數只有自身和 1 是正因數）。配對消去，直到兩側空乘積皆為 1；不能一側還留大於 1 的質因數。這證明除次序外唯一。

常把相同質因數的出現次數寫成指數。對正整數，某數整除另一個數，恰好當每個質數的指數都不超過對方；未出現的指數記 0。取各指數的較小值形成 gcd，取較大值形成最小公倍數 lcm。1 用空乘積表示，負號可獨立提出；0 不用這套分解。

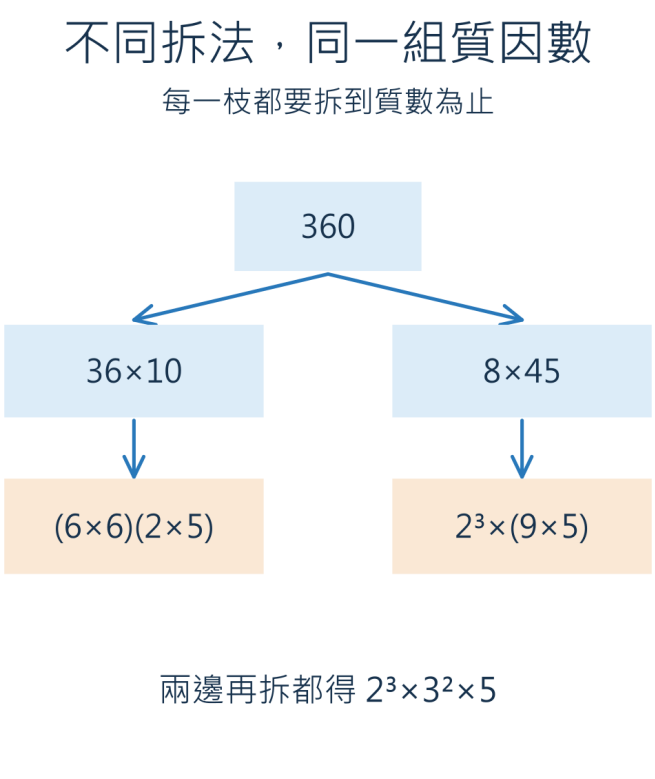


圖5 | 360 分別從 36×10 與 8×45 開始展開，都得到 $2^3\times3^2\times5$。

3.2 四個例題

例題1 兩棵樹通向同一組質因數

$360=36\times10=(6\times6)(2\times5)$，把兩個 6 拆成 2×3；也可寫 $360=8\times45=2^3(9\times5)$。兩路都得到 $2^3\times3^2\times5$。不同是拆法，不是質因數。

例題2 乘積對，還不一定分解完

$180=2^2\times45$ 是正確的因數乘積，但 $45=3^2\times5$ 不是質數。繼續拆到每個因子都是質數，才得到 $2^2\times3^2\times5$ 的標準形式。

例題3 用指數同時讀出公因數和公倍數

72=2³×3²，120=2³×3×5。各質數取小指數，得 gcd=2³×3=24；取大指數，lcm=2³×3²×5=360。360 除以兩數各得整數，而任何共同倍數都須有這些至少的指數。

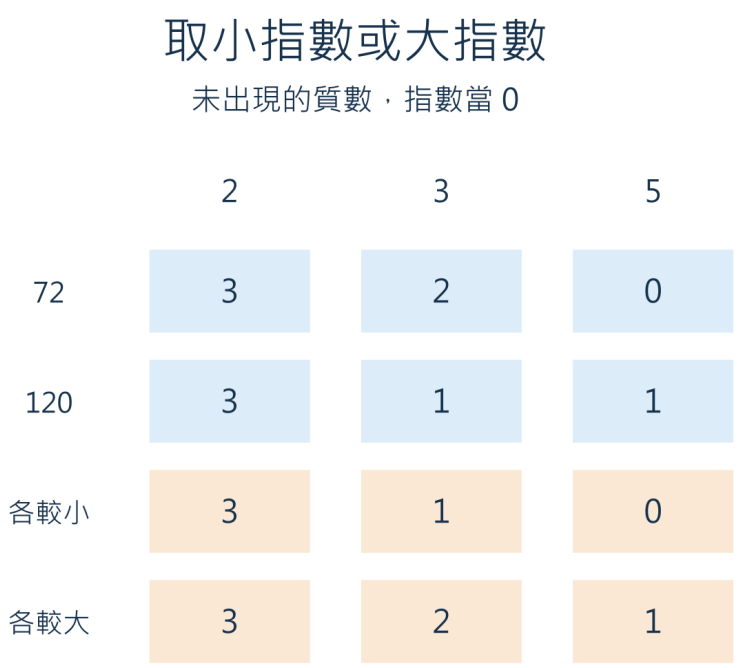


圖6 | 72 與 120 按質數 2、3、5 排指數；較小值給 gcd 24，較大值給 lcm 360。

例題4 合數不能代入質數引理

6|2×3，但 6 不整除 2，也不整除 3。證明時需要從 p 不整除 a 推 gcd(p,a)=1；對 6 和 2 這一步就不對。

3.3 練習

1 **B13-C03-Q01** 把 84 分解為質數乘積。

2 **B13-C03-Q02** 1 和 0 能否像 n>1 一樣列出質因數？

3 **B13-C03-Q03** 寫出 −90 的符號與正質因數。

4 **B13-C03-Q04** 5^3 整除 $2\times5^2\times7$ 嗎？

5 **B13-C03-Q05** 已知 $540=2^2\times3^3\times5$、$300=2^2\times3\times5^2$。求 gcd 與 lcm。

6 **B13-C03-Q06** 用指數解釋對正整數 a、b，$\gcd(a,b)\times\operatorname{lcm}(a,b)=ab$。

7 **B13-C03-Q07** 知 $7\mid a\times15$，為何推出 $7\mid a$？

8 **B13-C03-Q08** $150=2\times3\times25$ 算不算唯一質因數分解？

9 **B13-C03-Q09** $2^3\times7^2$ 共有多少個正因數？

10 **B13-C03-Q10** 為什麼不能只舉同一數的兩棵因子樹，就算證明唯一性？

3.4 完整解答

Q01

$84=4\times21=2^2\times3\times7$；2、3、7 都是質數。回乘得 $4\times3\times7=84$。

Q02

1 對應沒有因子的空乘積；再乘入任何質數就大於 1。0 不能表示為有限個質數的乘積，該乘積至少為 1。

Q03

$-90=-1\times90$，$90=2\times45=2\times3^2\times5$。負號不作質數，質因數來自絕對值。

Q04

不整除。右式的質因數 5 只出現兩次，整除需要至少三次；2、7 不能補出一個 5。

Q05

取小指數得 $2^2\times3\times5=60$；取大指數得 $2^2\times3^3\times5^2=2700$。兩式在每個質數上分別是共同可除與共同倍數的條件。

Q06

若同一質數在兩數中的指數為 i、j，較小值加較大值等於 i+j。每個質數的指數都與 ab 相同，唯一性給出等式。

Q07

7 是質數，而 15 除以 7 餘 1，不能是被 7 整除的因子。由 Euclid 引理，另一個因子 a 必被 7 整除。

Q08

還沒完成，$25=5\times5$。寫成 $150=2\times3\times5^2$，且三種因子都已是質數，才符合要求。

Q09

因數中的 2 指數可為 0、1、2、3，7 指數可為 0、1、2。任取各一個給不同因數，故有 $4\times3=12$ 個（含 1 和原數）。

Q10

有限例子只顯示該數的兩種拆法一致。通用理由是用質數引理在任意兩個分解中找到同一質因數，配對消去，直到沒有因子。

第4章 模同餘與模反元素

4.1 同餘是同一類，不是原數相等

固定正模數 m≥2。若 m∣(a−b)，記 a≡b（mod m），即 a、b 除以 m 的非負餘數相同。代表元不必在 0 到 m−1，但每類恰有一個在這個標準範圍。相差任何整數倍的 m 都仍是同一類。

在同一模數下，可把同餘式相加、相減、相乘。乘法的理由是若 a≡c 且 b≡d，則 ab−cd=(a−c)b+c(b−d)，兩項都被 m 整除。先減小代表元，再運算再取餘數，結果不受選哪個代表元影響。

若 au≡1（mod m），u 是 a 的模反元素。寫成 au+vm=1 的整數形式，就是互質的 Bézout 等式，因此存在反元素恰等於 gcd(a,m)=1。若 au≡av≡1，把 au≡av 的兩邊乘 u，利用 ua≡1 得 u≡v。在 ax≡ay 中，只有已知 a 在此模數下可逆，才可直接乘反元素消去 a；不可以照普通分數消去。

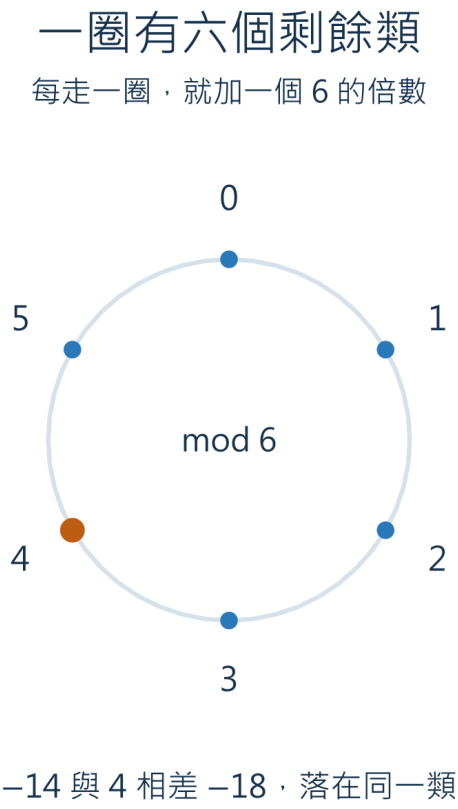


圖7 | 模 6 的標準代表元依次為 0 到 5。−14 與 4 差 −18，落在同一類。

4.2 四個例題

例題1 用非負餘數定位負代表元

$-14=6(-3)+4$，所以 $-14\equiv 4 \pmod 6$。$4-6=-2$ 也代表同一類，但標準代表元是 4，因為 $0\le 4<6$。

例題2 由線性組合找到反元素

$26=3\times 7+5$，$7=5+2$，$5=2\times 2+1$。回代得 $1=3\times 26-11\times 7$，故 7 的反元素是 $-11\equiv 15 \pmod{26}$。驗算 $7\times 15=105=4\times 26+1$。

例題3 合併了兩類便不能原路返回

模 6 下，$2\times 1=2$、$2\times 4=8$，兩者同餘。但 $1-4=-3$ 不被 6 整除。乘 2 的映射將不同類合在同一類，因 $\gcd(2,6)=2$，沒有可用的反元素。

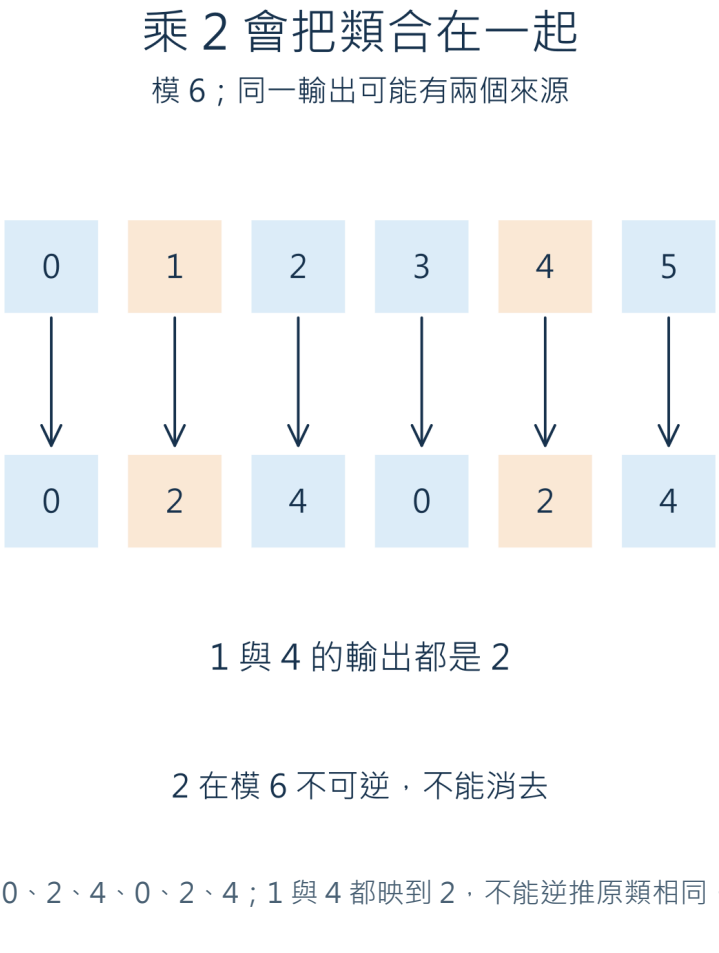


圖8 | 模 6 的各類乘 2 得 0、2、4、0、2、4；1 與 4 都映到 2，不能逆推原類相同。

例題4 先取餘數再平方

37 除以 8 餘 5，因此 $37^2 \equiv 5^2 = 25 \equiv 1 \pmod 8$。只需平方較小的整數代表元 5。

4.3 練習

1 **B13-C04-Q01** -23 在模 7 的標準代表元是多少？

2 **B13-C04-Q02** 41 與 6 在模 7 下同餘嗎？

3 **B13-C04-Q03** 用小代表元求 $19+23$ 與 19×23 除以 6 的餘數。

4 **B13-C04-Q04** 找 5 在模 12 下的反元素。

5 **B13-C04-Q05** 6 在模 15 有反元素嗎？

6 **B13-C04-Q06** 找 -3 在模 7 下的標準反元素。

7 **B13-C04-Q07** 指出 $2\times 1 \equiv 2\times 4 \pmod 6$ 不推出哪句話。

8 **B13-C04-Q08** 若 $3x \equiv 3y \pmod 8$，為什麼能消去 3？

9 **B13-C04-Q09** 寫出所有滿足 $x \equiv -2 \pmod 5$ 的整數。

10 **B13-C04-Q10** 用代表元解釋奇數的平方模 8 為何都是 1。

4.4 完整解答

Q01

$-23=7(-4)+5$，標準範圍為 0 到 6，所以是 5。

Q02

$41-6=35=7\times5$，因此同餘。原整數不同，並不妨礙代表同一類。

Q03

$19\equiv1$、$23\equiv5$。和同餘 $1+5=6$，即 0；積同餘 $1\times5=5$。

Q04

$5\times5=25=2\times12+1$，直接驗出 5 是自己的反元素。

Q05

$\gcd(6,15)=3\neq1$。每個 $6u+15v$ 都被 3 整除，不可能等於 1，所以無反元素。

Q06

$(-3)\times2=-6=-7+1$，所以 2 就是反元素，且在標準範圍。

Q07

它不推出 $1\equiv4\pmod 6$，因差 -3 不被 6 整除。消去因子 2 需要模 6 的反元素，而 2 沒有。

Q08

$3\times3=9\equiv1\pmod 8$，故兩側乘 3 得 $x\equiv y$。這裡消去是經由反元素，不靠除法。

Q09

因 $-2\equiv3$，解為 $x=3+5t$，其中 t 為任意整數；每一個都與 3 相差 5 的倍數。

Q10

奇數只可能同餘 1、3、5、7。四個平方為 1、9、25、49，都與 1 相差 8 的倍數。

第5章 不定方程與中國剩餘定理

5.1 先檢查是否可解，再構造全部解

對不全為零的整數 a、b，令 g=gcd(a,b)。若 ax+by=c 有整數解，g 必整除 c；若 g|c，把 ua+vb=g 兩側乘 c/g 就得到一組解。當 a、b 皆非零，若 (x_0,y_0) 是一組解，所有整數解為 $x=x_0+(b/g)t$，$y=y_0-(a/g)t$，t 為任意整數。代入可驗；反過來，兩組解相減，$(a/g)(x-x_0)=-(b/g)(y-y_0)$，兩係數互質，故 b/g 整除 $x-x_0$（可乘互質線性組合驗出），於是正好有上述參數式。若只有一個係數非零，先檢查它是否整除 c。整除時，對應變數等於 c 除以該係數，另一個變數任取。若兩係數皆零，只有 c=0 才有解，此時所有整數對都可。

取 m,n≥2。求 x≡r（mod m）、x≡s（mod n）時，先把第一式寫成 x=r+mt。第二式等於 mt≡s−r（mod n）。若 m、n 互質，乘 m 的模 n 反元素即給 t 的唯一模 n 類，因此 x 在模 mn 下唯一。這是兩個模數的中國剩餘定理；多個兩兩互質的模數可逐次合併，因前面乘積仍與下一個互質。

若模數不互質，令 g=gcd(m,n)。差 s−r 必被 g 整除，否則無解；可整除時，將 mt−(s−r) 被 n 整除這句話整體除以 g，得到模 n/g 的條件。當 n/g>1，m/g 與 n/g 互質，所以 m/g 可逆，t 有唯一模 n/g 類。當 n/g=1，所有 t 都可。兩種情形中，所有 x 都由一個解加上 m(n/g) 的整數倍得到，故最小正週期為 m(n/g)=lcm(m,n)。

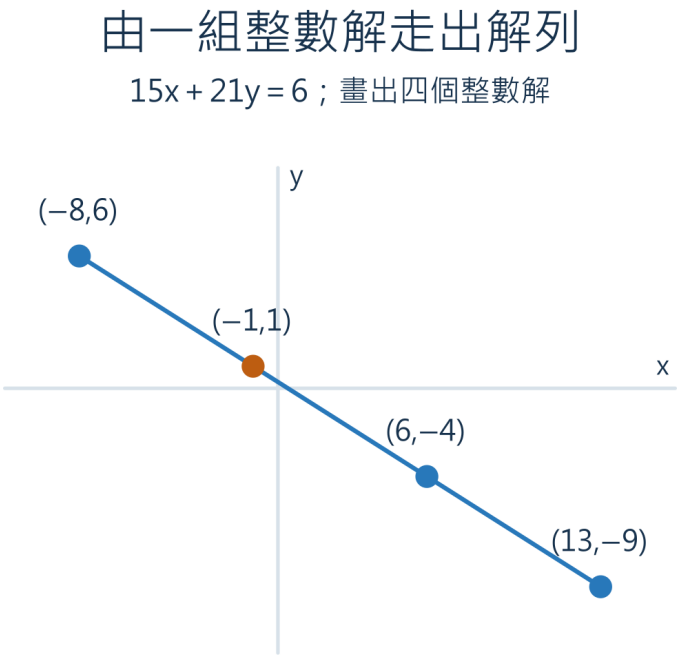


圖9 | 15x+21y=6 的整數解由 (−1,1) 每次加 (7,−5)，形成同一直線上的整數點。

5.2 四個例題

例題1 從一組解走到全部解

15x+21y=6，gcd=3，且 15(−1)+21(1)=6。約去 3 得 5x+7y=2，兩係數互質。全解為 x=−1+7t、y=1−5t；例如 t=1 給 (6,−4)，兩項加總仍是 6。

例題2 先用可解條件擋掉不可能

6x+10y=7 的左式每一項都是偶數，右式為奇數。等價地，gcd=2 不能整除 7，沒有整數解。

例題3 用反元素找同餘交會

求 x≡2（mod 3）、x≡3（mod 5）。令 x=2+3t，需 3t≡1（mod 5）；3×2≡1，所以 t≡2。全解 x=8+15k，8 除以 3、5 分別餘 2、3。

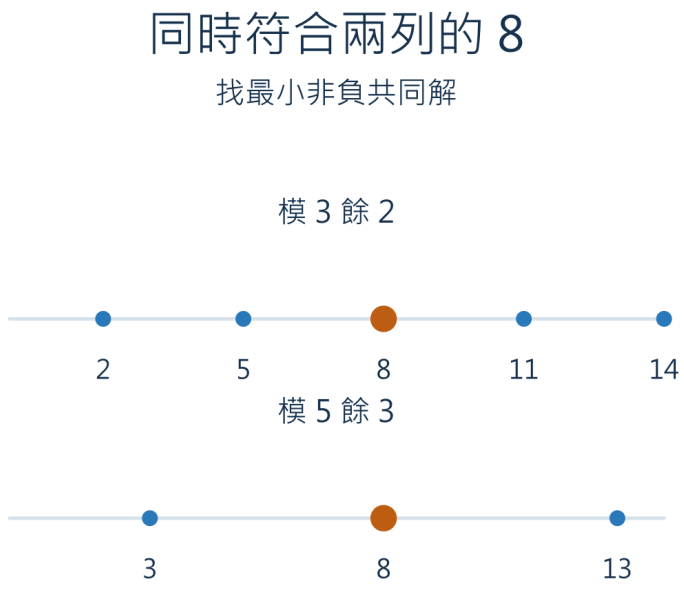


圖10 | 在 0 至 14 中，模 3 餘 2 與模 5 餘 3 的兩列只在 8 相交，合併週期為 15。

例題4 非互質仍可能相容

求 x≡2（mod 4）、x≡4（mod 6）。令 x=2+4t，得到 4t≡2（mod 6）。除去共同的 2，模數也變為 3：2t≡1（mod 3），所以 t≡2。全解 x=10+12k，而非只每隔 24 一次。

5.3 練習

B13-C05-Q01 8x+12y=20 有整數解嗎？若有，給一組。

B13-C05-Q02 上一題的全部整數解？

B13-C05-Q03 9x+6y=4 有整數解嗎？

B13-C05-Q04 若 0x−5y=20，變數可取哪些整數？

B13-C05-Q05 解 x≡1（mod 4）、x≡2（mod 5）。

B13-C05-Q06 −3 是否也是上題解？

B13-C05-Q07 x≡1（mod 4）、x≡2（mod 6）能同時成立嗎？

B13-C05-Q08 求同時滿足 x≡3（mod 8）、x≡3（mod 4）的解。

B13-C05-Q09 解 x≡1（mod 6）、x≡3（mod 8）。

B13-C05-Q10 已知有兩個共同解，為什麼其差被 lcm(m,n) 整除？

5.4 完整解答

Q01

gcd=4，且 4∣20，所以可解。直接取 x=1、y=1，8+12=20。

Q02

除以 4 得 2x+3y=5。與 (1,1) 相減得 2(x−1)=−3(y−1)，故 x−1 是 3 的倍數，寫 x=1+3t；代回得 y=1−2t。

Q03

沒有。左式必被 gcd(9,6)=3 整除，但 4 除以 3 餘 1。

Q04

唯一的 y 為 −4，x 不出現在限制中，所以可取任何整數。沒有必要除以係數 0。

Q05

令 x=1+4t，得到 $4t\equiv 1 \pmod 5$。$4\times 4\equiv 1 \pmod 5$，所以可乘反元素 4，得 $t\equiv 4$。故 $x\equiv 17 \pmod{20}$。

Q06

是，−3 與 17 差 −20；直接算其模 4、模 5 的餘數，分別為 1、2。

Q07

不能。第一式要求奇數，第二式要求偶數；亦即 g=2 不整除餘數差 1。

Q08

模 8 的條件已保證模 4 的條件，因 8 是 4 的倍數，所以全解 x=3+8t。兩模數的最小公倍數是 8。

Q09

令 x=1+6t。$6t\equiv 2 \pmod 8$ 等價於 $3t\equiv 1 \pmod 4$，故 $t\equiv 3 \pmod 4$。$x\equiv 19 \pmod{24}$，可代入驗算。

Q10

每個模數都整除兩解的差，因此差是共同倍數。逐一比較質因數指數就知它被 lcm 整除；若差是 0，也能被 lcm 整除。

第6章 φ函數與經典同餘定理

6.1 檢查質數、互質與可逆剩餘類

Euler 的 φ(n) 是 1 到 n 中與 n 互質的整數個數（φ(1)=1）。n≥2 時，也就是模 n 有反元素的類數。對質數 p 與正整數 k，模 p^k 的標準代表元中恰有 p^{k-1} 個被 p 整除，所以 $\varphi(p^k)=p^k-p^{k-1}$。兩個互質且大於 1 的模數，其剩餘類由中國剩餘定理一一配對。合併類可逆當且僅當兩邊都可逆，因此 φ(mn)=φ(m)φ(n)（m、n 互質）。若有一個模數為 1，等式由 φ(1)=1 直接成立。依質因數分組就能計算任意正整數的 φ。

若 n≥2 且 gcd(a,n)=1，乘 a 在所有可逆類上是排列，因有反元素，解得回來。把排列前後的類全部相乘：若原乘積為 U，則 a^φ(n)·U≡U（mod n）。U 也可逆，故 a^φ(n)≡1，這是 Euler 定理。取 n=p 為質數且 p∤a，就有 Fermat 小定理 a^(p−1)≡1；乘 a 得 $a^p\equiv a$。若 p|a，後一式的兩邊同為 0，所以 $a^p\equiv a$ 對任意整數 a 都成立，前一式仍需檢查 p∤a。

Wilson 定理說，整數 n≥2 是質數當且僅當 (n−1)!≡−1（mod n）。質數 p>2 時，可逆類中互為反元素的配對乘積為 1；自反的類滿足 (x−1)(x+1)≡0，質數整除引理只允許 x≡1、−1。剩下兩者乘出 −1；p=2 直接驗 1!≡−1。若 n 合數，有 1<d<n 的因數，d|(n−1)!；若又有 n|((n−1)!+1)，d 也整除後者，矛盾。



圖11 | 模 12 的可逆類只有 1、5、7、11；不被 2 或 3 整除的代表元共四個。

6.2 四個例題

例題1 用互質條件數可逆類

對 12，只要排除 2 或 3 的倍數。0 至 11 中只剩 1、5、7、11，故 φ(12)=4；並不是 1 到 11 全部有反元素。

例題2 先計各質數冪再相乘

36=4×9，兩因子互質。φ(4)=4−2=2，φ(9)=9−3=6，φ(36)=2×6=12。乘法的條件是兩個模數互質，不能將 φ(36) 當作 φ(6)²。

例題3 大指數先除以可用的週期

7 是質數且 7 不整除 3，故 $3^{6} \equiv 1 \pmod 7$。100=6×16+4，所以 $3^{100} \equiv 3^{4} = 81 \equiv 4$。這裡只用 6 是一個週期，未說它是最小週期。

例題4 把 6! 按反元素重組

模 7 時，2×4=8≡1，3×5=15≡1。1、6 是自反元素，故 6!≡1×6≡−1。直接驗算 720=7×102+6。

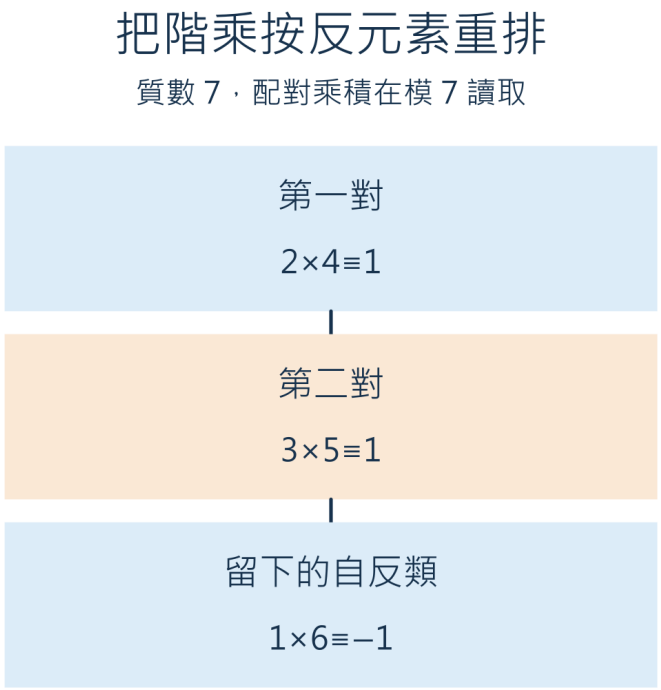


圖12 | 模 7 的反元素配對 2×4、3×5 同餘 1，留下 1 和 6；6! 同餘 −1。

6.3 練習

1 **B13-C06-Q01** 求 φ(18)。

2 **B13-C06-Q02** 求 φ(25)。

3 **B13-C06-Q03** 求 φ(24)。

4 **B13-C06-Q04** 用 Euler 定理求 5^{18} 除以 12 的餘數。

5 **B13-C06-Q05** 用 Fermat 小定理判斷 4^{6} 在模 7 的餘數。

6 **B13-C06-Q06** 在模 7 下，7^{7} 是否同餘 7？7^{6} 又能否同餘 1？

7 **B13-C06-Q07** φ(8)=4，為什麼不能寫 $2^{4}\equiv 1 \pmod 8$？

8 **B13-C06-Q08** 用 Wilson 同餘核對 5 的情形。

9 **B13-C06-Q09** 不必算出 8!，為什麼 n=9 不會符合 Wilson 同餘？

10 **B13-C06-Q10** p=2 時，自反的 1 和 –1 是不同類嗎？Wilson 是否仍成立？

6.4 完整解答

Q01

$18=2\times9$，兩因子互質，$\varphi(18)=(2-1)(9-3)=6$。

Q02

$25=5^2$，恰有 5 個被 5 整除的代表，故 $\varphi(25)=25-5=20$。

Q03

$24=8\times3$ 且互質；$\varphi(8)=8-4=4$、$\varphi(3)=3-1=2$，乘得 8。

Q04

5 與 12 互質，$\varphi(12)=4$。$18=4\times4+2$，故同餘 $5^2=25$，其非負餘數為 1。

Q05

7 為質數，且不整除 4；$p-1=6$，所以餘數是 1。

Q06

7^7 和 7 都是 7 的倍數，所以同餘 0。7^6 也同餘 0，不同餘 1；帶 $p-1$ 的式子不適用於這個底數。

Q07

2 與 8 不互質。直接算 $2^4=16\equiv0$，不是 1，顯示少掉可逆條件就不能取消乘積。

Q08

$(5-1)!=4!=24=5\times4+4$，餘數 4 即 -1 的代表，符合質數情形。

Q09

$8!$ 含因子 3 與 6，乘積被 9 整除，所以 $8!\equiv0\pmod 9$，並非 -1。

Q10

不是不同類，因 $1-(-1)=2$。直接算 $(2-1)!=1\equiv-1\pmod 2$，仍成立，不能搬用兩個不同自反類的計數。

第7章 乘法階與週期

7.1 找最短的返回週期，而不是任一週期

固定 $m\geq 2$，且 a 與 m 互質。從 $a^0\equiv 1$ 開始，逐次乘 a、取餘數，都留在可逆類中。Euler 定理保證第 $\varphi(m)$ 步會回到 1，因此首次正回返至遲在這一步。最小的正整數 d 使 $a^d\equiv 1$，稱為 a 在模 m 下的乘法階。因為是最小正數，不能把剛好找到的回返指數都叫作階。

若 $a^h\equiv 1$ 且 $h>0$，把 h 除以 d，寫成 $h=qd+r$、$0\leq r<d$。由 $a^d\equiv 1$ 知 $a^r\equiv 1$，最小性迫使 $r=0$。所以所有回返指數正是 d 的正倍數，特別有 $d\mid\varphi(m)$。要證明某候選 d 確是階，除了證明 d 會回來，還須排除其較小的正因數。

已知 a 的階 d 時，a^k 的階為 $d/\gcd(d,k)$（k 為正整數）。當 h 為正整數，$(a^k)^h\equiv 1$ 當且僅當 $d\mid kh$。令 $g=\gcd(d,k)$，則 d/g 與 k/g 互質，所以這等價於 $d/g\mid h$。最小的 h 就是 d/g。若 a 不可逆，從 a^0 開始的序列仍可能走進循環，但不能有正次方回到 1：那會直接給 a 的反元素。

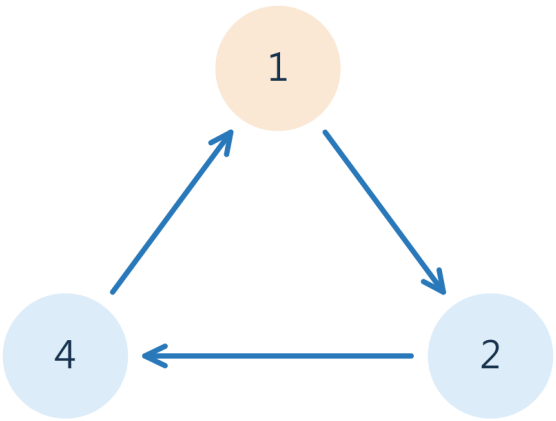


圖13 | 模 7 依次乘 2，從 1 經 2、4 回到 1；首次正回返在第 3 步。

7.2 四個例題

例題1 用回到 1 的第一刻定階

模 7 從 1 起乘 2，得到 2、4、8≡1。前兩步不是 1，第三步第一次回來，故階為 3。φ(7)=6 也是一個返回指數，但不是最小。

例題2 只用階就能減少大指數

3 在模 10 的冪依序為 3、9、7、1，階是 4。202=4×50+2，所以 $3^{202}\equiv 3^2\equiv 9 \pmod{10}$。不用把餘數 2 誤報成冪值。

例題3 取冪後，階可能變短

2 在模 5 的階是 4，因 2、4、3、1 首次在第四步回返。$4\equiv 2^2$，故 4 的階為 $4/\gcd(4,2)=2$，也可核對 $4\not\equiv 1 \pmod 5$，且 $4^2=16\equiv 1 \pmod 5$。

例題4 有循環不表示有乘法階

2 在模 8 不互質。從 1 起冪序列是 1、2、4、0、0、…。0 的循環長度是 1，但沒有正次方同餘 1（mod 8），所以不能稱 2 的乘法階為 1。

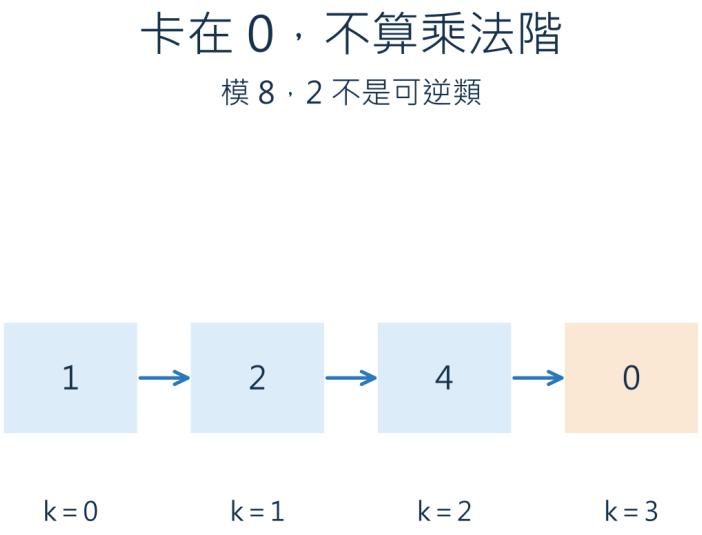


圖14 | 模 8 依次乘 2，從 1 經 2、4 到 0，之後停在 0；這不是乘法階。

7.3 練習

1 **B13-C07-Q01** 求 3 在模 7 的階。

2 **B13-C07-Q02** 已知 2 在模 7 階為 3，求 4 的階。

3 **B13-C07-Q03** 用階求 2^{36} 模 7 的餘數。

4 **B13-C07-Q04** 求 2^{38} 模 7 的餘數。

5 **B13-C07-Q05** 求 9 在模 10 的階。

6 **B13-C07-Q06** 求 2 在模 9 的階，先用 φ 限制。

7 **B13-C07-Q07** 若 $a^{12}\equiv 1 \pmod m$，其階可能是 7 嗎？

8 **B13-C07-Q08** 若 $a^{8}\equiv a^{12}\equiv 1 \pmod m$，階有何限制？

9 **B13-C07-Q09** 求 5 在模 8 的階；它一定等於 φ(8) 嗎？

10 **B13-C07-Q10** 為什麼不可逆的 a 不可能有 $a^{k}\equiv 1$，其中 $k>0$？

7.4 完整解答

Q01

$\varphi(7)=6$，故只需查其正因數 1、2、3、6。前三者的冪餘數為 3、2、6，都不是 1；第 6 次為 1，階是 6。

Q02

因 $4=2^2$，階為 $3/\gcd(3,2)=3$。直接核對 4、2、1 也見第一次在第 3 步。

Q03

$36=3\times12$，是階 3 的倍數，因此餘數 1。

Q04

$38=3\times12+2$，先去掉 12 個完整週期，餘下 $2^2=4$。

Q05

$9\not\equiv1\pmod{10}$，且 $9^2\equiv1\pmod{10}$，故最小正指數是 2。

Q06

$\varphi(9)=6$，階只能是 1、2、3、6；2^1、2^2、2^3 的餘數為 2、4、8，皆非 1。故階為 6。

Q07

不能。能回到 1 已給出可逆性，階必整除 12，但 7 不整除 12。

Q08

階同時整除 8 和 12，因此整除 $\gcd(8,12)=4$。只由這兩式，可能階為 1、2 或 4。

Q09

$5\not\equiv1\pmod{8}$，且 $5^2=25\equiv1\pmod{8}$，故階為 2。$\varphi(8)=4$，只要求階整除 4，並非相等。

Q10

若成立，a·a^(k–1)≡1 就明示 a^(k–1) 是反元素，和不可逆的假設矛盾。

第8章 二次剩餘與Legendre符號

8.1 把平方的配對和判準都放在奇質數模下

取奇質數 p。本冊把不為 0 且可寫成 x² 模 p 的類稱為非零二次剩餘；0 也有平方根，但另外算。若 a≠0（mod p），x²≡y²≡a 則 p∣(x−y)(x+y)，所以 x≡y 或 x≡−y。兩者不同，因 p 為奇數而 x 非零。非零類的平方因此恰成 (p−1)/2 種。

Legendre 符號記作 (a/p)：p∣a 記 0，非零二次剩餘記 1，其餘記 −1。這是三種判定值，不是把 a 除以 p。Euler 判準為 a^((p−1)/2)≡(a/p)（mod p）。要證明非零情形，先平方並用 Fermat，得這個冪的平方同餘 1，故只能是 ±1。若 a=x²，冪是 x^(p−1)≡1。

為何非剩餘必給 −1？在模質數 p 的運算中，每個非零類可逆，乘積為零時至少一因子為零。若多項式有根 r，可用因子定理提出 X−r。對任何另一個根 s，s−r 可逆，因此 s 必是剩下那個多項式的根。反覆提出線性因子便得到，非零多項式的相異根數至多其度數。X^((p−1)/2)−1 已被 (p−1)/2 個非零平方類填滿，不能再有其他根。a≡0 時冪為 0。模合數會出現非零因子的乘積為零，不能搬用配對或根數結論。

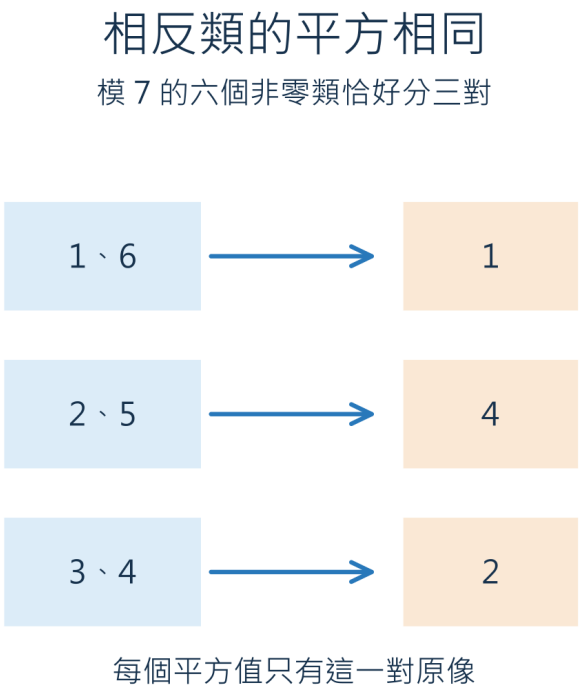


圖15 | 模 7 的非零類分成三對相反數；平方結果分別是 1、4、2。

8.2 四個例題

例題1 模 7：用三對就列完

(1,6)、(2,5)、(3,4) 是相反的非零配對，平方餘數依次為 1、4、2。故 2 的根是 3 與 4，且 $3^2-7=2$。剩餘 3、5、6 不在非零平方的清單內。

例題2 用判準而不逐次試根

判斷 5 在模 11 是否為二次剩餘。$5^2\equiv3$，$5^4\equiv9$，$5^5\equiv9\times5=45\equiv1$；$(11-1)/2=5$，故符號為 1。需要一個根時，可再驗 $4^2=16\equiv5$，但符號本身不輸出根。

例題3 負號判定和零情形不同

$p=5$、$a=2$，判準冪為 $2^2=4\equiv-1$，故符號 -1，沒有根。若 $a=10$，則先看 $5\mid10$，符號為 0；這並非非剩餘，而是對應零類。

例題4 模 8 有四個平方根

1^2、3^2、5^2、7^2 都同餘 1。偶數平方模 8 只能是 0 或 4，故模 8 的解恰四個。不能用奇質數下的「只有 ±一對」排除其餘兩根。

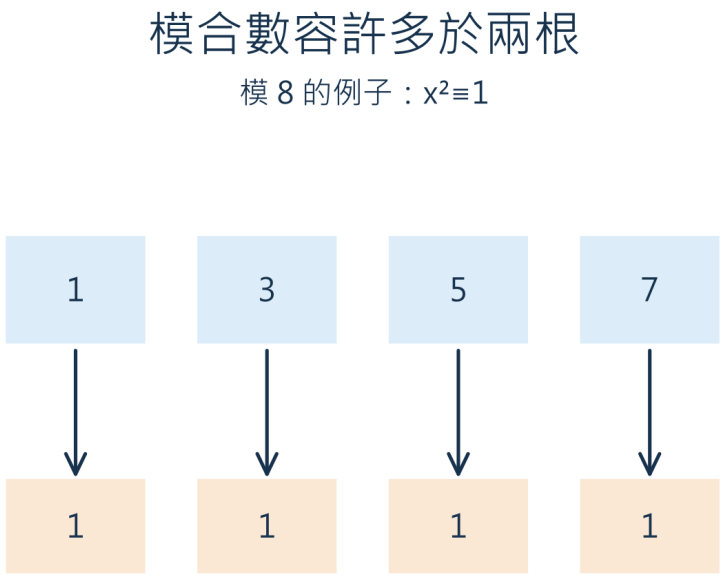


圖16 | 模 8 中 1、3、5、7 全是 1 的平方根，顯示模合數不受兩根結論限制。

8.3 練習

1 **B13-C08-Q01** 列出模 5 的非零二次剩餘。

2 **B13-C08-Q02** (22/11) 的 Legendre 符號是多少？

3 **B13-C08-Q03** 用 Euler 判準算 (3/7)。

4 **B13-C08-Q04** 算 (2/7)，再驗一個平方根。

5 **B13-C08-Q05** 判斷 -1 在模 13 是否是二次剩餘。

6 **B13-C08-Q06** 判斷 -1 在模 7 是否是二次剩餘。

7 **B13-C08-Q07** 解 $x^2 \equiv 9 \pmod{11}$。

8 **B13-C08-Q08** 模 9 解 $x^2 \equiv 0$。為什麼根數不受二次式度數限制？

9 **B13-C08-Q09** 能將本章 Legendre 判準直接用在 $p=2$ 嗎？

10 **B13-C08-Q10** 不列出每個平方值，說明模 11 的非零平方類有幾個。

8.4 完整解答

Q01

兩對相反類 1、4 與 2、3，平方同餘 1、4。這已列完 4 個非零類。

Q02

$11 \mid 22$，所以 22 是零類，依定義符號 0。不是因 22/11 的普通除法得 2 而用 2 判定。

Q03

指數 $(7-1)/2=3$，$3^3=27=4\times7-1$，所以冪同餘 -1，符號 -1。

Q04

$2^3=8\equiv1$，所以符號是 1。$3^2=9\equiv2$，故 3 是根；其相反類 4 也是。

Q05

指數 $(13-1)/2=6$ 為偶數，$(-1)^6=1$，故 Legendre 符號為 1。

Q06

指數 $(7-1)/2=3$ 為奇數，$(-1)^3=-1$，所以符號 -1、無根。

Q07

先驗 3；其相反類 $-3\equiv8$ 也是根。因 11 為奇質數、9 非零，不再有第三個根。

Q08

0、3、6 皆是解，其餘類不被 3 整除、平方也不會被 9 整除。模 9 存在非零類 $3\times3\equiv0$，破壞模質數的根數論證。

Q09

不能。這裡定義限奇質數，$(p-1)/2$ 在 $p=2$ 不是整數，且相反類可能相同。小模數 2 可直接列 0、1 的平方。

Q10

十個非零類每兩個相反類一組，各組有一個平方值。若兩組平方相同，質數引理會讓它們其實是同組，故恰 $10/2=5$ 個。

第9章 p進賦值與Möbius反演

9.1 一邊數質因數，一邊沿因數格拆回原值

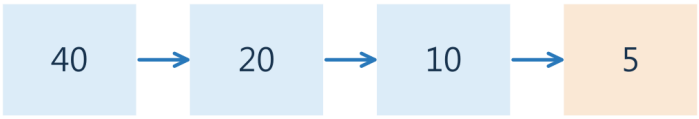
固定質數 p。對非零整數 a，$v_p(a)$ 是 |a| 的質因數 p 的指數，也就是 $p^k \mid a$ 的最大非負整數 k。由唯一分解，非零整數 a、b 滿足 $v_p(ab)=v_p(a)+v_p(b)$。a、b 與 a+b 都非零時，提出較低次的共同因子 p^k，得 $v_p(a+b)$≥較小的賦值；兩賦值不同時，括號內一項不被 p 整除、另一項被 p 整除，因此恰好相等。若兩者同次，括號可能再多出 p 因子；不能把加法當乘法。

Möbius 函數 μ(n) 用於正整數：μ(1)=1；若某個質數平方整除 n，μ(n)=0；其餘若有 r 個相異質因數，$\mu(n)=(-1)^r$。將 μ(d) 對 n 的正因數 d 加總，只有不含平方的因數有貢獻。它們由 n 的相異質數任選子集給出，故 n>1 時正負抵消，總和 0；n=1 時總和 1。

若 $g(n)=\Sigma f(d)$（對所有正因數 $d \mid n$ 加總），要回推出 f(n)，可算 $\Sigma \mu(d)g(n/d)$，仍對同一批因數 d 加總。展開 g 後，一個 f(e)（$e \mid n$）出現的條件是 $de \mid n$，係數就是對 n/e 的所有因數加總 μ。除 e=n 時係數為 1 外，其他全抵消，所以結果是 f(n)。這是有限因數和的反演，不需要談無限級數或收斂。

除得動幾次，就是幾次方

計算 40 的 2 賦值



每條箭頭除以 2

5 已不能再除以 2

$40 = 2^3 \times 5$；$v_2(40) = 3$

圖17 | 40 連除 2 得 20、10、5，第一次到不再能除的 5，已除三次，所以 $v_2(40)=3$。

9.2 四個例題

例題1 用乘法累加指數

$40=2^3\times5$，$12=2^2\times3$，故 $v_2(40\times12)=3+2=5$。回算 $480=2^5\times15$，15 是奇數，沒有漏掉另一個 2。

例題2 加法須看兩邊指數是否相等

40 與 12 的 2 賦值分別 3、2，$52=2^2\times13$，指數為較小的 2。若改把 40 與 56 相加，兩個指數都為 3，$96=2^5\times3$，提升到 5。

例題3 先看平方因數，再決定正負

12 的因數是 1、2、3、4、6、12。4 與 12 都含 2^2，$\mu=0$；2、3 各有一個質因數，$\mu=-1$；6 有兩個，$\mu=1$。連同 $\mu(1)=1$，加總 $1-1-1+0+1+0=0$。

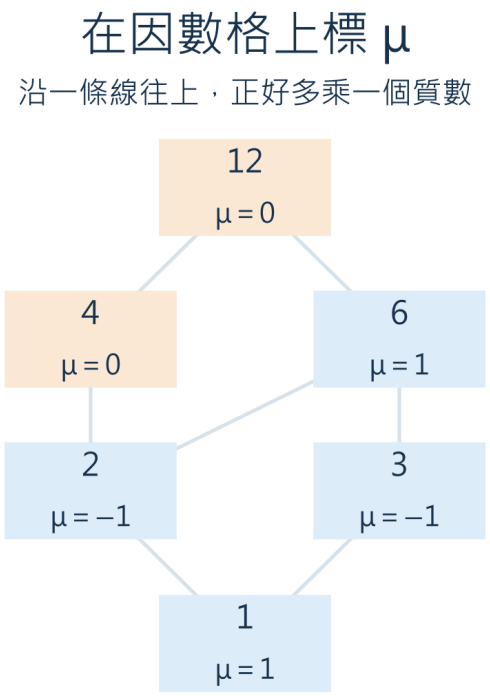


圖18 | 12 的正因數 1、2、3、4、6、12 的 μ 值為 1、−1、−1、0、1、0，總和是 0。

例題4 用反演把總和拆開

若 g(n) 是所有正因數的和，也就是 f(d)=d。取 n=12，g(12)=28、g(6)=12、g(4)=7、g(2)=3；μ(4)=μ(12)=0，不用其對應項。反演為 28−12−7+3=12，正好取回 f(12)。

9.3 練習

1 **B13-C09-Q01** 求 $v_3(54)$。

2 **B13-C09-Q02** 求 $v_2(-72)$，負號影響它嗎？

3 **B13-C09-Q03** 求 $v_5(125\times20)$。

4 **B13-C09-Q04** 求 $v_3(18+27)$，不用先做質因數分解。

5 **B13-C09-Q05** 求 $v_2(12+20)$。為何不能直接取較小指數？

6 **B13-C09-Q06** 算 $\mu(30)$、$\mu(18)$。

7 **B13-C09-Q07** 算 $\mu(1)$、$\mu(12)$，各用哪個條件？

8 **B13-C09-Q08** 列出 $d \mid 6$ 的 $\mu(d)$ 並求和。

9 **B13-C09-Q09** 若 $g(n)=\Sigma\, f(d)$（對 n 的正因數 d 加總），且 $g(n)$ 為 n 的正因數個數，用反演算 $f(6)$。

10 **B13-C09-Q10** 能否把質數 p 改為 4，仍保證用最大 k 的指數在乘法下相加？

9.4 完整解答

Q01

$54=2\times27=2\times3^3$，因子 2 不再被 3 整除，故值為 3。

Q02

取絕對值 $72=2^3\times9$，9 為奇數，所以值是 3。負號不增加任何 2 因子。

Q03

$125=5^3$、$20=5\times4$，兩指數分別 3、1。相乘相加得 4。

Q04

$v_3(18)=2$、$v_3(27)=3$，指數不同，提出 3^2 後括號為 2+3，不被 3 整除，故值 2。

Q05

兩項都是 $v_2=2$。提出 4，括號是 3+5=8，還有三個 2，故結果 2+3=5。

Q06

$30=2\times3\times5$ 不含平方，三個相異質數給 $(-1)^3=-1$。$18=2\times3^2$ 含平方，所以為 0。

Q07

1 是空乘積，特別取 1；12 含質數平方 2^2，取 0。不能把 1 當作有一個質因數。

Q08

因數 1、2、3、6 的值依序 1、−1、−1、1，加總 0，符合 $6>1$ 的抵消。

Q09

6 的因數 1、2、3、6 給 $g(6)-g(3)-g(2)+g(1)=4-2-2+1=1$。原本正好是把每個因數的 1 加起來。

Q10

不能。2 中最大的 4 指數為 0，但 $2\times2=4$ 的指數為 1，不是 0+0。這不是本章的質數賦值。

第10章 數論綜合與證明比較

10.1 同一題先判斷要構造、排除，還是推出矛盾

要證明有解，可直接構造一個並代回，再用週期或公因數說明是否已列完。要證明無解，可先取模，檢查假定的整數解會不會產生不可能的餘數。餘數矛盾足以排除；沒有矛盾只表示通過這一關，不能當作已有原題的解。

反證也常從『假設有解』出發，但要說清矛盾在哪個量出現。例如，若非零整數 a、b 滿足 $a^2=2b^2$，便要求同一整數的 2 賦值同時為奇數和偶數，矛盾不依賴先試多少組 a、b。又如假設所有質數已列完，構造乘積加 1 迫使出現新的質因數。構造和反證可以在同一份證明中合作。

習慣留下三項東西：假設（數的範圍、模數與可逆性）、驗證（把構造的值代回，或找出確切矛盾）、邊界（只證必要或已證充分）。前九章的最小回返、平方配對和因數格都依賴各自前提；不要把有限試驗、證明了的定理與未測的猜想寫成同一件事。

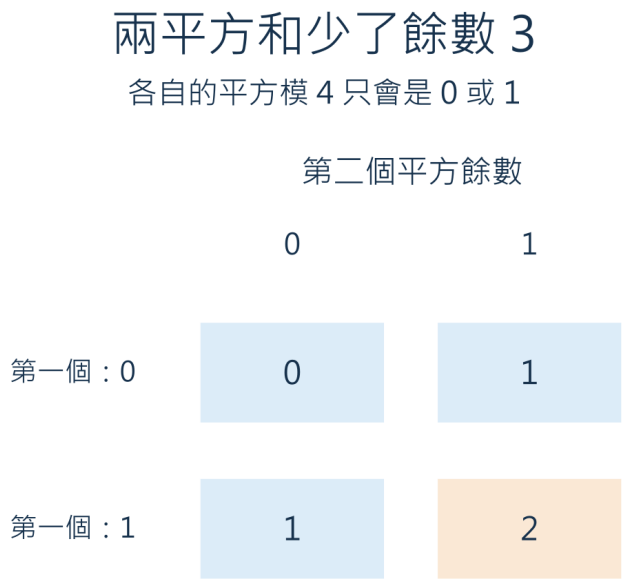


圖19 | 平方模 4 只能是 0、1，兩平方相加只能是 0、1、2，無法得到 3。

10.2 四個例題

例題1 用餘數排除整數解

偶數平方是 4 的倍數；奇數 $(2k+1)$ 的平方為 $4k(k+1)+1$。因此兩個平方的和模 4 只可能是 0、1、2。$2027=4\times506+3$，不可能是兩個整數平方的和。

例題2 乘積加一保證新質因數，不保證質數

假設全部質數只有 $p_1,\dots,p_r$。令 $N=p_1\cdots p_r+1>1$，N 有質因數，但每個 p_i 對 N 都餘 1，故 N 的任何質因數不在原清單，矛盾。方法不要求 N 本身是質數；例如從 2、5、11 得 $111=3\times37$。

例題3 用構造和週期證明全解

求 x≡1（mod 4）、x≡2（mod 9）。令 x=1+4t，需 4t≡1（mod 9）。4×7=28≡1，故 t≡7，得 x=29+36k。29 除以 4、9 分別餘 1、2；週期 36 給全部解。



圖20 | 要證存在可構造並代回；要證不可能可找同餘或賦值矛盾；通過一個模數只表示尚未被排除。

例題4 同一質因數的指數不能同時奇偶

若 √2=a/b，a、b 可取正整數，故 $a^2=2b^2$。左側 v_2 值是 $2v_2(a)$，偶數；右側是 $1+2v_2(b)$，奇數。相等就要求同一個整數有兩個不同奇偶性的賦值，故 √2 不可能是有理數。

10.3 練習

1 **B13-C10-Q01** 只用模 4 判斷 79 能否寫成兩平方和。

2 **B13-C10-Q02** 6 通過模 4 的必要條件，是否真的可以寫成兩平方和？

3 **B13-C10-Q03** 列出 2、3、5，取乘積加一；所得數能被它們整除嗎？

4 **B13-C10-Q04** 例題中的 111 是合數，會破壞新質數的論證嗎？

5 **B13-C10-Q05** 構造 $x\equiv -1 \pmod 3$、$x\equiv 1 \pmod 5$ 的全解。

6 **B13-C10-Q06** 證明 $x\equiv 1 \pmod 2$ 和 $x\equiv 0 \pmod 4$ 無共同解。

7 **B13-C10-Q07** 證明 $n^2\equiv 1 \pmod 4$ 與 n 是奇數互相推出。

8 **B13-C10-Q08** 用 3 賦值證明 $\sqrt{3}$ 不是有理數。

9 **B13-C10-Q09** $ax\equiv 0$ 可以直接推出 $x\equiv 0$ 嗎？附條件或反例。

10 **B13-C10-Q10** 前幾個 n 令 n^2+n+41 都是質數。用一個反例檢查『所有非負整數 n 都如此』。

10.4 完整解答

Q01

79=4×19+3，餘 3；兩平方和的可能餘數只有 0、1、2，因此不能。

Q02

不能。6 模 4 餘 2，沒有被此測試排除；但兩平方都不得超過 6，只能取 0、1、4，沒有兩個能加成 6。這說明通過只是一項必要條件。

Q03

2×3×5+1=31。每個清單內的質數皆整除 30，故 31 除以每一個都餘 1。

Q04

不會。論證需要的是它的一個質因數不在清單，而不是 111 自己是質數。3 和 37 都不在當時列出的 2、5、11。

Q05

令 x=1+5t；模 3 得 1+2t≡2，所以 2t≡1，t≡2。故 x=11+15k；11 確實模 3 餘 2、模 5 餘 1。

Q06

模 4 餘 0 的整數一定被 2 整除，模 2 只能餘 0，與餘 1 矛盾。直接用範圍比試數更快。

Q07

奇數帶入 $(2k+1)^2$ 餘 1；偶數 2k 的平方餘 0。整數非奇即偶，所以若平方餘 1 必為奇數。

Q08

若 $\sqrt{3}=a/b$，正整數 a、b 滿足 $a^2=3b^2$。取 v_3 得 $2v_3(a)=1+2v_3(b)$，一偶一奇，不能相等。

Q09

若 gcd(a,m)=1，兩側乘反元素便可。若條件缺失不行，例如 $2\times3\equiv0\pmod 6$，3 卻不同餘 0。

Q10

取 n=40，得 $40^2+40+41=1681=41^2$。它有正因數 41，且 1<41<1681，故原命題為假。