同餘數及質數在密碼學上的應用

黃文璋
國立高雄大學應用數學系

1 前言

讀過金庸(1996)所著射鵰英雄傳的人皆知, 有一位住在黑沼中, 自稱神算子的瑛姑, 武功高強, 數學卻不甚高明, 經常苦思數月解一些算術或代數中的問題。郭靖與黃蓉因逃避裘千仞的追蹤, 誤入瑛姑住的污泥湖沼, 臨離開前, 黃蓉用竹杖在地下細沙上寫了三道算題。其中一道爲"鬼谷算題":今有物不知其數, 三三數之賸二, 五五數之賸三, 七七數之賸二, 問物幾何? 黃蓉對郭靖說"這三道題目, 半年之內她必算不出, 叫她的花白頭髮全都白了"。

事實上黃蓉所出的問題, 便是後來被西方數學家稱爲中國剩餘定理(Chinese Remainder Theorem)之一特例, 最早出現在"孫子算經"中(因此在中國亦稱此定理爲孫子定理), 後來流傳於民間, 以不同的故事出現, 如"韓信點兵"即是一例。劉邦想捉拿韓信, 但不知他究竟實力如何, 便問韓信有多少兵卒? 韓信答"啓奏陛下, 兵不知其數, 三三數之賸二, 五五數之賸三, 七七數之賸二"。陳平 絞盡腦汁也無法算出, 連張良亦說"兵數無法算, 不可數"。劉邦聞後心怯, 韓信也因此暫時逃過一劫。後來有一些詩或口訣給出此題之解, 如: 三人同行七十稀, 五樹梅花廿一枝, 七子團圓正半月, 除百零五便得知(其含義可參考莫宗堅(1970))。我們只是想先藉上述故事說明自古以來, 人們對餘數便很感興趣。

自小學學習除法, 我們便知道餘數; 學習因數分解, 也必接觸質數(prime, 或稱prime number) 。經由討論同餘數及質數, 可使大家對整數的基本性質, 便能有一充分的了解 。

2 同餘數

設a, b爲二整數, n爲一正整數, 若$a-b$可被n整除, 或說$a-b$爲n之整數倍, 則稱a, b 對模 (modulus)b 同餘(congruent), 記作

$$a \equiv b \pmod{n}$$

(稱爲a is congruent to b modulo n) 。反之, 若a與b對模n不同餘, 則以

$$a \not\equiv b \pmod{n}$$

表之。例如,$32 \equiv 5 \pmod{3}$,$3 \not\equiv -2 \pmod{4}$。可看出$a \equiv b \pmod{n}$,若且唯若分別以a, b除以n, 得到相同的餘數 。

同餘之概念在日常生活中亦常遇到。如我國民俗中的十二生肖, 在數某人屬那一生肖時, 即爲以12爲模之算法 。而天干地支即爲以60爲模之計年法 。再如若今天是星期二, 18天後是星期幾? 將2+18去除以7得餘數6, 即知18天後爲星期六 。很多時候我們就是對餘數有興趣 。如求十進位裡整數123在7進位下的表示法 。先以123除以7, 得商17, 餘數4, 所以最末項爲4 。次以17除以7, 得商2, 餘數3, 故在7進位下, 123可表示爲234_7 。

同餘關係滿足下述三性質:

(i) 反身性(reflexivity) 。即對每一整數a及正整數$n, a \equiv a \pmod{n}$ 。

(ii)對稱性(symmetry) 。即對任二整數a, b及正整數n,若$a \equiv b \pmod{n}$, 則$b \equiv a \pmod{n}$ 。

(iii)遞移性 (transitivity) 。即對任三整數a, b, c及正整數n, 若$a \equiv b \pmod{n}$ 且$b \equiv c \pmod{n}$,則$a \equiv c \pmod{n}$ 。

在數學上, 一關係若具有這三個性質便稱爲一等價關係 (equivalence relation) 。例如三角形的相似 即爲一等價關係 。又同餘的概念是高斯(Gauss, 1777-1855)在他於西元1801年出版的算學研究(Disquisitiones Arithmeticae) 一書中最先引進的 。同餘關係滿足此三性質之證明皆不難, 因此留給讀者自行練習 。由此三性質, 任給一整數k, 可以將全部整數分爲

若干類, 在同一類中, 任二數皆同餘, 而在不同類中任二數皆不同餘。例如, 可將所有整數分爲4類: $4n$, $4n+1$, $4n+2$, $4n+3$, 即分別表除以4餘0, 1, 2及3。當然諸如$4n+3$類與$4n-1$類是同一類。而在以4爲模之下, 整數的平方只有$4n$及$4n+1$二類。

同餘亦滿足下述性質:

(iv)設有四整數a, b, c, d及正整數n,若$a \equiv b \pmod{n}$且$c \equiv d \pmod{n}$,則$a+c \equiv b+d \pmod{n}$,且$ac \equiv bd \pmod{n}$。

例**1.**由性質(iv)得, 若$a \equiv b \pmod{n}$, 其中a, b爲整數, n爲正整數, 則對每一非負整數k, $ka \equiv kb \pmod{n}$, 且$a^k \equiv b^k \pmod{n}$。

例**2.**因$5 \equiv 2 \pmod{3}$且$7 \equiv 1 \pmod{3}$,故$12 \equiv 3 \pmod{3}$, $35 \equiv 2 \pmod{3}$,
$5^4 \equiv 2^4 \pmod{3}, 5^2 \cdot 7 \equiv 2^2 \cdot 1 \pmod{3}$。

至於除法則不成立。例如, $2 \cdot 2 \equiv 8 \cdot 2 \pmod{4}$,且$2 \not\equiv 0 \pmod{4}$。但$2 \not\equiv 8 \pmod{4}$。不過卻可證明對任意整數$a, b, c, d$及正整數$n$, 若

$$ac \equiv bc \pmod{n}, \text{且} (c, n) = 1,$$

則$a \equiv b \pmod{n}$。在此對任二整數a, b, 以(a, b)表其最大公因數, $(a, b) = 1$即表此二整數互質(relatively prime)。而一大於1之自然數p, 若除了1與p之外無其他因數, 則p稱爲質數, 否則稱爲合成數(composite number)。至於1 則既非質數也非合成數。對二整數a, b, 以$a|b$表b可被a整除, 以$a \nmid b$表不能整除。

例**3.**分別求2^{31}除以11之餘數,及3^{100}除以5之餘數。

解.首先

$$2^{30} = (2^6)^5 = 64^5,$$

而$64 \equiv 9 \pmod{11}$,故

$$64^5 \equiv 9^5 \pmod{11}。$$

再用類似的手法得

$$9^5 = 81 \cdot 81 \cdot 9 \equiv 4 \cdot 4 \cdot 9 \equiv 1 \pmod{11}。$$

故知$2^{30} \equiv 1 \pmod{11}$,而$2 \equiv 2 \pmod{11}$,故$2^{31} \equiv 2 \pmod{11}$, 即餘數爲2。另外, 亦可如下得到$2^{30} \equiv 1 \pmod{11}$。

$$2^{30} = (2^5)^6 = 32^6 \equiv (-1)^6 = 1 \pmod{11}。$$

其次, 如下即得3^{100}除以5之餘數爲1:

$$3^{100} = (3^4)^{25} = (81)^{25} \equiv 1^{25} = 1 \pmod{5}。$$

例**4.**分別求$2^{1,000}$之個位數字及$2^{2,000}$之末兩位數字。

解.一數之個位數字即爲此數除以10之餘數。因$2^5 = 32 \equiv 2 \pmod{10}$, 故

$$2^{1,000} = (2^5)^{200} \equiv 2^{200} \equiv (2^5)^{5\cdot 8} \equiv (2^5)^8 \equiv 2^8 = 256 \equiv 6 \pmod{10}。$$

即得$2^{1,000}$之個位數字爲6。

其次,因$2^{10} = 1{,}024 \equiv 24 \equiv -1 \pmod{25}$,故

$$2^{2,000} = (2^{10})^{200} \equiv (-1)^{200} = 1 \pmod{25}。$$

即得$2^{2,000}$之末兩位可能爲1, 26, 51或76 。因顯然$2^{2,000}$爲4的倍數, 故末兩位爲76 。

底下亦爲一有趣的結果。

例**5.**試證對任一正整數n, 必存在另一正整數m, 使得$nm = 9\cdots 90\cdots 0$ 。

證明.分別以9, 99, 999,$\cdots$除以n, 各得餘數$r_1, r_2, \cdots$, 且$0 \le r_a < n, \forall a \ge 1$。故存在$i, j, i < j$,使得$r_i = r_j$。亦即存在整數$k_i, k_j \ge 0$, 且$k_j > k_i$, 使得

$$9\cdots 9 = k_i n + r_i,$$

且

$$9\cdots 9\cdots 9 = k_j n + r_i。$$

將上二式兩側分別相減即得

$$9\cdots 90\cdots 0 = (k_j - k_i)n,$$

得證。

例**6.**欲檢驗一整數是否爲37的倍數, 可有如下的作法。首先留意到$10^3 \equiv 1 \pmod{37}$。故原數與將其自右起每三位數相加所得之新整數, 對37 同餘(爲什麼?)。如設$N = 15{,}653{,}782$, 則

$$N \equiv 15 + 653 + 782 = 1{,}450 \equiv 1 + 450 = 451 \equiv 7 \pmod{37}。$$

故N非37的倍數,且N除以37餘7。

次求37^{13}除以11之餘數。首先因$37 \equiv 4 \pmod{11}$。故

$$37^{13} \equiv 4^{13} = (4^3)^4 \cdot 4 \equiv (-2)^4 \cdot 4 \equiv 9 \pmod{11}。$$

例**7.**(ISBN碼). 現今每本書皆有一國際書碼(International Standard Book Number, 簡稱ISBN), 共有十個數字。例如, 某本書之ISBN碼爲0-02-424201-2, 其中第一個數字表語言(如0表英文), 下二數字表出版社(如02表Macmillan Publishing Company), 接著的6個數字爲該出版社對該書給的編號。最後一個數字則爲檢查碼, 以使此十個數字$x_1, x_2, \cdots, x_{10}$ 滿足下述檢查式

$$\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}。 \tag{1}$$

不過連字號"-"有時會出現在不同的位置。例如, 有一本在台灣發行的書, 其編號爲957-21-0686-4, 另一本爲957-708-050-2,皆爲十位數字, 且皆滿足(**??**)式。

ISBN碼可查出(i)任何一單一的錯誤, 或(ii)任何因兩個數字位置互相交換所產生的錯誤。若收到一書碼$y_1, y_2, \cdots, y_{10}$,則求其$S = \sum_{i=1}^{10} i y_i$。若$S \equiv 0 \pmod{11}$, 則$y_1, y_2, \cdots, y_{10}$爲一合法的書碼,且我們視爲沒有錯誤。若$S \not\equiv 0 \pmod{11}$, 我們知道必有錯誤, 而會要求重新傳送書碼。關於這方面的討論可參考Hill (1990/91)。

例**8.**求某日爲星期幾。

有時我們需要知道某年某月某日爲星期幾, 同餘在這裡也用得上。我們給一做法, 其中年代皆以西元計。

每年的天數並不相同, 爲了使閏年多出的那天爲每年最後一天, 我們將月份重排, 使3 月成爲第一個月, 而次年的1月即爲11月, 次年

的2月即爲12月。如1994年1月1日成爲1993年11 月1日。對某一特定的日子, 以C表該日之世紀數, y表年代的末兩位, m表月份, d表日期,該日之星期則以D表之。首先選定1600年1月(原來的3月)1日爲起始日, 該日設爲星期t。因

$$365 \equiv 1 \pmod 7,$$

故若無閏年, 則$t + (100C + y - 1600)$除以7之餘數爲該年之1月(原來的3月)1日的星期。但因每4年有一次閏年, 而非4的倍數的整世紀(如1700, 1800, 1900年)不是閏年, 所以每年1月(原來的3月)1 日的星期應爲下數除以7之餘數:

$$A = t + (100C + y - 1600) + [\frac{1}{4}(100C + y - 1600)] - [\frac{3}{4}(C - 15)],$$

其中$[\cdot]$表最大整數函數 (greatest integer function), [ ]又稱爲高斯符號,即對每一實數a, $[a]$ =小於或等於a之最大整數,如[7.2]=7, [6]=6。利用底下二簡單的性質:

(i)若a爲一整數, b爲任一實數,則$[a + b] = a + [b]$,

(ii)若a, b爲整數,n爲一正整數,且$a \equiv 0 \pmod n$, 則$ab \equiv 0 \pmod n$,

則A可如下地簡化:

$$\begin{aligned} A &= t + 125C - [\frac{3}{4}(C + 1)] + y + [\frac{1}{4}y] - 1988 \\ &\equiv t - 2C + [\frac{1}{4}C] + y + [\frac{1}{4}y] \pmod 7 。 \end{aligned}$$

這裡用到$-[3(C + 1)/4] = -C - [3/4 - C/4] = -C + [C/4]$。

現再加上月份及日期的考慮, 如因3月(新算法的1月)有$31 \equiv 3 \pmod 7$天, 故4月1日的星期爲3月1日的星期加3(以7爲模之餘數); 而4月(新算法的2月) 因有$30 \equiv 2 \pmod 7$天, 故5月1日的星期又爲4月1日的星期加2(以7爲模之同餘數), 餘此類推。我們發現數列$[\frac{1}{5}(13m - 1)] - 2, m = 1, \cdots, 12$,剛好能滿足因考慮月份而需加上的數,見下數列:

$$\left.\begin{array}{ll} m = 1 \quad (\text{原來3月}), & [\frac{1}{5}(13 - 1)] - 2 = 0 \\ m = 2 \quad (\text{原來4月}), & [\frac{1}{5}(26 - 1)] - 2 = 3 \end{array}\right) \begin{array}{l} 3 \\ 2 \end{array}$$

$$\left.\begin{array}{ll} m=3 & (\text{原來5月}), \quad [\frac{1}{5}(39-1)]-2=5 \\ m=4 & (\text{原來6月}), \quad [\frac{1}{5}(52-1)]-2=8 \end{array}\right) 3$$
$$\vdots$$

因此星期爲

$$\begin{aligned} D &\equiv A+[\frac{1}{5}(13m-1)]-2+d \\ &\equiv t-2C+[\frac{1}{4}C]+y+[\frac{1}{4}y]+[\frac{1}{5}(13m-1)]-2+d \pmod 7 \text{。} \end{aligned}$$

再利用一已知星期的日期即可求出t。如西元1999年1月1日爲星期五, 即$C=19, y=98, m=11, d=1$。則

$$\begin{aligned} & t-38+[\frac{19}{4}]+98+[\frac{98}{4}]+[\frac{142}{5}]-2+1 \\ =\ & t-38+4+98+24+28-2+1 \\ =\ & t+115 \\ \equiv\ & 5 \pmod 7, \end{aligned}$$

因此$t=2$。故星期的公式爲

$$(2) \quad D \equiv d-2C+[\frac{1}{4}C]+y+[\frac{1}{4}y]+[\frac{1}{5}(13m-1)] \pmod 7 \text{。}$$

註. 16世紀前的曆法與現在的不相同, 40世紀後可能又有變化(見Rogosinski (1972/73)), 不過現今的前後幾世紀(??)式皆可適用。

舉一例子來看看: 民國50年之教師節爲星期幾? 本例即$C=19, y=61, m=7, d=28$。代入(??)式得

$$D \equiv 28-38+4+61+15+18=88 \equiv 4 \pmod 7,$$

即該日爲星期四。

3 質數

關於質數, 有一些大家熟知的性質。如每一個大於1之自然數, 至少有一質因數; 及一不爲質數之自然數n, 必有一質因數$a \le \sqrt{n}$。另外, 歐

幾里得(Euclid ,約在西元前375-330年, 他寫過原本(Elements), 也被稱爲幾何原本), 就證出質數有無限多個。其證明不難: 假設質數只有有限多個, 設有k個, 且以$n_1, n_2, \cdots, n_k$表之。則易見$N = n_1 \cdot n_2 \cdots n_k + 1$亦爲一質數,而$N$比$n_1, n_2, \cdots, n_k$皆大, 此矛盾導致質數有無限多個。歐幾里得的證明可說極簡單不過, 但此證明並未對新的質數給出任何資訊。即若已知首k個質數$n_1, n_2, \cdots, n_k$, 則雖知質數有無限多個, 卻無法指出下一個質數爲何。這是數學理論令人嘆賞之處,我們並不知無限多個質數在那裡, 但我們"確實"知道其存在。這與宗教裡的一些信念(譬如相信神的存在), 往往是主觀的相信, 是不一樣的。歐幾里得亦證明每一大於1之整數可分解成質因數之乘積, 且分解法爲唯一, 此結果被稱爲算術基本定理(Fundamental Theorem of Arithmetic)。另外, 由下述定理立即也可導至質數有無限多個。在此$n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1, n \geq 1$, 且$0! = 1$。

定理1. 設$n > 2$爲一整數, 則介於n與$n!$ 間至少有一質數。

[證明]: 因$n > 2$,故$n!-1 > 1$, 因此$n!-1$至少有一質因數p。由於$p \leq n!-1$, 故$p < n!$。但$p \leq n$不成立, 否則$p|n!$, 如此一來$p|(n!-(n!-1))$, 即$p|1$不合, 故$p > n$。得證。

在西元1878年, Kummer (1810-1893)如下證明質數有無限多個: 設只有有限多個質數$n_1 < n_2 < \cdots < n_k$。令$N = n_1 n_2 \cdots n_k > 2$。則$N-1$與$N$必有某一共同的質因數$n_i \geq 2$(爲什麼?)。如此$n_i$可除盡$N-(N-1) = 1$。此矛盾導至質數有無限多個。

此證明也是簡單美妙地令人喜愛。三言兩語就解決了這一關於無限的問題。其他還有許多不同的關於質數有無限多個的證明, 在此不再多介紹。

質數既然有無限多個, 但其出現有沒有什麼規律呢? 上定理只是告訴我們, 隨著n的增大, 在愈來愈大的區間$(n, n!)$中, 一直可找到一個質數, 但並沒有指出該質數爲何? 除了2以外的質數皆爲奇數,奇數又可寫成$4n+1$或$4n-1$(即$4n+3$)等二種型式。可證明型如$4n+1$的質數有無限多個, 型如$4n-1$的質數也有無限多個(見習題第27題)。還有一些其他的算術級數(即等差級數), 皆可證明它們中包含無限多個質數(見林聰源譯(1976))。若以$\phi(n)$表不超過n之質數的個數, 在西元1896年, Hadamard 與de la Vallie Poussin 證出(高斯在西元1792 年便提

出此猜測,請留意那時高斯的年齡), 當n趨近至無限大時, $\phi(n)$ 與$n/\log n$的比值趨近至1。由此可看出

(i) 質數的個數有無限多個(此因n趨近至無限大時, $n/\log n$亦趨近至無限大);

(ii) 質數在自然數中甚爲稀薄,此含意爲n趨近至無限大時, $\phi(n)/n$ 趨近至0。

質數雖有無限多個, 但卻無法明確地以一公式表示出所有質數。又質數的分佈很不規則, 很難預料在什麼地方會出現下一個質數。在過去許多數學家均曾致力於找出一整係數的多項式以造出質數。例如,

令$f_1(n) = n^2 - n + 41$,則當$n = 0, 1, \cdots, 40$時, $f_1(n)$皆爲質數;

令$f_2(n) = n^2 + n + 17$,則當$n = 0, 1, \cdots, 15$時, $f_2(n)$皆爲質數;

令$f_3(n) = 2n^2 + 29$,則當$n = 0, 1, \cdots, 28$時, $f_3(n)$皆爲質數。

上述f_1是歐拉(Euler, 1707-1783)所給的, f_3是西元1798年時Legendre (1752-1833) 所給的。甚至亦可證明, 當$0 \le n \le 11{,}000$時, $n^2 - n + 72{,}491$皆爲質數。其實不難證明(這也是歐拉證出的) 無法找到一整係數之多項式$f(x)$, 使得分別以正整數$1, 2, \cdots$代入x, 皆得到質數(見習題第7題)。至於是否對任給之一正整數N, 必存在一質數p, 使得當$0 \le n \le N$時, $n^2 - n + p$皆爲質數, 則是一仍未解決的問題。

事實上, 不但無法指出無限多個質數在那裡, 連要檢驗一數是否爲質數也相當困難。最根本的困難是, 對整數的分解, 沒有什麼規律。例如,$120 = 2^3 \cdot 3 \cdot 5$, $121 = 11^2$, $122 = 2 \cdot 61$, $123 = 3 \cdot 41, \cdots$。對相鄰的整數, 其因數可說關連性很小。對一正整數n, 我們知道只要以不超過$\sqrt{n}$之質數去試除n, 若都除不盡, 則n爲質數。但當n很大時,$\sqrt{n}$其實也很大, 此時在$\sqrt{n}$之前的質數便仍很多, 要將那些質數都找出已非易事,還要去除n,其艱鉅可想像。所以除了快速的計算機之外,還要有一些好的方法來協助檢驗才行。

4 費馬小定理

底下我們給一簡單的非質數之檢定法, 這就是著名的費馬(Fermat, 1601-1665)小定理(Fermat's Little Theorem)。

定理2. 設p爲一質數, 則對每一正整數m, $m^p \equiv m \pmod{p}$。

[證明]:首先由二項式定理(Binomial Theorem)可得下述展式:

$$(x+y)^p = x^p + \sum_{r=1}^{p-1} \binom{p}{r} x^{p-r} y^r + y^p,$$

其中二項式係數 (binomial coefficient)

$$\binom{p}{r} = \frac{p!}{r!(p-r)!} = \frac{p(p-1)\cdots(p-r+1)}{r!} \text{。} \tag{3}$$

若p爲質數,則易見$\binom{p}{r}$爲p之倍數, $r = 1, \cdots, p-1$,即$\binom{p}{r} \equiv 0 \pmod{p}, r = 1, \cdots, p-1$。故

$$(x+y)^p \equiv x^p + y^p \pmod{p} \text{。} \tag{4}$$

由上式得

$$\begin{aligned} 2^p &= (1+1)^p \equiv 1^p + 1^p \equiv 2 \pmod{p}, \\ 3^p &\equiv (2+1)^p \equiv 2^p + 1^p \equiv 3 \pmod{p}, \\ &\vdots \\ m^p &\equiv m \pmod{p}, \end{aligned}$$

得證。

由定理2, 可得到下述推論, 當然若先有系理1, 也可得定理2。

系理1. 設p爲一質數, m爲一正整數, 且$(m,p) = 1$, 則

$$m^{p-1} \equiv 1 \pmod{p} \text{。} \tag{5}$$

費馬小定理最初是在西元1640年時, 費馬寫給他朋友的一封信中提到。歐拉在西元1736 年給了一目前所知道最早的證明, 雖然一般認爲萊布尼茲(Leibnitz, 1646-1716) 也知道如何證明, 只是他並未公開其證法。歐拉後來又推廣此結果至更一般的情況。

定理3.設$(m,n) = 1$, 則$m^{\pi(n)} \equiv 1 \pmod{n}$。

其中對$\forall\, n \geq 1$, $\pi(n)$表小於n, 且與n互質的自然數之個數。若n爲一質數, 則$\pi(n) = n-1$, 因此系理1的確爲定理3之一特例。試取$m = 3, n = 10$, 則$(m,n) = 1$。因小於10且與10互質的有1, 3, 7, 9等,故$\pi(10) = 4$ 。而果

然$3^4 \equiv 1 \pmod{10}$。定理3有許多不同的證明, Heinrich and Horak (1994) 給了一基本上是用組合學 (combinatorial) 的證法,也可以參考。

系理1可用來檢驗一數是否不爲質數。即以2^{n-1}去除以n,若其餘數不爲1, 則n爲一合成數。不過系理1之逆不眞。最簡單的一例爲

$$2^{340} \equiv 1 \pmod{341},$$

但341並非一質數。另外, 尚有$91|(3^{90}-1)$,$15|(4^{14}-1)$, 但91及15皆非質數。不過有人統計過, 在10^{10}之內, 只要n能整除$2^{n-1}-1$, 則其中約有99.9967% 爲質數。若先剔除那些能整除$2^{n-1}-1$的合成數, 則此法倒是一有效的鑑定質數的方法。西元1950年, Lehmer 證出161,038爲$2^{161,038}-2$之因數。西元1951 年, Beeger證出存在無限多個偶數n, 使得$n|(2^n-2)$。故有無限多個偶數反例, 使得定理2之逆不眞。至於有無限多個奇數反例, 使得定理2之逆不眞,可如下證明。

設$n = ab$爲一奇合成數, 其中$a, b > 1$,且$n|(2^n-2)$。這種n確實存在, 如上所述, $341 = 11 \cdot 31$爲一例。若能證出存在一奇合成數$m > n$,且$m|(2^m-2)$, 便得證了。取$m = 2^n - 1 > n$,爲一奇合成數(爲什麼?) 因$n|(2^{n-1}-1)$, 故存在正整數k, 使得$2^{n-1}-1 = kn$。因此

$$2^{m-1} = 2^{2^n-2} = 2^{2(2^{n-1}-1)} = 2^{2kn} = (2^n)^{2k}。$$

故

$$2^{m-1}-1 = (2^n)^{2k}-1 = (2^n-1)\sum_{i=0}^{2k-1}(2^n)^i = m\sum_{i=0}^{2k-1}(2^n)^i。$$

因此$m|(2^{m-1}-1)$,且$m|(2^m-m)$,證畢。

對一正整數n, 只要$1 \le m < n$,則當n爲質數時,$(m,n) = 1$。現若$m^{n-1} \equiv 1 \pmod{n}$, 我們已指出此時並不一定導至$n$爲質數。但可換另一$m$ 試試, 只要找到一m, 使得$m^{n-1} \not\equiv 1 \pmod{n}$, 則由系理1知, n必不爲質數, 見下例。

例**9.**取$n = 15$, 則

$$11^{14} = 121^7 \equiv 1^7 = 1 \pmod{15}。$$

但若再試$m = 2, 3, \cdots, 10$, 便發現除了$m = 4$外, $m^{14} - 1$皆非15的倍數。故15 不是質數。只要有一m, 使得$m^{14} - 1$不能被15除盡, 由系理1便得知15不爲質數。

不過卻存在非質數之整數n, 使得對每一正整數m, 只要$(m, n) = 1$,則$m^{n-1} \equiv 1 \pmod{n}$; 或等價地說, 使得對每一整數$m$,$n|(m^n - m)$。561 (=$3 \cdot 11 \cdot 17$) 爲最小的這種整數。由於Carmichael在西元1910年發現561有此性質, 故這種數稱爲Carmichael數(Carmichael numbers)。自Carmichael 起, 數學家便想知道究竟有那些這種數。在1,000之內只有561, 下一個爲1,729(= $7 \cdot 13 \cdot 19$), 順便問你此數尚有何特性呢? 在10,000之內共有7個, 在10^6之內則共有43個。

利用計算機, 英國劍橋大學(Cambridge University)的Pinch在西元1992年初發現在10^{15} 之內, 共有105,212 個Carmichael數。數學家於是猜測, 如同質數有無限多個, 也存在無限多個Carmichael 數。所以使用費馬小定理來檢驗質數, 其風險仍是存在的。即若$n \nmid (m^n - m)$時, 可決定n爲合成數, 但若$n|(m^n - m)$時, 就要再輔以其他檢定法了。

近年來美國喬治亞大學(University of Georgia) 數學系的三位教授Granville, Pomerance 及Alford 證出, 存在一正整數k, 使得$x > k$時, 在1與x間之Carmichael數超過$x^{2/7}$個。雖他們並不知道k之值究竟有多大, 他們卻可證明k存在。因此Carmichael數有無限多個。看到此結果你會不會有些感嘆, 兩千多年前歐幾里得輕描淡寫地證出質數有無限多個, 但直到今日與質數相關的問題, 仍吸引著許多數學家窮年累月地探討(Carmichael數的討論, 見Delvin (1992/93)) 。

回頭看費馬小定理之另一推論,證明便略過了。

系理2.(Wilson's Theorem).設p爲一質數, 則

$$(p-1)! \equiv -1 \pmod{p} \text{。} \tag{6}$$

例如,$(5-1)! \equiv -1 \pmod{5}$。設$A = mn$不爲一質數, 其中$2 \le m, n \le A - 2$。則$m|(A-1)!$, 因此$m \nmid ([(A-1)! + 1])$。由此便得$(A-1)! \nmid -1 \pmod{A}$,即$(A-1)! \not\equiv -1 \pmod{A}$。即證出系理2之逆成立(記住系理1之逆並不成立)。因此系理2可用來檢驗一正整數是否爲質數。不過並不實用, 因$A!$成長極快, 且並無快速的方法來計算$A!$。

對檢驗一很大的數是否爲質數, 當然要藉助計算機, 只是要給計算機一有效的程序來檢驗。有些特別的數, 是有較好的方法。例如, 對梅仙尼數(Mersenne number), 也就是型如$2^n - 1$ 的正整數, 其中n爲一質數, 利用Lucas-Lehmer法(見"完全數與梅仙尼質數"一文),可"很快速地"檢驗出是否爲質數。例如, 當$n = 86{,}243$, 在西元1982年, 以CRAY-1電腦, 花了1小時多一點, 便證實爲質數。

不過對於一隨意給的整數, 一般而言, 除了費馬小定理, 就沒有較有效的方法來檢驗它是否爲質數。至於對一合成數, 如果它的因數很大的話, 要將其因數找出, 那是更困難的。這就是爲什麼那些已被證實爲合成數的梅仙尼數,往往我們仍無法分解。再如於西元1909年便已證出$2^{128}+1$及$2^{256}+1$皆爲合成數, 但前者直至西元1970年才被分解, 後者至西元1978年仍未被分解。值得一提的是, 近年來英國數學家J. M. Pollard基於機率論裡的想法, 發展出一套分解整數的方法, 其法"有時"會較傳統的分解法快速, 可參考Godwin (1978/79)。

5 在密碼學上的應用

目前對一任給的兩百位的合成數, 即使窮宇宙的壽命, 也極不可能分解。你一定覺得我們言過其實, 現試說明如下: 若採用試除法(分解其實有一些較快的方法), 假設計算機一秒鐘可做一億次除法, 則一年約可做$3.1536 \cdot 10^{15}$次除法。而分解一兩百位的數約要做10^{100}次試除, 換句話說, 約要$3.17 \cdot 10^{84}$ 年。而估計地球的壽命不過約$5 \cdot 10^9$年而已。就算計算機運算速度增快, 一秒鐘可做一兆次(10^{12}) 除法, 仍約要$3.17 \cdot 10^{80}$年。目前最安全的密碼技術就是利用這種整數之難以分解的特性。這套技術是美國麻省理工學院 (Massachusetts Institute of Technology, 簡稱MIT) 的幾位數學家Rivest, Shamir 及Adleman於西元1977年提出, 論文並於1978年刊登的, 所謂公開鑰匙密碼法 (Public-Key Cryptography)。

通常號碼鎖若有四位數字, 則最多試一萬次, 便可解開。對於下圖, 若先猜出它是加法,則花些時間嘗試, 也可將$a, b, c, \cdots, j$等分別代表的數字

解出:

$$\begin{array}{cccccccccc} & a & b & e & g & j & d & i & h & f & c \\ & f & h & b & e & i & j & a & g & d & c \\ \hline c & e & f & d & b & e & g & b & c & f & b \end{array} \tag{7}$$

只要時間夠長, 任何密碼總可解出。Rivest 他們的方法, 就是利用整數之難以分解的性質來編碼, 因此在敵方能解碼之前, 便已成功地達到傳遞情報的目的。我們略述其方法如下。

用數學語言來說, 所謂編碼與解碼, 只不過是一些函數與反函數的應用, 我們以圖1 來說明:

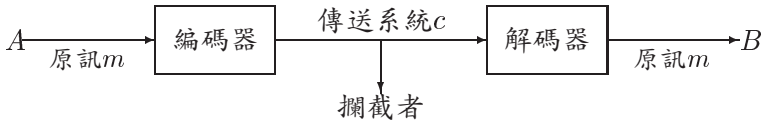

圖1.密碼傳送圖

設A想送一訊息m給B, 但A將m僞裝, 使得即使被攔截也無法解讀此訊息。也就是經過編碼器, 傳送出密碼c,B收到密碼c 之後, 再設法轉換爲原來的訊息m。事先A與B要約定好, 如何編碼。由於攔截者有可能知道編碼的方式, A與B就須約定好一隻祕密的鑰匙。這隻祕密鑰匙就是用來防止攔截者即使攔到密碼c, 也無法解出m。因此A就像有一袋子的函數,依據他與B約好的鑰匙k, A選一函數。若以f_k表此函數, 則$c = f_k(m)$。由於B知道k,因此B知道A採用的函數是f_k, 故經由f_k之反函數, 便可由c得到m。

我們給一簡單的例子。首先分別以數字0至25代表英文字母A至Z。編碼的方式是加一整數k後以26爲模, 鑰匙k即爲加數, 因此1至25的整數皆可以當作鑰匙(若k爲0便沒有達到僞裝的目的)。例如, 若$k = 7$, 而訊息爲CAT, 則密碼爲JHA。收到JHA後, 將每個字母減7, 便得訊息CAT。

一旦知道編碼的函數, 只要決定其反函數便可解碼。對於上例, 解碼專家經過一段時間比對(例如, 英文中常有冠詞a, the等), 不難看出編碼的方式是將每個字母加7, 便可輕易破解了。任何密碼幾乎沒有破不了的, 因它們就是有一定的編碼方式。但如果能發展出一套編碼法, 使得破解要花很長的時間, 且此時間遠超過要保密的訊息之有效期限, 則便可充分達到

保密的效果了。

美國史丹福大學(Stanford University)的兩位教授Diffie 及Hellman在西元1976 年發表了一篇對現代編碼理論有重要影響的論文(見Diffie and Hellman (1976)) 。在該論文中, 他們提出了一所謂單一方向進行(trapdoor one-way)的密碼函數, 這種函數須具備下述特性:

(i)對每一自然數x, 有唯一之自然數$y = f(x)$與之對應;

(ii)反函數f^{-1}存在, 使$f^{-1}(f(x)) = x$;

(iii)對這種函數f及其反函數f^{-1}, 存在有效之演算法(algorithm);

(iv)即使密碼函數f及其運算被知道了, 反函數並無法得到。

上述四條件中, 條件(iv)當然是最關鍵的。而Rivest等三人便提出了一個這種密碼函數。在他們的論文中提到, 一個130位的數字, 利用PDP-10的計算機約7分鐘可測出是否爲質數(即使至西元1983年, 一個100位的數須30秒才能檢驗出是否爲質數, 而200位的話則須8 分鐘), 但對一爲兩個63位的質數相乘的合成數, 以那時最快的計算機, 約須$4 \cdot 10^{16}$年才能找出其因數。根據這個事實, Rivest等三人提出了一套編碼法(各取他們姓的第一個字母稱做RSA法)。要解此密碼, 就須知道這個巨大的數是由那兩個質數相乘, 而要憑運氣猜出的機會可說是微乎其微的(想想有63位, 而且還不一定知道此二質數之位數)。

我們敘述RSA法如下。

第一步, 先產生兩個很大的質數p, q, 此二質數須保密。

第二步, 計算$n = pq$。

第三步, 選一整數h, 使得h與$(p-1)(q-1)$互質。

第四步, 求整數d, 使得

$$dh \equiv 1 \pmod{(p-1)(q-1)}。 \tag{8}$$

這種d存在, 此因h與$(p-1)(q-1)$互質。

第五步, 公佈n與h, 但d保密。

只要n夠大, 即使知道n與h, 並無法(或說極困難)得知p與q, 因此d就得不到了。

若以適當的數字取代, 所有文字的訊息皆可轉換爲(小於n之)數字。欲

傳送訊息m(爲一小於n之整數), 先計算c,其中

$$c \equiv m^h \pmod{n}, \tag{9}$$

然後將密碼c送出。這樣做安全嗎? 由於攔截者可能知道h及n(因h及n是公開的)。因此他們知道h, n及$c(\equiv m^h \pmod{n})$, 由此想得到m。但這是極困難的(一般而言, 除非n的因數知道, 否則並無簡易的方法)。不妨一試, 不用給太大的數字, 看你能否由

$$m^{49} \equiv 3 \pmod{401}$$

解出m。

但若知道n的因數p與q, 便可求出d, 則收到c之後, 經由計算c^d便可得到訊息m了。證明如下。

(i)若$(m, pq) = 1$,則$(m, p) = 1$且$(m, q) = 1$。而由(??)式, 存在整數b, 使得$dh = 1 + b(p-1)(q-1)$,

$$\begin{aligned} c^d \equiv m^{dh} &= m^{1+b(p-1)(q-1)} \\ &= \begin{cases} m \cdot (m^{p-1})^{b(q-1)} & \equiv m \cdot 1 = m \pmod{p}, \\ m \cdot (m^{q-1})^{b(p-1)} & \equiv m \cdot 1 = m \pmod{q}。 \end{cases} \end{aligned}$$

此處用到系理1, $m^{p-1} \equiv 1 \pmod{p}$,且$m^{q-1} \equiv 1 \pmod{q}$。而$(p, q) = 1$, $n = pq$,故得$c^d \equiv m \pmod{n}$。

(ii)若$(m, pq) \neq 1$, 因$m < pq$, 故$p|m$且$q \nmid m$(因此$(m, q) = 1$), 或$q|m$且$p \nmid m$(因此$(m, p) = 1$)。先看前者。仍由系理1, 且如(i),

$$\begin{aligned} c^d - m &= m^{dh} - m = m(m^{b(p-1)(q-1)} - 1) \\ &= m((m^{q-1})^{b(p-1)} - 1) \\ &\equiv m(1-1) = 0 \pmod{q} \end{aligned}$$

故$q|(m^{dh} - m)$,而$p|m$又導至$p|(m^{dh} - m)$,故$n|(m^{dh} - m)$。即得

$$c^d \equiv m \pmod{n}。$$

同理若$q|m$且$p \nmid m$仍有$c^d \equiv m \pmod{n}$。

由上討論知, 收到密碼c之後, 只要知道d, 則可由c^d得到m。而若無法分解n,則p, q不知, 如此無法由(??)式得到d, 因此雖攔截到c, 也得不到原訊m 了。

例**10.**我們以較小的數字來說明。取n=143,則$p = 11, q = 13$。再取$h = 7$與$(p-1)(q-1) = 120$互質。次求d滿足

$$7d \equiv 1 \pmod{120}。$$

因$7 \cdot 17 \equiv -1 \pmod{120}$, 故$7 \cdot (120-17) \equiv 7 \cdot 103 \equiv 1 \pmod{120}$。即可取$d = 103$。現若$m = 14$, 要傳的密碼$c$即滿足

$$c \equiv 14^7 \pmod{143}。$$

因$14^7 \equiv 53 \pmod{143}$,故$c$=53。

驗算看看。收到c之後, 計算c^d便又得回m(計算過程留在習題第37題):

$$c^d = 53^{103} \equiv 14 \pmod{143}。$$

在提出RSA法後, 爲了顯示對此法之信心, MIT的研究人員用一個129位數的n和一個4 位數的h, 將一個代表一訊息之128位數編碼。此密碼及n與h並登在西元1977年8月號的科學的美國人(Scientific American), Gardner的專欄中。MIT 研究小組並懸賞100美元給第一位破譯者。

這100美元看起來是很安全的, MIT研究小組估計要花23,000年才可能分解該129 位數。雖100美元似乎不是一筆很大的錢。但你要不要估計經過23,000 年後, 100美元成爲多少? 若以年利率6%的複利計, 爲一筆有585位的錢, 夠嚇人的吧! 也許計算機速度的增快, 可使破解的時間降低一兩個位數, 但仍是很安全的。

可惜人算不如天算, 這個叫陣的RSA數經過17年, 便敗下陣來, 而將它打下擂台的計算, 全部只花不到一年的時間。由一批約六百餘位因數分解迷所組成的鬆散組織, 分散在20多個國家, 經過8個月的努力, 於西元1994年4月, 成功地將該129位數分解成一64位的質數與一65位的質數之積, 因而破譯密碼。

之所以能這麼快便成功, 一方面是靠今日網際網路的發達, 一方面是靠新技術, 所謂二次篩法(Quadratic Sieve)以加速找因數的工作。而這兩項技術的威力, 都是在西元1977年提出RSA法時所未想到的。

不過由於分解很大的數基本上還是很困難的, 所以只要提高n的位數, 則以目前的能力, 要破解密碼還是須花相當長的時間。RSA法仍是現今最安全的密碼系統。有關上述挑戰RSA數的過程之報導, 可見Cipra (1996) pp.90-99, 倪錄群譯(1997)爲其譯稿。

對利用質數之難以分解來編碼的RSA法有興趣的讀者, 可參考楊重駿、楊照崑 (1983, 1986a, 1986b) 、楊淑芬 (1991) 、Devlin (1983/84) 、Stewart (1987/88) 、Piper (1988/89) 及Williams and Allen (1998/9)。我們看到一純粹數學上的結果, 居然有如此實際的用途。另外, 近年來也發展出以機率的方法來檢定一整數是否爲質數的方法, 可參考Jammalamadaka and Uppuluri (1989) 及其中所列的參考文獻。

習　題

1.試證$4^{14} \equiv 1 \pmod{29}$, $4^{14} \equiv 1 \pmod{15}$, $2^{340} \equiv 1 \pmod{341}$, $3^{90} \equiv 1 \pmod{91}$, $53^{103} \equiv 14 \pmod{143}$。

2.令$f(n) = n^2 - 79n + 1{,}601$。找出一使$f(n)$不爲質數的最小正整數$n = n_0$。

3.求$7^{1{,}987}$之末兩位數。

4.求1,998! 之不爲0的最小位數的數字。

5.試以同餘的概念說明: 可以一數之各位數字和是否爲3之倍數來判斷此數是否爲3 的倍數,及數字和是否爲9之倍數來判斷此數是否爲9的倍數。

6.試說明例6中,求一整數除以37之餘數的作法。

7.試證不存在一整係數之多項式$f(x)$, 使得若分別以$1, 2, \cdots$代入x, 皆能得到質數。

8.試找出二正整數, 其數字皆不含零, 但二數乘積爲1,000,000,000。

9.求$1^2 - 2^2 + 3^2 - 4^2 + \cdots + 1{,}993^2 - 1{,}994^2$之值。

10.試證對每一正整數n, $1{,}946|(1{,}492^n - 1{,}770^n - 1{,}863^n + 2{,}141^n)$ 。

11.設$a_1 = 2, a_2 = 3, a_3 = 5, a_4 = 7, \cdots$,爲質數列 。判斷$a_1 + 1$, $a_1a_2 + 1$, $a_1a_2a_3 + 1, \cdots$, 是否皆爲質數?

12.設有一正整數n, 以3除之餘2, 以5除之餘3, 以7除之餘2, 問n之最小值爲何? 一般值爲何?

13.令$b = \frac{10^{20,000}}{10^{100}+3}$ 。求
(i) b之整數部分;
(ii)b之整數部分的個位數 。

14.試證對任一$n > 1$, $\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}$必不爲整數 。

15.設p, q爲二大於5之質數,試證$240|(p^4 - q^4)$ 。

16.試證對任一正整數n, $9n + 8$與$6n + 5$必互質 。

17.諸如3 與5 或5 與7 皆稱爲孿生質數(twin primes), 即兩個差爲2之質數 。
(i)列出100至200間之孿生質數;
(ii)設p 與q 爲孿生質數,試問$p^2 + q^2$除以72之餘數爲何?

18.設m爲一正有理數 。試證若$m + 1/m$爲一整數,則$m = 1$ 。

19.小明玩數手指的遊戲: 大姆指爲1, 食指爲2, 中指爲3,無名指爲4,小姆指爲5;然後反方向,無名指爲6,中指爲7,食指爲8,大姆指爲9;再反方向,食指爲10,餘類推 。試問3,457 落在那一指上 。

20.設有一火車在分針指著整數時離開火車站 。行駛8公里後,司機發現他錶上的分針與時針恰重疊 。假設在這8公里的行程中,火車的平均時速爲33公里,試問在幾時幾分火車離開火車站 。

21.對任一正整數n, 試證$98|(15^n - 2^{3n+1} + 1)$ 。

22.試將二十世紀中, 有五個星期日之二月找出 。

23.利用費馬小定理,證明若p爲一質數,則$p|(1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}+1)$。

24.試證任一$3n+1$型之質數必爲$6n+1$型。

25.試證任一$3n+2$型之正整數, 必有一同型之質因數。

26.設k爲一大於1之正整數,令p表$(k!)^2+1$之一質因數。試證

(i)$p>k$;

(ii)p爲$4n+1$型的質數;

(iii)$4n+1$型的質數有無限多個。

27. (i)試證每一$4n-1$型之正整數至少有一同型之質因數;

(ii)對任一自然數k, 試證$4(k!)-1$有一$4n-1$型之質因數p,且$p>k$;

(iii)試證$4n-1$型之質數有無限多個。

28.求出所有質數p, 使得$2p-1$及$2p+1$皆爲質數。

29.試證存在無限多個奇數n,使得下述數列之任一皆不能除盡n:

$$a^a+1,\ a^{a^a}+1,\ a^{a^{a^a}}+1,\cdots,$$

其中$a=1{,}994$。對其他的整數a是否有類似的結果?

30.試證對每一正整數n及每一正奇數k,

$$(1+2+\cdots+n)|(1^k+2^k+\cdots+n^k)。$$

31.設t,m,k均爲正整數,且t不是3的倍數。令$n=t^m$,n爲一$10k$位數。試證n 的數字中,必有一數字至少出現$k+1$次。

32.試證對每一質數p及正整數k,$\pi(p^k)=p^{k-1}(p-1)$。

33.利用定理3,經由取$m=2$及$n=5^4$,求$2^{1{,}000}$之末四位數字。

34.利用系理2,試證$p>2$爲一質數,若且唯若$p|((p-2)!-1)$。

35.試證若一質數可寫成二正整數之平方和, 則其寫法唯一(不計先後順序)。

36.試解出(7)式中之$a, b, \cdots, j$。

37.在例10中,若$m = 17$,求c,並經由計算c^d解回m。

38.設$n = 91$,$h = 7$,$m = 54$。利用RSA法,求d, c,並經計算c^d得回m。

39.存100美元在銀行, 以年利率6%的複利計, 試估計經23,000年後, 成爲多大一筆錢?

參考文獻

1. 林聰源譯(1976). 整數論的問題。楓城出版社,新竹。

2. 金庸 (1996). 射鵰英雄傳, 第三版。遠流出版社,台北。

3. 倪錄群譯(1997). 大數秘史。數學譯林, 第16卷第4期, 296-302 。

4. 莫宗堅(1970). 韓信點兵。科學月刊, 第1卷第1期,48-52。

5. 楊淑芬 (1991). 踏著歷史的足跡學數學－數學在數論教學上之應用。科學月刊, 第22卷第1期, 64-71。

6. 楊重駿、楊照崑 (1983). 數論在密碼上的應用(上)、(下)。數學傳播季刊, 第7卷第2期, 16-22,第3期, 2-7。

7. 楊重駿、楊照崑(1986a). 質數的建造、分佈及檢驗。數學傳播季刊,第10卷第1期, 94-101。

8.楊重駿、楊照崑(1986b). 數字密碼的一些新研究。數學傳播季刊,第10卷第3期, 29-34。

9. Beeger, N. G. W. H. (1951). On even numbers m dividing $2^m - 2$. *American Mathematical Monthly* 58, 553-555.

10. Cipra, B. (1996). 1995-1996 *What's Happening in the Mathematical Sciences.* American Mathematical Society, Providence, Rhode Island.

11. Devlin, K. (1983/84). Prime numbers and secret codes. *Mathematical Spectrum* 20, 74-77.

12. Devlin, K. (1992/93). Carmichael numbers. *Mathematical Spectrum* 25, 1-2.

13. Diffie, W. and Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory IT* 22, 644-645.

14. Godwin, H. J. (1978/79). Fartorization and random numbers. *Mathematical Spectrum* 11, 18-23.

15. Heinrich, K. and Horak, P. (1994). Euler's Theorem. *The American Mathematical Monthly* 101, 260-261.

16. Hill, R. (1990/91). Error-correcting codes II. *Mathematical Spectrum* 23, 14-22.

17. Jammalamadaka, S. R. and Uppuluri, V.R.R. (1989). Is p a prime number? Some probabilistic tests for primality. *The Mathematical Scientist* 14, 55-61.

18. Piper, F. (1988/89). Cryptographic uses of large numbers. *Mathematical Spectrum* 21, 1-7.

19. Rivest, R. L., Shamir, A. and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *ACM Communications* 21, 120-126.

20. Rogosinski, H. P. (1972/73). The perpetual calendar. *Mathematical Spectrum* 5, 42-46.

21. Stewart, I. (1987/88). Fartorizing large numbers. *Mathematical Spectrum* 20, 74-77.

22. Williams, M. J. and Allen, L. J. S. (1998/9). The RSA algorithm: a public-key cryptosystem. *Mathematical Spectrum* 31, 9-13.