離散對數真是難

愛寂寞另立山頭

May 21, 2014

在瑞沙葉演算法當中，我們看到了， 分解因數的困難性造就出一個非常實用的密碼系統。 是不是有其他數論上的難題具有類似的特性呢？ 這是密碼學家所渴望、所切盼、所追求、所夢想的。 說不定那天，你也發現一個類似的數學難題， 從而將密碼學推向更上一層樓的境界。 我們先來思考一個跟上一講末了的原根相關的問題。

1 離散對數惹問題

還記得質數 65537嗎？就在剛剛上一講末了的例題 10.10出現過， 也出現在介紹黑爾曼突破鑰匙交換時；更早在第一講介紹特殊質數類就現身過， 其實這個數就是目前已知五個飛馬質數 (Fermat Primes)中最大的一個。 在第九講時我們問過

請問同餘式 $3^x \equiv 2 \pmod{65537}$中 x的解是多少？

那兒，我們的解答是「聰明的你，可以告訴我嗎？」現在我們要正面回答這個問題。 因為例題 10.10告訴我們： 3是 65537的原根， 因此同餘式

$3^x \equiv 1 \pmod{65537}$最小的正整數解就是 65536 而其他解都是 65536的倍數，且每一個非零整數都是原根 3的一個次冪； 這確保我們所面臨的同餘方程式在 $0 \le x \le 65536$ 必定有解。

怎麼解呢？在同餘式 $3^x \equiv 2 \pmod{65537}$兩邊同時取16次冪得

$$3^{16x} \equiv 2^{16} = 65536 \equiv -1 \pmod{65537}\ ， \tag{1}$$

再平方後即得

$$3^{32x} \equiv 1 \pmod{65537}\ ；$$

因此原根的基本性質告訴我們

$$65536 \,|\, 32x \iff 2048 \,|\, x \iff x = 2^{11}m\ ，$$

其中 m為正整數。但 $x = 2^{11}m \le 2^{16} \Longrightarrow 1 \le m \le 2^5$， 所以有32個可能的 x值： $2^{11}m$， 其中 $m = 1, 2, 3, \cdots, 31$。 然而

$$4096 \nmid x = 2^{11}m \iff 2 \nmid m$$

《若 $4096 \mid x \Rightarrow 3^{16x} \equiv 1 \pmod{65537}$與 (1)式矛盾》， 所以實際上只有16個可能的 x值： $2^{11}m$， 其中 $m = 1, 3, 5, \cdots, 31$。

最後得將這16個可能的 x值算出對應的 $3^x \pmod{65537}$ 看看哪一個會是 2， 結果得到 $m = 27 \Rightarrow x = 2^{11} \cdot 27 = 55296$是正確的解。

聰明的你當然會說，這個方程式太特殊了，才讓你如此這般地就解出來了。 不過這裡要禿顯得乃是，即使這麼特殊，最後的步驟還是比對。將原先的全面搜索降為局部搜索！總而言之，問題不簡單喔！

固定一質數 p。 令 α 與 β為模 p之下的兩個非零整數並考慮方程式

$$\alpha^x \equiv \beta \pmod{p}。$$

此同餘方程式中，解 x的問題稱之為離散對數問題[1]。 令 n為滿足同餘式 $\alpha^n \equiv 1 \pmod{p}$ 的最小正整數，因此我們可以假設 $0 \leq x < n$ 且用符號

$$x = L_\alpha(\beta)$$

表示之，並稱之為以 α 為底 β的離散對數 (質數 p在符號中省略) 。

【例題11.1】令 $p = 11, \alpha = 2$。因為 $2^6 \equiv 9 \pmod{11}$，我們有

$$L_2(9) = 6。$$

當然, $2^6 \equiv 2^{16} \equiv 2^{26} \equiv 9 \pmod{11}$， 所以我們可考慮取 $6, 16, 26, \cdots$之一當成其離散對數。 不過我們固定取那個最小的正整數，亦即 6。 注意此處我們大可以就定義其離散對數就是模10之下 6的同餘類。 從某種角度來看，這可能更自然些，但在有些應用上 給一個數字說不定更方便，而不僅僅是一個同餘類。

通常我們選取 α 為模 p的原根， 亦即每一非零元素 $\beta \pmod{p}$都是 α 的一個次冪。 如果 α 不是原根，那麼就會有一些 β值其離散對數沒有定義了。 對任意給予的質數 p，在理論上原根必定存在；上一講的最後一節已經說過。 用代數的術語描述，也就是乘法群 $\mathbb{Z}_p^\times = \mathbb{Z} \setminus \{0\}$ 為一循環群。而原根就是此循環群的生成元素 (generator)。 其證明是一理論性而非建構性的論證，這種情況跟最大公因數完全一樣。 所以尋找原根的演算法就變成另外值得探討的問題。

[1]其定義可推廣至有限循環群中來考慮，請參閱網頁
http://en.wikipedia.org/wiki/Discrete_logarithm。

離散對數在許多方面的表現跟一般的對數很像。 特別而言，若 α 是模 p 的一個原根，則

$$L_\alpha(\beta_1\beta_2) \equiv L_\alpha(\beta_1) + L_\alpha(\beta_2) \pmod{p-1},$$

此即對數律的第一律。

2 全面搜索第一法

為了簡單起見，取 α 為模 p之原根，所以 $p-1$為滿足同餘式

$$\alpha^n \equiv 1 \pmod{p}$$

的最小正整數次冪 n。假設有模 p之下的同餘式：

$$\alpha^x \equiv \beta \pmod{p} \tag{2}$$

我們要尋找 x的值 $0 \le x < p-1$ 。從(2)式來計算離散對數 x 最簡單、最原始的方法就是將 α 取 x次冪 $x = 0, 1, 2, \cdots$ 看是否滿足(2)式。一旦答案是肯定的， 我們就找到了 β的離散對數 $x = L_\alpha(\beta)$。 此法稱之為窮舉法(enumeration)或試誤法，需要執行 $x-1$個乘法以及比較兩個數 x次； 但僅需儲存三個數 α, β與 α^x ，故窮舉法僅需儲存的空間數為 3。

【例題11.2】計算離散對數 $5^x \equiv 3 \pmod{2017}$。窮舉法得到 $x = 1030$，用到了1029次模2017下的乘法運算。

聰明的你，也許會說：「何不從2017的中間1008切入開始計算？ 如此一來，只需要22次的模乘法運算就得到了所要的離散對數。」 問題是，你根本不知道 x會是多少。所以，從何處開始會是最好呢？沒人知道。 因此

這相當於全面搜索所有 $p-1$個可能的次冪。 對小質數 p而言，此法還好；然而，當 p逐漸變大那就會感覺萬分吃力。

在密碼術的應用，我們的 x大到 2^{160}； 此種情況下窮舉法不只是感覺吃力而已，乃是無能為力也。 因此之故，我們需要尋找新的演算法來解決大 p的問題。

3 嬰步巨步第二法

上面的窮舉法，僅需三個儲存的空間；但需要更長的時間，來試誤。因此新方法突破之點就在如何用空間來換取時間，這是時間與空間的交易場所。 尚可思[2]乃是第一個贏家，其步驟數減為 $\sqrt{p-1}$； 尚可思稱此演算法為嬰兒步巨人步演算法(Baby-Step Giant-Step Algorithm)。

令 $m = \lceil p-1 \rceil$為大於 $p-1$的最小整數。 將未知的離散對數 x寫成

$$x = qm + r\,, \quad 0 \le x < m \ ;$$

也就是說，將 x被 m除得到商為 q而餘數為 r的等式。 尚可思(Shanks)藉由試誤法來計算 q與 r，接下來 x就水落石出； 其想法如下：

$$(2)\text{式} \Longrightarrow \alpha^{qm+r} = \alpha^x \equiv \beta \Longrightarrow (\alpha^m)^q \equiv \beta\alpha^{-r} \pmod{p} \ 。$$

首先計算嬰兒步集合

$$B = \left\{ (\beta\alpha^{-r} \pmod{p}, \quad r)\,; \quad 0 \le x < m \right\} \ 。$$

[2]但以理・尚可思(Daniel Shanks) 美國數學家， 1917年 1月17日生於伊利諾州的芝加哥市；1996年 9月 6日在馬利蘭州過世，享年79歲。 他主要的工作在計算數論，以第一個將圓周率 π算到十萬位數著稱； 大作「未解及已解之數論問題(Solved and Unsolved Problems in Number Theory)」 享譽於數學界多年。

如果這個集合出現 $(1, r)$的數對，那麼

$$\beta\alpha^{-r} \equiv 1 \Longrightarrow \alpha^r \equiv \beta \pmod{p} \text{。}$$

因此， $x = r$就是所要求的離散對數。否則的話，我們算出

$$\delta \equiv \alpha^m \pmod{p} \text{，}$$

然後依序一一檢驗

$$\delta^q \pmod{p}, \quad q = 1, 2, 3, \cdots \text{；}$$

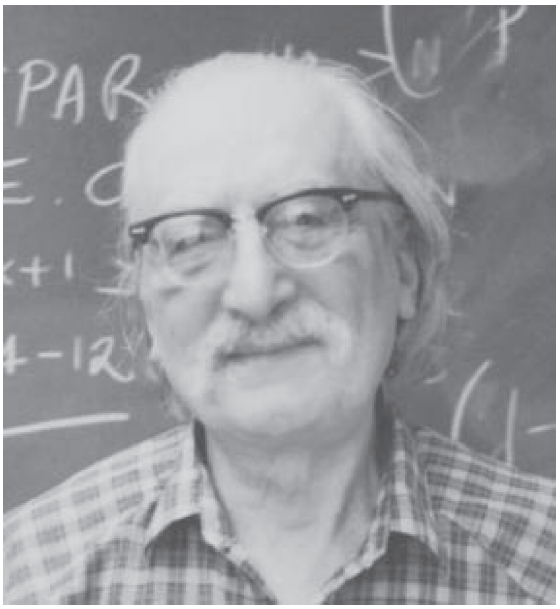
是否出現在嬰兒步集合 B中的第一個分量。果真如此，我們就有

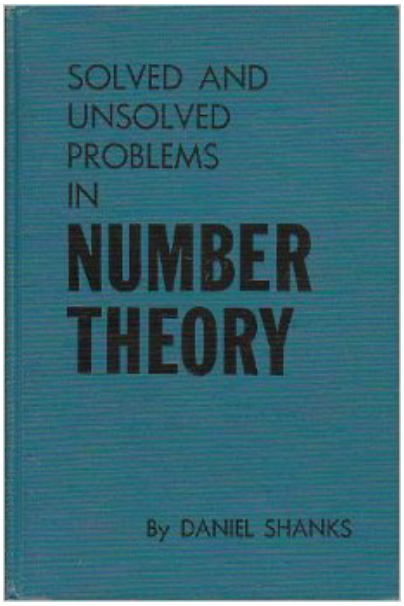
$$\beta\alpha^{-r} \equiv \delta^q \equiv \alpha^{qm} \pmod{p} \text{；}$$

這告訴我們 $\beta \equiv \alpha^{qm+r} \pmod{p}$。 所以這個 q與 r造就了我們所正在尋找的離散對數

$$x = qm + r \text{。}$$

這些數 $\delta^q \pmod{p}$, $q = 1, 2, 3, \cdots$； 就稱為巨人步。 我們必須把巨人步中的每一個數 $\delta^q \pmod{p}$ 跟嬰兒步集合 B中的 每一個數對中的第一個分量一一比對。為要有效率，得將集合 B每一個數對 中的第一個分量那些數儲存。且看下面舉例說明：





【例題11.3】重温上例，計算離散對數　　$5^x \equiv 3 \pmod{2017}$

我們有 $p = 2017, \alpha = 5, \beta = 3$，而 $m = \lceil p - 1 \rceil = 45$。 嬰兒步集合 B是

{(3, 0), (404, 1), (1291,2), (1065,3), (213,4), (446,5), (896, 6), (986, 7), (1004, 8), (1411, 9), (1089, 10), (1428, 11), (689,12), (1348,13), (673, 14), (538, 15), (511, 16), (909, 17), (1392,18), (1892,19), (1992,20), (2012,21), (2016,22), (1210,23), (242, 24), (1662,25), (1946,26), (1196,27), (1046,28), (1016,29), (1010,30), (202, 31), (1654,32), (1541,33), (1115,34), (223, 35), (448, 36), (493, 37), (502, 38), (1714,39), (1553,40), (714, 41), (1353,42), (674, 43), (1345, 44)}

尋尋覓覓知「頭獎不中」，因不見這個集合出現 $(1, r)$的數對； 那麼我們必須得訴諸於「巨人」

$$\delta \equiv \alpha^m = 5^{45} \equiv 45 \pmod{2017}，$$

然後依序一一檢驗巨人步 $45^q \pmod{2017}$, $q = 1, 2, 3, \cdots$；得到

45, 8, 360, 64, 863, 512, 853, 62, 773, 496, 133, 1951, 1064, 1489, 444, 1827, 1535, 497, 178, 1959, 1424, 1553。

當 $q = 22$時，$\delta^q = 1553 \pmod{2017}$終於出現在嬰兒步集合 B中的第一個分量 $(1553, 40)$。因此，

$$\beta\alpha^{-40} \equiv \delta^{22} \equiv \alpha^{22\times 45} \pmod{2017}\ ;$$

所以我們正在尋找的離散對數就是

$$x = 22 \times 45 + 40 = 1030\ 。$$

在計算嬰兒步集合時，需要45個模乘法運算加上巨人步21個共需66個模乘法運算； 但窮舉法則需1029個模乘法運算才能了事。另一方面，嬰兒步中需要儲存45個元素的空間； 但窮舉法僅需 3個。這就是前面提及的「以空間(3增加到45) 換取時間 (1029減少到66) 。」 此法所需要的時間與空間同樣大約是 $\sqrt{p-1}$ 。 若 $p > 2^{160}$，則此法計算離散對數依舊行不通。 這意味著，計算離散對數的演算法仍需聰明的你繼續努力；還有一條漫長的路要走。

下面我們會提供一些更有效的解離散對數問題的方法。 雖然如此，人們還是相信，計算離散對數一般來講是困難的。 這個假設乃是一些密碼系統的理論基礎。

更一般地，一個函數 $f(x)$ 稱之為單向函數 (one-way function)如果函數值 $f(x)$ 是容易並可快速計算的； 但給予 y, 要找滿足 $f(x) = y$ 的 x 在計算上是不可行的。 模次冪可能就是這種函數的一個例子。 計算 $\alpha^x \pmod{p}$ 是容易的；但在同餘方程式 $\alpha^x \equiv \beta \pmod{p}$當中計算次冪 x，則有可能是困難無比的。 大質數相乘也可以看成是一個單向函數：兩個質數相乘是容易的， 但反過來，要分解其結果尋回原來的質因數，那可就困難重重了。

一方面，單向函數在密碼學上不僅提供了建構密碼系統的理論基礎，還有許多不同的應用。 另一方面，從知道是單向函數到設計一套實用的密碼；看起來，似乎也是一條漫漫長路。 如何利用數學領域的難題，打造成一個銅牆鐵壁般的密碼； 這需要活潑有生氣的靈感，來讓死胡同變成活巷弄。 面對我們的乃是一門不折不扣貨真價實的藝術課程。

4 密碼系統愛寂寞

如何利用離散對數問題的困難，來打造設計密碼呢？

聰明的你，有任何腹案或想法嗎？

現在就有請三毛、四郎出場，帶領大家來看看當年愛寂寞 (ElGamal) 所想出來的東西。假設三毛要傳遞數位信息 x給四郎，演算法如下：

1. 首先四郎選取一個大質數 p及整數 $\alpha \pmod{p}$ 。
2. 同時他也選取一秘密整數 a並計算 $\beta \equiv \alpha^a \pmod{p}$。
3. 四郎將 (p, α, β) 公開，但將 a保持私密。
4. 三毛則根據四郎所公開的鑰匙，選取一個隨機整數 k
   並算出密碼文 (y_1, y_2) ，此處 $y_1 \equiv \alpha^k,\ y_2 \equiv x\beta^k \pmod{p}$ 。
5. 她送出密碼文 (y_1, y_2) 給四郎
6. 最後四郎據此解密如下： $y_2 y_1^{-a} \pmod{p}$ ，此乃原來的明文 x。

這就是愛寂寞[3] 於 1985 年所提出的密碼系統[?]。 這個系統是一個非定性的系統，因密文不僅與明文有關，且跟三毛選的隨機整數 k有關。 所以同一明文就會產生許許多多不同的密文。

[3]塔賀・愛寂寞(Taher ElGamal) 乃埃及裔美國人， 1955年 8月18日出生於埃及開羅；1977年開羅大學畢業並於1981及1984年在 史丹福大學分別拿到碩士及博士學位，是黑爾曼的博士生。 被稱為安全套接層（Secure Sockets Layer，SSL ）之父。 SSL採用公開密鑰技術，保證兩個應用間通信的保密性和可靠性， 使客戶與伺服器應用之間的通信不被攻擊者竊聽。 它在伺服器和客戶機兩端可同時被支持，目前已成為網際網路上保密通訊的工業標準。 現行的Web瀏覽器亦普遍將HTTP和SSL相結合，從而實現安全通信。此協議其繼任者是TLS。

用口語化的方式來描述，這個系統是如此運作的。 明文 x 透過乘以 β^k 來偽裝產生密文 y_2， 而 α^k之值也當成密文的一部分一起送過去。 四郎因為知道秘密次冪 a，故可透過 α^k 之值來算出 β^k 之值； 然後他再將 y_2除以 β^k來解除偽裝得回原有的信息 x。

【例題11.4】假設 $p = 13457, \alpha = 3, a = 711$，因而 $\beta \equiv \alpha^a \equiv 12103 \pmod{p}$。 現在，假設三毛想要傳遞信息 $x = 12345$ 給四郎。 三毛選一隨機整數 $k = 1753$ 並算出

$$y_1 \equiv \alpha^k \equiv 7151 \quad 及 \quad y_2 \equiv x\beta^k \equiv 5194 \pmod{p}。$$

當四郎接到密文 $y = (y_1, y_2) = (7151, 5194)$ 後，他可算出

$$x \equiv y_2 y_1^{-a} \equiv 12345 \pmod{p}，$$

這就是三毛所送的原信息 x。

若三毛選另一隨機整數 $k' = 3149$ 並算出

$$y_1' \equiv \alpha^{k'} \equiv 13107 \quad 及 \quad y_2' \equiv x\beta^{k'} \equiv 8645 \pmod{p}。$$

這次四郎接到的密文是 $y' = (y_1', y_2') = (13107, 8645)$ ，當他算出

$$y_2' y_1'^{-a} \equiv 12345 \pmod{p}時，$$

發現這還是三毛原來的那個信息 x。 所以同一個明文會隨著加密者所選的隨機整數 k得到不同的密文。

5 離散對數波黑法

前面已經提到過，對小質數而言，計算離散對數沒什麼了不起的；試誤法或頂多用嬰兒步巨人步演算法即綽綽有餘也。 但當質數變大時，這兩個方法就都失效了。 所以接下來這兩節，我們提供兩個計算大質數離散對數的演算法， 即波立格 -黑爾曼演算法與指數計算法。 另外還有一個重要的方法，就是所謂的生日攻擊法， 請參閱密碼學之旅－與MATHEMATICA 同行[?]第九章第四節。

如上， α 為質數，我們要尋找 x的值 $0 \le x < p-1$ 滿足(2)式：

$$\alpha^x \equiv \beta \pmod{p}。$$

【決定 x 的奇偶性】

首先，我們決定 x的奇偶性，亦即尋求在模 2之下的 x值。但這非常簡單，因為

$$\left(\alpha^{(p-1)/2}\right)^2 \equiv \alpha^{p-1} \equiv 1 \pmod{p},$$

所以 $\alpha^{(p-1)/2} \equiv \pm 1 \pmod{p}$。但不要忘記，我們前面假設 $p-1$ 是滿足同餘式 $\alpha^n \equiv 1 \pmod{p}$的最小正整數次冪 n，所以我們一定有

$$\alpha^{(p-1)/2} \equiv -1 \pmod{p}。$$

回到原來的同餘方程式(2)，兩邊取 $(p-1)/2$ 次冪可得

$$\beta^{(p-1)/2} \equiv \alpha^{x(p-1)/2} \equiv (-1)^x \pmod{p}。$$

因此之故，若 $\beta^{(p-1)/2} \equiv +1$ ，則 x為偶數；否則 x為奇數。

【例題11.5】假設我們要解同餘方程式 $2^x \equiv 9 \pmod{11}$。因為

$$\beta^{(p-1)/2} \equiv 9^5 \equiv (-2)^5 \equiv 1 \pmod{11}，$$

所以 x一定是偶數。實際上，$x = 6$ 如前面例題11.1所見。

【波立格 -黑爾曼演算法(Pohlig-Hellman Algorithm)】

波立格[4] 及黑爾曼兩個人在 1978 年將上述的方法推廣， 得到一套計算離散對數的演算法[?]。 可惜，這套方法只適用於 $p-1$僅僅包含小質因子時。 現在假設 $p-1$ 的標準分解式為

$$p - 1 = q_1^{r_1} q_2^{r_2} q_3^{r_3} \cdots q_d^{r_d} 。$$

為簡便計，將下標省略；所以假設 q^r 為其中之一。 我們得先計算每一個 $L_\alpha(\beta) \pmod{q^r}$之值，再透過孫子定理合併起來得到

$$L_\alpha(\beta) \pmod{p-1} 。$$

回到(2)式，將所要解的 x寫成 q進制的表示法如下：

$$x = x_0 + x_1 q + x_2 q^2 + \cdots + x_{r-1} q^{r-1}, \quad 0 \le x_i \le q-1 \tag{3}$$

我們將依序決定 $x_0, x_1, x_2, \cdots x_{r-1}$，而後就可得到 $x \pmod{q^r}$。 將(3)式兩邊同時乘上 $(p-1)/q$ 並整理之得：

$$x \frac{p-1}{q} = x_0 \frac{p-1}{q} + (p-1)u, \tag{4}$$

[4]史提芬・波立格 (Stephen C. Pohlig)是美國電機工程師， 目前在M.I.T.林肯實驗室工作；曾在研究生時於史丹福大學協助其指導教授 黑爾曼開發冪密碼(Exponential Cipher)並取得 4424414號美國專利權， 另外也提出解離散對數問題改進的演算法。

此處 $u = x_1 + x_2q + \cdots + x_{r-1}q^{r-1}$ 為一整數。 回到所要解的同餘式(2), 兩邊取 $(p-1)/q$ 次冪得到

$$\beta^{(p-1)/q} \equiv \alpha^{x(p-1)/q} \overset{(4)}{\equiv\equiv} \alpha^{x_0(p-1)/q}(\alpha^{p-1})^u \equiv \alpha^{x_0(p-1)/q} \pmod{p}。$$

最後一個同餘式，我們用到了飛馬小定理：$\alpha^{p-1} \equiv 1 \pmod{p}$。 怎麼找這樣的 x_0呢？ q是小質數的假設提醒我們， 該是下達全面搜索令的時候了！只要列舉所有 $\alpha^{(p-1)/q}$ 的次冪

$$\alpha^{k(p-1)/q}, \qquad k = 0, 1, 2, 3, \cdots, q-1,$$

然後依次過濾，直等到整數 $\beta^{(p-1)/q} \pmod{p}$ 出現時的那個 k就是我們所要的 x_0。注意，因為 $\alpha^{m_1} \equiv \alpha^{m_2} \pmod{p} \iff m_1 \equiv m_2 \pmod{p-1}$，且因在模 $p-1$之下，次冪 $k(p-1)/q$ 兩兩相異， 所以有唯一的一個 k會是我們所要尋找的 x_0。

我們可依次施行此法來計算其他的係數 $x_1, x_2, \cdots$， 不過得先改寫成同樣的形式。假設 $q^2 \mid p-1$，則令 $\beta_1 \equiv \beta\alpha^{-x_0} \equiv \alpha^{q(x_1+x_2q+\cdots)} \pmod{p}$。兩邊同時取 $(p-1)/q^2$ 次冪得到

$$\beta_1^{(p-1)/q^2} \equiv \alpha^{(p-1)(x_1+x_2q+\cdots)/q} \equiv \alpha^{x_1(p-1)/q}(\alpha^{p-1})^{x_2+\cdots} \equiv \alpha^{x_1(p-1)/q} \pmod{p}。$$

再一次地，最後一個同餘式用到了飛馬小定理。 我們不可以計算 $(\beta_1^{p-1})^{1/q^2}$來充當 $\beta_1^{(p-1)/q^2}$， 此乃因為分數次冪會惹麻煩多多。注意到，所有我們用到的次冪都是整數次冪。 怎麼找 x_1 呢？方法如上，只要列舉所有 $\alpha^{(p-1)/q}$ 的次冪

$$\alpha^{k(p-1)/q}, \qquad k = 0, 1, 2, 3, \cdots, q-1,$$

直等到整數 $\beta_1^{(p-1)/q^2} \pmod p$ 出現時的那個 k就是我們的 x_1。

若 $q^3 \mid p-1$ ，則令 $\beta_2 \equiv \beta_1 \alpha^{-x_1 q}$ 且將同餘式兩邊取 $(p-1)/q^3$ 次冪，計算可得到 x_2。 如此這般地可繼續直到 $q^{r+1} \nmid p-1$為止。 因為我們無法使用分數次冪，所以必須停止。不過，我們已經找到了 $x_0, x_1, x_2, \cdots, x_{r-1}$, 當然就知道 $x \pmod{q^r}$。

【例題11.6】解同餘方程式　　$7^x \equiv 11 \pmod{41}$

【解】令 $p = 41, \alpha = 7, \beta = 11$。 因 $p-1 = 2^3 \cdot 5$，故有兩個質因子 $q = 2$與 $q = 5$。 首先分別求出 $L_7(11) \pmod 8$ 與 $L_7(11) \pmod 5$之值。

(1) $q = 2$：尋找模 8下 x之值，將 x寫成 $x \equiv x_0 + 2x_1 + 4x_2 \pmod 8$；

原同餘方程式變成　　$7^{x_0+2x_1+4x_2} \equiv 11 \pmod{41}$　　$(\dagger_1)$

在$(\dagger_1)$式兩邊取 $20 = (p-1)/2$次方，我們有

$$(7^{x_0+2x_1+4x_2})^{20} \equiv 11^{20} \xrightarrow{\text{飛馬小}} (7^{20})^{x_0} \equiv -1 \Longrightarrow (-1)^{x_0} \equiv -1 \pmod{41}；$$

所以得到 $x_0 = 1$。代回$(\dagger_1)$式且將兩邊在模 p下除以 7變成

$$7^{2x_1+4x_2} \equiv 11 \times 7^{-1} \equiv 11 \times 6 \equiv 25 \pmod{41} \qquad (\dagger_2)$$

在$(\dagger_2)$式兩邊取 $10 = (p-1)/2^2$次方，我們有

$$(7^{2x_1+4x_2})^{10} \equiv 25^{10} \xrightarrow{\text{飛馬小}} (7^{20})^{x_1} \equiv 1 \Longrightarrow (-1)^{x_1} \equiv 1 \pmod{41}；$$

所以得到 $x_1 = 0$。代回$(\dagger_2)$式變成

$$7^{4x_2} \equiv 25 \pmod{41} \qquad (\dagger_3)$$

在($\dagger_3$)式兩邊取 $5=(p-1)/2^3$次方，我們有

$$(7^{4x_2})^5 \equiv 25^5 \equiv -1 \Longrightarrow (-1)^{x_2} \equiv -1 \pmod{41}；$$

所以得到 $x_2=1$，因而模 8下 x之值為

$$x \equiv x_0+2x_1+4x_2 = 1+0+4 = 5 \pmod{8}。$$

(2) $q=5$：我們要找的是，在模 5下 x之值。原同餘方程式兩邊取 $8=(p-1)/5$次方，我們有

$$(7^8)^x \equiv 11^8 \Longrightarrow (-4)^x \equiv 16 \pmod{41}；$$

所以得到 $x \equiv 2 \pmod{5}$。

總結以上，我們有 $x \equiv 5 \pmod{8}$ 及 $x \equiv 2 \pmod{5}$，透過孫子定理將這些數結合在一起得到 $x \equiv 37 \pmod{40}$。驗算一下：連續平方得 $7^2 \equiv -8,\ 7^4 \equiv -18,\ 7^8 \equiv -4,\ 7^{16} \equiv 16,\ 7^{32} \equiv 10 \pmod{41}$；我們有 $7^{37} = 7^{32}\cdot 7^4 \cdot 7 \equiv 10\cdot(-18)\cdot 7 \equiv (-16)\cdot 7 \equiv 11 \pmod{41}$，如所求。