基礎數論

李華介

國立台灣師範大學數學系

前言

本講義主要目的是針對大一學生介紹有關整數論一些基本的代數和算數上的性質, 以作為將來學習抽象代數之準備. 基於這樣的理由, 在此我們將不介紹有關於整數論之歷史和典故以及其應用. 對整數論之應用 (尤其在資訊方面的應用) 有興趣的讀者, 我們推薦 Silverman 的「A Friendly Introduction to Number Theory」(Prentice Hall, Third Edition 2006). 相信若對本講義內容有相當認識之後應可輕鬆閱讀這本書.

Chapter 5

二次的 Congruence Equations

這一章中我們要專注於解二次的 congruence equation. 我們先從解一般的二次 congruence equation 開始, 然後慢慢化簡成簡單的形式, 最後介紹 quadratic reciprocity law. 整體來說我們會得到一個有效判別二次 congruence equation 是否有解的方法, 至於若有解如何求解就不在本章的討論範圍了. 我們希望能著重於學習如何由繁化簡的步驟.

5.1. 二次 Congruence Equation 的化簡

所謂二次的 congruence equation, 即給定 $m \in \mathbb{N}$, 考慮 $ax^2+bx+c \equiv 0 \pmod{m}$, 其中 $a,b,c \in \mathbb{Z}$ 且 $m \nmid a$ 這樣的 equation.

大家看到這樣的方程式, 首先會想到用配方法來解. 沒錯, 我們也是要用配方法. 不過這裡有一點要特別注意, 就是我們都是在整數的情況, 所以須避免用到除法. 例如大家要解 $ax^2+bx+c=0$ 時, 第一個想到的是將 x^2 項的係數 a 除去得 $x^2+(b/a)x+(c/a)=0$. 由於我們在談 congruence equation, 多項式需要求為整係數, 這個方法就行不通了 (除非 $a|b$ 且 $a|c$). 當然了, 當 a 和 m 互質時存在 $e \in \mathbb{Z}$ 使得 $ae \equiv 1 \pmod{m}$, 所以此時我們可以將 $ax^2+bx+c \equiv 0 \pmod{m}$ 兩邊乘上 e 而得 $x^2+bex+ce \equiv 0 \pmod{m}$. 不過這個方法要限制在 $\gcd(m,a)=1$ 的情形, 而我們要探討的是一般情況, 所以我們需想辦法處理. 不管怎樣為了讓多項式為整係數, 我們不要用除的方法, 儘量用乘的. 所以為了使用配方法我們可以讓 x^2 項係數成為完全平方, 也就是將 $ax^2+bx+c \equiv 0 \pmod{m}$ 兩邊乘上 a 而得 $(ax)^2+abx+ac \equiv 0 \pmod{m}$. 接著處理 x 項係數, 由於不能用除的所以不能將 abx 寫成 $2(ab/2)x$, 但用配方法 x 項係數需偶數, 因此好的方法是將原式兩邊乘以 2. 不過這樣一來又破壞了原先 x^2 項係數為完全平方的好處, 所以我們再多乘一個 2 使得 x^2 項係數仍為完全平方.

也就是說, 在解 $ax^2+bx+c \equiv 0 \pmod{m}$ 時我們可以將兩邊乘上 $4a$ 使得原式成為 $4a^2x^2+4abx+4ac=(2ax)^2+2(2ax)b+4ac \equiv 0 \pmod{m}$. 接下來就可用配方法常用步驟將式子寫成 $(2ax+b)^2 \equiv b^2-4ac \pmod{m}$. 因此我們將問題簡化成解 $y^2 \equiv b^2-4ac$

$(\mathrm{mod}\ m)$. 今若沒有整數 k 滿足 $k^2 \equiv b^2-4ac\ (\mathrm{mod}\ m)$, 那麼我們便知原 congruence equation, $ax^2+bx+c\equiv 0\ (\mathrm{mod}\ m)$ 無解. 若可找到 $k\in\mathbb{Z}$ 滿足 $k^2\equiv b^2-4ac\ (\mathrm{mod}\ m)$, 那麼我們便可依前面探討一次的 congruence equation 的方法解 $2ax+b\equiv k\ (\mathrm{mod}\ m)$, 而得到 $ax^2+bx+c\equiv 0\ (\mathrm{mod}\ m)$ 的解.

總之, 解二次 congruence equation, $ax^2+bx+c\equiv 0\ (\mathrm{mod}\ m)$ 的問題, 可化簡成解 $y^2\equiv d\ (\mathrm{mod}\ m)$ 其中 $d=b^2-4ac$. 因此我們接下來僅探討 $x^2\equiv a\ (\mathrm{mod}\ m)$ 這樣的 congruence equation.

假設 $m=p_1^{n_1}\cdots p_t^{n_r}$, 其中這些 p_i 為相異質數. 由 Corollary 4.4.3 知, $x^2\equiv a\ (\mathrm{mod}\ m)$ 有解若且唯若對所有的 p_i, $x^2\equiv a\ (\mathrm{mod}\ p_i^{n_i})$ 有解. 因此我們又將問題化簡為求 $x^2\equiv a\ (\mathrm{mod}\ p^n)$, 其中 p 為質數且 $n\in\mathbb{N}$ 的情形.

我們來看一個綜合以上結果的例子.

Example 5.1.1. 我們試著解 $29x^2+15x+1\equiv 0\ (\mathrm{mod}\ 45)$. 首先將式子兩邊乘上 4×29, 得 $(58x)^2+2\times 58\times 15x+116\equiv 0\ (\mathrm{mod}\ 45)$. 接著利用配方法得 $(58x+15)^2\equiv 109\ (\mathrm{mod}\ 45)$, 即 $(13x+15)^2\equiv 19\ (\mathrm{mod}\ 45)$ (別忘了 $58x\equiv 13x\ (\mathrm{mod}\ 45)$).

接著因為 $45=3^2\times 5$, 我們可以將式子轉化成解 $(13x+15)^2\equiv 19\ (\mathrm{mod}\ 9)$ 及 $(13x+15)^2\equiv 19\ (\mathrm{mod}\ 5)$. 也就是說分別解 $(4x+6)^2\equiv 1\ (\mathrm{mod}\ 9)$ 以及 $(3x)^2\equiv 4\ (\mathrm{mod}\ 5)$. 由於 $y\equiv\pm 1\ (\mathrm{mod}\ 9)$ 為 $y^2\equiv 1\ (\mathrm{mod}\ 9)$ 之解, 故知 $4x+6\equiv\pm 1\ (\mathrm{mod}\ 9)$, 解得 $x\equiv 1,5\ (\mathrm{mod}\ 9)$ 為 $(13x+15)^2\equiv 19\ (\mathrm{mod}\ 9)$ 之解. 另一方面 $y\equiv\pm 2\ (\mathrm{mod}\ 5)$ 為 $y^2\equiv 4\ (\mathrm{mod}\ 5)$ 之解, 故得 $3x\equiv\pm 2\ (\mathrm{mod}\ 5)$, 解得 $x\equiv 1,4\ (\mathrm{mod}\ 5)$ 為 $(13x^2+15)^2\equiv 19\ (\mathrm{mod}\ 5)$ 之解.

最後要解 $29x^2+15x+1\equiv 0\ (\mathrm{mod}\ 45)$, 由前知 x 需符合:

$$(1)\begin{cases} x\equiv 1 & (\mathrm{mod}\ 9)\\ x\equiv 1 & (\mathrm{mod}\ 5)\end{cases},(2)\begin{cases} x\equiv 1 & (\mathrm{mod}\ 9)\\ x\equiv 4 & (\mathrm{mod}\ 5)\end{cases},$$

$$(3)\begin{cases} x\equiv 5 & (\mathrm{mod}\ 9)\\ x\equiv 1 & (\mathrm{mod}\ 5)\end{cases}\text{或}(4)\begin{cases} x\equiv 5 & (\mathrm{mod}\ 9)\\ x\equiv 4 & (\mathrm{mod}\ 5)\end{cases}.$$

因此求得 $x\equiv 1,14,19,41\ (\mathrm{mod}\ 45)$ 為 $29x^2+15x+1\equiv 0\ (\mathrm{mod}\ 45)$ 之解.

回到我們的主題. 我們將要解一般二次的 congruence equation 化解成解 $x^2\equiv a\ (\mathrm{mod}\ p^n)$, 其中 p 為質數且 $n\in\mathbb{N}$ 的情形. 我們先來看 a 和 p 不互質的情形. 假設 $p^n|a$ 等於解 $x^2\equiv 0\ (\mathrm{mod}\ p^n)$, 此時當然有解. 若 $a=p^ia'$ 其中 $p\nmid a'$ 且 $1\le i\le n-1$ 怎麼辦? 現假若 i 是奇數, 我們要說明此時 $x^2\equiv p^ia'\ (\mathrm{mod}\ p^n)$ 無解. 若有解且 b 為 $x^2\equiv p^ia'\ (\mathrm{mod}\ p^n)$ 之一解, 我們將 b 寫成 $b=p^sb'$, 其中 $p\nmid b'$. 此時因假設 $b^2\equiv p^ia'\ (\mathrm{mod}\ p^n)$, 可得 $p^n|p^{2s}b'^2-p^ia'$. 由於 $2s$ 是偶數而 i 是奇數, 知 $2s\neq i$. 如果 $2s>i$, 則 $p^{2s}b'^2-p^ia'=p^i(p^{2s-i}b'^2-a')$. 但由於 $p|p^{2s-i}$ 且 $p\nmid a'$, 我們知 $p\nmid p^{2s-i}b'^2-a'$. 換言之 $p^{i+1}\nmid p^{2s}b'^2-p^ia'$. 此和 $p^n|p^{2s}b'^2-p^ia'$ 且 $n\ge i+1$ 相矛盾. 同理, 若 $2s<i$, 我們也可得矛盾的情形. 所以當 $i<n$ 且是奇數時 $x^2\equiv p^ia'$ $(\mathrm{mod}\ p^n)$ 無解.

當 $a=p^ia'$ 其中 $p\nmid a'$, $0<i<n$ 且 $i=2k$ 是偶數時, 若我們將 x 寫成 $x=p^kt$, 此時解 $x^2\equiv a\ (\mathrm{mod}\ p^n)$ 等同於解 $(p^kt)^2\equiv p^{2k}a'\ (\mathrm{mod}\ p^n)$, 也就是解 $p^{2k}t^2\equiv p^{2k}a'\ (\mathrm{mod}\ p^n)$. 由於

$2k < n$, Proposition 4.2.1 告訴我們此式等同於解 $t^2 \equiv a' \pmod{p^{n-2k}}$. 我們將以上討論寫成結論.

Proposition 5.1.2. 給定一質數 p 及 $n \in \mathbb{N}$. 假設 $a = p^i a'$ 其中 $p \nmid a'$ 且 $1 \le i \le n-1$.

(1) 若 i 是奇數, 則 $x^2 \equiv a \pmod{p^n}$ 無解.

(2) 若 i 是偶數, 則 $x^2 \equiv a \pmod{p^n}$ 有解若且唯若 $x^2 \equiv a' \pmod{p^{n-i}}$ 有解.

從以上的討論我們知道要解一個二次的 congruence equation 都可以簡化到 $x^2 \equiv a \pmod{p^n}$, 其中 $p \nmid a$ 的情況. 所以以後我們僅專注於 $x^2 \equiv a \pmod{p^n}$ 其中 $p \nmid a$ 的情形.

5.2. 解 $x^2 \equiv a \pmod{p^n}$

在前一節中我們知道一個二次的 congruence equation 可化簡成 $x^2 \equiv a \pmod{p^n}$, 其中 p 為質數, $n \in \mathbb{N}$ 且 $p \nmid a$ 這種形式的問題. 要注意此時由於 $p \nmid a$, 若 $x^2 \equiv a \pmod{p^n}$ 有解, 則其解必也與 p 互質, 否則會造成 $p|a$ 之矛盾. 接著我們就依 $p = 2$ 和 p 為奇質數兩種情形來討論 $x^2 \equiv a \pmod{p^n}$ 解之情況.

5.2.1. $p = 2$ 的情形. 我們先考慮 $x^2 \equiv a \pmod{2^n}$, 其中 $2 \nmid a$ 的情形. 由於 a 是奇數, 所以若有解其解必為奇數. 一開始當然是考慮 $n = 1$ 的情形, 此時因 a 是奇數, 得 $a \equiv 1 \pmod 2$. 所以 $x^2 \equiv a \pmod 2$, 即為 $x^2 \equiv 1 \pmod 2$, 故必有解且解為 $x \equiv 1 \pmod 2$.

當 $n = 2$ 時, 因為 $a \equiv 1, 3 \pmod 4$, 我們僅要考慮 $x^2 \equiv 1 \pmod 4$ 以及 $x^2 \equiv 3 \pmod 4$ 兩種 congruence equations. 由於解必為奇數我們可以假設 $2k+1$ 為一解. 因此由 $(2k+1)^2 = 4k(k+1)+1 \equiv 1 \pmod 8$, 我們知 $x^2 \equiv 3 \pmod 4$ 無解. 而 $x^2 \equiv 1 \pmod 4$ 之解為 $x \equiv \pm 1 \pmod 4$ (即所有奇數).

由上面討論知當 $n = 3$ 時, $x^2 \equiv 3, 5, 7 \pmod 8$ 無解, 而 $x^2 \equiv 1 \pmod 8$ 有解且解為 $x \equiv \pm 1, \pm 3 \pmod 8$. $n > 3$ 時, 我們知道不能如此硬作下去, 可以利用數學歸納法得到以下結果.

Proposition 5.2.1. 假設 $n \ge 3$ 且 a 是一個奇數. 則 $x^2 \equiv a \pmod{2^n}$ 有解若且唯若 $a \equiv 1 \pmod 8$.

Proof. 若 $a \equiv 3, 5, 7 \pmod 8$, 則由前知 $x^2 \equiv a \pmod 8$ 無解. 因為 $n \ge 3$, 故由 Lemma 4.2.3 知 $x^2 \equiv a \pmod{2^n}$ 無解. 因為 a 為奇數故僅剩下 $a \equiv 1 \pmod 8$ 的情形未討論. 所以我們只要證明 $a \equiv 1 \pmod 8$ 時 $x^2 \equiv a \pmod{2^n}$ 有解.

已知 $n = 3$ 時成立. 假設 $n = k-1$ $(k \ge 4)$ 時成立, 即當 $a \equiv 1 \pmod 8$ 時, $x^2 \equiv a \pmod{2^{k-1}}$ 有解. 假設 $c \in \mathbb{Z}$ 是 $x^2 \equiv a \pmod{2^{k-1}}$ 的一個解 (即 $2^{k-1} | c^2 - a$), 也就是說 $c^2 = a + 2^{k-1} b$, 其中 $b \in \mathbb{Z}$. 我們想利用 c 找到 $x^2 \equiv a \pmod{2^k}$ 之解. 若 $c^2 = a + 2^{k-1} b$ 其中 b 為偶數, 則自然 $2^k | c^2 - a$, 得 c 為 $x^2 \equiv a \pmod{2^k}$ 之一解. 若 b 為奇數, 則考慮 $c' = c + 2^{k-2}$. 此時 $c'^2 = c^2 + 2^{k-1} c + 2^{2k-4} = a + 2^{k-1}(b+c) + 2^{2k-4}$. 由於 b 和 c 皆為奇數知 $2 | b+c$, 而且 $2k - 4 = k + k - 4 \ge k$ (因 $k \ge 4$), 故得 $c'^2 \equiv a \pmod{2^k}$. 得證 $x^2 \equiv a \pmod{2^k}$ 有解. □

我們已知 $x^2 \equiv a \pmod{2^n}$ 何時有解何時無解. 若有解時, 其在 modulo 2^n 之下會有多少解呢? 我們依然用兩個解之間的關係來探討.

Proposition 5.2.2. 假設 $n \geq 3$ 且 $a \equiv 1 \pmod 8$. 若 $x \equiv c \pmod{2^n}$ 是 $x^2 \equiv a \pmod{2^n}$ 的一個解, 則 $x \equiv c, c+2^{n-1}, -c, -c+2^{n-1} \pmod{2^n}$ 為 $x^2 \equiv a \pmod{2^n}$ 所有的解.

Proof. 若 $c' \in \mathbb{Z}$ 亦為一解, 則 $2^n | c^2 - c'^2$, 即 $2^n | (c-c')(c+c')$. 要注意因為 c 和 c' 皆為奇數, 我們可以有 $c \equiv \pm 1 \pmod 4$ 和 $c' \equiv \pm 1 \pmod 4$, 四種情形. 不過不管是哪一種情形 $c-c'$ 和 $c+c'$ 之中必有一個 (且僅有一個) 不能被 4 整除 (但仍為偶數). 例如在 $c \equiv 1 \pmod 4$ 及 $c' \equiv -1 \pmod 4$ 的情況, 我們有 $c+c' \equiv 0 \pmod 4$ 但 $c-c' \equiv 2 \pmod 4$. 即 $2 | c-c'$ 但 $4 \nmid c-c'$. 我們先考慮 $4 \nmid c+c'$ 這種情形. 此時 $c+c' = 2\lambda$, 其中 λ 為奇數. 因此由前面已知 $2^n | (c-c')(c+c')$, 得 $2^n | 2\lambda(c-c')$, 即 $2^{n-1} | \lambda(c-c')$. 現由於 $\gcd(2, \lambda) = 1$, 故由 Proposition 1.2.6(1) 得 $2^{n-1} | c-c'$. 同理若 $4 \nmid c-c'$, 則知 $2^{n-1} | c+c'$.

總結來說, 若 c' 是 $x^2 \equiv a \pmod{2^n}$ 之一解, 則存在 $t \in \mathbb{Z}$ 使得 $c' = c + t2^{n-1}$ 或 $c' = -c + t2^{n-1}$. 反之若 $c' = c + 2^{n-1}$, 則 $c'^2 = c^2 + 2^n ct + 2^{2n-2} t^2$. 由於 $2n-2 \geq n+1$, 得 $c'^2 \equiv c^2 \equiv a \pmod{2^n}$. 故知 c' 為 $x^2 \equiv a \pmod{2^n}$ 之一解. 同理 $c' = -c + t2^{n-1}$ 亦為 $x^2 \equiv a \pmod{2^n}$ 之一解. 然而當 t 是奇數時 $c' = c + t2^{n-1} \equiv c + 2^{n-1} \pmod{2^n}$ 且 $c' = -c + t2^{n-1} \equiv -c + 2^{n-1} \pmod{2^n}$. 而當 t 是偶數時 $c' = c + t2^{n-1} \equiv c \pmod{2^n}$ 且 $c' = -c + t2^{n-1} \equiv -c \pmod{2^n}$. 故得知在 modulo 2^n 之下 $x^2 \equiv a \pmod{2^n}$ 共有 $x \equiv c, c+2^{n-1}, -c+2^{n-1}, -c \pmod{2^n}$ 這 4 個根 (注意因 c 為奇數, 所以這些數在 modulo 2^n 之下皆相異). □

我們來看個例子.

Example 5.2.3. 解 $x^2 \equiv 17 \pmod{32}$. 由於 $17 \equiv 1 \pmod 8$, 由 Proposition 5.2.1 知必有解. 我們利用 Proposition 5.2.1 證明中所用的方法來找出一個解. 首先解 $x^2 \equiv 17 \pmod{2^{5-1}}$, 即 $x^2 \equiv 1 \pmod{16}$. 可知 $x = 1$ 為 $x^2 \equiv 17 \pmod{16}$ 之一解. 但由於 $1^2 - 17 = 2^4 \times (-1)$ 且 -1 是奇數, 故利用 Proposition 5.2.1 的證明知 $1 + 2^{(5-2)} = 9$ 為 $x^2 \equiv 17 \pmod{32}$ 之一解. 找到一解後, 最後利用 Proposition 5.2.2 知 $x \equiv 9, 25, 7, 23 \pmod{32}$ 為 $x^2 \equiv 17 \pmod{32}$ 所有的解.

5.2.2. p 為奇質數的情形. 當 p 是奇質數時, 我們當然不能如 $p = 2$ 的情形討論. 不過由 Lemma 4.2.3 我們知若 $x^2 \equiv a \pmod p$ 無解, 則對任意 $n \in \mathbb{N}$, $x^2 \equiv a \pmod{p^n}$ 亦無解. 我們要用數學歸納法證明若 $x^2 \equiv a \pmod p$ 有解, 則對任意 $n \in \mathbb{N}$, $x^2 \equiv a \pmod{p^n}$ 亦有解.

Proposition 5.2.4. 假設 p 為一奇質數且 $p \nmid a$. 則 $x^2 \equiv a \mod p$ 有解若且唯若對任意 $n \in \mathbb{N}$, $x^2 \equiv a \pmod{p^n}$ 有解.

Proof. 我們僅要證明若 $x^2 \equiv a \pmod p$ 有解則 $x^2 \equiv a \pmod{p^n}$ 亦有解.

若 c 為 $x^2 \equiv a \pmod p$ 之一解, 即存在 $\lambda \in \mathbb{Z}$ 使得 $c^2 = a + \lambda p$. 現考慮 $c' = c + tp$. 由於 $c'^2 = c^2 + 2ctp + t^2 p^2 = a + (2ct + \lambda)p + t^2 p^2$. 若要 $c'^2 \equiv a \pmod{p^2}$, 則需找到 $t \in \mathbb{Z}$ 使得 $2ct \equiv -\lambda \pmod p$. 然而由於 $2c$ 和 p 互質, Theorem 4.3.4 告訴我們這樣的 t 一定存在. 故此時若令 $c' = c + tp$, 則 $x \equiv c' \pmod{p^2}$ 為 $x^2 \equiv a \pmod{p^2}$ 之一解.

現利用數學歸納法假設 $n = k-1$ $(k \geq 2)$ 時 $x^2 \equiv a \pmod{p^{k-1}}$ 有解, 且假設 $x \equiv c \pmod{p^{k-1}}$ 為其一解. 我們想利用 c 找到 $x^2 \equiv a \pmod{p^k}$ 的解. 由於存在 $\lambda \in \mathbb{Z}$ 使得 $c^2 - a = \lambda p^{k-1}$, 我們考慮 $c' = c + tp^{k-1}$. 此時 $c'^2 = c^2 + 2ctp^{k-1} + t^2p^{2k-2} = a + (2ct+\lambda)p^{k-1} + t^2p^{2k-2}$. 由於 $2k-2 = k+k-2 \geq k$ (因 $k \geq 2$) 我們得 $c'^2 \equiv a + (2ct+\lambda)p^{k-1} \pmod{p^k}$. 又因為 $2c$ 和 p 互質, 故存在 $t' \in \mathbb{Z}$ 使得 $2ct' + \lambda \equiv 0 \pmod{p}$. 此時若令 $c' = c + t'p$, 則 $x \equiv c' \pmod{p^k}$ 為 $x^2 \equiv a \pmod{p^k}$ 之一解. □

如果 $x^2 \equiv a \pmod{p^n}$ 有解, 我們當然有興趣知道在 modulo p^n 之下, $x^2 \equiv a \pmod{p^n}$ 其解的個數.

Proposition 5.2.5. 假設 p 為一奇質數, $p \nmid a$ 且 $n \in \mathbb{N}$. 若 $x^2 \equiv a \mod p^n$ 有解且 $x \equiv c \pmod{p^n}$ 為其一解, 則 $x \equiv \pm c \pmod{p^n}$ 為 $x^2 \equiv a \pmod{p^n}$ 所有的解.

Proof. 假設 c' 為 $x^2 \equiv a \pmod{p^n}$ 之另一解, 知 $p^n | c^2 - c'^2$. 由於 c 和 c' 皆與 p 互質, $c+c'$ 和 $c-c'$ 知中必有一個與 p 互質, 否則由 $p|c+c'$ 及 $p|c-c'$ 可得 $p|2c$, 而又 $p \neq 2$, 可得 $p|c$ 之矛盾. 現假設 $c+c'$ 與 p 互質, 此時 $\gcd(c+c', p^n) = 1$, 故由 $p^n | (c+c')(c-c')$ 及 Proposition 1.2.6(1), 得知 $p^n | c-c'$, 即 $c' \equiv c \pmod{p^n}$. 同理, 若 $c-c'$ 與 p 互質, 可得 $c' \equiv -c \pmod{p^n}$.

另一方面, 由 $c^2 \equiv a \pmod{p^n}$ 知 $(-c)^2 = c^2 \equiv a \pmod{p^n}$, 故知 $x \equiv \pm c \pmod{p^n}$ 為 $x^2 \equiv a \pmod{p^n}$ 所有的解. □

我們再來看個例子.

Example 5.2.6. 解 $x^2 \equiv 14 \pmod{125}$. 由於 $x^2 \equiv 14 \equiv 4 \pmod{5}$ 有解 ($x = 2$ 為一解), 由 Proposition 5.2.4 知 $x^2 \equiv 14 \pmod{125}$ 必有解. 我們利用 Proposition 5.2.4 證明中所用的方法來找出一個解. 首先找出 $x^2 \equiv 14 \pmod{25}$ 之一個解. 利用 2 為 $x^2 \equiv 14 \pmod{5}$ 之一解, 考慮 $(2+5t)^2 = 4 + 20t + 25t^2$. 因此 $(2+5t)^2 - 14 \equiv -10 + 20t \pmod{25}$. 也就是說需解出 $t \in \mathbb{Z}$ 使得 $20t \equiv 10 \pmod{25}$, 即解 $4t \equiv 2 \pmod{5}$. 可得 $t = 3$ 為一解, 故帶入 $2+5t$ 得 $x = 17$ 為 $x^2 \equiv 14 \pmod{25}$ 之一解. 現再利用 17 求 $x^2 \equiv 14 \pmod{125}$ 之一解. 考慮 $(17+25t)^2 = 289 + 850t + 625t^2$. 因此 $(17+25t)^2 - 14 \equiv 275 + 850t \equiv 25 + 100t \pmod{125}$. 也就是說需解出 $t \in \mathbb{Z}$ 使得 $100t \equiv -25 \pmod{125}$, 即解 $4t \equiv -1 \pmod{5}$. 可得 $t = 1$ 為一解, 故帶入 $17+25t$ 得 $x = 42$ 為 $x^2 \equiv 14 \pmod{125}$ 之一解. 找到一解後, 最後利用 Proposition 5.2.2 知 $x \equiv \pm 42 \pmod{125}$ 為 $x^2 \equiv 14 \pmod{125}$ 所有的解.

我們已完全了解 $x^2 \equiv a \pmod{2^n}$ 的解的情況. 而當 p 是奇質數時, 對任意 $n \in \mathbb{N}$, $x^2 \equiv a \pmod{p^n}$ (其中 $p \nmid a$) 的解的情況完全取決於 $x^2 \equiv a \pmod{p}$ 的解的情況. 所以以後我們僅專注於 $x^2 \equiv a \pmod{p}$ 其中 p 為奇質數且 $p \nmid a$ 的情形.

5.3. The Legendre Symbol

我們已經把解一般的二次 congruence equation 一步一步的化簡到解 $x^2 \equiv a \pmod{p}$, 其中 p 為奇質數且 $p \nmid a$ 的情形. 這裡我們將探討何時 $x^2 \equiv a \pmod{p}$ 有解. 至於若有解如何找解, 我們留待下一章學習更多方法後再處理.

由於我們只關注 $x^2 \equiv a \pmod{p}$ 何時有解, 何時無解, 我們介紹一個符號稱 (Legendre symbol) 來表示其有解或無解.

Definition 5.3.1. 給定奇質數 p 以及 $a \in \mathbb{Z}$ 滿足 $p \nmid a$. 若 $x^2 \equiv a \pmod{p}$ 有解, 我們稱 a 是一個 *quadratic residue* modulo p 並以 $\left(\frac{a}{p}\right) = 1$ 表示之. 反之, 若 $x^2 \equiv a \pmod{p}$ 無解, 我們稱 a 是一個 *quadratic nonresidue* modulo p 並以 $\left(\frac{a}{p}\right) = -1$ 表示之.

首先要注意的是 Legendre symbol 不要和分數搞混. 在本講義中的分數如三分之二的平方我們會用 $(\frac{2}{3})^2$ 或 $(2/3)^2$ 這兩種方法表示, 括號比較小. 而 Legendre symbol $\left(\frac{2}{3}\right)$ 的括號比較大. 另外依定義 Legendre symbol 的分母一定是一個奇質數且分子一定和分母互質 (有的書規定不同, 這裡為了不讓同學搞混我們嚴格如此規定). 例如在本講義中 $\left(\frac{5}{6}\right)$ 或 $\left(\frac{6}{3}\right)$ 這樣的符號是沒意義的.

接下來我們來看 Legedre symbol 直接依定義所得之性質.

Lemma 5.3.2. 假設 p 是一個奇質數且 $a \in \mathbb{Z}$ 滿足 $p \nmid a$.

(1) $\left(\frac{a^2}{p}\right) = 1$.

(2) 若 $b \in \mathbb{Z}$ 滿足 $b \equiv a \pmod{p}$, 則 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proof. (1) 要判斷 a^2 是否為 quadratic residue modulo p, 也就是要判斷 $x^2 \equiv a^2 \pmod{p}$ 是否有解. 然而很容易知道 $x = a$ 是 $x^2 \equiv a^2 \pmod{p}$ 的解, 故知 $\left(\frac{a^2}{p}\right) = 1$.

(2) 要判斷 b 是否為 quadratic residue modulo p, 也就是要判斷 $x^2 \equiv b \pmod{p}$ 是否有解. 然而依假設 $b \equiv a \pmod{p}$ 故要解 $x^2 \equiv b \pmod{p}$ 就等同於解 $x^2 \equiv a \pmod{p}$. 故知 $\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)$. □

其實 $x^2 \equiv a \pmod{p}$ 要不然有解要不然就無解. 所以若僅將 Legendre symbol 看成只是一個符號表示有解無解就太小看它了. 若要定符號, 我們也可以將有解定為 1 無解定為 0, 或其他相異的兩個數, 為何要將有解定為 1 無解定為 -1 呢? 說實話若僅想用兩個數字來表示有解或無解的情況, 那真的是怎麼定值都可以, 然而如此一來這樣的符號頂多僅讓我們方便表達有解或無解的情況, 沒有什麼太大的意義. Legendre symbol 之所以要將有解定為 1 無解定為 -1, 主要是我們可以將它們看成整數的 1 和 -1 來做乘法運算. 其原因就是下面這一個定理.

Theorem 5.3.3 (Euler's Criterion)**.** 假設 p 是一個奇質數且 $a \in \mathbb{Z}$ 滿足 $p \nmid a$.

(1) 若 $x^2 \equiv a \pmod{p}$ 有解, 則 $a^{(p-1)/2} \equiv 1 \pmod{p}$.

(2) 若 $x^2 \equiv a \pmod{p}$ 無解, 則 $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Proof. (1) 若 $x^2 \equiv a \pmod{p}$ 有解且 $x = c$ 為其一解, 即 $c^2 \equiv a \pmod{p}$. 此時

$$a^{\frac{p-1}{2}} \equiv (c^2)^{\frac{p-1}{2}} \equiv c^{p-1} \pmod{p}.$$

由於 a 和 p 互質, 所以 $x^2 \equiv a \pmod{p}$ 之解 c 亦與 p 互質. 因此利用 Fermat's Little Theorem (3.3.4) 知 $c^{p-1} \equiv 1 \pmod{p}$, 故得證 $a^{(p-1)/2} \equiv 1 \pmod{p}$.

(2) 考慮 $S = \{1, 2, \ldots, p-1\}$ 這一個 reduced residue system modulo p. 對任意 $i \in S$, 由於 i 和 p 互質, 故由 Theorem 4.3.4 知 $ix \equiv a \pmod{p}$ 在 modulo p 之下有唯一解. 由於 a 和 p 互質, 故知其解必也與 p 互質. 換句話說, 給定 $i \in S$ 必存在唯一的 $j \in S$ 滿足 $ij \equiv a \pmod{p}$. 要注意此時 $j \neq i$, 否則會得到 $i^2 \equiv a \pmod{p}$, 也就是說 $x = i$ 是 $x^2 \equiv a \pmod{p}$ 的一個解, 此與 $x^2 \equiv a \pmod{p}$ 無解的假設相矛盾. 另一方面也要注意因為 $jx \equiv a \pmod{p}$ 在 modulo p 之下其解唯一且已知 $x = i$ 為其一解, 所以不可能找到另一個 $i' \in S$ 使得 $i'j \equiv a \pmod{p}$. 因此對於 S 中的元素, 我們可以將之兩兩配對, 也就是對任意 $i \in S$ 將 i 和滿足 $ij \equiv a \pmod{p}$ 唯一的 $j \in S$ 相配對. 如此一來我們共有 $(p-1)/2$ 對. 由於每一對相乘在 modulo p 之下和 a congruent, 故可得

$$(p-1)! = 1 \cdot 2 \cdots p-1 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

不過 Wilson's Theorem (3.4.3) 告訴我們 $(p-1)! \equiv -1 \pmod{p}$, 故得證 $a^{(p-1)/2} \equiv -1 \pmod{p}$. □

如果大家不健忘的話, 當初在證明 Wilson's Theorem 我們是將 $S = \{1, \ldots, p-1\}$ 中之元素依 $ij \equiv 1 \pmod{p}$ 來配對. 所以 Wilson's Theorem 和 Euler's Criterion 的證明有異曲同工之妙.

當 $p \nmid a$ 時 $a^{(p-1)/2}$ 在 modulo p 之下之值不是 1 就是 -1. 這是因為若令 $b = a^{(p-1)/2}$, 則 $b^2 = a^{p-1} \equiv 1 \pmod{p}$, 也就是說 $x = b$ 為 $x^2 \equiv 1 \pmod{p}$ 之一根. 因此由 Lemma 3.4.2 知 $b \equiv \pm 1 \pmod{p}$. 因此, 給定 $a \in \mathbb{Z}$ 滿足 $p \nmid a$, 我們可以由 $a^{(p-1)/2}$ modulo p 為 1 或 -1 來判斷 $x^2 \equiv a \pmod{p}$ 是否有解. 例如, 若 $a^{(p-1)/2} \equiv 1 \pmod{p}$ 而又 $\left(\frac{a}{p}\right) = -1$, 則因 $x^2 \equiv a \pmod{p}$ 無解由 Theorem 5.3.3 知 $a^{(p-1)/2} \equiv -1 \pmod{p}$. 這會造成 $1 \equiv -1 \pmod{p}$ 即 $p|2$ 的矛盾. 因此我們知, 若 $a^{(p-1)/2} \equiv 1 \pmod{p}$, 則 $\left(\frac{a}{p}\right) = 1$. 同理, 若 $a^{(p-1)/2} \equiv -1 \pmod{p}$, 則 $\left(\frac{a}{p}\right) = -1$. 這就是 Legendre symbol 取 1 和 -1 為值的理由. 我們有以下之結論.

Corollary 5.3.4. 假設 p 是一個奇質數且 $a \in \mathbb{Z}$ 滿足 $p \nmid a$. 則

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

所以今後我們要知道 $x^2 \equiv a \pmod{p}$ 有解或無解, 只要去算 $a^{(p-1)/2}$ 除以 p 的餘數是 1 或 $p-1$. 若餘數是 1 則有解, 若餘數是 $p-1$ 則無解. 不過這個方法在實際狀況下仍很費事, 因為要計算 $a^{(p-1)/2}$ 一般來說當 p 很大時仍很很麻煩. 不過這個 criterion 在證明一般抽象的定理時就很管用了. 我們有以下有關 Legendre symbol 的重要性質.

Proposition 5.3.5. 假設 p 是一個奇質數且 $a,b \in \mathbb{Z}$ 滿足 $p \nmid a$ 且 $p \nmid b$. 則

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. 由 Corollary 5.3.4 知

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

由於 $\left(\frac{ab}{p}\right)$ 和 $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ 之值要不是 1 就是 -1, 所以他們在 modulo p 之下同餘表示必相等 (否則又會得 $p|2$ 之矛盾). 故得 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

Proposition 5.3.5 可以推出很令人吃驚的結果. 例如假設 $x^2 \equiv a \pmod{a}$ 和 $x^2 \equiv b \pmod{p}$ 皆有解且設 $x = c$ 和 $x = c'$ 分別為其一解. 那麼我們很容易推得 $x^2 \equiv ab \pmod{p}$ 必有解. 因為 $x = cc'$ 就是其中之一解. 不過若 $x^2 \equiv a \pmod{a}$ 和 $x^2 \equiv b \pmod{p}$ 其中有一個無解或是皆無解, 那們我們就很難利用解方程式的方法來處理 $x^2 \equiv ab \pmod{p}$ 是否有解了. 不過若利用 Proposition 5.3.5, 我們很快的便知若 $x^2 \equiv a \pmod{p}$ 有解但 $x^2 \equiv b \pmod{p}$ 無解 (即 $\left(\frac{a}{p}\right) = 1$, $\left(\frac{b}{p}\right) = -1$), 則 $x^2 \equiv ab \pmod{p}$ 便無解 (因為此時 $\left(\frac{ab}{p}\right) = 1 \times (-1) = -1$). 更令人訝異的是若 $x^2 \equiv a \pmod{p}$ 和 $x^2 \equiv b \pmod{p}$ 皆無解, 我們可以知 $x^2 \equiv ab \pmod{p}$ 必有解 (因為此時 $\left(\frac{ab}{p}\right) = (-1) \times (-1) = 1$). 這個結果是很難用有解無解這樣的角度來判斷的.

Proposition 5.3.5 另一個好處是對任意整數 a 我們可以分解成 $a = (-1)^m 2^{n_0} q_1^{n_1} \cdots q_r^{n_r}$, 其中 q_i 為奇質數 (且 $p \neq q_i$ 因 $p \nmid a$), $m \in \{0,1\}$, $n_i \geq 0$. 因此可得

$$\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)^m \left(\frac{2}{p}\right)^{n_0} \left(\frac{q_1}{p}\right)^{n_1} \cdots \left(\frac{q_r}{p}\right)^{n_r}.$$

也就是說給定一奇質數 p, 我們只要知道 $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ 和 $\left(\frac{q}{p}\right)$ (q 為任意與 p 相異的奇質數) 之值, 那麼對任意與 p 互質的整數 a, 就可以算出 $\left(\frac{a}{p}\right)$ 之值了.

我們從原來要了解一般二次的 congruence equation 解的情形, 一路化簡到現在只要了解 $x^2 \equiv -1 \pmod{p}$, $x^2 \equiv 2 \pmod{p}$ 和 $x^2 \equiv q \pmod{p}$ (其中 q 是與 p 相異的奇質數), 這三種簡單形式的情形. 這就是解決數學問題常遇到的由繁化簡的過程, 值得大家細細體會其中的演化. 另一件有趣的是 Legendre symbol 和 Euler's Criterion 幫助我們將一個原本解二次 congruence equation 的問題換成另外一個和解方程式完全無關的方法來處理. 接下來

我們就是要利用這樣的方式來處理 $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ 和 $\left(\frac{q}{p}\right)$, 而不再直接探討 $x^2 \equiv -1, 2, q \pmod{p}$ 有解或是無解.

5.4. Quadratic Reciprocity Law

我們僅剩下要討論 $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ 和 $\left(\frac{q}{p}\right)$ 之值. 在這節中 p 和 q 永遠表示兩相異奇質數, 我們就不另加說明了.

5.4.1. 求 $\left(\frac{-1}{p}\right)$. 我們首先探討 $\left(\frac{-1}{p}\right)$ 的取值情形. 或許大家會疑惑當 a 是一個負整數時, 一定可以找到一正整數 b 使得 $a \equiv b \pmod{p}$, 因此利用 Lemma 5.3.2(2) 我們有 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, 所以只要探討正整數的情況就好了為何還要考慮負的情況呢? 沒錯, 一般來說我們只要知道正整數的情形就足夠了, 不過考慮負整數也有其方便性. 例如我們要求 $\left(\frac{97}{101}\right)$. 因為 $97 \equiv -4 = (-1) \times 2^2 \pmod{101}$, 利用 Lemma 5.3.2 以及 Proposition 5.3.5 馬上可得 $\left(\frac{97}{101}\right) = \left(\frac{-1}{101}\right)$. 另一方面在 modulo p 之下是否有元素像複數中的 i 一樣滿足 $i^2 = -1$ 原本也就是一個有趣的問題. 所以了解 $\left(\frac{-1}{p}\right)$ 之值事實上是必要的.

Euler's Criterion 雖然在算一般的 $\left(\frac{a}{p}\right)$ 不是很好用, 不過在算 $\left(\frac{-1}{p}\right)$ 就很好用了.

Theorem 5.4.1. 假設 p 是奇質數, 則

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{當 } p \equiv 1 \pmod{4}; \\ -1, & \text{當 } p \equiv -1 \pmod{4}. \end{cases}$$

Proof. 利用 Corollary 5.3.4 我們知

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

若 $p \equiv 1 \pmod{4}$, 表示存在 $k \in \mathbb{N}$ 使得 $p = 4k+1$, 故得 $(-1)^{(p-1)/2} = (-1)^{2k} = 1$. 因此得證 $\left(\frac{-1}{p}\right) = 1$. 若 $p \equiv -1 \pmod{4}$, 表示存在 $k \in \mathbb{N}$ 使得 $p = 4k-1$, 故得 $(-1)^{(p-1)/2} = (-1)^{2k-1} = -1$. 因此得證 $\left(\frac{-1}{p}\right) = -1$. □

要注意由於 p 是奇質數, 因此 p 在 modulo 4 之下要不然和 1 同餘要不然就和 -1 同餘, 所以 Theorem 5.4.1 給了 $\left(\frac{-1}{p}\right)$ 完整的答案. 今後我們要知道 $x^2 \equiv -1 \pmod{p}$ 是否有解時, 只要看 p 在 modulo 4 之情形就可以知道答案. 例如剛才我們想知道 $x^2 \equiv 97 \pmod{101}$ 是否有解, 由 $\left(\frac{97}{101}\right) = \left(\frac{-1}{101}\right)$ 以及 $101 \equiv 1 \pmod{4}$ 馬上知道 $x^2 \equiv 97 \pmod{101}$ 是有解的.

5.4.2. 求 $\left(\frac{2}{p}\right)$. 接下來我們要探討 $\left(\frac{2}{p}\right)$ 的取值情形. 會將 2 和一般的奇質數分開討論的原因是因為 2 是唯一的偶質數, 其表現在很多狀況是和奇質數不同的, 事實上我們在前面已經看到許多在 2 的情況和一般奇質數有很大不同的情形例如 $x^2 \equiv a \pmod{2^n}$ 和 $x^2 \equiv a \pmod{p^n}$ 這兩種 congruence equation 其解的形態就完全不同.

我們還是要用 Euler's criterion 的精神來求 $\left(\frac{2}{p}\right)$ 而不是直接探討 $x^2 \equiv 2 \pmod{p}$ 何時有解. 然而 Euler's criterion 並不能直接套用來求 $\left(\frac{2}{p}\right)$, 主要原因是我們這裡的 p 是一般的奇質數而不是特定的奇質數, 所以根本無法估計 $2^{(p-1)/2}$ 在 modulo p 之下為 1 或 -1. 我們必須推導出另外的方法可以幫助我們求 $2^{(p-1)/2}$ 在 modulo p 之情形.

Lemma 5.4.2 (Gauss's Lemma)**.** 假設 p 是奇質數且 $a \in \mathbb{Z}$ 滿足 $p \nmid a$. 考慮集合 $S = \{a, 2a, \ldots, \frac{p-1}{2}a\}$. 若 S 中共有 n 個元素其除以 p 的餘數大於 $(p-1)/2$, 則

$$a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}.$$

Proof. 我們將 S 中的元素除以 p 的餘數分成 $r_1, \ldots, r_n$ 及 $s_1, \ldots, s_m$ 兩部份, 其中 r_i 是大於 $(p-1)/2$ 的部份, 而 s_j 表小於等於 $(p-1)/2$ 的部份. 由於 S 中的元素皆與 p 互質, 所以對所有的 $i \in \{1, \ldots, n\}$ 和 $j \in \{1, \ldots, m\}$ 依 r_i, s_j 的定義我們知存在 $1 \le n_i \le (p-1)/2$ 使得 $n_i a$ 除以 p 的餘數為 r_i 且 $(p+1)/2 \le r_i \le p-1$, 另一方面存在 $1 \le m_j \le (p-1)/2$ 使得 $m_j a$ 除以 p 的餘數為 s_j 且 $1 \le s_j \le (p-1)/2$. 要注意此時 $n+m = (p-1)/2$, 現考慮 $T = \{p-r_1, \ldots, p-r_n, s_1, \ldots, s_m\}$, 我們要證明 $T = \{1, 2, \ldots, (p-1)/2\}$.

要證明 $T = \{1, 2, \ldots, (p-1)/2\}$. 我們先證明 $T \subseteq \{1, 2, \ldots, (p-1)/2\}$. 然而對任意的 $i \in \{1, \ldots, n\}$ 我們有 $p - r_i \le p - (p+1)/2 = (p-1)/2$ 且 $p - r_i \ge p - (p-1) = 1$, 故知 $p - r_i \in \{1, 2, \ldots, (p-1)/2\}$. 另一方面對任意 $j \in \{1, \ldots, m\}$ 已知 $1 \le s_j \le (p-1)/2$ 故得證 $T \subseteq \{1, 2, \ldots, (p-1)/2\}$.

接下來我們證明 $p - r_i$, $i \in \{1, \ldots, n\}$ 和 s_j, $j \in \{1, \ldots, m\}$ 這 $n+m$ (即 $(p-1)/2$) 個元素皆相異, 便可得證 $T = \{1, 2, \ldots, (p-1)/2\}$. 所以我們要證明 (1): $1 \le i \ne i' \le n$ 時, $p - r_i \ne p - r_{i'}$; (2): $1 \le j \ne j' \le m$ 時, $s_j \ne s_{j'}$ 以及 (3): 對任意 $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, m\}$, $p - r_i \ne s_j$.

當 $1 \le i \ne i' \le n$ 時, 若 $p - r_i = p - r_{i'}$ 表示 $r_i = r_{i'}$, 依定義即 $n_i a$ 和 $n_{i'} a$ 除以 p 的餘數相同, 也就是說 $n_i a \equiv n_{i'} a \pmod{p}$. 然而已假設 a 和 p 互質故由 Corollary 3.2.4 知 $n_i \equiv n_{i'} \pmod{p}$. 但此與 $1 \le n_i \ne n_{i'} \le (p-1)/2$ 的假設矛盾, 故得證 $p - r_i \ne p - r_{i'}$, 即 (1) 是對的. 同理可證得 (2) 是對的. 至於 (3), 若 $p - r_i = s_j$, 表示 $r_i + s_j = p$, 可得 $n_i a + m_j a \equiv 0 \pmod{p}$. 故再由 Corollary 3.2.4 得 $n_i + m_j \equiv 0 \pmod{p}$. 然而 $1 \le n_i, m_j \le (p-1)/2$, 得 $2 \le n_i + m_j \le p-1$, 不可能滿足 $p | n_i + m_j$, 故得證 $p - r_i \ne s_j$.

既然 $T = \{1, 2, \ldots, (p-1)/2\}$, 我們得

$$\frac{p-1}{2}! = (p-r_1)\cdots(p-r_n)\cdot s_1 \cdots s_m \equiv (-1)^n r_1 \cdots r_n \cdot s_1 \cdots s_m \pmod{p}.$$

另一方面 $S=\{a,2a,\dots,\frac{p-1}{2}a\}$ 中元素除以 p 的餘數所成的集合為 $\{r_1,\dots,r_n,s_1,\dots,s_m\}$, 故得

$$r_1\cdots r_n\cdot s_1\cdots s_m\equiv a\cdot 2a\cdots\frac{p-1}{2}a=\frac{p-1}{2}!\cdot a^{\frac{p-1}{2}}\pmod p.$$

和上式整理得

$$\frac{p-1}{2}!\equiv(-1)^n\frac{p-1}{2}!\cdot a^{\frac{p-1}{2}}\pmod p.$$

因為 $\frac{p-1}{2}!$ 和 p 互質, 故由 Corollary 3.2.4 知

$$1\equiv(-1)^n a^{\frac{p-1}{2}}\pmod p,$$

即

$$a^{\frac{p-1}{2}}\equiv(-1)^n\pmod p.$$

□

若 $\{a,2a,\dots,\frac{p-1}{2}a\}$ 中共有 n 個元素除以 p 的餘數大於 $(p-1)/2$, 則由 Corollary 5.3.4 以及 Lemma 5.4.2 知

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\equiv(-1)^n\pmod p.$$

故由 $\left(\frac{a}{p}\right)$ 的取值為 ±1, 得

$$\left(\frac{a}{p}\right)=(-1)^n.$$

Gauss's Lemma 將繁複 $a^{(p-1)/2}$ 的計算換成計算 $\{a,2a,\dots,\frac{p-1}{2}a\}$ 中有多少個除以 p 的餘數大於 $(p-1)/2$, 確實將問題簡化了. 我們可以利用它來計算 $\left(\frac{2}{p}\right)$.

Theorem 5.4.3. 假設 p 是奇質數, 則

$$\left(\frac{2}{p}\right)=\begin{cases}1, & \text{當 } p\equiv\pm1\pmod 8;\\ -1, & \text{當 } p\equiv\pm3\pmod 8.\end{cases}$$

Proof. 考慮 $S=\{2,2\times2,\dots,\frac{p-1}{2}\times2\}$, 我們得 $S=\{2,4,\dots,p-1\}$. 也就是說 S 中的元數除以 p 所得餘數所成的集合恰為 S, 即小於 p 的正偶數所成之集合. 由於 p 是奇數, 我們將之分成 $p\equiv\pm1,\pm3\pmod 8$ 四種情形來討論. 看看 S 中有多少元素大於 $(p-1)/2$.

當 $p=8k+1$ (即 $p\equiv1\pmod 8$) 時, $(p-1)/2=4k$. 因此 S 中大於 $(p-1)/2$ 的元素個數即為小於等於 $p-1=8k$ 且大於 $4k$ 的偶數之個數. 知其共有 $(8k-4k)/2=2k$. 故由 Corollary 5.3.4 以及 Lemma 5.4.2 知

$$\left(\frac{2}{p}\right)=(-1)^{2k}=1.$$

當 $p=8k-1$ (即 $p\equiv-1\pmod 8$) 時, $(p-1)/2=4k-1$. 因此 S 中大於 $(p-1)/2$ 的元素個數即為小於等於 $p-1=8k-2$ 且大於 $4k-1$ 的偶數之個數. 知其共有 $(8k-2-(4k-$

$2))/2 = 2k$. 故由 Corollary 5.3.4 以及 Lemma 5.4.2 知

$$\left(\frac{2}{p}\right) = (-1)^{2k} = 1.$$

當 $p = 8k+3$ (即 $p \equiv 3 \pmod 8$) 時, $(p-1)/2 = 4k+1$. 因此 S 中大於 $(p-1)/2$ 的元素個數即為小於等於 $p-1 = 8k+2$ 且大於 $4k+1$ 的偶數之個數. 知其共有 $(8k+2-4k)/2 = 2k+1$. 故由 Corollary 5.3.4 以及 Lemma 5.4.2 知

$$\left(\frac{2}{p}\right) = (-1)^{2k+1} = -1.$$

當 $p = 8k-3$ (即 $p \equiv -3 \pmod 8$) 時, $(p-1)/2 = 4k-2$. 因此 S 中大於 $(p-1)/2$ 的元素個數即為小於等於 $p-1 = 8k-4$ 且大於 $4k-2$ 的偶數之個數. 知其共有 $(8k-4-(4k-2))/2 = 2k-1$. 故由 Corollary 5.3.4 以及 Lemma 5.4.2 知

$$\left(\frac{2}{p}\right) = (-1)^{2k-1} = -1.$$

□

有了 Theorem 5.4.3, 給定一奇質數 p, 我們將很容易知道 $x^2 \equiv 2 \pmod p$ 是否有解. 例如因為 $101 \equiv 5 \equiv -3 \pmod 8$, 故知 $x^2 \equiv 2 \pmod{101}$ 無解. 而 $23 \equiv -1 \pmod 8$ 故知 $x^2 \equiv 2 \pmod{23}$ 有解. 事實上 $5^2 \equiv 2 \pmod{23}$, 故知 $x \equiv \pm 5 \pmod{23}$ 為 $x^2 \equiv 2 \pmod{23}$ 之解.

5.4.3. 求 $\left(\frac{q}{p}\right)$. 最後我們來探討 p,q 為相異奇質數的情形. 若給定了 p 和 q 我們當然就可以利用 Gauss's Lemma 求 $\left(\frac{q}{p}\right)$, 不過現在要討論的是一般的 p 和 q, 我們必須考慮別的方法.

在 Gauss's Lemma 中我們需要算出 $\{a, 2a, \ldots, \frac{p-1}{2}a\}$ 中有多少元素其除以 p 的餘數大於 $(p-1)/2$. 若其個數為 n, 則 $\left(\frac{a}{p}\right) = (-1)^n$. 由於 $(-1)^n$ 的取值完全取決於 n 是奇數或偶數, 所以我們並不需精確地算出 n 為多少, 只需確認其為奇數或偶數即可. 以下我們將介紹一個判別 n 為奇或偶的方法, 不過由於我們要考慮的 $\left(\frac{q}{p}\right)$ 其中 q 為奇質數, 所以底下的方法中我們僅考慮 a 為奇數的情況.

為了方便我們先介紹一個符號. 給定一實數 r, 我們令 $[r]$ 表示小於等於 r 的整數中最大的整數. 例如若 π 表圓周率, 則 $[\pi] = 3$. 又例如 $[-5.2] = -6$. 要注意當 m,n 是正整數時 $[m/n]$ 即為 m 除以 n 的商.

Lemma 5.4.4. 給定一奇質數 p 及一正奇數 a 滿足 $p \nmid a$. 若令 n 表示集合 $\{a, 2a, \ldots, \frac{p-1}{2}a\}$ 中除以 p 餘數大於 $(p-1)/2$ 的元素個數, 則

$$n \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] \pmod 2.$$

Proof. 假設 ka 除以 p 的餘數為 r, 則依定義我們有 $ka = p[ka/p] + r$. 故若依 Lemma 5.4.2 的證明我們將 $\{a, 2a, \cdots, \frac{p-1}{2}a\}$ 中的元素除以 p 的餘數分成 $r_1, \ldots, r_n$ 及 $s_1, \ldots, s_m$ 兩部份, 其中 r_i 是大於 $(p-1)/2$ 的部份, 而 s_j 表小於等於 $(p-1)/2$ 的部份, 則

$$\sum_{k=1}^{(p-1)/2} ka = \sum_{k=1}^{(p-1)/2} p\left[\frac{ka}{p}\right] + \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j.$$

由於我們僅在乎奇或偶, 所以可考慮上式在 modulo 2 的情況, 故利用 a 和 p 皆為奇數 (即 $a \equiv p \equiv 1 \pmod 2$) 我們得

$$\sum_{k=1}^{(p-1)/2} k \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] + \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j \pmod 2. \tag{5.1}$$

另一方面在 Lemma 5.4.2 的證明中我們證得

$$\{p - r_1, \ldots, p - r_n, s_1, \ldots, s_m\} = \{1, 2, \ldots, (p-1)/2\}.$$

故得

$$\sum_{k=1}^{(p-1)/2} k = \sum_{i=1}^{n} (p - r_i) + \sum_{j=1}^{m} s_j = np - \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j.$$

再利用 $p \equiv 1 \pmod 2$ 得

$$\sum_{k=1}^{(p-1)/2} k \equiv n - \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j \pmod 2. \tag{5.2}$$

合併式子 (5.1) 和 (5.2) 得證

$$n \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] + 2\sum_{i=1}^{n} r_i \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] \pmod 2.$$

□

再次強調在 Lemma 5.4.4 的證明中我們用到 a 是奇數 (即 $a \equiv 1 \pmod 2$) 的假設, 所以此結果僅適用於 a 為奇數的情況, 千萬別用此法來算 $\left(\frac{2}{p}\right)$.

利用 Corollary 5.3.4 以及 Lemma 5.4.2, Lemma 5.4.4, 我們知給定一奇質數 p, 要計算一個正奇數 a 其 $\left(\frac{a}{p}\right)$ 之值, 我們只要計算 $\sum_{k=1}^{(p-1)/2}[ka/p]$ 之值即可. 若其值為 N, 則得 $\left(\frac{a}{p}\right) = (-1)^N$. 例如要求 $\left(\frac{5}{11}\right)$, 我們只要計算 $[5/11]+[10/11]+[15/11]+[20/11]+[25/11]$. 算出其值為 4, 故知 $\left(\frac{5}{11}\right) = (-1)^4 = 1$.

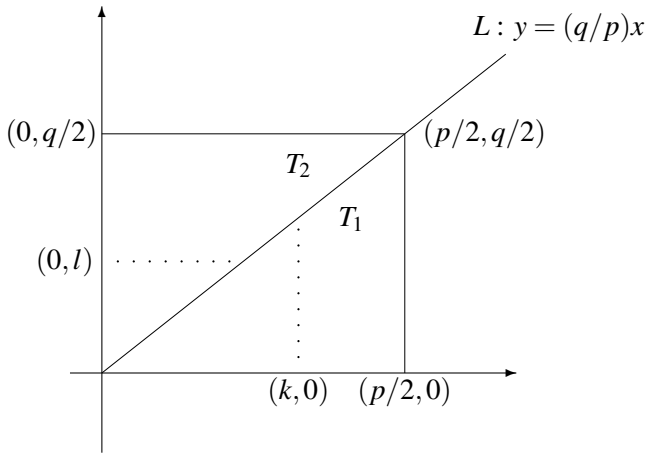
接著我們要利用 Lemma 5.4.4 來計算 $\left(\frac{q}{p}\right)$. 很容易理解算 $\left(\frac{q}{p}\right)$ 不止和 p 有關也和 q 有關, 所以我們要探討 $\left(\frac{q}{p}\right)$ 和 $\left(\frac{p}{q}\right)$ 的關係. 由於 p, q 皆為奇質數, 我們都可以利用 Lemma 5.4.4 來計算 $\left(\frac{q}{p}\right)$ 和 $\left(\frac{p}{q}\right)$. 因此我們要探討 $\sum_{k=1}^{(p-1)/2}[kq/p]$ 和 $\sum_{l=1}^{(q-1)/2}[lp/q]$ 之間的關係.

在探討此問題前, 我們再從另一個角度來看 $[r]$ 這個整數. 當 r 是正的實數時, $[r]$ 之值就是所有滿足 $0 \le n \le r$ 的正整數 n 的個數. 在坐標 xy-平面上, 我們稱 x-軸及 y-軸坐標皆為正整數的點為 "正格子點". 依此看法, 當 k 是正整數時, $[kq/p]$ 之值就是直線 $x = k$ 在 $0 \le y \le kq/p$ 之間的正格子點個數. 而當 l 是正整數時, $[lp/q]$ 之值就是直線 $y = l$ 在 $0 \le x \le lp/q$ 之間的正格子點個數. 利用這種觀點, 我們有以下之結果.

Lemma 5.4.5. 假設 p 和 q 為相異奇質數. 則

$$\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{l=1}^{(q-1)/2} \left[\frac{lp}{q}\right] = \frac{p-1}{2}\frac{q-1}{2}.$$

Proof. 在 xy-平面上, 考慮以 $(0,0)$, $(p/2,0)$, $(p/2,q/2)$ 以及 $(0,q/2)$ 四點為頂點的長方形區域 T, 並以直線 $L : y = (q/p)x$ 將此區域分成 T_1 和 T_2 兩部份. 其中 T_1 表直線 L 下方的部份, 而 T_2 表直線 L 上方的部份, 如下圖.



在 T 中的任意正格子點 (m,n), 依定義需滿足 $m,n \in \mathbb{N}$ 且 $0 \le m \le p/2$ 及 $0 \le n \le q/2$. 因此由 p,q 為奇數知在 T 中的正格子點個數為 $\dfrac{p-1}{2}\dfrac{q-1}{2}$.

另一方面在 T_1 中的正格子點 (k,s), 依定義需滿足 $k,s \in \mathbb{N}$ 且 $0 \le k \le p/2$ 及 $0 \le s \le kq/p$. 也就是說 $k \in \mathbb{N}$ 需滿足 $1 \le k \le (p-1)/2$, 且給定 k, 則 $0 \le s \le kq/p$. 換句話說要計算在 T_1 中的格子點, 等於在計算給定 $k \in \mathbb{N}$ 且 $1 \le k \le (p-1)/2$ 時會有多少 $s \in \mathbb{N}$ 滿足 $0 \le s \le kq/p$, 再將所有 k 所算得之結果加起來. 然而對任意的正整數 k 符合 $0 \le s \le kq/p$ 的正整數 s 的個數為 $[kq/p]$. 所以在 T_1 中的正格子點數為 $\sum_{k=1}^{(p-1)/2}[kq/p]$. 同理在 T_2 中的正格子點數為 $\sum_{l=1}^{(q-1)/2}[lp/q]$.

在 T_1 和 T_2 的交界, 即滿足 $y = (q/p)x$ 且 $0 \le x \le p/2$ 的線段上會不會有正格子點呢? 若 (m,n) 為其上之一正格子點, 則我們有 $pn = qm$ 且 $1 \le m \le (p-1)/2$. 然而由 $pn = qm$ 可得 $p|qm$, 再因 p,q 為相異質數故由 Proposition 1.2.6(1) 知 $p|m$, 此和 $1 \le m \le (p-1)/2$ 相矛盾. 故知在 T_1 和 T_2 交界的線段上無正格子點. 因此在 T_1 和 T_2 上的正格子點數之和恰為

在 T 上的正格子點數, 故得證

$$\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]+\sum_{l=1}^{(q-1)/2}\left[\frac{lp}{q}\right]=\frac{p-1}{2}\frac{q-1}{2}.$$

□

當 p,q 為相異奇質數, 若 $M=\sum_{k=1}^{(p-1)/2}[kq/p]$ 且 $N=\sum_{l=1}^{(q-1)/2}[lp/q]$ 由 Lemma 5.4.4 知 $\left(\frac{q}{p}\right)=(-1)^M$ 且 $\left(\frac{p}{q}\right)=(-1)^N$. 而 Lemma 5.4.5 告訴我們 $M+N=(p-1)(q-1)/4$, 故得

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{M+N}=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

因此我們有以下之結果.

Theorem 5.4.6 (Quadratic Reciprocity Law)**.** 假設 p 和 q 為相異奇質數. 則

$$\left(\frac{q}{p}\right)=\begin{cases}-\left(\frac{p}{q}\right), & \text{若 } p\equiv q\equiv -1 \pmod 4;\\ \left(\frac{p}{q}\right), & \text{其他情形.}\end{cases}$$

Proof. 由於 p,q 皆為奇數, 我們依 $p\equiv\pm1 \pmod 4$ 以及 $q\equiv\pm1 \pmod 4$ 四種情形來討論.

假設 $p=4k-1$ 且 $q=4k'-1$ 其中 $k,k'\in\mathbb{N}$ (即 $p\equiv q\equiv -1 \pmod 4$). 則 $(p-1)/2=2k-1$ 且 $(q-1)/2=2k'-1$, 故得

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{(2k-1)(2k'-1)}=-1.$$

也就是說 $\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$.

剩下的情況為 p 和 q 中至少有一個在 modulo 4 之後餘 1. 不失一般性就假設 $p\equiv 1 \pmod 4$. 此時 $p=4k+1$, 其中 $k\in\mathbb{N}$, 故得 $(p-1)/2=2k$. 而 $(q-1)/2$ 必為整數故知

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{(2k)\frac{q-1}{2}}=1^{\frac{q-1}{2}}=1.$$

也就是說 $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$. □

要注意 Theorem 5.4.6 要在 p,q 為相異奇質數時才適用, 否則若 q 不是奇質數, $\left(\frac{p}{q}\right)$ 這個符號是沒有定義的. 雖然 Theorem 5.4.6 並沒有明確告訴我們 $\left(\frac{q}{p}\right)$ 之值為何, 但是可利用 $\left(\frac{p}{q}\right)$ 之值來求得 $\left(\frac{q}{p}\right)$. 一般來說將 $\left(\frac{q}{p}\right)$ 的問題反轉成 $\left(\frac{p}{q}\right)$ 的問題就像輾轉相除法一樣, 可以快速的將問題簡化. 這是因為一般來說利用 Lemma 5.3.2(2), 要求 $\left(\frac{q}{p}\right)$ 時, 可假設 $q<p$, 所以一反轉成 $\left(\frac{p}{q}\right)$ 時我們已將一個 modulo 比較大的 p 的問題簡化成一個 modulo 比較小的 q 的問題. 例如求 $\left(\frac{7}{101}\right)$, 由於 $101\equiv 1 \pmod 4$, 故得 $\left(\frac{7}{101}\right)=\left(\frac{101}{7}\right)$. 所以馬上將 modulo 101 的問題轉成 modulo 7 的問題, 自然變得

簡單. 事實上 $\left(\frac{101}{7}\right)=\left(\frac{3}{7}\right)$, 可馬上驗證知 $\left(\frac{3}{7}\right)=-1$ (或再用一次 Theorem 5.4.6 得 $\left(\frac{3}{7}\right)=-\left(\frac{7}{3}\right)=-\left(\frac{1}{3}\right)=-1$). 所以得知 $\left(\frac{7}{101}\right)=-1$. 總而言之, 對於一般的相異奇質數 p,q, 我們沒有辦法由 p 和 q 馬上得知 $\left(\frac{q}{p}\right)$ 之值. 但是利用 Theorem 5.4.6, 我們可以很快速的將問題化簡而求出其值. 最後我們來看一個例子整合這一節中學到的方法.

Example 5.4.7. 考慮二次 congruence equation $x^2\equiv 539 \pmod{631}$ 是否有解. 要注意若要用 Legendre symbol 處理, 首先要檢查 631 是否為質數. 我們可以利用篩法 (Proposition 1.4.6) 檢查小於 $\sqrt{631}$ 的質數是否可整除 631. 由於小餘 25 的質數皆不能整除 631, 所以 Proposition 1.4.6 告訴我們 631 是質數. 因此我們就是要計算 $\left(\frac{539}{631}\right)$ 之值. 由於 539 和 631 頗近, 我們利用 $539\equiv -92 \pmod{631}$ 以及 Lemma 5.3.2(2) 知 $\left(\frac{539}{631}\right)=\left(\frac{-92}{631}\right)$ 接著將 92 作質因數分解得 $92=2^2\times 23$. 故利用 Proposition 5.3.5 知

$$\left(\frac{539}{631}\right)=\left(\frac{-92}{631}\right)=\left(\frac{-1}{631}\right)\left(\frac{4}{631}\right)\left(\frac{23}{631}\right).$$

由於 $631\equiv 3\equiv -1 \pmod 4$, 故由 Theorem 5.4.1 知 $\left(\frac{-1}{631}\right)=-1$. 而 $4=2^2$, 故由 Lemma 5.3.2(1) 知 $\left(\frac{4}{631}\right)=1$, 因此得 $\left(\frac{539}{631}\right)=-\left(\frac{23}{631}\right)$. 由於 $631\equiv 23\equiv 3 \pmod 4$, 故由 Theorem 5.4.6 知 $\left(\frac{23}{631}\right)=-\left(\frac{631}{23}\right)$. 又由 $631\equiv 10 \pmod{23}$ 因此知

$$\left(\frac{539}{631}\right)=-\left(\frac{23}{631}\right)=\left(\frac{631}{23}\right)=\left(\frac{10}{23}\right)=\left(\frac{2}{23}\right)\left(\frac{5}{23}\right).$$

因為 $23\equiv 7\equiv -1 \pmod 8$, 故由 Theorem 5.4.3 知 $\left(\frac{2}{23}\right)=1$. 又因 $5\equiv 1 \pmod 4$, 故由 Theorem 5.4.6 知 $\left(\frac{5}{23}\right)=\left(\frac{23}{5}\right)$. 因此得 $\left(\frac{539}{631}\right)=\left(\frac{2}{23}\right)\left(\frac{5}{23}\right)=\left(\frac{23}{5}\right)$. 再由 $23\equiv 3 \pmod 5$ 以及 $5\equiv 1 \pmod 4$ 知 $\left(\frac{23}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)$. 所以知 $\left(\frac{539}{631}\right)=\left(\frac{2}{3}\right)=-1$. 也就是說 $x^2\equiv 539 \pmod{631}$ 無解.

當然了當初若看出 $539=7^2\times 11$, 則馬上得 $\left(\frac{539}{631}\right)=\left(\frac{7^2}{631}\right)\left(\frac{11}{631}\right)=\left(\frac{11}{631}\right)$. 再因 $631\equiv 11\equiv 3 \pmod 4$ 以及 $631\equiv 4 \pmod{11}$ 知

$$\left(\frac{539}{631}\right)=\left(\frac{11}{631}\right)=-\left(\frac{631}{11}\right)=-\left(\frac{4}{11}\right)=-1.$$

所以不管用哪種看法只要善用 Legendre symbol 且正確地使用 quadratic reciprocity law (記得只有奇質數才能置於 Legendre symbol 的下方), 便能快速且正確的求出 Legendre symbol 之值.