Chapter 5

Congruence 中的平方根問題

這一章中我們要專注於 congruence equation 中有關平方根是否存在的問題. 我們先從 modulo p^n 開始，推導出可化簡成 modulo p 的情況處理，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. 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.

5.1.1. $p = 2$ 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 5.1.1. 假設 $n \geq 3$ 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 $n\geq 3$, 故由 Lemma 4.2.4 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 $n=k-1$ $(k\geq 4)$ 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 $2k-4=k+k-4\geq k$ (因 $k\geq 4$), 故得 $c'^2\equiv a \pmod{2^k}$. 得證 $x^2\equiv a \pmod{2^k}$ 有解. □

Proposition 5.1.1 不只告訴我們如何判斷 congruence equation $x^2\equiv a \pmod{2^n}$ 是否有解，而且在其證明中也告訴我們如何從 $x^2\equiv a \pmod{2^{n-1}}$ 的解找到 $x^2\equiv a \pmod{2^n}$ 的解。也就是說，假設 c 是 $x^2\equiv a \pmod{2^{n-1}}$ 的一個解，則我們可以將 c 帶入檢查是否滿足 $x^2\equiv a \pmod{2^n}$。若滿足，當然 c 就是所要的一個解；若不滿足，則利用證明中所述，可得 $c+2^{n-2}$ 就是 $x^2\equiv a \pmod{2^n}$ 的一個解。例如要找到 $x^2\equiv 9 \pmod{16}$ 除了 ± 3 以外的解，我們可以先考慮 $x^2\equiv 9 \pmod 8$ 除了 ± 3 以外的解。此時 $x\equiv 1 \pmod 8$ 就是一解，但 $x=1$ 並不滿足 $x^2\equiv 9 \pmod{16}$, 因此知 $x\equiv 1+2^{4-2}\equiv 5 \pmod{16}$ 就會是 $x^2\equiv 9 \pmod{16}$ 的一個解。

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 5.1.2. 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. 首先當 c 為 $x^2\equiv a \pmod{2^n}$ 的一解，我們檢查 $-c$, $c+2^{n-1}$ 以及 $-c+2^{n-1}$ 也會是 $x^2\equiv a \pmod{2^n}$ 的一解。由於 $(-c)^2=c\equiv a \pmod{2^n}$，知 $-c$ 也是一解。現考慮 $(c+2^{n-1})^2=c^2+2^nc+2^{2n-2}$。由於 $2n-2=n+(n-2)>n$，故得 $(c+2^{n-1})^2\equiv c^2\equiv a \pmod{2^n}$。因此 $c+2^{n-1}$ 也是 $x^2\equiv a \pmod{2^n}$ 的一解。同理因 $-c$ 已是一解，故 $-c+2^{n-1}$ 也是一解。注意因 c 為奇數且 $n\geq 3$，所以 $c, c+2^{n-1}, -c, -c+2^{n-1}$ 在 modulo 2^n 之下皆相異。接下來我們要說明，在 modulo 2^n 之下確實僅有此四個解。

若 $c'\in\mathbb{Z}$ 亦為一解, 則 $2^n|c^2-c'^2$, 即 $2^n|(c-c')(c+c')$. 因為 c 和 c' 皆為奇數, 我們可分成以下兩種情況。

(1) $c\equiv c' \pmod 4$：此時我們有 $c+c'\equiv 2c\equiv 2 \pmod 4$，亦即 $c+c'=2\lambda$, 其中 λ 為奇數。因此由 $2^n|(c-c')(c+c')$ 得 $2^n\mid 2\lambda(c-c')$ 再由 $\gcd(2,\lambda)=1$ 知 $2^{n-1}|(c-c')$. 也就是 $c'=c+2^{n-1}t$，因此我們有 $c'\equiv c \pmod{2^n}$ 或 $c'\equiv c+2^{n-1} \pmod{2^n}$。

(2) $c\equiv -c' \pmod 4$：此時我們有 $c-c'\equiv 2c\equiv 2 \pmod 4$，亦即 $c-c'=2\lambda$, 其中 λ 為奇數。因此由 $2^n|(c-c')(c+c')$ 得 $2^n\mid 2\lambda(c+c')$ 再由 $\gcd(2,\lambda)=1$ 知 $2^{n-1}|(c+c')$. 也就是 $c'=-c+2^{n-1}t$，因此我們有 $c'\equiv -c \pmod{2^n}$ 或 $c'\equiv -c+2^{n-1} \pmod{2^n}$。 □

Example 5.1.3. 解 $x^2 \equiv 17 \pmod{32}$. 由於 $17 \equiv 1 \pmod 8$, 由 Proposition 5.1.1 知必有解. 我們利用 Proposition 5.1.1 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 $x = 1$ 不符合 $x^2 \equiv 17 \pmod{32}$，故利用 Proposition 5.1.1 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 5.1.2 知 $x \equiv 9, 25, 7, 23 \pmod{32}$ 為 $x^2 \equiv 17 \pmod{32}$ 所有的解.

5.1.2. 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 4.2.4 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 5.1.4. 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 $c'^2 = c^2 + 2ctp + t^2p^2 = a + (2ct + \lambda)p + t^2p^2$. 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 5.1.5. 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. 當 c 為 $x^2 \equiv a \pmod{p^n}$ 的一解時，自然 $-c$ 也是一解。我們僅要說明，在 modulo p^n 之下確實僅有此二解。

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 $c' \equiv -c \pmod{p^n}$. □

Example 5.1.6. 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 5.1.4 知 $x^2 \equiv 14 \pmod{125}$ 必有解. 我們利用 Proposition 5.1.4 證明中所用的

方法來找出一個解. 首先利用 2 為 $x^2 \equiv 14 \pmod 5$ 之一解，找出 $x^2 \equiv 14 \pmod{25}$ 之一個解。考慮 $(2+5t)^2 = 4+20t+25t^2$. 因此由 $(2+5t)^2 \equiv 4+20t \equiv 14 \pmod{25}$，我們需解出 $t \in \mathbb{Z}$ 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 $(17+25t)^2 = 289+850t+625t^2$. 因此由 $(17+25t)^2 \equiv 289+850t \equiv 39+100t \equiv 14 \pmod{125}$，我們需解出 $t \in \mathbb{Z}$ 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 5.1.2 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.

Exercise 5.1. 試判斷以下二次的 congruence equations 是否有解。若有解，請寫下所有解。

(1) $x^2 \equiv 21 \pmod 4$

(2) $x^2 \equiv 21 \pmod{32}$

(3) $x^2 \equiv 33 \pmod{64}$

(4) $2x^2 \equiv 40 \pmod{64}$

Exercise 5.2. 試解以下二次的 congruence equations.

(1) $x^2 \equiv 33 \pmod{64}$

(2) $x^2 \equiv 31 \pmod{81}$

(3) $x^2 + 7x \equiv 15 \pmod{216}$

(4) $x^2 + 11x \equiv 18 \pmod{216}$