

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。

Primitive Roots

給定 $m \in \mathbb{N}$, 若存在 $a \in \mathbb{Z}$ 使得 $\{a, a^2, \dots, a^{\phi(m)}\}$ 成為一個 reduced residue system modulo m , 則稱 a 是 modulo m 之下的 primitive root. Primitive roots 的概念可以幫助我們解高次的 congruence equation. 在本章中我們將探討 Primitive Root Theorem, 即了解怎樣的正整數 m 會使得在 modulo m 之下有 primitive root. 並依此來解高次的 congruence equation.

6.1. Order 與 Primitive Roots

給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$, 我們已知如何判別 $x^2 \equiv a \pmod{m}$ 有解或無解, 而 primitive root 的概念可以幫助我們找到解.

考慮 $x^2 \equiv 5 \pmod{11}$. 利用 quadratic reciprocity law 我們知 $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$, 故知 $x^2 \equiv 5 \pmod{11}$ 有解. 然而解為何呢? 我們可以利用 2 在 modulo 11 之下特有的性質幫助我們找解. 下表為 2^n 在 modulo 11 的情形.

| | | | | | | | | | | |
|-----------------|---|---|---|---|----|---|---|---|---|----|
| n | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| $2^n \pmod{11}$ | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |

我們發現第二行 (即 a^n 那一行) 中這 10 ($= \phi(11)$) 個數在 modulo 11 之下皆相異, 而且因 2 和 11 互質所以自然 2^n 和 11 互質, 因此由 reduced residue system 的定義知 $\{2, 2^2, \dots, 2^{10}\}$ 是一個 reduced residue system modulo 11. 這代表的意義是每個和 11 互質的數 a , 都可以找到 $1 \leq n \leq 10$ 使得 $a \equiv 2^n \pmod{11}$. 另一方面我們僅將 n 列到 10 的原因是因為 $2^{10} \equiv 1 \pmod{11}$, 如果 $m = 10k + i$ 其中 $0 \leq i \leq 9$, 則 $2^m \equiv 2^i \pmod{11}$. 也就是每 10 次方一循環, 所以列出 10 次就夠了. 又由於已知當 $1 \leq i \neq j \leq 10$ 時, $2^i \not\equiv 2^j \pmod{11}$, 我們知 $2^i \equiv 2^j \pmod{11}$ 若且唯若 $i \equiv j \pmod{10}$. 結合這些結果可以幫助我們解 $x^2 \equiv 5 \pmod{11}$. 原因如下: 假設 $x = c$ 是一解, 由於 5 和 11 互質, 故知 c 和 11 互質. 因此知存在 $t \in \mathbb{N}$ 使得 $c \equiv 2^t \pmod{11}$. 然而 $5 \equiv 2^4 \pmod{11}$, 故由 $2^{2t} \equiv c^2 \equiv 5 \equiv 2^4 \pmod{11}$ 得 $2t \equiv 4 \pmod{10}$. 我們很巧妙的將解二次的 $x^2 \equiv 5 \pmod{11}$ 轉化成解一次的 $2t \equiv 4 \pmod{10}$ (注意 modulo 不同的數). 故利用 Proposition 4.2.1 解得 $t \equiv 2 \pmod{5}$, 也就是說 $t = 2, 7, \dots$ 為 $2t \equiv 4$

(mod 10) 之解. 將之代回 $c = 2^t$, 得 $c \equiv 4, 7 \pmod{11}$. 故知 $x \equiv \pm 4 \pmod{11}$ 為 $x^2 \equiv 5 \pmod{11}$ 之解.

可依此法解二次 congruence equation 歸功於在 modulo 11 之下 $\{2, 2^2, \dots, 2^{11}\}$ 是 reduced residue system. 要注意並不是 2 永遠有此特性. 例如 $2^3 \equiv 1 \pmod{7}$, 所以 $\{2, 2^2, \dots, 2^6\}$ 在 modulo 7 之下並不是 reduced residue system. 我們將有此特性的元素給一個特定的名子.

Definition 6.1.1. 給定 $m \in \mathbb{N}$, 若 $a \in \mathbb{Z}$ 且與 m 互質滿足 $\{a, a^2, \dots, a^{\phi(m)}\}$ 是一個 reduced residue system modulo m , 則稱 a 為 modulo m 之下的一個 *primitive root*.

要注意並不是對所有的 m 皆有 primitive root. 例如在 modulo 15 之下, 所有和 15 互質的數 a 皆有 $a^4 \equiv 1 \pmod{15}$, 所以又因 $a^{\phi(15)} = a^8 \equiv 1 \pmod{15}$ 知 $\{a, a^2, a^3, a^4, \dots, a^8\}$ 不可能形成 reduced residue system modulo 15. 也就是說在 modulo 15 之下並無 primitive root. 我們最主要的目的就是要探討哪些 $m \in \mathbb{N}$ 在 modulo m 之下會有 primitive root.

首先我們必須了解怎樣的 a 在 modulo m 之下會是 primitive root. 由於

$$S = \{a, a^2, \dots, a^{\phi(m)}\}$$

是 reduced residue system modulo m , 所以若 $1 \leq i \neq j \leq \phi(m)$, 則 $a^i \not\equiv a^j \pmod{m}$. 否則 S 在 modulo m 之下會有少於 $\phi(m)$ 個同餘類, 無法形成 reduced residue system modulo m . 然而 a 和 m 互質, Euler's Theorem (3.3.2) 告訴我們 $a^{\phi(m)} \equiv 1 \pmod{m}$, 所以 a 在 modulo m 之下是 primitive root 的先決條件是若 $1 \leq i \leq \phi(m) - 1$, 則 $a^i \not\equiv 1 \pmod{m}$ (否則會造成 $1 \leq i < \phi(m)$ 且 $a^i \equiv a^{\phi(m)} \pmod{m}$ 的矛盾). 也就是說滿足 $a^n \equiv 1 \pmod{m}$ 的最小正整數 n 為 $n = \phi(m)$. 因此給定 $a \in \mathbb{Z}$ 且 $\gcd(a, m) = 1$, 最小的正整數 n 滿足 $a^n \equiv 1 \pmod{m}$ 為何, 是判斷 a 在 modulo m 之下是否為 primitive root 的重要依據. 我們自然有以下之定義.

Definition 6.1.2. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 若 $n \in \mathbb{N}$ 是最小的正整數滿足 $a^n \equiv 1 \pmod{m}$, 則稱 n 為 a 在 modulo m 之下的 *order*, 並以 $\text{ord}_m(a) = n$ 表之.

要注意由於 $\gcd(a, m) = 1$, Euler's Theorem 告訴我們 $a^{\phi(m)} \equiv 1 \pmod{m}$, 所以 $\text{ord}_m(a)$ 必存在且依定義知 $\text{ord}_m(a) \leq \phi(m)$. 首先我們來看依定義馬上可得之性質.

Lemma 6.1.3. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$.

- (1) 若 $a \equiv b \pmod{m}$ 則 $\text{ord}_m(a) = \text{ord}_m(b)$.
- (2) $\text{ord}_m(a) = 1$ 若且唯若 $a \equiv 1 \pmod{m}$.

Proof. (1) 若 $a \equiv b \pmod{m}$, 知對任意 $i \in \mathbb{N}$ 皆有 $a^i \equiv b^i \pmod{m}$, 故若 n 是最小的正整數使得 $a^n \equiv 1 \pmod{m}$, 則 n 也會是最小的正整數使得 $b^n \equiv 1 \pmod{m}$. 因此知 $\text{ord}_m(a) = \text{ord}_m(b)$.

(2) 若 $\text{ord}_m(a) = 1$, 表示 $a^1 \equiv 1 \pmod{m}$, 故得 $a \equiv 1 \pmod{m}$. 反之, 若 $a \equiv 1 \pmod{m}$, 當然 $n = 1$ 是最小的正整數使得 $a^n \equiv 1 \pmod{m}$, 故知 $\text{ord}_m(a) = 1$. \square

其實 order 的定義和最大公因數的定義類似，我們要說 $\text{ord}_m(a) = n$ 等於要說兩件事：

- (1) $a^n \equiv 1 \pmod{m}$.
- (2) 若 $1 \leq i \leq n-1$, 則 $a^i \not\equiv 1 \pmod{m}$.

要記住這兩件事缺一不可才能保證 $\text{ord}_m(a) = n$. 接下來我們就來看依此兩點可推得 $\text{ord}_m(a)$ 的性質.

Proposition 6.1.4. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 假設 $\text{ord}_m(a) = n$. 則 $a^k \equiv 1 \pmod{m}$ 若且唯若 $n|k$.

Proof. 假設 $a^k \equiv 1 \pmod{m}$. 利用 Division Algorithm (Theorem 1.2.1) 知存在 $h, r \in \mathbb{Z}$ 滿足 $k = nh + r$, 其中 $0 \leq r < n$. 由 $a^n \equiv 1 \pmod{m}$ 知 $a^k = a^{nh+r} = (a^n)^h a^r \equiv a^r \pmod{m}$. 現假設 $r \neq 0$ (即 $1 \leq r < n$), 則由 $a^k \equiv 1 \pmod{m}$ 之假設知 $a^r \equiv 1 \pmod{m}$. 此和 n 是最小的正整數滿足 $a^n \equiv 1 \pmod{m}$ 相違背, 故知 $r = 0$, 即 $n|k$.

反之若 $n|k$, 即存在 $h \in \mathbb{Z}$ 滿足 $k = nh$, 故得 $a^k = a^{nh} = (a^n)^h \equiv 1 \pmod{m}$. □

若 a 和 m 互質, Euler's Theorem 告訴我們 $a^{\phi(m)} \equiv 1 \pmod{m}$, 故由 Proposition 6.1.4 知 $\text{ord}_m(a) | \phi(m)$, 這比我們前面依定義知 $\text{ord}_m(a) \leq \phi(m)$ 好多了. 同樣的, 利用 Proposition 6.1.4, 我們可以有更好的方式來判定 $\text{ord}_m(a)$ 之值.

Corollary 6.1.5. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 則 $\text{ord}_m(a) = n$ 若且唯若 n 滿足以下兩條件:

- (1) $a^n \equiv 1 \pmod{m}$.
- (2) 若 $a^k \equiv 1 \pmod{m}$, 則 $n|k$.

Proof. 若 $\text{ord}_m(a) = n$, 則自然有 $a^n \equiv 1 \pmod{m}$, 再利用 Proposition 6.1.4 知, 若 $a^k \equiv 1 \pmod{m}$, 則 $n|k$.

反之若 n 滿足 (1), (2) 兩項, 我們要證明 $\text{ord}_m(a) = n$. 由於 (1) 已知 $a^n \equiv 1 \pmod{m}$, 故僅剩要證明若 $1 \leq i < n$, 則 $a^i \not\equiv 1 \pmod{m}$. 我們用反證法, 假設 $a^i \equiv 1 \pmod{m}$, 則由 (2) 知 $n|i$. 此和 $1 \leq i < n$ 相矛盾, 故知 $a^i \not\equiv 1 \pmod{m}$. 也就是說 $\text{ord}_m(a) = n$. □

Corollary 6.1.5 的 (2) 將 $\text{ord}_m(a) = n$ 原本表最小的正整數滿足 $a^n \equiv 1 \pmod{m}$ 的性質轉換成看似更強的性質 (就如同當初原本最大公因數是最大的公因數可轉換成為所有的公因數的倍數這樣的性質) 在以後有關 order 的理論推導中有很大的幫助.

計算 order 的另一個重要的原因是我們可以知道 a^i 在 modulo m 之下的週期.

Proposition 6.1.6. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 假設 $\text{ord}_m(a) = n$ 且 $i, j \in \mathbb{N}$. 則 $a^i \equiv a^j \pmod{m}$ 若且唯若 $i \equiv j \pmod{n}$.

Proof. 假設 $a^i \equiv a^j \pmod{m}$, 不失一般性我們也假設 $i \geq j$, 此時 $a^i - a^j = a^j(a^{i-j} - 1)$. 利用 $m|a^i - a^j$ 以及 m 和 a^j 互質 (因 m 和 a 互質), Proposition 1.2.6 告訴我們 $m|a^{i-j} - 1$, 即 $a^{i-j} \equiv 1 \pmod{m}$. 故利用 $\text{ord}_m(a) = n$ 以及 Proposition 6.1.4 知 $n|i-j$, 亦即 $i \equiv j \pmod{n}$.

反之, 若 $i \equiv j \pmod{n}$, 不失一般性我們假設 $i \geq j$, 則有 $n|i-j$. 故再利用 Proposition 6.1.4 知 $a^{i-j} \equiv 1 \pmod{m}$. 兩邊乘上 a^j 因此有 $a^i = a^j a^{i-j} \equiv a^j \pmod{m}$. \square

若 $\text{ord}_m(a) = n$, Proposition 6.1.6 不只告訴我們 $a, a^2, \dots, a^i, \dots$ 在 modulo m 之下的週期為 n (即每隔 n 個 i , a^i 會形成一循環) 而且告訴我們, a, a^2, \dots, a^n 在 modulo m 之下皆相異. 否則若存在 $1 \leq j < i \leq n$ 使得 $a^i \equiv a^j \pmod{m}$, 可得 $n|i-j$ 而與 $0 < i-j < n-1$ 相矛盾. 依此我們可以確定可以用 $\text{ord}_m(a)$ 之值來判定 a 在 modulo m 之下是否為 primitive root.

Corollary 6.1.7. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 則 $\text{ord}_m(a) = \phi(m)$ 若且唯若 a 在 modulo m 之下是一個 primitive root.

Proof. 假設 a 是 modulo m 之下的一個 primitive root. 由於 $a, a^2, \dots, a^{\phi(m)}$ 在 modulo m 之下皆不同餘, 故知若 $1 \leq i \leq \phi(m)$, 則 $a^i \not\equiv a^{\phi(m)} \pmod{m}$. 又由於 Euler's Theorem 知 $a^{\phi(m)} \equiv 1 \pmod{m}$, 故知 $\text{ord}_m(a) = \phi(m)$.

反之, 假設 $\text{ord}_m(a) = \phi(m)$, 由 Proposition 6.1.6 知若 $a^i \equiv a^j \pmod{m}$, 則 $\phi(m)|i-j$. 因此 $a, a^2, \dots, a^{\phi(m)}$ 在 modulo m 之下皆不同餘. 又由於 a 和 m 互質, 知 a^i 皆與 m 互質, 故 $\{a, a^2, \dots, a^{\phi(m)}\}$ 是一個 reduced residue system modulo m , 也就是說 a 在 modulo m 之下是一個 primitive root. \square

若已知 a 在 modulo m 的 order, 則對任意 $i \in \mathbb{N}$, 利用 Corollary 6.1.5 我們都可算出 a^i 在 modulo m 之下的 order.

Proposition 6.1.8. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 若 $\text{ord}_m(a) = n$, 則對於任意的正整數 i ,

$$\text{ord}_m(a^i) = \frac{n}{\gcd(i, n)}.$$

Proof. 為了方便, 我們令 $d = \gcd(i, n)$. 欲證明 $\text{ord}_m(a^i) = n/d$, 首先得證明 $(a^i)^{n/d} \equiv 1 \pmod{m}$. 事實上因為 d 是 i 的因數, i/d 是個整數. 再加上由假設 $\text{ord}_m(a) = n$, 故 $a^n \equiv 1 \pmod{m}$. 所以可得

$$(a^i)^{n/d} = (a^n)^{i/d} \equiv 1 \pmod{m}.$$

接下來我們須證明, 若 $(a^i)^k \equiv 1 \pmod{m}$ 則 $(n/d)|k$ (參見 Corollary 6.1.5(2)). 若 $(a^i)^k \equiv 1 \pmod{m}$, 即 $a^{ki} \equiv 1 \pmod{m}$. 故由 Proposition 6.1.4, 我們可得 $n|ki$. 但因 d 是 n 和 i 的最大公因數. 我們有 n/d 和 i/d 皆為整數且互質. 故由 $n|ki$ 可得 $(n/d)|k(i/d)$. 再由 n/d 和 i/d 互質, 得 $(n/d)|k$. \square

由 Proposition 6.1.8, 我們知 $\text{ord}_m(a^i)$ 整除 $\text{ord}_m(a)$ 而且 $\text{ord}_m(a^i) = \text{ord}_m(a)$ 若且唯若 $\gcd(i, \text{ord}_m(a)) = 1$. 因此在 modulo m 之下 primitive root 若存在, 則我們可推知在 modulo m 之下會有多少個 primitive roots.

Corollary 6.1.9. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 若 $\text{ord}_m(a) = n$, 則 $\{a, a^2, \dots, a^n\}$ 中共有 $\phi(n)$ 個元素其在 modulo m 之下的 order 為 n . 特別地, 若在 modulo m 之下 primitive root 是存在的, 則在 modulo m 之下共有 $\phi(\phi(m))$ 個 primitive roots.

Proof. 已知 $\text{ord}_m(a) = n$, 由 Proposition 6.1.8 知 $\text{ord}_m(a^i) = n$ 若且唯若 $\gcd(n, i) = 1$. 又由於 a, a^2, \dots, a^n 在 modulo m 之下皆相異, 故 $\{a, a^2, \dots, a^n\}$ 中在 modulo m 之下 order 為 n 的元素個數等於和 n 互質且小於 n 的正整數的個數, 依定義知此數為 $\phi(n)$.

現假設在 modulo m 之下有 primitive root 且 a 為一個 primitive root. 故知 $\text{ord}_m(a) = \phi(m)$ 且所有和 m 互質的整數在 modulo m 之下皆和 $S = \{a, a^2, \dots, a^{\phi(m)}\}$ 中某個元素同餘. 所以在 modulo m 之下所有的 primitive root 皆可在 S 中找到. 然而由前知 S 中共有 $\phi(\phi(m))$ 個元素其在 modulo m 之下的 order 為 $\phi(m)$, 且 Corollary 6.1.7 告訴我們在 modulo m 之下只有這些元素為 primitive root. 故知在 modulo m 之下共有 $\phi(\phi(m))$ 個 primitive roots. \square

6.2. 沒有 Primitive Root 的情況

我們將探討有哪些 m 在 modulo m 之下沒有 primitive root.

我們仍然從唯一的偶質數 2 出發. 在 modulo 2 之下 $\phi(2) = 1$, 而任何的奇數在 modulo 2 之下皆餘 1, 故所有的奇數皆為 primitive root. 在 modulo 4 時, $\{1, 3\}$ 是一個 reduced residue system modulo 4, 而 $3^1 \not\equiv 1 \pmod{4}$ 且 $3^2 \equiv 1 \pmod{4}$ 故得 $\text{ord}_4(3) = 2 = \phi(4)$, 故知 3 在 modulo 4 之下是 primitive root. 事實上若 $a \in \mathbb{Z}$ 滿足 $a \equiv 3 \pmod{4}$ 則 a 在 modulo 4 之下為 primitive root.

接著我們來看 8 情形, 由於 $\{1, 3, 5, 7\}$ 是一個 reduced residue system modulo 8, 我們來看看它們在 modulo 8 之下之 order 為何. 很明顯的 $\text{ord}_8(1) = 1$ 且因為 $7 \equiv -1 \pmod{8}$, 故知 $\text{ord}_8(7) = 2$. 另外 $3^1 \equiv 3 \pmod{8}$ 且 $3^2 \equiv 1 \pmod{8}$, 故知 $\text{ord}_8(3) = 2$. 同理得 $\text{ord}_8(5) = 2$. 由於所有和 8 互質的數在 modulo 8 之下必和 1, 3, 5, 7 中某一數同餘, 因此由 Lemma 6.1.3(1) 知沒有一個和 8 互質的數其在 modulo 8 之下的 order 為 $\phi(8) = 4$. 故知在 modulo 8 之下沒有 primitive root.

或許大家看到 modulo 8 之下沒有 primitive root 很自然會認為那麼在 modulo 16 之下也沒有 primitive root. 事實上這件事並不能直接用 order 的定義得到. 也就是說若已知 $\text{ord}_8(a) = n$ 並不能直接用 order 的性質推出 $\text{ord}_{16}(a)$ 之值. 頂多我們知道若 $\text{ord}_{16}(a) = n'$, 則由 $a^{n'} \equiv 1 \pmod{16}$ 可知 $a^{n'} \equiv 1 \pmod{8}$, 故利用 Proposition 6.1.4 得 $n|n'$. 但我們並不能由此以及 $n < \phi(8)$ 推出 $n' < \phi(16)$. 所以要推出在 modulo 16 或甚至 modulo 2^n , $n > 3$ 時沒有 primitive root, 是需要多下功夫的. 在前面我們已算出對任意奇數 a , 皆滿足 $a^2 \equiv 1 \pmod{2^3}$. 我們要用歸納法推出以下結果.

Lemma 6.2.1. 假設 a 為一奇數, 則對任意 $n \in \mathbb{N}$ 皆有 $a^{2^n} \equiv 1 \pmod{2^{n+2}}$.

Proof. 我們已知當 $n = 1$ 時這是對的. 假設當 $n = k$ 時皆有 $a^{2^k} \equiv 1 \pmod{2^{k+2}}$, 我們要證明當 $n = k + 1$ 時亦成立. 依假設我們知存在 $b \in \mathbb{Z}$ 使得 $a^{2^k} = 1 + 2^{k+2}b$. 故

$$a^{2^{k+1}} = (a^{2^k})^2 = (1 + 2^{k+2}b)^2 = 1 + 2(2^{k+2}b) + (2^{k+2}b)^2.$$

由於 $2(k+2) = k + (k+4) > k+3$, 我們得 $a^{2^{k+1}} \equiv 1 \pmod{2^{k+3}}$. 也就是說當 $n = k + 1$ 時 $a^{2^n} \equiv 1 \pmod{2^{n+2}}$ 亦成立, 故由數學歸納法得證本定理. \square

依 order 的定義我們馬上由 Lemma 6.2.1 知當 a 為奇數且 $n \in \mathbb{N}$ 時,

$$\text{ord}_{2^{n+2}}(a) \leq 2^n < 2^{n+1} = \phi(2^{n+2}),$$

故得證以下重要的結果.

Proposition 6.2.2. 當 $n \in \mathbb{N}$ 且 $n \geq 3$ 時, 在 modulo 2^n 之下沒有 primitive root.

接下來我們要探討另一種沒有 primitive root 的情況, 首先我們來看另一個有關 order 簡單的性質.

Lemma 6.2.3. 給定互質的兩正整數 m, n 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, mn) = 1$. 則

$$\text{ord}_{mn}(a) \leq \frac{\phi(mn)}{\gcd(\phi(m), \phi(n))}.$$

Proof. 令 $d = \gcd(\phi(m), \phi(n))$. 由於 $\gcd(a, mn) = 1$, 我們知 $\gcd(a, m) = \gcd(a, n) = 1$. 因此由 Euler's Theorem 我們有 $a^{\phi(m)} \equiv 1 \pmod{m}$ 以及 $a^{\phi(n)} \equiv 1 \pmod{n}$. 因此由 $\phi(mn) = \phi(m)\phi(n)$ (因 $\gcd(m, n) = 1$) 以及 $\phi(n)/d \in \mathbb{N}$ 可得

$$a^{\frac{\phi(mn)}{d}} = (a^{\phi(m)})^{\frac{\phi(n)}{d}} \equiv 1 \pmod{m}.$$

同理可得 $a^{\phi(mn)/d} \equiv 1 \pmod{n}$. 也就是說 $m | a^{\phi(mn)/d} - 1$ 且 $n | a^{\phi(mn)/d} - 1$, 故再因 $\gcd(m, n) = 1$ 利用 Proposition 1.2.6(2) 可得 $mn | a^{\phi(mn)/d} - 1$, 即 $a^{\phi(mn)/d} \equiv 1 \pmod{mn}$. 故依 order 之定義得 $\text{ord}_{mn}(a) \leq \phi(mn)/d$. \square

特別地, 假設 m 是一個大於 2 的整數. 若 m 沒有奇的質因數, 即 $m = 2^k$ 其中 $k \geq 2$. 此時 $\phi(m) = \phi(2^k) = 2^{k-1}$, 故得 $2 | \phi(m)$. 若 m 有奇的質因數, 即存在一奇質數 p 使得 $m = p^l m'$, 其中 $l \in \mathbb{N}$ 且 $p \nmid m'$. 此時 $\phi(m) = \phi(p^l)\phi(m') = (p-1)p^{l-1}\phi(m')$, 同樣可得 $2 | \phi(m)$. 因此可知當 $m, n > 2$ 時 $\gcd(\phi(m), \phi(n)) \geq 2$. 利用此一結果, 我們馬上可得另一個重要結論.

Proposition 6.2.4. 當 $m > 2$ 且 $n > 2$ 為兩互質的整數時, 在 modulo mn 之下沒有 primitive root.

Proof. 因 m, n 皆大於 2 我們知 $2 | \phi(m)$ 且 $2 | \phi(n)$ 故得 $\gcd(\phi(m), \phi(n)) \geq 2$. 另一方面 m 和 n 是互質的, 故對任一與 mn 互質的整數 a , 由 Lemma 6.2.3 知

$$\text{ord}_{mn}(a) \leq \frac{\phi(mn)}{\gcd(\phi(m), \phi(n))} \leq \frac{\phi(mn)}{2} < \phi(mn).$$

故知在 modulo mn 之下無 primitive root. \square

當 $m > 1$ 且沒有奇的質因數時, 我們知道當 $m = 2, 4$ 時在 modulo m 之下有 primitive root, 而在其他狀況 (即 $m = 2^n$ 且 $n \geq 3$) Proposition 6.2.2 告訴我們在 modulo m 之下沒有 primitive root. 當 m 有奇的質因數時, Proposition 6.2.4 告訴我們若 m 有兩個或兩個以上奇的質因數時, 在 modulo m 之下沒有 primitive root. 而當 m 只有一個奇的質因數時, Proposition 6.2.4 也告訴我們若 $4|m$, 在 modulo m 之下沒有 primitive root. 所以我們僅剩下 m 僅有一個奇的質因數且 $4 \nmid m$ 的情形未討論, 即 $m = p^n$ 或 $m = 2p^n$, 其中 p 為奇質數的情形.

6.3. The Primitive Root Theorem

我們僅剩下 $m = p^n$ 或 $m = 2p^n$, 其中 p 為奇質數的情形尚未探討. 事實上在這剩下的情況中, primitive root 皆存在. 在這節中我們將先得到當 p 是一個奇質數時, 在 modulo p 之下可找到 primitive root. 再利用 modulo p 所得的 primitive root 得到在 modulo p^2 之下的 primitive root. 最後利用 modulo p^2 所得的 primitive root 得到 modulo p^n 以及 modulo $2p^n$ 的 primitive root. 在本節中 p 永遠表示為奇質數, 我們就不再多說明.

6.3.1. Modulo p 的 Primitive Root. 我們要說明當 p 是一個奇質數時在 modulo p 之下可以找到 primitive root. 我們曾經提及要證明存在性, 一般來說有兩種方法: 第一種就是提供一個可以找到東西的方法; 另一種就是利用邏輯推演的方式來推導出東西一定存在 (例如用反證法證明若找不到會導致矛盾). 第一種方法的好處是它提供了找到東西的方法所以不只告訴你東西存在且告訴你如何找到. 不過這在一般抽象理論的推導中不是容易的, 例如前一章提過找二次 congruence equation 的解並不容易, 但我們可發展一套理論來確認何時有解. 同樣地, 在證明 primitive root 存在的問題上, 即使已知存在到目前為止仍沒有一套完善的方法可以直接找到 primitive root, 所以我們仍是用邏輯推演的方式來證明存在性.

在 modulo p 時, 有一件事是很特殊的即 Theorem 4.1.3 告訴我們一個 n 次的整係數多項式在 modulo p 之下最多有 n 個解. 然而若 $p \nmid a$ 且 $\text{ord}_p(a) = n$, 已知 a, a^2, \dots, a^n 在 modulo p 之下皆相異, 且由於 $a^n \equiv 1 \pmod{p}$, 故 $(a^i)^n \equiv 1 \pmod{p}$. 由此可知 a, a^2, \dots, a^n 這 n 個在 modulo p 之下皆不同餘的數皆為 $x^n \equiv 1 \pmod{p}$ 的一個解, 但由於此式在 modulo p 之下至多有 n 個解, 所以它們就是 $x^n \equiv 1 \pmod{p}$ 所有的解. 另一方面, 若 $p \nmid b$ 且 $\text{ord}_p(b) = n$, 則由於 b 是 $x^n \equiv 1 \pmod{p}$ 之一解, 故由前知存在 $i \in \{1, \dots, n\}$ 使得 $b \equiv a^i \pmod{p}$. 換言之, 所有在 modulo p 之下 order 為 n 的元素, 在 modulo p 之下必和 $\{a, a^2, \dots, a^n\}$ 中某個元素同餘, 故利用 Corollary 6.1.9 知在 modulo p 之下僅有 $\phi(n)$ 個元素其 order 為 n . 我們將此結果總結如下.

Lemma 6.3.1. 假設 p 為質數且在 modulo p 之下有一元素其 order 為 n , 則在 modulo p 之下共有 $\phi(n)$ 個元素其 order 為 n .

再次強調, 此結果在質數時才對. 例如在 modulo 15 時, 共有 4, 11 和 14 三個元素在 modulo 15 之下的 order 為 2, 而不是 $\phi(2) = 1$ 個.

我們要說在 modulo p 之下有 primitive root 主要的方法便是將 modulo p 之下的元素依其 order 分類. 最後說明 order 為 $\phi(p) = p-1$ 那一類元素所成的集合不是 \emptyset (空集合). 下面就是依這樣分類所得之結果.

Lemma 6.3.2. 假設 p 是質數且令 $S = \{1, 2, \dots, p-1\}$. 現對於 $d \in \mathbb{N}$ 滿足 $d|p-1$, 我們考慮 $S_d = \{i \in S \mid \text{ord}_p(i) = d\}$.

- (1) 若 $d \neq d'$, 則 $S_d \cap S_{d'} = \emptyset$.
- (2) $\bigcup_{d|p-1, d>0} S_d = S$.
- (3) 若 $S_d \neq \emptyset$, 則 S_d 共有 $\phi(d)$ 個元素.

Proof. (1) 若 $a \in S_d \cap S_{d'}$, 即表示 $\text{ord}_p(a) = d$ 且 $\text{ord}_p(a) = d'$. 但依 order 的定義每一個和 p 互質的數在 modulo p 之下其 order 是唯一的, 此與 $d \neq d'$ 之假設相矛盾, 故知 $S_d \cap S_{d'} = \emptyset$.

(2) $\bigcup_{d|p-1, d>0} S_d$ 這個符號的意思是將所有 S_d 其中 $d \in \mathbb{N}$ 且 $d|p-1$ 聯集起來. 由於對所有 $d|p-1$ 皆有 $S_d \subseteq S$, 所以 $\bigcup_{d|p-1, d>0} S_d \subseteq S$. 另一方面若 $i \in S$, 由於 $p \nmid i$, 故由 Theorem 3.3.4 知 $i^{p-1} \equiv 1 \pmod{p}$. 因此由 Proposition 6.1.4 知 $\text{ord}_p(i)|p-1$. 換句話說, 若 $\text{ord}_p(i) = d$, 則 $d|p-1$, 故知存在 $d|p-1$ 使得 $i \in S_d$. 得證 $S \subseteq \bigcup_{d|p-1, d>0} S_d$, 因此知 $\bigcup_{d|p-1, d>0} S_d = S$.

(3) 若 $S_d \neq \emptyset$, 表示存在 $a \in S_d$. 此時 $p \nmid a$ 且 $\text{ord}_p(a) = d$, 故利用 Lemma 6.3.1 知在 modulo p 之下共有 $\phi(d)$ 個元素其 order 為 d . 由於 S 是 reduced residue system modulo p , 這 $\phi(d)$ 個元素在 modulo p 之下必和 S 中 $\phi(d)$ 個元素同餘. 因此 S 中這 $\phi(d)$ 個元素剛好組成 S_d , 故知 S_d 共有 $\phi(d)$ 個元素. \square

Lemma 6.3.2(1,2) 告訴我們 $S = \{1, 2, \dots, p-1\}$ 中的每一個元素必會落在某個且恰有一個 S_d 中, 其中 $d \in \mathbb{N}$ 且 $d|p-1$. 因此若計算每個 S_d 中的元素個數再加總起來其值應為 S 中的元素個數 $p-1$. 依此我們可以得到以下重要的結果.

Theorem 6.3.3. 假設 p 是一個質數且 $d \in \mathbb{N}$ 滿足 $d|p-1$. 則在 modulo p 之下共有 $\phi(d)$ 個元素其 order 為 d . 特別地, 在 modulo p 之下 primitive root 必存在.

Proof. 我們沿用 Lemma 6.3.2 中所用的符號, 並令 $\#(S_d)$ 表示 $S_d = \{i \in S \mid \text{ord}_p(i) = d\}$ 中元素的個數, 即 $\#(S_d)$ 為在 modulo p 之下 order 為 d 的元素個數.

由 Lemma 6.3.2(1,2) 我們知 $\sum_{d|p-1, d>0} \#(S_d) = p-1$ 而且 Lemma 6.3.2(3) 告訴我們 $\#(S_d) = 0$ 或 $\#(S_d) = \phi(d)$. 另一方面利用 Corollary 2.3.6 我們知 $\sum_{d|p-1, d>0} \phi(d) = p-1$, 故比較

$$p-1 = \sum_{d|p-1, d>0} \#(S_d) \leq \sum_{d|p-1, d>0} \phi(d) = p-1,$$

可得對所有的 $d \in \mathbb{N}$ 滿足 $d|p-1$ 皆有 $\#(S_d) = \phi(d)$.

特別地 $\#(S_{p-1}) = \phi(p-1)$ 表示在 modulo p 之下有 $\phi(p-1) \neq 0$ 個元素其 order 為 $p-1$, 也就是說這些元素皆為 primitive root. 故知在 modulo p 之下 primitive root 存在. \square

我們證明了在 modulo p 之下 primitive root 是存在的. 這個證明方式很明顯的並沒有告訴我們如何找到 primitive root. 事實上我們所用的證明方式有點像反證法, 也就是說如果沒有 primitive root, 那麼在計算上面那些元素個數時會發生數目兜不攏的情形而造成矛盾.

6.3.2. Modulo p^2 的 primitive root. 很容易去猜測若在 modulo p^2 之下有 primitive root, 那麼這個 primitive root 應來自於 modulo p 之下的 primitive root. 因此我們將利用 modulo p 的 primitive root 來找到 modulo p^2 的 primitive root. 這裡的存在性的證明就比較具體, 也就是說如果能找到 modulo p 的 primitive root, 那麼我們的證明能給出具體的方法來找到 modulo p^2 的 primitive root.

首先我們來看如何判別一個 modulo p 的 primitive root 在 modulo p^2 之下是否為 primitive root.

Lemma 6.3.4. 假設 $a \in \mathbb{Z}$ 是一個 primitive root modulo p . 則 $\text{ord}_{p^2}(a) = p-1$ 或 $\text{ord}_{p^2}(a) = p(p-1)$. 特別地, $a^{p-1} \not\equiv 1 \pmod{p^2}$ 若且唯若 a 在 modulo p^2 之下是一個 primitive root.

Proof. 依假設 a 在 modulo p 之下是 primitive root 表示 $\text{ord}_p(a) = p-1$. 現假設 $\text{ord}_{p^2}(a) = n$, 則 $a^n \equiv 1 \pmod{p^2}$, 因此知 $a^n \equiv 1 \pmod{p}$. 故依 $\text{ord}_p(a) = p-1$ 及 Proposition 6.1.4 知 $p-1|n$. 又因為 a 與 p 互質, 故 a 與 p^2 互質, 故由 Euler's Theorem 知 $a^{\phi(p^2)} \equiv 1 \pmod{p^2}$, 因此在 modulo p^2 的情況再利用 Proposition 6.1.4 知 $n|\phi(p^2)$. 由於 $\phi(p^2) = p(p-1)$, 我們得 $p-1|n$ 且 $n|p(p-1)$. 也就是 $n = \lambda(p-1)$ 且又 $\lambda(p-1)|p(p-1)$, 故知 $\lambda|p$. 因此由 p 是質數知 $\lambda = 1$ 或 $\lambda = p$. 故得證 $\text{ord}_{p^2}(a) = p-1$ 或 $\text{ord}_{p^2}(a) = p(p-1)$.

現若 $a^{p-1} \not\equiv 1 \pmod{p^2}$, 知 a 在 modulo p^2 之下其 order 一定不是 $p-1$, 故得 $\text{ord}_{p^2}(a) = p(p-1) = \phi(p^2)$. 由 Corollary 6.1.7 得證 a 在 modulo p^2 之下是一個 primitive root. 反之若 a 在 modulo p^2 之下是 primitive root, 即 $\text{ord}_{p^2}(a) = p(p-1)$, 故由 order 的定義知 $a^{p-1} \not\equiv 1 \pmod{p^2}$. \square

知道如何判別 modulo p 的 primitive root 在 modulo p^2 亦是 primitive root 後, 接下來我們就要找到哪些 modulo p 的 primitive root 在 modulo p^2 之下仍為 primitive root. 現假設 a 在 modulo p 之下是 primitive root, 那麼那些在 modulo p 之下和 a 同餘的數在 modulo p 之下也都是 primitive root, 但這些數在 modulo p^2 之下可能不同餘, 我們就將它們一一列出. 也就是說, $a, a+p, \dots, a+(p-1)p$, 共有這 p 個數是在 modulo p 之下同餘但在 modulo p^2 之下不同餘.

Proposition 6.3.5. 假設 p 是一個質數且 $a \in \mathbb{Z}$ 為一個在 modulo p 之下的 primitive root. 令 $S = \{a, a+p, a+2p+\dots, a+(p-1)p\}$, 則在 S 中僅有一個元素在 modulo p 之下不是 primitive root, 其餘 $p-1$ 個元素在 modulo p 之下是 primitive root.

Proof. 已知 a 在 modulo p 之下是 primitive root 且 S 中的元素在 modulo p 之下皆與 a 同餘, 故知 S 中的元素在 modulo p 之下皆為 primitive root. 所以我們可以利用 Lemma 6.3.4 檢查 S 中哪些元素 $a+tp$ 會使得 $(a+tp)^{p-1} \equiv 1 \pmod{p^2}$.

由於 $a^{p-1} \equiv 1 \pmod{p}$, 故存在 $\lambda \in \mathbb{Z}$ 使得 $a^{p-1} = 1 + \lambda p$. 因此

$$(a+tp)^{p-1} = a^{p-1} + (p-1)a^{p-2}(tp) + \frac{(p-1)(p-2)}{2}a^{p-3}(tp)^2 + \dots$$

由於 $C_2^{p-1}a^{p-3}(tp)^2$ 這一項以及其之後每一項 $C_k^{p-1}a^{p-1-k}(tp)^k$, $k \geq 3$ 在 modulo p^2 之下皆為 0, 所以我們得

$$(a+tp)^{p-1} \equiv a^{p-1} - a^{p-2}tp \equiv 1 + (\lambda - a^{p-2}t)p \pmod{p^2}.$$

因此要找到 t 使得 $(a+tp)^{p-1} \equiv 1 \pmod{p^2}$ 若且唯若 $p \mid \lambda - a^{p-2}t$. 也就是說我們要找到 $t \in \{0, 1, 2, \dots, p-1\}$ 使得 $a^{p-2}t \equiv \lambda \pmod{p}$. 然而 $a^{p-1} \equiv 1 \pmod{p}$, 故上式兩邊乘上 a 得 $t \equiv a\lambda \pmod{p}$. 也就是說當 $0 \leq t \leq p-1$, 僅在 $t \equiv a\lambda \pmod{p}$ 時, 會使得 $(a+tp)^{p-1} \equiv 1 \pmod{p^2}$, 此時 $a+tp$ 在 modulo p^2 之下不是 primitive root. 其餘 S 中的元素 $a+rp$ 由於皆會使得 $(a+rp)^{p-1} \not\equiv 1 \pmod{p^2}$, 故由 Lemma 6.3.4 知皆為 modulo p^2 之下的 primitive root. \square

從 Theorem 6.3.3 以及 Proposition 6.3.5 我們知道由於 modulo p 的 primitive root 存在, 所以 modulo p^2 的 primitive root 也存在. 事實上若 a 是 modulo p 的 primitive root, 我們僅要檢驗是否 $a^{p-1} \equiv 1 \pmod{p^2}$. 要是 $a^{p-1} \not\equiv 1 \pmod{p^2}$, 那麼由 Lemma 6.3.4, 我們知 a 在 modulo p^2 之下是 primitive root. 要是 $a^{p-1} \equiv 1 \pmod{p^2}$, 那麼 a 在 modulo p^2 之下不是 primitive root, 故由 Proposition 6.3.5 知 $a+p$ 在 modulo p^2 之下必為 primitive root.

6.3.3. Modulo p^n 的 Primitive Root. 由於 modulo p 的 primitive root 存在, 利用 Corollary 6.1.9 知在 modulo p 之下共有 $\phi(\phi(p)) = \phi(p-1)$ 個 primitive roots. Proposition 6.3.5 告訴我們每一個 modulo p 的 primitive root 在 modulo p^2 之下可得 $p-1$ 個 primitive roots, 所以在 modulo p^2 之下我們共找到了 $(p-1)\phi(p-1)$ 個 primitive roots. 然而由於 modulo p^2 的 primitive root 存在, Corollary 6.1.9 告訴我們在 modulo p^2 之下共有 $\phi(\phi(p^2)) = \phi(p(p-1))$ 個 primitive roots. 由於 p 和 $p-1$ 互質, 我們有 $\phi(\phi(p^2)) = \phi(p)\phi(p-1) = (p-1)\phi(p-1)$. 此值恰與前面由 modulo p 的 primitive root 所得 modulo p^2 的 primitive roots 的個數相吻合. 也就是說每一個 modulo p^2 的 primitive root 的確來自於某個 modulo p 的 primitive root. 我們可以如此一直估算下去, 若 modulo p^3 的 primitive root 存在, 則由 Corollary 6.1.9 知在 modulo p^3 之下共有

$$\phi(\phi(p^3)) = \phi(p^2(p-1)) = \phi(p^2)\phi(p-1) = p(p-1)\phi(p-1)$$

個 primitive roots. 而又已知在 modulo p^2 之下共有 $(p-1)\phi(p-1)$ 個 primitive roots. 每一個 modulo p^2 的 primitive root, 在 modulo p^3 之下共可產生 p 個不同餘類, 所以這 $(p-1)\phi(p-1)$ 個 modulo p^2 的 primitive roots 在 modulo p^3 之下共產生了 $p(p-1)\phi(p-1)$ 個不同餘類. 這個數字恰與前面所提若 modulo p^3 的 primitive root 存在則在 modulo p^3 之下共有 $p(p-1)\phi(p-1)$ 個 primitive roots 相吻合. 也就是說每一個 modulo p^2 的 primitive root, 在 modulo p^3 之下產生的 p 個不同餘類“應該”在 modulo p^3 仍為 primitive root.

接下來我們就是要用數學歸納法來驗證此事，我們要證明當 $n \geq 3$ 時任何數只要在 modulo p^2 是 primitive root，則在 modulo p^n 必也是 primitive root. 首先我們來看如何判別一個 modulo p^n 的 primitive root 在 modulo p^{n+1} 之下是否為 primitive root.

Lemma 6.3.6. 假設 $a \in \mathbb{Z}$ 是一個 primitive root modulo p^n . 則 $\text{ord}_{p^{n+1}}(a) = p^{n-1}(p-1)$ 或 $\text{ord}_{p^{n+1}}(a) = p^n(p-1)$. 特別地, $a^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$ 若且唯若 a 在 modulo p^{n+1} 之下是一個 primitive root.

Proof. 依假設 a 在 modulo p^n 之下是 primitive root 表示 $\text{ord}_{p^n}(a) = \phi(p^n) = p^{n-1}(p-1)$. 現假設 $\text{ord}_{p^{n+1}}(a) = k$, 則 $a^k \equiv 1 \pmod{p^{n+1}}$, 因此知 $a^k \equiv 1 \pmod{p^n}$. 故依 $\text{ord}_{p^n}(a) = p^{n-1}(p-1)$ 及 Proposition 6.1.4 知 $p^{n-1}(p-1) | k$. 又因為 a 與 p 互質, 故 a 與 p^{n+1} 互質, 故由 Euler's Theorem 知 $a^{\phi(p^{n+1})} \equiv 1 \pmod{p^{n+1}}$, 因此在 modulo p^{n+1} 的情況再利用 Proposition 6.1.4 知 $k | \phi(p^{n+1})$. 由於 $\phi(p^{n+1}) = p^n(p-1)$, 我們得 $p^{n-1}(p-1) | k$ 且 $k | p^n(p-1)$. 也就是 $k = \lambda p^{n-1}(p-1)$ 且又 $\lambda p^{n-1}(p-1) | p^n(p-1)$, 故知 $\lambda | p$. 因此由 p 是質數知 $\lambda = 1$ 或 $\lambda = p$. 故得證 $\text{ord}_{p^{n+1}}(a) = p^{n-1}(p-1)$ 或 $\text{ord}_{p^{n+1}}(a) = p^n(p-1)$.

現若 $a^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$, 知 a 在 modulo p^{n+1} 之下其 order 一定不是 $p^{n-1}(p-1)$, 故得 $\text{ord}_{p^{n+1}}(a) = p^n(p-1) = \phi(p^{n+1})$. 由 Corollary 6.1.7 得證 a 在 modulo p^{n+1} 之下是一個 primitive root. 反之若 a 在 modulo p^{n+1} 之下是 primitive root, 即 $\text{ord}_{p^{n+1}}(a) = p^n(p-1)$, 故由 order 的定義知 $a^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$. \square

現若我們找到 a 在 modulo p^2 之下是 primitive root, 要檢查 a 在 modulo p^3 之下是否為 primitive root, 依 Lemma 6.3.6, 我們要檢查 $a^{p(p-1)}$ 在 modulo p^3 之下是否與 1 同餘. 然而已知 $a^{p-1} \equiv 1 \pmod{p}$ (Fermat's Little Theorem) 我們可令 $a^{p-1} = 1 + \lambda p$. 此時由於 a 在 modulo p^2 之下是 primitive root 故由 Lemma 6.3.4 知 $a^{p-1} \not\equiv 1 \pmod{p^2}$, 即 $p \nmid \lambda$. 依此可得

$$a^{p(p-1)} = (a^{p-1})^p = (1 + \lambda p)^p = 1 + p(\lambda p) + \frac{p(p-1)}{2}(\lambda p)^2 + \dots$$

這裡由於 p 是奇數所以 $p | p(p-1)/2$ (注意這就是為何此結果在 $p=2$ 時不成立的原因), 再加上之後每一項 $C_k^p(\lambda p)^k$, $k \geq 3$ 在 modulo p^3 之下皆為 0, 所以我們得

$$a^{p(p-1)} \equiv 1 + \lambda p^2 \pmod{p^3}.$$

故由 $p \nmid \lambda$ 得證 $a^{p(p-1)} \not\equiv 1 \pmod{p^3}$, 所以依 Lemma 6.3.6 知 a 在 modulo p^3 之下亦為 primitive root. 如此一直下去, 我們可證得當 $n \geq 3$ 時, a 在 modulo p^n 之下皆為 primitive root.

Proposition 6.3.7. 假設 a 在 modulo p^2 之下是一個 primitive root. 則對任意 $n \geq 3$, a 在 modulo p^n 之下也是 primitive root.

Proof. 前面我們已證得 a 在 modulo p^3 之下是 primitive root. 現在依歸納法, 我們假設 a 在 modulo p^n ($n \geq 3$) 之下是 primitive root, 要證明 a 在 modulo p^{n+1} 之下仍為 primitive root.

由於 a 與 p 互質, 依 Euler's Theorem 知 $a^{\phi(p^{n-1})} = a^{p^{n-2}(p-1)} \equiv 1 \pmod{p^{n-1}}$. 現假設 $a^{p^{n-2}(p-1)} = 1 + \lambda p^{n-1}$. 由於 a 在 modulo p^n 之下是 primitive root, 依 Lemma 6.3.6 知 $a^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}$, 故知 $p \nmid \lambda$. 現考慮

$$a^{p^{n-1}(p-1)} = (a^{p^{n-2}(p-1)})^p = (1 + \lambda p^{n-1})^p = 1 + p(\lambda p^{n-1}) + \frac{p(p-1)}{2}(\lambda p^{n-1})^2 + \dots$$

在 $p(\lambda p^{n-1})$ 之後每一項 $C_k^p(\lambda p^{n-1})^k$, $k \geq 2$ 中由於 $k(n-1) \geq 2(n-1) = n + (n-2) \geq n+1$ (因為 $n \geq 3$), 所以當 $k \geq 2$ 時在 modulo p^{n+1} 之下 $C_k^p(\lambda p^{n-1})^k$ 皆為 0, 所以我們得

$$a^{p^{n-1}(p-1)} \equiv 1 + \lambda p^n \pmod{p^{n+1}}.$$

故由 $p \nmid \lambda$ 得證 $a^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$, 所以依 Lemma 6.3.6 知 a 在 modulo p^{n+1} 之下亦為 primitive root. \square

從 Theorem 6.3.3 以及 Proposition 6.3.5 我們知道 modulo p^2 的 primitive root 存在, 所以再由 Proposition 6.3.7 得知當 $n \geq 3$ 時 modulo p^n 的 primitive root 也存在. 再次強調由於從 modulo p^2 的 primitive root 推得 modulo p^3 的 primitive root 之過程需用到 p 是奇數所以當 $n \geq 3$ 時 modulo p^n 的 primitive root 存在需在 p 是奇質數才成立. 事實上之前我們已知在 modulo $2^3 = 8$ 時 primitive root 是不存在的.

6.3.4. Modulo $2p^n$ 的 Primitive Root. 我們已知在 modulo p^n 之下皆有 primitive root. 現在我們將由 modulo p^n 的 primitive root 找出 modulo $2p^n$ 的 primitive. 首先我們來看當 m 是奇數時 modulo m 的 order 和 modulo $2m$ 的 order 間之關係.

Lemma 6.3.8. 給定一奇數 m , 且 $a \in \mathbb{Z}$ 是一個和 m 互質的奇數. 若 $\text{ord}_m(a) = n$, 則 $\text{ord}_{2m}(a) = n$.

Proof. 由於 a 是奇數且與 m 互質, 故知 $\text{gcd}(a, 2m) = 1$. 因此 a 在 modulo $2m$ 之下的 order 是有定義的, 就假設 $\text{ord}_{2m}(a) = k$. 由 $a^k \equiv 1 \pmod{2m}$ 可得 $a^k \equiv 1 \pmod{m}$. 故由 $\text{ord}_m(a) = n$ 以及 Proposition 6.1.4 知 $n|k$. 另一方面由於 $a^n \equiv 1 \pmod{m}$ 且 a 為奇數知 $a^n \equiv 1 \pmod{2}$, 故知 $m|a^n - 1$ 且 $2|a^n - 1$. 又由於 m 是奇數知 $\text{gcd}(2, m) = 1$, 故由 Proposition 1.2.6(2) 知 $2m|a^n - 1$, 也就是說 $a^n \equiv 1 \pmod{2m}$. 因假設 $\text{ord}_{2m}(a) = k$, 故再利用 Proposition 6.1.4 得 $k|n$. 因此得證 $k = n$ 也就是說 $\text{ord}_{2m}(a) = n$. \square

假設 a 為 modulo p^n 的 primitive root, 即 $\text{ord}_{p^n}(a) = \phi(p^n)$. 若 a 又是奇數則由 Lemma 6.3.8 知 $\text{ord}_{2p^n}(a) = \phi(p^n)$. 但由於 p 是奇質數與 2 互質, 故知 $\phi(2p^n) = \phi(2)\phi(p^n) = \phi(p^n)$. 也就是說 $\text{ord}_{2p^n}(a) = \phi(2p^n)$. 故由 Corollary 6.1.7 知 a 在 modulo $2p^n$ 之下亦為 primitive root. 利用此結果我們可找到 modulo $2p^n$ 的 primitive root.

Proposition 6.3.9. 給定 p 是一個奇質數, 則一定可找到一奇數 a 使其在 modulo p^2 之下是一個 primitive root. 特別地, 此時對任意 $n \in \mathbb{N}$, a 在 modulo $2p^n$ 之下亦為 primitive root.

Proof. 當 $p = 3$ 時, 由於 $\text{ord}_3(5) = \text{ord}_3(2) = 2$ 故知 5 在 modulo 3 之下是一個 primitive root. 又由於 $5^{3-1} = 25 \not\equiv 1 \pmod{9}$, 故由 Lemma 6.3.4 知 5 在 modulo 3^2 之下是一個 primitive root.

當 $p \geq 5$ 是一個奇質數時, Theorem 6.3.3 告訴我們在 modulo p 之下的 primitive root 存在. 現假設 α 是一個 modulo p 之下的 primitive root. 利用 Proposition 6.3.5 知 $\{\alpha, \alpha + p, \dots, \alpha + (p-1)p\}$ 中僅有一個在 modulo p^2 之下不是 primitive root. 由於 $p \geq 5$, 得 $p-1 \geq 4$, 故知 $\{\alpha, \alpha + p, \alpha + 2p, \alpha + 3p\}$ 中至多有一個在 modulo p^2 之下不是 primitive root. 因此若 α 是奇數, 則得 $\alpha, \alpha + 2p$ 這兩個奇數中必有一個在 modulo p^2 之下是 primitive root. 若 α 是偶數, 則得 $\alpha + p, \alpha + 3p$ 這兩個奇數中必有一個在 modulo p^2 之下是 primitive root. 我們得證必存在一奇數在 modulo p^2 之下是 primitive root.

現假設 a 是一奇數且在 modulo p^2 之下是 primitive root. 由 Proposition 6.3.7 知 a 在 modulo p^n 之下亦為 primitive root. 故由 Lemma 6.3.8 知 $\text{ord}_{2p^n}(a) = \text{ord}_{p^n}(a) = \phi(p^n) = \phi(2p^n)$, 故得證 a 在 modulo $2p^n$ 之下亦為 primitive root. \square

事實上要找到一奇數使其在 modulo p^2 之下是 primitive root 並不需如 Proposition 6.3.9 的證明中那麼複雜. 若 a 是偶數且在 modulo p^2 之下是 primitive root, 那麼 $a + p^2$ 必為奇數且由於 $a + p^2 \equiv a \pmod{p^2}$ 所以 $a + p^2$ 當然也是在 modulo p^2 之下的 primitive root. 不過由於考慮 $a + p^2$ 數值較大, 我們若要找較小的 primitive root, 證明中最大只要考慮到 $a + 3p$, 這個數當 p 很大時當然比 $a + p^2$ 要小得多.

我們總結這兩節 Proposition 6.2.2, Proposition 6.2.4, Theorem 6.3.3, Proposition 6.3.5, Proposition 6.3.7 以及 Proposition 6.3.9 之結果得到以下所謂的 primitive root Theorem.

Theorem 6.3.10 (Primitive Root Theorem). 只有當 $m = 2, 4, p^n, 2p^n$ 時, 其中 p 為奇質數且 $n \in \mathbb{N}$, 在 modulo m 之下會有 primitive root.

6.4. 高次的 Congruence Equation

所謂高次的 congruence equation 指的是次數大於 2 的 congruence equation. 我們這裡要處理的當然不是一般的 congruence equation. 我們想利用 primitive root 來幫我們解如 $x^n \equiv a \pmod{m}$ 其中 $\text{gcd}(a, m) = 1$ 這樣的 congruence equation.

首先我們將 m 寫成質因數的乘積, 即 $m = 2^{n_0} p_1^{n_1} \cdots p_r^{n_r}$, 其中這些 p_i 為相異奇質數而 $n_0 \geq 0$. 利用 Corollary 4.4.3, 我們知道 $x^n \equiv a \pmod{m}$ 有解若且唯若 $x^n \equiv a \pmod{2^{n_0}}$ 以及所有的 $i \in \{1, \dots, r\}$, $x^n \equiv a \pmod{p_i^{n_i}}$ 皆有解. 所以我們只要探討 $x^n \equiv a \pmod{2^{n_0}}$ 及 $x^n \equiv a \pmod{p_i^{n_i}}$ 解的情況. 當 $n_0 \geq 3$ 時, 由於在 modulo 2^{n_0} 沒有 primitive root, 討論解的情形較複雜, 這裡我們不多做討論. 我們僅討論當 $n_0 \leq 2$ 的情形, 也就是說此處我們探討解 $x^n \equiv a \pmod{m}$ 的方法僅適用於 $8 \nmid m$ 的情況. 在此情況之下我們只要解 $x^n \equiv a \pmod{2^{n_0}}$, 其中 $n_0 \leq 2$, 以及解 $x^n \equiv a \pmod{p_i^{n_i}}$. 這兩種情況 (即 modulo 2^{n_0} 和 modulo $p_i^{n_i}$), 由於 primitive root 皆存在, 我們利用下面的方法就可判別其解是否存在.

Theorem 6.4.1. 給定 $m \in \mathbb{N}$, 假設在 modulo m 之下 primitive root 存在. 考慮 $x^n \equiv a \pmod{m}$, 其中 $n \in \mathbb{N}$ 且 $\gcd(a, m) = 1$. 令 $d = \gcd(n, \phi(m))$. 則 $x^n \equiv a \pmod{m}$ 有解若且唯若

$$a^{\phi(m)/d} \equiv 1 \pmod{m}.$$

Proof. 首先假設 $x^n \equiv a \pmod{m}$ 有解, 即存在 $c \in \mathbb{Z}$ 滿足 $c^n \equiv a \pmod{m}$. 因為 $\gcd(a, m) = 1$, 所以 $\gcd(c, m) = 1$, 故由 Euler's Theorem (3.3.2) 知 $c^{\phi(m)} \equiv 1 \pmod{m}$. 此時由於 $d|\phi(m)$ 且 $d|n$, 故得

$$a^{\phi(m)/d} \equiv (c^n)^{\phi(m)/d} = (c^{\phi(m)})^{n/d} \equiv 1 \pmod{m}.$$

(注意此部分的證明是不需 modulo m 的 primitive root 存在之假設.)

反之, 假設 γ 為 modulo m 之下的一個 primitive root. 依定義 $\{\gamma, \gamma^2, \dots, \gamma^{\phi(m)}\}$ 是一個 reduced residue system modulo m , 也就是說任何和 m 互質的數 b , 皆存在 $i \in \mathbb{N}$ 使得 $\gamma^i \equiv b \pmod{m}$. 因此存在 $r \in \mathbb{N}$ 使得 $a \equiv \gamma^r \pmod{m}$. 另一方面若 c 是 $x^n \equiv a \pmod{m}$ 的一個解, 則由於 $\gcd(c, m) = 1$, 一定也存在 $t \in \mathbb{N}$ 使得 $c \equiv \gamma^t \pmod{m}$. 因此要解 $x^n \equiv a \pmod{m}$ 就等同於要找到 $t \in \mathbb{N}$ 使得

$$(\gamma^t)^n = \gamma^{nt} \equiv \gamma^r \pmod{m}.$$

由於 γ 是 modulo m 的 primitive root, 我們有 $\text{ord}_m(\gamma) = \phi(m)$, 故利用 Proposition 6.1.6, 知 $\gamma^{nt} \equiv \gamma^r \pmod{m}$ 若且唯若 $nt \equiv r \pmod{\phi(m)}$, 也就是說我們要找到 $t \in \mathbb{N}$ 滿足

$$nt \equiv r \pmod{\phi(m)}.$$

另一方面依假設 $a^{\phi(m)/d} \equiv 1 \pmod{m}$, 即 $\gamma^{r\phi(m)/d} \equiv 1 \pmod{m}$, 故由 Proposition 6.1.4 知 $\phi(m)|r\phi(m)/d$. 這表示 $\phi(m)r/d$ 必須是 $\phi(m)$ 的倍數, 亦即 $r/d \in \mathbb{Z}$, 也就是說 $d|r$. 然而 Proposition 4.3.1 告訴我們給定 n, r , 一次的 congruence equation, $nt \equiv r \pmod{\phi(m)}$ 有解若且唯若 $d = \gcd(n, \phi(m))|r$. 所以我們由 $a^{\phi(m)/d} \equiv 1 \pmod{m}$ 之假設知 $nt \equiv r \pmod{\phi(m)}$ 必有解. 若 t_0 為其一解, 令 $c = \gamma^{t_0}$, 則得

$$c^n = \gamma^{nt_0} \equiv \gamma^r \equiv a \pmod{m}.$$

故知 c 為 $x^n \equiv a \pmod{m}$ 的一個解. □

當 $m = p$ 為一質數 (此時 modulo p 當然有 primitive root) 且 $n = 2$ 時, Theorem 6.4.1 就是 Euler's criterion (Theorem 5.3.3). 所以 Theorem 6.4.1 可以說是 Theorem 5.3.3 的推廣.

接下來我們要知道 $x^n \equiv a \pmod{m}$ 要是解, 那麼在 modulo m 之下會有多少解. 和往常一樣, 我們所用的方法是直接探討兩個解之間的關係, 如此一來不只可以精確地算出解的個數, 而且可以很快的利用一個已知解將其他的解求出.

Proposition 6.4.2. 給定 $m \in \mathbb{N}$, 假設在 modulo m 之下 primitive root 存在. 考慮 $x^n \equiv a \pmod{m}$, 其中 $n \in \mathbb{N}$ 且 $\gcd(a, m) = 1$. 令 $d = \gcd(n, \phi(m))$. 若 $x^n \equiv a \pmod{m}$ 有解, 則在 modulo m 之下共有 d 個解.

事實上, 若 $x \equiv c \pmod{m}$ 是 $x^n \equiv a \pmod{m}$ 的一個解且 γ 是 modulo m 之下的一個 primitive root, 則在 modulo m 之下 $x \equiv c\gamma^{t\phi(m)/d} \pmod{m}$, 其中 $t \in \{0, 1, \dots, d-1\}$ 是 $x^n \equiv a \pmod{m}$ 所有的解.

Proof. 由於 a 和 m 互質, $x^n \equiv a \pmod{m}$ 的解皆與 m 互質. 又由於 γ 是 modulo m 之下的一個 primitive root, 所以對於 $x^n \equiv a \pmod{m}$ 的任兩個解, 我們可假設其分別為 γ^r 和 γ^s , 其中 $r, s \in \mathbb{N}$. 也就是說

$$\gamma^r = (\gamma^r)^n \equiv a \equiv (\gamma^s)^n \equiv \gamma^{sn} \pmod{m}.$$

因此利用 $\text{ord}_m(\gamma) = \phi(m)$ 以及 Proposition 6.1.6 得 $rn \equiv sn \pmod{\phi(m)}$. 因此由於 $d = \text{gcd}(n, \phi(m))$ 依 Proposition 3.2.3 知 $r \equiv s \pmod{\phi(m)/d}$. 也就是說存在 $\lambda \in \mathbb{Z}$ 使得 $s = r + \lambda\phi(m)/d$. 反之, 若 γ^r 是 $x^n \equiv a \pmod{m}$ 的一個解且 $s = r + \lambda\phi(m)/d$, 則

$$(\gamma^s)^n = (\gamma^r \gamma^{\lambda\phi(m)/d})^n = \gamma^{rn} \gamma^{\lambda\phi(m)n/d} \equiv a (\gamma^{\phi(m)})^{\lambda n/d} \equiv a \pmod{m}.$$

因此 γ^s 也是 $x^n \equiv a \pmod{m}$ 的一個解.

我們證得了若 $x \equiv c \equiv \gamma^r \pmod{m}$, 是 $x^n \equiv a \pmod{m}$ 的一個解, 則 $x \equiv c\gamma^{\lambda\phi(m)/d} \pmod{m}$, 其中 $\lambda \in \mathbb{Z}$, 是 $x^n \equiv a \pmod{m}$ 所有的解. 不過這些解在 modulo m 之下有許多是相同的, 我們必須將有哪些相異解找出. 然而 c 和 m 互質, 故由 Corollary 3.2.4 知 $c\gamma^{\lambda\phi(m)/d} \equiv c\gamma^{\lambda'\phi(m)/d} \pmod{m}$ 若且唯若 $\gamma^{\lambda\phi(m)/d} \equiv \gamma^{\lambda'\phi(m)/d} \pmod{m}$. 再利用 $\text{ord}_m(\gamma) = \phi(m)$ 以及 Proposition 6.1.6 知 $\gamma^{\lambda\phi(m)/d} \equiv \gamma^{\lambda'\phi(m)/d} \pmod{m}$ 若且唯若 $\lambda\phi(m)/d \equiv \lambda'\phi(m)/d \pmod{\phi(m)}$ 也就是說 $\phi(m)|(\lambda - \lambda')\phi(m)/d$ 亦即 $d|\lambda - \lambda'$. 因此當 $0 \leq t \leq d-1$ 時, $c\gamma^{t\phi(m)/d}$ 在 modulo m 之下皆相異. 另一方面對任意 $\lambda \in \mathbb{Z}$ 皆存在 $h, t \in \mathbb{Z}$ 使得 $\lambda = hd + t$, 其中 $0 \leq t \leq d-1$. 所以 $c\gamma^{\lambda\phi(m)/d}$ 在 modulo m 之下都會與某個 $c\gamma^{t\phi(m)/d}$ 同餘, 其中 $t \in \{0, 1, \dots, d-1\}$. 因此我們得證 $x^n \equiv a \pmod{m}$ 若有 $x \equiv c \pmod{m}$ 這一個解則在 modulo m 之下 $x^n \equiv a \pmod{m}$ 共有 $x \equiv c, c\gamma^{\phi(m)/d}, c\gamma^{2\phi(m)/d}, \dots, c\gamma^{(d-1)\phi(m)/d}$ 這 d 個解. \square

接下來我們利用一個實際的例子解釋 Proposition 6.4.1 和 Proposition 6.4.2 所得之結果.

Example 6.4.3. 我們來探討 $x^{12} \equiv 10 \pmod{27}$ 和 $x^{12} \equiv 11 \pmod{27}$ 解的情形.

由於 $27 = 3^3$ 所以在 modulo 27 之下 primitive root 是存在的. 又 $\phi(27) = 18$ 且 $\text{gcd}(12, \phi(27)) = \text{gcd}(12, 18) = 6$ 利用 Proposition 6.4.1 我們可分別由 $10^{\phi(27)/6} = 10^3$ 和 11^3 在 modulo 27 是否為 1 來判定 $x^{12} \equiv 10 \pmod{27}$ 和 $x^{12} \equiv 11 \pmod{27}$ 是否有解. 事實上 $10^3 \equiv 1 \pmod{27}$ 且 $11^3 \equiv 8 \not\equiv 1 \pmod{27}$, 所以 $x^{12} \equiv 10 \pmod{27}$ 有解而 $x^{12} \equiv 11 \pmod{27}$ 無解.

要找出 $x^{12} \equiv 10 \pmod{27}$ 的解, 首先需先找到 modulo 27 的一個 primitive root. 由於 2 是 modulo 3 的 primitive root 且 $2^2 \equiv 4 \not\equiv 1 \pmod{9}$, 所以由 Lemma 6.3.4 知 2 在 modulo 9 是 primitive root. 因而由 Proposition 6.3.7 知 2 在 modulo 27 之下依然是 primitive root. 既然 2 是 modulo 27 的一個 primitive root 經計算我們知 $2^6 \equiv 10 \pmod{27}$ 且可以將

$x^{12} \equiv 10 \pmod{27}$ 的一解寫成 $x \equiv 2^t \pmod{27}$ 的形式. 也就是說我們要解

$$(2^t)^{12} \equiv 2^6 \pmod{27}.$$

因此由 $\text{ord}_{27}(2) = \phi(27) = 18$ 以及 Proposition 6.1.6 知此等價於解

$$12t \equiv 6 \pmod{18}.$$

故由 $\text{gcd}(18, 12) = 6$ 得 $2t \equiv 1 \pmod{3}$, 即 $t \equiv 2 \pmod{3}$. 解出 $x \equiv 2^2 \equiv 4 \pmod{27}$ 為 $x^{12} \equiv 10 \pmod{27}$ 的一個解. 再由 $\phi(27)/6 = 3$ 以及 Proposition 6.4.2 知 $x \equiv 4, 4 \times 2^3, 4 \times 2^6, 4 \times 2^9, 4 \times 2^{12}, 4 \times 2^{15} \pmod{27}$, 即 $x \equiv 4, 5, 13, 23, 22, 14 \pmod{27}$ 為 $x^{12} \equiv 10 \pmod{27}$ 所有的解. 事實上我們也可以由 $12t \equiv 6 \pmod{18}$ 找到 $t \equiv 2, 5, 8, 11, 14, 17 \pmod{18}$ 為其所有的解, 而得 $x \equiv 2^2, 2^5, 2^8, 2^{11}, 2^{14}, 2^{17} \pmod{27}$ 為 $x^{12} \equiv 10 \pmod{27}$ 所有的解.