Chapter 6

Primitive Roots

給定 $m \in \mathbb{N}$, 若存在 $a \in \mathbb{Z}$ 使得 $\{a, a^2, \ldots, a^{\phi(m)}\}$ 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 $\{2, 2^2, \ldots, 2^{10}\}$ 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 $1 \le n \le 10$ 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 $0 \le i \le 9$, 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 $1 \le i \ne j \le 10$ 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 $t = 2, 7, \ldots$ 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 $\{2,2^2,\ldots,2^{10}\}$ 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 $\{2,2^2,\ldots,2^6\}$ 在 modulo 7 之下並不是 reduced residue system. 我們將有此特性的元素給個特定的名子.

Definition 6.1.1. 給定 $m\in\mathbb{N}$, 若 $a\in\mathbb{Z}$ 且與 m 互質滿足 $\{a,a^2,\ldots,a^{\phi(m)}\}$ 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 $\{a,a^2,a^3,a^4,\ldots,a^8\}$ 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

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

是 reduced residue system modulo m, 所以若 $1\le i\ne j\le\phi(m)$, 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 $1\le i\le\phi(m)-1$, 則 $a^i\not\equiv 1 \pmod m$ (否則會造成 $1\le i<\phi(m)$ 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 $\mathrm{ord}_m(a)=n$ 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 $\mathrm{ord}_m(a)$ 必存在且依定義知 $\mathrm{ord}_m(a)\le\phi(m)$. 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 $\mathrm{ord}_m(a)=\mathrm{ord}_m(b)$.

(2) $\mathrm{ord}_m(a)=1$ 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 $\mathrm{ord}_m(a)=\mathrm{ord}_m(b)$.

(2) 若 $\mathrm{ord}_m(a)=1$, 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 $\mathrm{ord}_m(a)=1$. □

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

(1) $a^n \equiv 1 \pmod m$.

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

要記住這兩件事缺一不可才能保證 $\mathrm{ord}_m(a)=n$. 接下來我們就來看依此兩點可推得 $\mathrm{ord}_m(a)$ 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 $\mathrm{ord}_m(a)=n$. 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 $0 \le r \le n-1$. 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 $1 \le r \le n-1$), 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 $a^{\phi(m)} \equiv 1 \pmod 1$, 故由 Proposition 6.1.4 知 $\mathrm{ord}_m(a) | \phi(m)$, 這比我們前面依定義知 $\mathrm{ord}_m(a) \le \phi(m)$ 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 $\mathrm{ord}_m(a)$ 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 $\mathrm{ord}_m(a)=n$ 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 $\mathrm{ord}_m(a)=n$, 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 $\mathrm{ord}_m(a)=n$. 由於 (1) 已知 $a^n \equiv 1 \pmod m$, 故僅剩要證明若 $1 \le i \le n-1$, 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 $1 \le i \le n-1$ 相矛盾, 故知 $a^i \not\equiv 1 \pmod m$. 也就是說 $\mathrm{ord}_m(a)=n$. □

Corollary 6.1.5 的 (2) 將 $\mathrm{ord}_m(a)=n$ 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 $\mathrm{ord}_m(a)=n$ 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 $i \ge j$, 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 $\mathrm{ord}_m(a)=n$ 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 $a^i = a^j a^{i-j} \equiv a^j \pmod{m}$. □

若 $\mathrm{ord}_m(a) = n$, Proposition 6.1.6 不只告訴我們 $a, a^2, \ldots, a^i, \ldots$ 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, $a, a^2, \ldots, a^n$ 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 $\mathrm{ord}_m(a)$ 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 $\mathrm{ord}_m(a) = \phi(m)$ 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 $a, a^2, \ldots, a^{\phi(m)}$ 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 $\mathrm{ord}_m(a) = \phi(m)$.

反之, 假設 $\mathrm{ord}_m(a) = \phi(m)$, 由 Proposition 6.1.6 知若 $a^i \equiv a^j \pmod{m}$, 則 $\phi(m)|i-j$. 因此 $a, a^2, \ldots, a^{\phi(m)}$ 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 $\{a, a^2, \ldots, a^{\phi(m)}\}$ 是一個 reduced residue system modulo m, 也就是說 a 在 modulo m 之下是一個 primitive root. □

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 $\mathrm{ord}_m(a) = n$, 則對於任意的正整數 i,

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

Proof. 為了方便, 我們令 $d = \gcd(i,n)$ 且 $i = i'd$ 以及 $n = n'd$. 欲證明 $\mathrm{ord}_m(a^i) = n/d = n'$, 首先得證明 $(a^i)^{n'} \equiv 1 \pmod{m}$. 事實上因由假設 $\mathrm{ord}_m(a) = n$, 知

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

接下來我們須證明, 若 $(a^i)^k \equiv 1 \pmod{m}$ 則 $n'|k$ (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' 和 i' 皆為整數且互質. 故由 $n'd|ki'd$ 可得 $n'|ki'$. 再由 n' 和 i' 互質, 得 $n'|k$. □

由 Proposition 6.1.8, 我們知 $\mathrm{ord}_m(a^i)$ 整除 $\mathrm{ord}_m(a)$ 而且 $\mathrm{ord}_m(a^i) = \mathrm{ord}_m(a)$ 若且唯若 $\gcd(i, \mathrm{ord}_m(a)) = 1$. 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 $\mathrm{ord}_m(a)=n$, 則 $\{a,a^2,\ldots,a^n\}$ 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 $\mathrm{ord}_m(a)=n$, 由 Proposition 6.1.8 知 $\mathrm{ord}_m(a^i)=n$ 若且唯若 $\gcd(n,i)=1$. 又由於 $a,a^2,\ldots,a^n$ 在 modulo m 之下皆相異, 故 $\{a,a^2,\ldots,a^n\}$ 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 $\mathrm{ord}_m(a)=\phi(m)$ 且所有和 m 互質的整數在 modulo m 之下皆和 $S=\{a,a^2,\ldots,a^{\phi(m)}\}$ 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. □

有時我們可利用整數 a 在 modulo m, n 之下的 order，得到 a 在 modulo mn 之下的 order.

Lemma 6.1.10. 假設 $m,n \in \mathbb{N}$ 且 $\gcd(a,mn)=1$，且 $\mathrm{ord}_m(a)=k$, $\mathrm{ord}_n(a)=l$，則 $\mathrm{lcm}(k,l)$ 整除 $\mathrm{ord}_{mn}(a)$. 若又假設 $\gcd(m,n)=1$, 則 $\mathrm{ord}_{mn}(a)=\mathrm{lcm}(k,l)$.

Proof. 為了方便，我們設 $\mathrm{ord}_{mn}(a)=c$。故由 $a^c \equiv 1 \pmod{mn}$ 得 $a^c \equiv 1 \pmod{m}$ 且 $a^c \equiv 1 \pmod{n}$，故由 order 的性質知 $\mathrm{ord}_m(a) \mid c$ 且 $\mathrm{ord}_n(a) \mid c$，因此 $\mathrm{ord}_m(a), \mathrm{ord}_n(a)$ 的最小公倍數 $\mathrm{lcm}(k,l)$ 會整除其公倍數 c。

現又因 $a^k \equiv 1 \pmod{m}$ 且 $\mathrm{lcm}(k,l)$ 為 k 的倍數，故 $a^{\mathrm{lcm}(k,l)} \equiv 1 \pmod{m}$。同理 $a^{\mathrm{lcm}(k,l)} \equiv 1 \pmod{n}$。亦即 $m \mid a^{\mathrm{lcm}(k,l)}-1$ 且 $n \mid a^{\mathrm{lcm}(k,l)}-1$ 因此若 $\gcd(m,n)=1$，可得 $mn \mid a^{\mathrm{lcm}(k,l)}-1$，亦即 $a^{\mathrm{lcm}(k,l)} \equiv 1 \pmod{mn}$。所以 $\mathrm{ord}_{mn}(a)=c$ 會整除 $\mathrm{lcm}(k,l)$。也因此，此時可得 $\mathrm{ord}_{mn}(a)=\mathrm{lcm}(k,l)$。 □

6.2. The Primitive Root Theorem

我們先探討有哪些 m 在 modulo m 之下沒有 primitive root. 接著證明其餘的情況 primitive root 皆存在。

我們提供兩個證明沒有 primitive root 的方法。

Lemma 6.2.1. 假設 $m>2$ 且在 *modulo* m 之下 *primitive root* 存在，則 *congruent equation* $x^2 \equiv 1 \pmod{m}$ 在 *modulo* m 之下僅能有 2 個解

Proof. 假設 α 為其中一個 primitive root，則 $x^2 \equiv 1 \pmod{m}$ 的解皆可表為 α^k。此時由 $(\alpha^k)^2=\alpha^{2k} \equiv 1 \pmod{m}$ 以及 $\mathrm{ord}_m(\alpha)=\phi(m)$，得 $\phi(m) \mid 2k$。因為當 $m>2$ 時 $\phi(m)$ 必為偶數，故知 $\frac{\phi(m)}{2} \mid k$，亦即 $k=\frac{\phi(m)}{2}$ 或 $k=\phi(m)$。得知 $\alpha^k \equiv \pm 1 \pmod{m}$。 □

現若 m 可分解成兩互質的整數相乘，即 $m = n_1 n_2$ 其中 $\gcd(n_1, n_2) = 1$，則 $x^2 \equiv 1 \pmod{m}$ 在 modulo m 之下的解可由 $x^2 \equiv 1 \pmod{n_1}$ 以及 $x^2 \equiv 1 \pmod{n_2}$ 的解，利用 Chinese Remainder Theorem 來求得。因此當 n_1, n_2 皆大於 2 時，由於 $x^2 \equiv 1 \pmod{n_1}$ 以及 $x^2 \equiv 1 \pmod{n_2}$ 分別至少有 $x \equiv \pm 1 \pmod{n_1}$ 以及 $x \equiv \pm 1 \pmod{n_2}$ 兩個解，所以在 modulo m 之下至少有 4 個解。因此知在此情況之下不可能有 primitive root. 我們得到以下之結論。

Proposition 6.2.2. 除了 $m = 2, 4$ 以及 $m = p^n, 2p^n$，其中 p 為奇質數, $n \in \mathbb{N}$ 外，其餘情形在 *modulo* m 之下，沒有 *primitive root.*

Proof. 只有在 $m = 2^n$, $m = p^n$ 以及 $m = 2p^n$, 其中 p 為奇質數，這三種情況之下 m 無法寫成兩個大於 2 且互質的整數乘積。不過當 $m = 2^n$ 且 $n \geq 3$ 時 $x^2 \equiv 1 \pmod{2^n}$ 有 4 個解，此與有 primitive root 時僅能有兩相違背。故僅當 $m = 2, 4$ 以及 $m = p^n, 2p^n$ 時，在 modulo m 之下可能有 primitive root. □

我們也可利用 Lemma 6.1.10 證明 Proposition 6.2.2。假設 m 可以寫成兩個大於 2 且互質的整數 n_1, n_2 的乘積。對任意與 m 互質的整數 a，由 Lemma 6.1.10 知 $\mathrm{ord}_m(a) = \mathrm{lcm}(\mathrm{ord}_{n_1}(a), \mathrm{ord}_{n_2}(a))$。然而 $\mathrm{ord}_{n_1}(a)$ 和 $\mathrm{ord}_{n_2}(a)$ 的最大值分別為 $\phi(n_1)$, $\phi(n_2)$。但 n_1, n_2 因為都大於 2，故 $\phi(n_1)$, $\phi(n_2)$ 皆為偶數。此時 $\mathrm{lcm}(\phi(n_1), \phi(n_2)) < \phi(n_1)\phi(n_2) = \phi(n_1 n_2)$，故 $\mathrm{ord}_m(a) < \phi(m)$，也因此在 modulo m 之下不會有 primitive root.

由於 $m = 2$ 時 1 為 primitive root，而 $m = 4$ 時 3 是 primitive root，故由 Proposition 6.2.2 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是否有 primitive root. 事實上 primitive root Theorem 說的便是在這剩下的情況中, primitive root 皆存在. 我們將先證明當 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. 接下來在本節中 p 永遠表示為奇質數, 我們就不再多說明.

6.2.1. 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.

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 $\mathrm{ord}_p(a) = n$, 已知 $a, a^2, \ldots, a^n$ 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 $a, a^2, \ldots, a^n$ 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 $\mathrm{ord}_p(b) = n$, 則由於 b 是 $x^n \equiv 1 \pmod{p}$ 之一解, 故由前知存在 $i \in \{1, \ldots, n\}$ 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 $\{a, a^2, \ldots, a^n\}$ 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 6.2.3. 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 6.2.4. 假設 p 是質數且令 $S=\{1,2,\ldots,p-1\}$. 現對於 $d\in\mathbb{N}$ 滿足 $d|p-1$, 我們考慮 $S_d=\{i\in S\mid \mathrm{ord}_p(i)=d\}$.

(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 $\mathrm{ord}_p(a)=d$ 且 $\mathrm{ord}_p(a)=d'$. 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 $\mathrm{ord}_p(i)|p-1$. 換句話說, 若 $\mathrm{ord}_p(i)=d$, 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 $\mathrm{ord}_p(a)=d$, 故利用 Lemma 6.2.3 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. □

Lemma 6.2.4(1,2) 告訴我們 $S=\{1,2,\ldots,p-1\}$ 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 6.2.5. 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 6.2.4 中所用的符號, 並令 $\#(S_d)$ 表示 $S_d=\{i\in S\mid \mathrm{ord}_p(i)=d\}$ 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 6.2.4(1,2) 我們知 $\sum_{d|p-1,d>0}\#(S_d)=p-1$ 而且 Lemma 6.2.4(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

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

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. □

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.

接下來，我們要利用 modulo p 的 primitive root 的存在性，證明 modulo p^n 之下 primitive root 的存在性。這裡一般會利用數學歸納法處理，所以我們先探討 a 在 modulo p^n 和 modulo p^{n+1} 之下，其 order 的變化。

Lemma 6.2.6. 假設 $a\in\mathbb{Z}$, $p\nmid a$ 且 $\mathrm{ord}_{p^n}(a)=k$，則 $\mathrm{ord}_{p^{n+1}}(a)=k$ 或 $\mathrm{ord}_{p^{n+1}}(a)=kp$.

Proof. 令 $\mathrm{ord}_{p^{n+1}}(a)=\ell$。因 $a^\ell\equiv 1\pmod{p^{n+1}}$ 得 $a^\ell\equiv 1\pmod{p^n}$，故由 $\mathrm{ord}_{p^n}(a)=k$ 的假設知 $k\mid\ell$。另一方面因為 $a^k\equiv 1\pmod{p^n}$ 知存在 $\lambda\in\mathbb{Z}$ 使得 $a^k=1+\lambda p^n$. 現考慮 $(a^k)^p=(1+\lambda p^n)^p=1+C_1^p\lambda p^n+C_2^p(\lambda p^n)^2+\cdots$，由於 $C_1^p\lambda p^n=\lambda p^{n+1}$ 這一項以及其之後每一項 $C_k^p(\lambda p^n)^k$, $k\ge 2$ 在 modulo p^{n+1} 之下皆為 0，我們有 $a^{kp}=(a^k)^p\equiv 1\pmod{p^{n+1}}$，故得 $\ell\mid kp$。然而前面已知 ℓ 為 k 的倍數，即 $\ell=km$，可得 $km\mid kp$，亦即 $m\mid p$。所以由 p 為質數，知 $m=1$ 或 $m=p$，故證明了 $\ell=k$ 或 $\ell=kp$。 □

6.2.2. 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, 那們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 6.2.7. 假設 $a\in\mathbb{Z}$ 是一個 *primitive root modulo* p. 則 $\mathrm{ord}_{p^2}(a)=p-1$ 或 $\mathrm{ord}_{p^2}(a)=p(p-1)$. 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 $\mathrm{ord}_p(a)=p-1$。故由 Lemma 6.2.6 知 $\mathrm{ord}_{p^2}(a)=p-1$ 或 $\mathrm{ord}_{p^2}(a)=p(p-1)$.

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 $\mathrm{ord}_{p^2}(a)=p(p-1)=\phi(p^2)$. 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 $\mathrm{ord}_{p^2}(a)=p(p-1)$, 故由 order 的定義知 $a^{p-1}\not\equiv 1\pmod{p^2}$. □

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, $a, a+p, \ldots, a+(p-1)p$, 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 6.2.8. 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 $S = \{a, a+p, a+2p+\cdots, a+(p-1)p\}$, 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* 之下都是 *primitive root.* 而不是 *primitive root* 的元素為 $a+tp$ 其中 t 滿足 $t \equiv a\lambda \pmod{p}$。

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 6.2.7 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

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

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 $p | \lambda - a^{p-2}t$. 也就是說我們要找到 $t \in \{0, 1, 2, \ldots, p-1\}$ 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 6.2.7 知皆為 modulo p^2 之下的 primitive root. □

從 Theorem 6.2.5 以及 Proposition 6.2.8 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 6.2.7, 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 6.2.8 知 $a+p$ 在 modulo p^2 之下必為 primitive root.

6.2.3. 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 6.2.8 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 6.2.9. 假設 $a \in \mathbb{Z}$ 是一個 *primitive root modulo* p^n. 則 $\mathrm{ord}_{p^{n+1}}(a) = p^{n-1}(p-1)$ 或 $\mathrm{ord}_{p^{n+1}}(a) = p^n(p-1)$. 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 $\mathrm{ord}_p(a) = \phi(p^n) = p^{n-1}(p-1)$。故由 Lemma 6.2.6 知 $\mathrm{ord}_{p^{n+1}}(a) = p^{n-1}(p-1)$ 或 $\mathrm{ord}_{p^2}(a) = p^n(p-1)$.

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 $\mathrm{ord}_{p^{n+1}}(a) = p^n(p-1) = \phi(p^{n+1})$. 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 $\mathrm{ord}_{p^{n+1}}(a) = p^n(p-1)$, 故由 order 的定義知 $a^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$. □

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 6.2.9, 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 6.2.7 知 $a^{p-1} \not\equiv 1 \pmod{p^2}$, 即 $p \nmid \lambda$. 依此可得

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

這裡由於 p 是奇數所以 $p \mid p(p-1)/2$ (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 6.2.9 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 6.2.10. 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 6.2.9 知 $a^{p^{n-2}(p-1)}\not\equiv 1 \pmod{p^n}$, 故知 $p\nmid\lambda$. 現考慮

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

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 6.2.9 知 a 在 modulo p^{n+1} 之下亦為 primitive root. □

從 Theorem 6.2.5 以及 Proposition 6.2.8 我們知道 modulo p^2 的 primitive root 存在, 所以再由 Proposition 6.2.10 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.

6.2.4. 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 6.2.11. 給定一奇數 m, 且 $a\in\mathbb{Z}$ 是一個和 m 互質的奇數. 若 $\mathrm{ord}_m(a)=n$, 則 $\mathrm{ord}_{2m}(a)=n$.

Proof. 由於 a 是奇數且與 m 互質, 故知 $\gcd(a,2m)=1$. 因此 a 在 modulo $2m$ 之下的 order 是有定義的, 就假設 $\mathrm{ord}_{2m}(a)=k$. 由 $a^k\equiv 1 \pmod{2m}$ 可得 $a^k\equiv 1 \pmod{m}$. 故由 $\mathrm{ord}_m(a)=n$ 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 $\gcd(2,m)=1$, 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 $\mathrm{ord}_{2m}(a)=k$, 故再利用 Proposition 6.1.4 得 $k|n$. 因此得證 $k=n$ 也就是說 $\mathrm{ord}_{2m}(a)=n$. □

假設 a 為 modulo p^n 的 primitive root, 即 $\mathrm{ord}_{p^n}(a)=\phi(p^n)$. 若 a 又是奇數則由 Lemma 6.2.11 知 $\mathrm{ord}_{2p^n}(a)=\phi(p^n)$. 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 $\mathrm{ord}_{2p^n}(a)=\phi(2p^n)$. 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 6.2.12. *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 $\mathrm{ord}_3(5)=\mathrm{ord}_3(2)=2$ 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 6.2.7 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 6.2.5 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 6.2.8 知 $\{\alpha,\alpha+p,\ldots,\alpha+(p-1)p\}$ 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 α, $\alpha+2p$ 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 6.2.10 知 a 在 modulo p^n 之下亦為 primitive root. 故由 Lemma 6.2.11 知 $\mathrm{ord}_{2p^n}(a)=\mathrm{ord}_{p^n}(a)=\phi(p^n)=\phi(2p^n)$, 故得證 a 在 modulo $2p^n$ 之下亦為 primitive root. □

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 6.2.12 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.

我們總結這節之結果得到以下所謂的 primitive root Theorem.

Theorem 6.2.13 (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.*

Exercise 6.1. 請回答以下問題並直接以計算方式驗證：

(1) 利用 $\mathrm{ord}_{15}(2)=4$ 試求 $\mathrm{ord}_{15}(8)$

(2) 3 是 modulo 17 的 primitive root，試求 $\mathrm{ord}_{17}(9)$.

(3) 利用 $\mathrm{ord}_7(2)=3$ 以及 2 是 modulo 13 的 primitive root，求 $\mathrm{ord}_{91}(2)$.

(4) 說明在 modulo 11 之下為何可由 $8^5\equiv -1 \pmod{11}$ 而說 8 是 primitive root.

(5) 說明在 modulo 13 之下為何不能由 $8^6\equiv -1 \pmod{13}$ 而說 8 是 primitive root.

Exercise 6.2. 已知 $\mathrm{ord}_{101}(14)=10$, 試找出在 modulo 101 之下所有 order 為 10 的元素並說明理由.

Exercise 6.3. 對於 $d\in\mathbb{N}$，考慮集合 $S_d=\{a\in\mathbb{N}:\mathrm{ord}_{13}(a)=d\}$

(1) 試列出所有可能的 $d\in\mathbb{N}$，使得 S_d 不是空集合。

(2) 對 (1) 中所找出的每個 d，找出 S_d 中最小的正整數 a，並以 a^i 的形式列出所有 S_d 的元素。

Exercise 6.4. 考慮 $a\in\mathbb{N}$ 且 $5\nmid a$。以下是探討在 modulo 5 和 modulo 25 之下 a 的 order 之關係。

(1) 試利用 order 的性質說明若 $a\not\equiv\pm1 \pmod 5$，則 a 為 modulo 5 之下的 primitive root.

(2) 假設 $a\equiv\delta \pmod 5$ 且 $a\not\equiv\delta \pmod{25}$ 試分別依 $\delta=1,-1$ 且利用 order 的性質說明 $\mathrm{ord}_{25}(a)$ 為何。

(3) 試找出在 modulo 25 之下不是 primitive root 但在 modulo 5 之下為 primitive root 的所有元素。

(4) 試說明“若 $d\mid\phi(25)$，則在 modulo 25 之下 order 為 d 的元素共有 $\phi(d)$ 個”是否正確？

Exercise 6.5. 利用 2 為 modulo 13 的 primitive root。找到最小的正整數 α 滿足 $\alpha\equiv2 \pmod{13}$ 且對任意 $m\in\mathbb{N}$ 在 modulo 2×13^m 為 primitive root.

Exercise 6.6. 假設 $m\in\mathbb{N}$ 且 $\gcd(a,m)=\gcd(b,m)=1$.

(1) 證明若 $\gcd(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1$ 則 $\mathrm{ord}_m(ab)=\mathrm{ord}_m(a)\cdot\mathrm{ord}_m(b)$.

(2) 試證明若 $\mathrm{ord}_m(a)=m-1$, 則 m 必為質數.

Exercise 6.7. 假設 $a,n\in\mathbb{N}$ 且 $a>1$. 試證明 $\mathrm{ord}_{a^n-1}(a)=n$, 並依此得證 $n\mid\phi(a^n-1)$.

Exercise 6.8. 令 p 為一奇質數且 a 為 modulo p 之下的一個 primitive root.

(1) 若 $b\in\mathbb{Z}$ 滿足 $ab\equiv1 \pmod p$, 試證明 b 是 modulo p 之下的一個 primitive root. 依此證明當 $p>3$ 時所有在 modulo p 之下的 primitive root 之乘積在 modulo p 之下為 congruent to 1.

(2) 試證明 Legendre symbol $\left(\dfrac{a}{p}\right)=-1$.

(3) 試證明

$$\mathrm{ord}_p(-a)=\begin{cases} p-1, & 若\ p\equiv1 \pmod 4;\\ (p-1)/2, & 若\ p\equiv3 \pmod 4.\end{cases}$$