# Multiplicative Inverse
# (模數乘法反元素)

**sjLin**

February 28, 2022

假設$a \in \mathbb{Z},\ n \in \mathbb{Z}^+$，$ax \equiv 1 \pmod n$，則稱$x$爲$a$在 $\bmod n$下的multiplicative inverse，而這個$x$有無限個，符合最小正整數$x$，稱爲$a$在 $\bmod n$下的最小乘法反元素(least multiplicative inverse)，這最小乘法反元素記作$a^{-1} \pmod n$。

## 定理

假設$a \in \mathbb{Z},\ n \in \mathbb{Z}^+$，若$\gcd(a, n) = 1$, 則$a$在 $\bmod n$的乘法反元素存在。

## 證明

因爲$\gcd(a, n) = 1$，所以$a, n$互質，使得$\exists s, t \in \mathbb{Z}$，則$as + nt = 1 \Rightarrow as + nt \equiv 1 \pmod n$。因爲$nt \equiv 0 \pmod n$，所以$as \equiv 1 \pmod n$。
因此$s$爲$a$在 $\pmod n$下的乘法反元素。

## 例題-92 台大資工

Find the inverse of $4$ modulo 7.

### Ans.

$\exists s, t \in Z$，使得$4s + 7t = 1$。
由Eulidean Algorithm得知，
$7 = 1 \cdot 4 + 3$
$4 = 1 \cdot 3 + 1$
$\Rightarrow 1 = 4 - 1 \cdot 3$
$1 = 4 - 1(7 - 1 \cdot 4)$
整理
$1 = (-1) \cdot 7 + 2 \cdot 4$
$\Rightarrow 1 = (-1 - 4k) \cdot 7 + (2 + 7k) \cdot 4,\ \forall k \in \mathbb{Z}$
因此，$2 + 7k, \forall k \in \mathbb{Z}$爲4在 $\pmod 7$下的乘法反元素。

## 例題-98政大資料

Find the least positive integer $x$ satisfying he congruence:

$$531x \equiv 1 \pmod{1769}$$

### Ans.

由Eulidean Algorithm得知，
$1769 = 3 \cdot 531 + 176$
$531 = 3 \cdot 176 + 3$
$176 = 58 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$\Rightarrow 1 = 3 - 2$
$= 3 - (176 - 58 \cdot 3)$
$= 3 - 176 + 58 \cdot 3$
$= (-1) \cdot 176 + 59 \cdot 3$
$= (-1) \cdot 176 + 59 \cdot 531 - 177 \cdot 176$
$= (-178) \cdot 176 + 59 \cdot 53$
$= (-178) \cdot (1769 - 3 \cdot 531) + 59 \cdot 531$
$= (-178) \cdot 1769 + 593 \cdot 531$
$\therefore 531^{-1}$在 $\pmod{1769}$下的最小乘法反元素爲593。

---

### 推廣

乘法反元素可以推廣到解一般的方程式$ax \equiv b \pmod{n}$

## 例題-98清大資工

Solve the linear congruence $7x \equiv 13 \pmod{19}$ to find all the integer solutions $x$.

### Ans.

因爲$\gcd(7,19) = 1$，所以有整數解$(s,t)$，使得$7s + 19t = 1$，由Eulidean Algorithm得知，
$19 = 2 \cdot 7 + 5$
$7 = 1 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$
$\Rightarrow 1 = 5 - 2 \cdot 2$
$= 5 - 2(7 - 5)$
$= 3 \cdot 5 + (-2) \cdot 7$
$= 3(19 - 2 \cdot 7) + (-2) \cdot 7$
$= 3 \cdot 19 + (-8) \cdot 7$
左右同乘13，即計算$7x \equiv 13 \pmod{19}$
$\Rightarrow 13 = 39 \cdot 19 + (-104) \cdot 7$
通式$13 = (39 - 7k) \cdot 19 + (-104 + 19k) \cdot 7,\ \forall k \in \mathbb{Z}$
$\Rightarrow -104 \equiv 10 \pmod{19}$
$\therefore 10 + 19k,\ \forall k \in \mathbb{Z}$爲$x$的所有可能解。

## 引理

假設$a \in \mathbb{Z}$且$p$爲一質數，則$a$爲$a$在 $\pmod p$下的乘法反元素$\leftrightarrow a \equiv \pm 1 \pmod p$

### 證明

$(\rightarrow)$
因爲$a$爲$a$在 $\pmod p$下的乘法反元素，
$\Rightarrow a^2 \equiv 1 \pmod p$
$p|(a^2-1)$
$p|(a-1)(a+1)$
所以$p|(a-1)$或$p|(a+1)$
因爲同餘的兩數相減的值，會被 $\bmod$ 的值整除
所以$a \equiv -1 \pmod p$或$a \equiv 1 \pmod p$
$(\leftarrow)$
因爲$a \equiv \pm 1 \pmod p$，所以$a^2 \equiv 1 \pmod p$
因此，$a$爲$a$在 $\pmod p$下的乘法反元素。