2016/4/14 8.2

إن $(Z/mZ)^*$ هو مجموعة عناصر قابلة للقلب أي:

$[a] \in (Z/mZ)^* \Leftarrow gcd(a, m) = 1$

إيجاد مقلوب العنصر $[a]$ في $(Z/mZ)^*$:

$gcd(m, a) = 1$

$1 = xm + ya$

عندها $[a]^{-1} = [y]$

مثال: في $(Z/1307Z)$ أوجد مقلوب $[99]$.

نتأكد أولاً من أن $gcd(99, 1307) = 1$ ✓

$1037 = 13 \cdot 99 + 20$

$99 = 4 \cdot 20 + 19$

$20 = 1 \cdot 19 + 1$

ومنه $1 = gcd(99, 1307)$

ومن ثم نكتب عكس خوارزمية أي:

$1 = 20 - 19$

$1 = 20 - (99 - 4 \cdot 20)$

$1 = -99 + 5(20)$

$1 = -99 + 5(1307 - 13(99))$

$1 = 5(1307) - \underbrace{66}_{y}(99)$

$[99]^{-1} = [y] = [-66]$

نكتبه بالموجب لذلك نضيف $m = 1307$

$$[99]^{-1} = [1241]$$

حل المعادلات في $\mathbb{Z}/m\mathbb{Z}$:

المعادلة الخطية من الشكل $ax \equiv b \pmod{m}$

هناك حالتين: 1) $\gcd(a,m)=1$ $\Leftarrow$ هناك حل وحيد

2) $\gcd(a,m) = d \neq 1$ $\Leftarrow$ أ) d لا يقسم b عندها المعادلة ليس لها حل.

ب) d يقسم b عندها يوجد d حل.

الحالة الأولى: إذا كان a, m عددان أوليان فيما بينهما في هذه الحالة نوجد مقلوب a أي $[a]^{-1}$ ومن ثم

$$x = [a]^{-1}[b]$$ هذا هو الحل.

مثال: $\underset{a}{7}x = 5 \pmod{\underset{m}{11}}$

$$\gcd(7,11) = 1 \Rightarrow [7]^{-1} = ?$$

$$\left.\begin{aligned} 11 &= 1.7 + 4 \\ 7 &= 1.4 + 3 \\ 4 &= 1.3 + 1 \end{aligned}\right\} \Rightarrow 1 = 4 - 3$$

$$1 = 4 - (7-4)$$

$$1 = \underset{}{4} - (7 - (11-7))$$

$$1 = \underset{y}{-3}\underset{a}{7} + \underset{x}{2}.\underset{m}{11}$$

$$[7]^{-1} = [-3] \xrightarrow{11+} = [8]$$

$$\Rightarrow x = [7]^{-1}[5] = [8][5] = [40] = [7]$$

$$11 \overline{)340} \quad 30 \quad 3$$
$$33$$
$$\boxed{7}$$

باقي قسمة 40 على 11.

الحالة الثانية: $\gcd(a,m) = d$ و $d \neq 1$ و d لا يقسم b فإن المعادلة مستحيلة.

الحالة الثالثة: $d = \gcd(a,m) \neq 1$ و d يقسم b $\quad ax \equiv b \pmod m$ ---**

$$a'x \equiv b' \pmod{m'} \quad \text{---} *$$

حيث $m' = \frac{m}{d}$ ، $b' = \frac{b}{d}$ ، $a' = \frac{a}{d}$

$$\Rightarrow \gcd(m', a') = 1$$

عدنا للحالة الأولى.

** لتكن x_0 حل المعادلة $(*)$ فيكون الحل للمعادلة هو:

$$x = x_0 + n m'$$

حيث $n = 0, 1, \dots, d-1$

مثال: أوجد حل المعادلة:

$$21x \equiv 15 \pmod{33}$$

لدينا $\gcd(21, 33) = 3 \neq 1$

و 3 تقسم $b = 15$ وبالتالي للحل

$$\Rightarrow 7x_0 \equiv 5 \pmod{11}$$

$$\Rightarrow x_0 = [7] \in \mathbb{Z}/11\mathbb{Z}$$ ← حل حسب السابق

ولكن حلول صنف $\mathbb{Z}/33\mathbb{Z}$

$$x = x_0 + n m' \quad ; \quad n = 0, 1, 2$$

$$x_1 = [7] \quad , \quad x_2 = [18]$$

$$x_3 = [29]$$

وهي كلها تنتمي لـ $\mathbb{Z}/33\mathbb{Z}$