

إن $(\mathbb{Z}/m\mathbb{Z})^*$ قوي عناصر قابلة للقلب أي

$$[a] \in (\mathbb{Z}/m\mathbb{Z})^* \Leftrightarrow \gcd(a, m) = 1$$

إيجاد مقلوب العنصر $[a]$ في $(\mathbb{Z}/m\mathbb{Z})^*$:

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

$$1 = xm + ya$$

$$[a]^{-1} = [y]$$

عندها

مثال: في $(\mathbb{Z}/1307\mathbb{Z})$ زوجد مقلوب $[99]$.

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

$$1307 = 13 \cdot 99 + 20$$

$$99 = 4 \cdot 20 + 19$$

$$20 = 1 \cdot 19 + 1$$

$$1 = \gcd(99, 1307)$$

ومن ثم نكتبه عكس (مقلوب) أي:

$$1 = 20 - 19$$

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

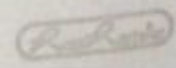
$$1 = -99 + 5(20)$$

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

$$1 = 5(1307) - 66(99)$$

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

نكتبه بالموجب لذلك نضيف $1307 = m$



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

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

$$ax \equiv b \pmod{m}$$

المعادلة الخطية من الشكل

يوجد حلين: (1) $\text{gcd}(a, m) = 1 \iff$ هناك حل واحد

(2) $\text{gcd}(a, m) = d \neq 1 \iff$ لا يتيم b عندها المعادلة متى

الحل.

(ب) d يتيم b عندها يوجد d

طالة (الأولى). إذا كان a, m عدداً أولياً فيما بينهما

ففي هذه الحالة توجد فلولب a أي $[a]^{-1}$ ومن ثم

$$x = [a]^{-1} [b]$$

$$\text{مثال: } 7x \equiv 5 \pmod{11}$$

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

$$11 = 1 \cdot 7 + 4$$

$$7 = 1 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1$$

$$\left. \begin{array}{l} 11 = 1 \cdot 7 + 4 \\ 7 = 1 \cdot 4 + 3 \\ 4 = 1 \cdot 3 + 1 \end{array} \right\} \implies 1 = 4 - 3$$

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

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

$$1 = \overset{11}{4} - 3 \cdot \overset{7}{7} + 2 \cdot \overset{11}{11}$$

$$[7]^{-1} = [-3] = [8]$$

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

$$\begin{array}{r} 11 \overline{) 346^{10}} \\ \underline{33} \\ 16 \end{array}$$

$$\boxed{7} \text{ باقي قسمة } 40 \text{ على } 11$$

Redmond

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

المعادلة مستحيلة.

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

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

$$a' = \frac{a}{d}, \quad b' = \frac{b}{d}, \quad m' = \frac{m}{d} \quad \text{حيث}$$
$$\Rightarrow \gcd(m', a') = 1$$

عادة للحالة الأولى.

ليكن x_0 حل المعادلة (*) فيكون الحل للمعادلة **

$$x = x_0 + nm'$$

$$\text{حيث } n = 0, 1, \dots$$

مثال: أوجد حل المعادلة:

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

$$\text{لدينا } \gcd(21, 33) = 3 \neq 1$$

و 3 تقسم $b = 15$ وبالتالي لياصل

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

$$\Rightarrow \text{حلها سابق} \quad x_0 = [7] \in \mathbb{Z}/11\mathbb{Z}$$

ولكن حلها ضمن $\mathbb{Z}/33\mathbb{Z}$

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

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

$$[x_3] = [29]$$

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