

9.3

2016/4/21

المعادلة الخطية:

برهان: ليكن m, n عددين طبيعيين أوليان فيما بينهما

$$x \equiv a \pmod{m} \quad \text{و } a, b \in \mathbb{Z} \text{ فإن:}$$

$$x \equiv b \pmod{n}$$

لها صنف حل وحيد في $\mathbb{Z}/(mn) \mathbb{Z}$ ^[ب]

طريقة إيجاراكل:

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

حسب على صيغة زقليدس نكتب 1 كتركيب خطي لعددين

العددين n و m أي:

$$1 = yn + zm$$

عندها لكل له الشكل التالي:

$$x = ay_n + bz_m$$

بإضافة n

$$x \equiv b \pmod{n}$$

بإضافة m

$$y \equiv a \pmod{m}$$

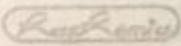
$$x \equiv 3 \pmod{5} \quad \text{مثال: أوجد حل}$$

$$x \equiv 8 \pmod{11}$$

$$\gcd(5, 11) = 1$$

$$\Rightarrow 1 = 1 \cdot 11 + (-2) \cdot 5$$

$$\Rightarrow x = 3 \cdot 1 \cdot 11 + 8 \cdot (-2) \cdot 5 = -47$$



$$m \cdot n = 55 \text{ تعريف}$$

$$[x] = [-47] = [8] \in \mathbb{Z} / 55 \mathbb{Z}$$

ملاحظة: لكن m_1, m_2, \dots, m_r أعداد أولية فيما بينها فنحن

$$x \equiv a_1 \pmod{m_1} \quad \text{فنحن عندها}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_r \pmod{m_r}$$

فنحن نريد حل وحيد في $\mathbb{Z} / (m_1 \cdot m_2 \cdot \dots \cdot m_r) \mathbb{Z}$

نأخذ كل معادلتين مع بعضنا وظلنا m ثابت ثم نأخذ حل

مع معادلة التالية وهكذا

أوجد حل معادلة حث للثنائي:

تمرين

$$\left. \begin{array}{l} \text{خلوهم لشكر} \\ x \equiv a_1 \pmod{m} \\ x \equiv a_2 \pmod{n} \end{array} \right\} \begin{array}{l} 2x \equiv 4 \pmod{11} \rightarrow [2] \\ 2x \equiv 4 \pmod{6} \end{array}$$

أوجد حل جملة معادلات:

$$x \equiv -1 \pmod{6}$$

$$2x \equiv 4 \pmod{11}$$

$$3x \equiv 1 \pmod{17}$$

الاعداد غير ضمنية:

$$f(x, y, z) \equiv 0 \pmod{m}$$

تعريف: سنستخدم الرمز $N \text{ sol}_p(m)$ عدد حلول f في $\mathbb{Z} / m \mathbb{Z}$

عدد الحلول

نقطة: إذا كان m و n أوليان فيما بينهما فإن:

$$NSOL_p(mn) = NSOL_p(m) \cdot NSOL_p(n) \quad \text{--- (1)}$$

عدد حلول

نتيجة: بتقليل m لمعامله الأولية

$$m = \prod_k p_k^{\alpha_k}$$

صيت p أعداد أولية و α_k أعداد طبيعية.

$$NSOL_p = \prod_k NSOL_p(p_k^{\alpha_k})$$

فذلك

ماهي حلول المعادلة:

$$* \quad x^2 - 1 \equiv 0 \pmod{15}$$

$$m = 15 = 5 \times 3$$

$$x^2 - 1 \equiv 0 \pmod{5}$$

الحلان و

$$x^2 - 1 \equiv 0 \pmod{3}$$

الحل

وبالتالي * حلين حسب تطبيق علاقة (1) وهما: $x \in \{4, 11\}$

طد المعادلة $x^2 + 1 \equiv 0 \pmod{6}$ هنا جرب الأعداد (1, 2, 3, 4, 5)

لم نجد هناك الأعداد التي تحقق أن باقي قسمة $(x^2 + 1)$ على 6

يكون صفر وعليه فإننا نلاحظ أننا بيننا المعادلة $x^2 + 1 \equiv 0 \pmod{6}$

الحلان هما $[1]$ و $[5]$. فمثلاً $x^2 + 1 \equiv 0 \pmod{5}$ هنا

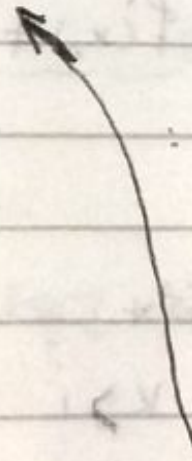
جرب (1, 2, 3, 4, 5) بل إننا نلاحظ أن أوليه فيما بينها أي 5×3

مكتوب

صارت 1 لتكن $G = \{1, a, b, c\}$ زمرة تبديلية حيث a هو صيدوي هذه الزمرة واضح جميع جداول كيبلي الممكنة.
 « ملاحظة: في جدول كيبلي كل عنصر يظهر مرة واحدة في كل عمود وفي كل سطر »

2- بين: $A_4 = \langle (1\ 2\ 3), (1\ 2\ 4) \rangle$

عندها نرى حجم حل للمعادلة عند $n = 3$ وحجم حلها عند $m = 5$ ويكون عدد الجداول هو عدد الحلول للمعادلة الأصلية.
 بينما لو $x^2 - 1 \equiv 0 \pmod{25}$ هنا أيضا لا تجيب عن $(24, 25)$ وإذا حللنا ذلك $25 = 5 \times 5$ لكن 5 و 5 ليس أوليا فيما بينهما فلا تختلف البرهنة لكن هنا نضطرهنة لاحقا تكون في حالة العدد حقيقيا أوليا.



١٥.٢

2016/4/27

المعادلات غير الخطية:

$$N_{Sol}_p(m, n) = N_{Sol}_p(m) \cdot N_{Sol}_p(n)$$

مثال:

$$f(x) = x^2 - 1 \equiv 0 \pmod{15}$$

$$\text{حين } f(x) \equiv 0 \pmod{3}$$

$$\text{حين } f(x) \equiv 0 \pmod{5}$$

$$\Rightarrow f(x) \equiv 0 \pmod{15}$$

لا أربع حلول.

مبرهنة هيرز:

ليكن p عدد أولي و $k \geq 1$ حيث $f(x)$ كثير حدود أضالته في \mathbb{Z} ليكن x_0 حل لـ $f(x) \equiv 0 \pmod{p^k}$ حيث $f'(x_0) \not\equiv 0 \pmod{p}$

فإن هناك حل وحيد t حيث $x_0 + t p^k$ حل لـ

$$\textcircled{2} \quad f(x) \equiv 0 \pmod{p^{2k}}$$

نتيجة 1: إذا وجد حل x_0 لـ $f(x) \equiv 0 \pmod{p}$ حيث $f'(x_0) \not\equiv 0 \pmod{p}$

فإن للمعادلة $f(x) \equiv 0 \pmod{p^k}$ حل واحد لكل $k \geq 1$

2. لا يوجد حل للمعادلة $\textcircled{2}$ بفرض x_0 حل لـ $\textcircled{1}$ حيث k حقيقة

نبحث عن t حيث

$$f(x_0 + p^k t) \equiv 0 \pmod{p^{2k}}$$

$$\Rightarrow x = x_0 + p^{kt}$$

حل لـ $\textcircled{2}$

$$\begin{array}{r} 1 \\ 9 \overline{) 12} \\ \underline{9} \\ 3 \end{array}$$

$$p^k = 3 \Rightarrow p=3 \text{ و } k=1$$

$$f(x) \equiv 0 \pmod{3} \quad \text{مثال:}$$

$$f(x) = x^2 - 1 \quad \text{حيث}$$

$$x_0 = 1 \quad \text{و حلها}$$

$$f(x) = x^2 - 1 \equiv 0 \pmod{3^2}$$

الآن: نطبق الطريقة:

$$f'(x) = (2x) \Rightarrow f'(1) = 2 \not\equiv 0 \pmod{3}$$

وهنا \otimes مكملة

$$x = x_0 + t p^k = 1 + 3t \quad (2)$$

$$f(1+3t) \equiv 0 \pmod{3^{2(1)}} \quad (2)$$

$$(1+3t)^2 - 1 \equiv 0 \pmod{9}$$

$$9t^2 + 6t + 4 - 1 \equiv 0 \pmod{9}$$

$$6t \equiv 0 \pmod{9}$$

$$4t + 1 \equiv 0 \pmod{3} \quad 2t \equiv 0 \pmod{3}$$

$$\Rightarrow t = 2 \quad \Rightarrow t = 3$$

$$\Downarrow x = 1 + 3(3) = 1 + 9 = 10 \in \mathbb{Z}/9\mathbb{Z}$$

$$x = 2 + 3(2) = 8 \in \mathbb{Z}/9\mathbb{Z} \quad \text{وهنا } x = 1$$

$$x_0 = 2 \quad \text{مثال آخر ولكن}$$

ملاحظة: في حال لم يتحقق الشرط \ast عندها ستكون p^k أكثر تقيداً $3^2 = 9 = 3^k$

سؤال: $f(x) = x^2 + x + 7 \equiv 0 \pmod{9}$

يا حل $x_0 = 1$

$f'(x) = 2x + 1 \Rightarrow f'(1) = 3 \equiv 0 \pmod{3}$

الشرط \ast غير محقق $f(x)$ ليس له حلول في $(\text{mod } 3^k)$ $k \geq 3$

سؤال: $f(x) = x^3 - 3x + 2 \equiv 0 \pmod{3}$ لا حل $x=1$

\ast أيضاً لا يتحقق

إلا أن $f(x)$ له حلول في $(\text{mod } 3^k)$ حيث $k > 1$

أي في مثال $f(x)$ غير محقق في مرحلة هزل عندها معادلة $f(x) \equiv 0 \pmod{3}$ ولكن أمارا له حلول أو ليس له حلول

طريقة ثانية لإيجاد حل في حال \ast محققة:

$x = x_0 + p^k t$

ليكن $a_1 = f'(x_0)$ و $b = \frac{f(x_0)}{p^k}$

~~حيث a_1 و b هما قيمتان ثابتتان~~

هذا التلويح

$b + a_1 t \equiv 0 \pmod{p^k}$

$x = x_0 + t p^k$ تم نوض في

في المسألة السابقة في حال $x_0 = 2$

$$a_1 = f'(x_0) = 4$$

$$b = \frac{f(x_0)}{f'(x_0)} = 1$$

$$\Rightarrow 1 + 4t \equiv 0 \pmod{3}$$

$$\Rightarrow t = 2$$

$$\Rightarrow x = x_0 + p^k t = 2 + 3(2) = [8] \in \mathbb{Z}/9\mathbb{Z}$$

مثال: ليكن $x^2 + 1 \equiv 0 \pmod{25}$

حل $x_0 = 7$ يوجد حل

$$(x^2 + 1) \equiv 0 \pmod{5^4}$$

م 11

2016/2/28

(1) ليكن $x=2$ حل $x^6 - 1 \equiv 0 \pmod{7}$

زوجد حل $x^6 - 1 \equiv 0 \pmod{7}$

(2) زوجد حل $f(x) = x^2 + 4x + 2 \equiv 0 \pmod{98}$

تجميع : (1) حل للمعد 98 ، العوامل الأولية من 98

(2) حل المعادلة لكن بحاصل أي :

(1) $f(x) \equiv 0 \pmod{2}$

$f(x) \equiv 0 \pmod{7}$ و $f(x) \equiv 0 \pmod{7^2}$ و $f(x) \equiv 0 \pmod{98}$

حل معادلتين خطيتين

(1) حل خطيين : $x \equiv -1 \pmod{6}$

$2x \equiv 4 \pmod{11} \Rightarrow 2x - 4 \equiv 0 \pmod{11}$

$3x \equiv 1 \pmod{17}$

$3x - 1 \equiv 0 \pmod{17}$

$x = 6$

(2) $x \equiv 2 \pmod{11}$ وبالتالي نضع معادلة

نضع معادلة بارنكل

(3) $x \equiv 6 \pmod{17}$

$\gcd(11, 6) = 1$ حل (1) و (2)

$1 = -1 \cdot 11 + 2 \cdot 6$

$$x = (-1)(-11 \cdot 11 + 2 \cdot 2)(6) = 35 \in \mathbb{Z}/66\mathbb{Z}$$

كل $x \equiv 35 \pmod{66}$ مع (3)

$$\gcd(66, 17) = 1$$

$$1 = 8 \cdot 66 + (-31) \cdot 17$$

$$x = (6)(8)(66) + 35 \cdot (-31)(17)$$

$$x = -15277 \in \mathbb{Z}/(11 \cdot 17)\mathbb{Z}$$

$$\Rightarrow x = -13 \times 1122 - 691$$

$$x = -691 = 431 \in \mathbb{Z}/1122\mathbb{Z}$$

هذا عدد أكبر من 1122 وبالتالي
 يجب أن نضيفه
 بل نكتبه على شكل ناتج قسمة
 صافي

$$G = \{1, a, b, c\}$$

جدول ضرب

لا يمكن تكرار عنصر ضمن شروط تبديلية أي جدول كيلي عتنا طر بالنسبة للوكر رئيسي

عالمود

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

	1	a	b	c
1	1	a	b	c
a	a	c	1	b
b	b	1	c	a
c	c	b	a	1

Handwritten signature or mark.

التتابع اربيية .

التتابع اربيية هو تابع منطلقه N ومستقره ϕ

$$f: N \rightarrow \phi$$

تعريف 1: يكون التتابع اربيية جديده (ضربه)

$$f(m \cdot n) = f(m) \cdot f(n)$$

حيث n و m اعداد اركبية فيما بينهما.

ويكون ضربه تام اذا كان

$$f(m \cdot n) = f(m) \cdot f(n) \quad \forall m, n$$

تابع اوليه يرزله ب ϕ .

ليكن $n \in N$ فان $\phi(n)$ يعرف بانه عدد الاعداد التي لا

مقلوب في Z/nZ

$$\phi(n) = | (Z/nZ)^* |$$

$$= | \{ a : 1 \leq a < n \text{ and } \gcd(a, n) = 1 \} |$$

n	1	2	3	4	5	6
$\phi(n)$	1	1	2	2	4	2

مبرهنة:

ان تابع اوليه هو ضرب وليكن ضربه غير تام

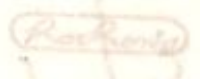
$$\phi(6) = \phi(2 \times 3) = \phi(2) \cdot \phi(3)$$

$$2 = 1 \cdot 2$$

ولكن ليس تام لان:

$$\phi(4) \neq \phi(2) \cdot \phi(2)$$

$$2 \neq 1 \cdot 1$$



$$n = \prod_k p_k^{a_k} \quad \text{ليكن } n \in \mathbb{N}^* \quad \text{نتيجه}$$

$$\varphi(n) = \prod_k \varphi(p_k^{a_k})$$

$$n = 50 = 5^2 \times 2$$

$$\varphi(50) = \varphi(5^2) \cdot \varphi(2)$$

ضرب في 2 لأن 2 ليس ضرب في 5 لأن $\varphi(5^2)$ ليس له تأثير على 2.