المعادلات الخطية:

مبرهنة: ليكن m, n عددان طبيعيان أوليان فيما بينهما، و $a, b \in \mathbb{Z}$، فإن:

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

لهما صف حل وحيد في $\mathbb{Z}/(mn)\mathbb{Z}$ [x]

طريقة إيجاد الحل:

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

حسب عكس مبرهنة أقليدس نكتب 1 كتركيب خطي بدلالة العددين n, m أي:

$$1 = yn + \beta m$$

عندها الحل له الشكل التالي:

$$x = ayn + b\beta m$$

بحيث:

$x \equiv b \pmod{n}$ باقي قسمة على n

$y \equiv a \pmod{m}$ باقي قسمة على m

مثال: أوجد حل

$$x \equiv 3 \pmod{5}$$
$$x \equiv 8 \pmod{11}$$

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

$$\Rightarrow 1 = \underbrace{1}_{y} \cdot 11 + \underbrace{(-2)}_{\beta} \cdot 5$$

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

حيث $m \cdot n = 55$

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

مبرهنة: لتكن $m_1, m_2, \dots, m_r$ أعداد أولية فيما بينها مثنى مثنى عندها

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

فهناك صف حل وحيد في $\mathbb{Z}/(m_1 \cdot m_2 \cdots m_r)\mathbb{Z}$

نأخذ كل معادلتين مع بعضهم ونحلهما كما سبق ثم نأخذ الحل مع المعادلة التالية وهكذا...

تمرين: أوجد حل المعادلة من الشكل:

$$\begin{cases} 2x \equiv 4 \pmod{11} \\ 2x \equiv 4 \pmod{6} \end{cases} \quad \dots [2]$$

فالحل لهكذا شكل $x \equiv a_1 \pmod{m}$, $x \equiv a_2 \pmod{n}$

أوجد حل جملة معادلات:

$$\begin{aligned} x &\equiv -1 \pmod 6 \\ 2x &\equiv 4 \pmod{11} \\ 3x &\equiv 1 \pmod{17} \end{aligned}$$

المعادلات غير خطية:

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

تعريف: سنستخدم الرمز $N\underbrace{Sol}_{\text{عدد الحلول}}(m)$ عدد حلول f في $\mathbb{Z}/m\mathbb{Z}$

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

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

عدد حلول.

نتيجة: بتحليل m لعوامله أولية

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

حيث p_k أعداد أولية و α_k أعداد طبيعية.

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

مثال:

ما هي حلول المعادلة:

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

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

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

لها حلان و

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

لها حل

$x = [1]$

وبالتالي لـ * حلين حسب تطبيق علاقة (1) وهي: $x = [4]$

حل المعادلة $x^2+1 \equiv 0 \pmod 5$ هنا نجرب الأعداد (0,1,2,3,4)

كل واحد من هذه الأعداد يحقق أن باقي قسمة (x^2+1) على 5

يساوي صفر وعليه فإنه ليس لها حل بينما المعادلة $x^2-1 \equiv 0 \pmod 5$

لها حلان هما [1] و [4]. مثلاً $x^2-1 \equiv 0 \pmod{15}$ هنا

لا نجرب (0, ..., 14) بل نحلل إلى عوامل أولية فيما بينها أي $15 = \underset{m}{5} \times \underset{n}{3}$

تمارين 1. لتكن $G = \{1, a, b, c\}$ زمرة تبديلية حيث 1 هو حيادي هذه الزمرة ما هي جميع جداول كيلي الممكنة.

«ملاحظة في جدول كيلي 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 كم حل للمعادلة عند $n = 3$ وكم حل لها عند $m = 5$ ويكون جداء عدد الحلول هو عدد الحلول للمعادلة الأصلية.

بينما لو $x^2 - 1 \equiv 0 \pmod{25}$ هنا نأخذ 6 تجرب من $(0, \_\_\_, 24)$

وإذا حللنا نحصل $25 = 5 \times 5$. لكن 5 و 5 ليس أوليان فيما بينهما فلا تتحقق المبرهنة لكن سنأخذ مبرهنة لاحقا تكون في حال الـ m قوى لعدد أولي.

المعادلات غير الخطية:

$$Nsol_f(m.n) = Nsol_f(m) \cdot Nsol_f(n)$$

مثال:

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

حلين $f(x) \equiv 0 \pmod 3$

حلين $f(x) \equiv 0 \pmod 5$

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

له أربع حلول.

مبرهنة هنزل:

ليكن لدينا عدد نطيه، $k \geq 1$ حيث $f(x)$ كثير حدود أمثالية Z ليكن x_0 حل لـ $f(x) \overset{①}{\equiv} 0 \pmod{p^k}$ حيث $f'(x_0) \not\equiv 0 \pmod p$

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

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

نتيجة: إذا وجد حل x_0 لـ $f(x) \equiv 0 \pmod p$ حيث $k \geq 1$ فإن للمعادلة $f(x) \equiv 0 \pmod{p^k}$ حل من أجل كل $k \geq 1$

٢. لإيجاد حل المعادلة ② نفرض x_0 حل لـ ① حيث k معلومة

نبحث عن t حيث

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

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

حل لـ ②

$p^k = 3 \Rightarrow p = 3 \; , \; k = 1$

مثال:

$f(x) \equiv 0 \pmod 3$

حيث $f(x) = x^2 - 1$

وحلها $x_0 = 1$

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

الحل: نطبق المرحلة:

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

وهنه (*) محققة.

$x = x_0 + t p^k = 1 + 3t$

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

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

$9t^2 + 12t + 4$

$9t^2 + 6t \equiv 0 \pmod 9$ خاتم $\mathbb{Z}/9\mathbb{Z}$

$6t \equiv 0 \pmod 9$ وبالتالي هي 0

$4t + 1 \equiv 0 \pmod 3$

$2t \equiv 0 \pmod 3$

$\Rightarrow t = 2$

$\Rightarrow t = 3$

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

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

هناك أخر ولكن $x_0 = 2$

ملاحظة: في حال لم يتحقق الشرط ⊛ عندها سيكون حلها أكثر تعقيداً $p^k = 9 = 3^2$

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

الحل

$x_0 = 1$

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

الشرط * غير محقق لكن $f(x)$ ليس لها حلول في $\pmod{3^k}$ حيث $k \geq 3$.

مثال: $f(x) = x^3 - 3x + 2 \equiv 0 \pmod 3$ لها حل $x = 1$

⊛ أيضاً لا يتحقق.

إلا أن $f(x)$ لها حلول في $\pmod{3^k}$ حيث $k > 1$

في هذه الحالة ⊛ غير محقق في هذه الحالة هنا عندها معادلة [illegible] أو ليس لها حلول

طريقة ثانية لإيجاد حل 2 في حال * محققة:

$$x = x_0 + p^k t$$

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

[illegible] نوجد أن

حل التالي:

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

ثم نعوض في $x = x_0 + t p^k$

في المسألة السابقة في حال $x_0 = 2$

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

$$b_1 = \frac{f(2)}{3^1} = 1$$

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

$$\Rightarrow t = 2$$

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

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

حلها أوجد حل $x_0 = 7$

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

م ١١ 2016/2/28

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

نوجد حل $x^6 - 1 \equiv 0 \pmod{7^3}$

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

تلميح: ١) نحل العدد 98 إلى عوامل أولية من ثم.

٢) نحل المعادلة لكل عامل أي:

$f(x) \equiv 0 \pmod 2$ — ①

$f(x) \equiv 0 \pmod 7$ ومنه نوجد حل $f(x) \equiv 0 \pmod{7^2}$ ②

نحل معادلتين خطيتين ١ و ٢

حل تمارين:

① -- $x \equiv -1 \pmod 6$

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

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

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

$x = 6$

ما هي x التي يكون ضربها بـ 2 وطرح منها 4 باقي قسمتها على 11 يساوي صفر هي $x = 2$ وبالتالي تصبح معادلة

② $x \equiv 2 \pmod{11}$

تصبح معادلة بالشكل

③ $x \equiv 6 \pmod{17}$

حل ① و ②

$\gcd(11, 6) = 1$

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

$x = (-1)(-11.11 + 2 \times 2)(6) = 35 \in \mathbb{Z}/66\mathbb{Z}$

حل: $x \equiv 35 \pmod{66}$ مع (3)

$\gcd(66, 17) = 1$

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

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

$x = -15277 \in \mathbb{Z}/(1122)\mathbb{Z}$ (11×17)

هذا عدد أكبر من 1122 وبالتالي لا يمكن إضافة بل نقسمه على ناتج قسمة وباقي ⇒ $x = -13 \times 1122 - 691$ (ناتج قسمة، باقي)

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

حل تمرين $G = \{1, a, b, c\}$

وعدم تكرار عنصر ضمن سطر و تبديلي أي جدول كيلي متناظر بالنسبة للقطر ضمن عامود

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

	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

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

التوابع الحسابية:

التابع الحسابي: هو تابع منطلقه $\mathbb{N}^*$ ومستقره $\mathbb{C}$

$$f: \mathbb{N}^* \to \mathbb{C}$$

تعريف 1: يكون التابع الحسابي جدائي (ضربي)

$$f(m.n) = f(m).f(n)$$

حيث n و m أعداد أولية فيما بينهما.

ويكون ضربي تام إذا كان

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

تابع أويلر: يرمز له بـ φ.

ليكن $n \in \mathbb{N}$ فإن $\varphi(n)$ يعرف بأنه عدد الأعداد الأولية لـ n مقلوب في $\mathbb{Z}/n\mathbb{Z}$

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = |\{a : 1 \leq a < n \quad gcd(a,n) = 1\}|$$

عدد عناصر هي زمرة

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

عدد أعداد طالب العلم

برهنة:

إن تابع أويلر هو ضربي ولكن ضربي غير تام.

$$\varphi(6) = \varphi(2\times 3) = \varphi(2).\varphi(3)$$

$$= 1 . 2 = 2$$

ولكن ليس تام لأن:

$$\varphi(4) \neq \varphi(2).\varphi(2)$$

$$2 \neq 1.1$$

نتيجة: ليكن $n \in \mathbb{N}^*$ و $n = \prod_k p_k^{\alpha_k}$

$$\varphi(n) = \prod \varphi(p_k^{\alpha_k})$$

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

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

ضرب لكن ليس ضروري تعلم لأن $\varphi(5^2)$ يمكن تبسيطه أكثر.