أولا: مبادئ العد

- مبادئ العد العامة:

- مبدأ العد الأول:

- مبدأ العد الثاني:

- مبدأ العد الثالث:

- تباديل الكرات وثيوتن:

- تباديل الكرات: $C(n,1,r)$ $C(n,r)$ $C(n,r)$

- مكونات ثيوتن:

$$(A+B)^n = \sum_{k=0}^{n} \binom{n}{r} A^{n-r} B^r$$

- خاصية مجموعة:

$$\binom{r}{r_1\ r_2 \dots r_n} = \frac{r!}{r_1!\, r_2! \dots r_n!}$$

r: عدد عناصر المجموعة الأساسية

$r_1, r_2, \dots r_n$: عدد عناصر المجموعة الجزئية

ثانيا: التباديل

- التباديل على الشكل

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 5 & 3 & n & \dots & \end{pmatrix}$$

العنصر الأول الذي يرتبط هو 1 ← n

إذا لم نعرف الارتباط لكن نرتبها عشوائي

- S_n: هي مجموعة كل التباديل من المرتبة n

- عدد عناصر S_n:

عدد عناصر S_n هو n

عدد التباديل بالمجموعة S_n هو:

أي $|S_n| = n!$

- متلوي ستيل: هو ترتيب العناصر المتباديل بتناوب ثم ترتيبها ترتيبا تصاعديا وفق بيداء الارتباط.

مثال:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

فالمتتالية المقابلة هي

$$\begin{pmatrix} 3 & 1 & 2 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

نرتب تصاعديا

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

- التبديل المحايد:

هو التحويل الذي يترك كل عنصر ويرمز له بـ Id_4

$$Id_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

- تركيب التباديل :

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\pi \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

π : 1 ← 3 ← 2 ← 1 ; 2 ← 1 ; 3 ← 2

τ : 1 ← 2 ← 3 ← 1 ; 2 ← 3 ← 1

$\pi \circ \tau$: 1 ← 1 ; 2 ← 2 ; 3 ← 3

$\Rightarrow \pi \circ \tau = Id_3$

$\tau \circ \pi$: 1 ← 3 ← 2 ← 1 ; 2 ← 1 ← 3 ← 2 ; 3 ← 2 ← 1 ← 3

$\Rightarrow \tau \circ \pi = Id_3$

إذن $\pi \circ \tau = \tau \circ \pi$

- الخلاصة :

يمكننا التعبير عن أي تبديل بشكل حلقة

$\tau = (1 \quad 3 \quad 2)$: 1 ← 3 ← 2 ← 1

$\tau = (1 \quad 2 \quad 3)$: 1 ← 2 ← 3 ← 1

مع ملاحظة بأن العنصر الذي لا يرتبط ببقية عناصر المجموعة يكتب منفرداً

$$N = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

$N = (2 \quad 3 \quad 4)$: 2 ← 4 ← 3 ← 2 ; 1 ⇄ 1

لكن بالنسبة للحرف الأخير فإننا نكتبه بالشكل

$Id_n = (1)(2)(3)(4)(5) \dots (n)$

ملاحظة :

يمكننا أيضاً التعبير عن التبديل بوساطة حلقات أو أكثر منفردة

$$S = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$$

$S = (1 \quad 2)(4 \quad 5)$

5 ← 4 ; 3 ⇄ 3 ; 1 ← 2 ← 1

ملاحظة:

$N = (1\ 2\ 3)(3\ 5)$

هذه ليست حلقة بل هي عبارة عن تركيب حلقتين لوجود العنصر (3) وهو عنصر مشترك

- التبديل الزوجي والتبديل الفردي نقول عن تبديل ما إنه زوجي إذا كان $(n!)$ عدد زوجي وإذا كان $(n-1)!$ عدد فردي سيكون التبديل فردي

- نرمز لمجموعة كل التباديل الزوجية بالرمز A_n بالرمز S_n بالمجموعة

$$|A_n| = \frac{n!}{2}$$ بـ:

ثالثاً: مجموعة جوانيي للعنصة $\mathbb{Z}/n\mathbb{Z}$

أولاً: $a \equiv b \pmod m$

+ أي باقي قسمة a على m هو b

+ نرمز لجميع الأعداد الباقي عند m بالرمز $[x]$

ونرمز لجميع رموز مجموعة العنصة $\mathbb{Z}/n\mathbb{Z}$ بـ:

مثالا التوضيحي عن $m=4$ أي

$a \equiv x \pmod 4$

$[0] = \{\dots, -8, -4, 0, 4, 8, \dots\}$

الأعداد التي باقي قسمتها على 4 هي $4\mathbb{Z} = [0]$

$[1] = \{\dots, -7, -3, 1, 5, 9, \dots\}$

$[1] = 1 + 4\mathbb{Z}$

$[2] = 2 + 4\mathbb{Z}$ وهكذا

$[3] = 3 + 4\mathbb{Z}$

$[4] = 4 + 4\mathbb{Z} = 4\mathbb{Z} = [0]$

وهكذا

$\mathbb{Z}/4\mathbb{Z} = \{[0], [1], [2], [3]\}$

أي:

$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$

حيث $|\mathbb{Z}/n\mathbb{Z}| = n$

+ أي $a, b \in \mathbb{Z}$ بأن

$a = bq + r$

+ ملاحظة هامة كل مسائل الـ mod

$-123 \equiv x \pmod 9$

بكسر بخده 3 أي $[-3+5] = [2]$

و منه $-123 \equiv 2 \pmod 9$

نستخدم مباشرة

$-123 - 2 \equiv 0 \pmod 9$

$\Rightarrow -123 \equiv 2 \pmod 9$

ثانياً: نعرف المجموعة $(\mathbb{Z}/n\mathbb{Z})^*$ بالشكل:

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[a] : 1 \le a \le n-1 \text{ و } \gcd(a,n)=1\}$$

أي هي مجموعة بواقي القسمة التي تكون أولية مع n.

ملاحظة: في حال كانت n عدداً أولياً فإن:

$$(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$$

رابعاً: .. الرمز ودراسة تراكيب المجموعات

السنة سنة

الجبارية هي [ ]

لـ:

S_n, A_n : $(S_n, \circ), (A_n, \circ)$

زمر أي كانت n الجبارية $[a]$

$(\mathbb{Z}_n/n\mathbb{Z}, +)$

زمرة. أي كانت n

+ رتبة العنصر:

نقول إن العنصر a له رتبة منتهية "دور عنصر" إذا وجد $n \in \mathbb{N}^*$ حيث إذا كانت العناصر a تنتمي إلى n أو d تنتمي إلى الجبارية

ونرمز لها بـ $|a| = o(a) = n$

وتكون مجموعة الصنف الجولدية في $(\mathbb{Z}/5\mathbb{Z}, +)$ أمثلة توضيحية.

نوجد دور الـ [3] و [4]

$K[3] = O_{(\mathbb{Z}/5\mathbb{Z},+)}$

$2[3] = [6] = [1]$

$3[3] = [9] = [4]$

$4[3] = [12] = [2]$

$5[3] = [15] = [0]$

$|[3]| = o([3]) = 5$ رتبة

$\langle [3] \rangle = \{K[3] : K = 0,1,2,3,4\}$

دور الـ [4]

$2[4] = [8] = [3]$

$\vdots$

$5[4] = [20] = [0]$

$|[4]| = 5$ رتبة

$\langle [4] \rangle = \{K[4] : K = 0,1,2,3,4\}$

± رتبة العنصر S_n:

رتبة التبديل π ستكون المضاعف المشترك الأصغر لطول حلقاته أي

$|\pi| = o(\pi) = lcm\{K : 1 \le K \le n\}$

ولو كان حلقة واحدة ستكون طول هذه الحلقة رتبة التبديل.

مثال توضيحي:

$$\pi = \underbrace{(1\ 2\ 3)}_{3}\underbrace{(4\ 5)}_{2}.$$

$$\Rightarrow |\pi| = lcm(3,2) = 6$$

$$\langle \pi \rangle = \{\pi^1, \pi^2, \pi^3, \dots \pi^6\}$$

نلاحظ أن π ضعف كعناصر

$$\tau = (1\ 2\ 3\ \dots\ 10)$$

$$\Rightarrow |\tau| = 10$$

* رتبة زمرة جزئية صادرة دورانية.

$G = \langle g \rangle$ و $H \leq G$

فإن

$$|H| = \frac{|G|}{gcd(n,k)}$$

$$\Rightarrow |H| = \frac{n}{\ell}$$

حيث: n: عدد عناصر G "رتبة G"

ℓ: $\ell = gcd(n,k)$

ℓ: عدد عناصر H (رتبة G)

"العدد المشترك"

مثال توضيحي: لتكن $G = \langle g \rangle$ و $H \leq G$ حيث

$$H = \langle g^{20} \rangle, \quad |G| = 25$$

$$\Rightarrow |H| = \frac{25}{gcd(25,20)} = \frac{25}{5} = 5$$

الزمرة C_n هي $\langle x \rangle$

$$C_n = \langle x \rangle = \{e, x, x^2, \dots x^{n-1}\}$$

حيث

$$x^i \cdot x^j = x^{(i+j) \bmod n}$$

أمثلة لزمرة الدوران و تطبيقات

تمارين

* رتبة الزمرة الجداء الديكارتي

$$|G \times H| = |G| \times |H|$$

وعنصر مثلها هو

$$|(g,h)| = lcm(|g|,|h|)$$

والمبادئ هو

$$e_{G \times H} = (e_G, e_H)$$

مثال: أوجد رتبة $([3]_5, \pi)$ حيث $G \times H$ هي الزمرة

$G = (\mathbb{Z}/5\mathbb{Z}, +)$

$H = S_4$

$\pi = (1\ 2)(3\ 4)$ حيث

$|[3]_5| = 5$, $|\pi| = 2$

$\Rightarrow |([3]_5, \pi)| = lcm(5,2) = 10$

خاصية ... مبرهنة الـ mod

أولاً: الـ gcd

- $gcd(a,b) = gcd(a, b+ka)$
  $= gcd(a+kb, b)$
- $gcd\left(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}\right) = 1$
- $gcd(a,b) = 1$
  $\Rightarrow a \not\equiv 0 \pmod{b}$.
  $b \not\equiv 0 \pmod{a}$.
- $gcd(a,b) = xa + yb = m$

= سنرى خوارزمية أقليدس لإيجاد m، x، y

المبرهنة ... برهنة بكس أقليدس

- $\mathbb{Z}/n\mathbb{Z}$ مقلوب عنصر في
نقول عن عنصر ما $[a] \in \mathbb{Z}/n\mathbb{Z}$
إنه قابل للقلب إذا تحقق
$gcd(a,n) = 1$
ويكون مقلوبه هو
$gcd(a,n) = xa + yn$.
$[a]^{-1} = [x]$

ملاحظة: إنما يجب أن نفهمه الآن
الزوج $\mathbb{Z}/n\mathbb{Z}$ إذا كان n أولياً.

مثال تمهيدي: أوجد مقلوب 99 في $\mathbb{Z}/1372\mathbb{Z}$

$gcd(99, 1372) = 1$ ~~[illegible]~~

99 ... 20

$1372 = 13(99) + 20$

$99 = 4(20) + 19$

$20 = 1(19) + 1$

$19 = 19(1) + 0$

$\Rightarrow gcd(99, 1372) = 1$

وهنه يوجد مقلوب لـ 99 في $\mathbb{Z}/1372\mathbb{Z}$

لإيجاده

$1 = 20 - 1(19)$

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

$= 20 - 1(99) + 4(20)$

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

$= 5(1372 - 13(99)) - 1(99)$

$= 5(1372) - 65(99) - 1(99)$

$= 5(1372) - 66(99)$

$\Rightarrow [99]^{-1} = [-66]$

$= [-66 + 1372]$

$= [1241]$

ثانياً: حل المعادلة الخطية في $\mathbb{Z}/n\mathbb{Z}$

④ حل معادلة واحدة خطية

$ax \equiv b \pmod n$

$gcd(a,m) = 1$ ← $gcd(a,m) = d \neq 1$

↓ ↓

وحيدة الحل modulo m ← d لا يقسم b ← d يقسم b

$[x] = [a]^{-1}[b]$ ← مسألة الكل ← المعادلة الأصلية

وهو نقوم بقسمة المعادلة على d

$\Rightarrow \frac{a}{d} x = \frac{b}{d} \pmod{\frac{n}{d}}$

$a' x = b' \pmod{n'}$

عدنا الى الحالة الأولى أي

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

حيث $gcd(a', n') = 1$

⑤ حل معادلتين خطيتين

$a_1 x \equiv b_1 \pmod n$

$a_2 x \equiv b_2 \pmod m$

نكتب المعادلتين على الشكل

$x \equiv b_1 \pmod n$

$x \equiv b_2 \pmod m$

ويكون لها حل وحيد شرط

$gcd(m,n) = 1$

$[x] = b_1 y m + b_2 \beta n$

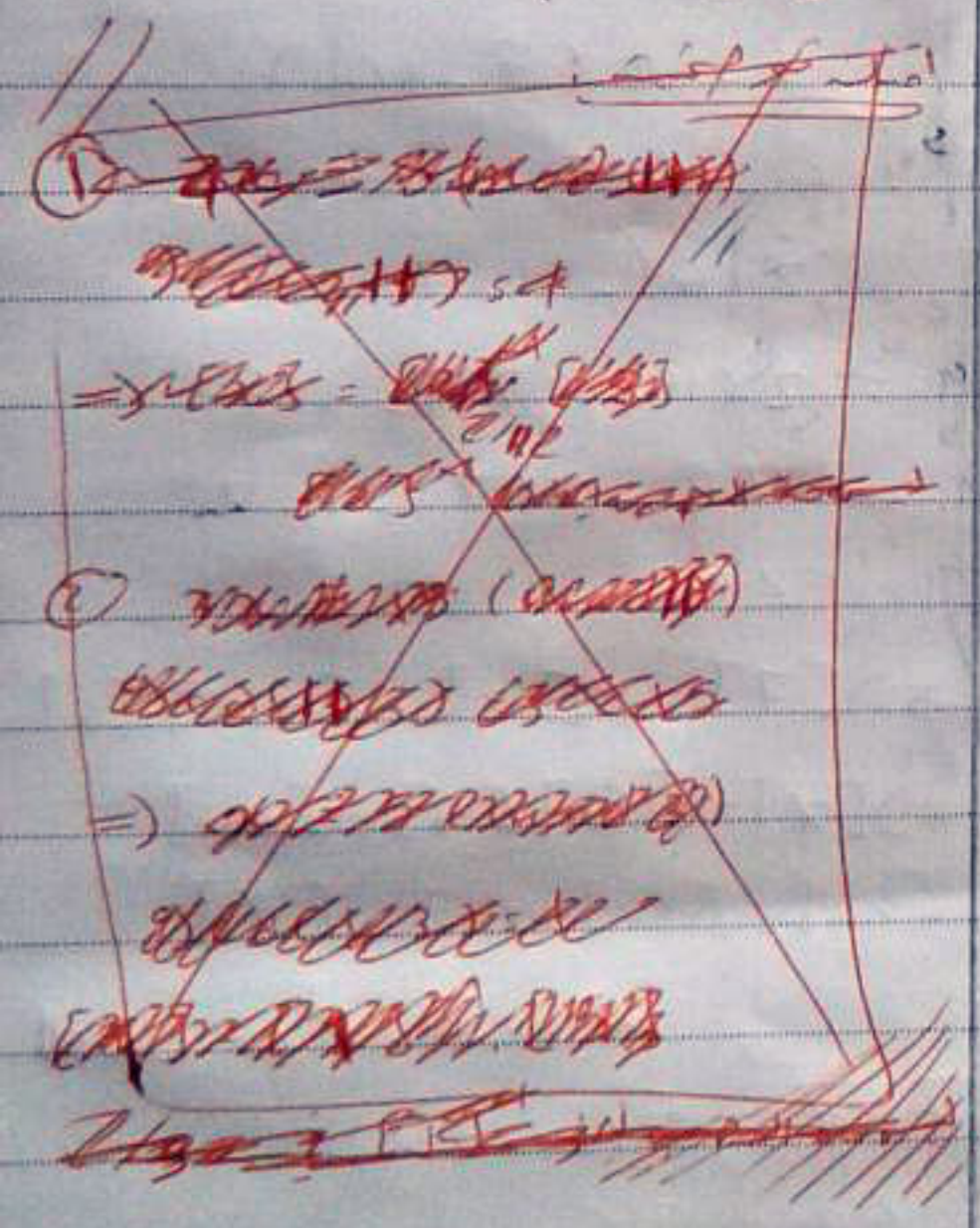
b_2 ← ويكتب كل ← b_1

حيث $\beta m + \gamma n$ هي التركيب الخطي الناتج عن $gcd(m,n) = 1$ الذي

$\mathbb{Z}/(n.m)\mathbb{Z}$

// خلاصة //

كل كثيرات حدود لها حل وحيد بالنسبة لكل كثير حدود مع معاملات في $\mathbb{Z}$



⑤. تمارين محلولة

① $7x \equiv 5 \pmod{11}$

$\gcd(7,11) \stackrel{?}{=} 1$

$11 = 1(7) + 4$

$7 = 1.(4) + 3$

$4 = 1.(3) + 1$

$\Rightarrow \gcd(7,11) = 1$

وهو كما نعلم، فإن $\bar{7}$ هو

$[x] = [7]^{-1}[5]$

حيث $[7^{-1}]$ في $\mathbb{Z}/11\mathbb{Z}$

$1 = 4 - 1(3)$

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

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

$= 2(4) - 1(7)$

$= 2(11 - 1(7)) - 1(7)$

$= 2(11) - 2(7) - 1(7)$

$= 2(11) - 3(7)$

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

$\Rightarrow [x] = [8][5] = [40]$

$[40] = [40 \bmod 11] = [7]$.

للتحقق من كما نعلم

$7 \times 7 \stackrel{?}{\equiv} 5 \pmod{11}$

$49 \equiv 5 \pmod{11}$

نعم صحيح لأن $49 - 5 = 44$ من مضاعفات 11

② $x \equiv 3 \pmod{5}$

$x \equiv 8 \pmod{11}$

$\gcd(11,5) \stackrel{?}{=} 1$

$11 = 2.5 + 1$

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

وهذه الجملة تكفي للحل.

$1 = (1)11 - 2(5)$

$\Rightarrow [x] = (3)(1)(11) - (8)(2)(5)$

$= [33] - [80]$

$= [-47]$

$= [-47 + 55]$

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

5×11

③ $x \equiv -1 \pmod{6}$

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

$3x \equiv 1 \pmod{7}$

لا يمكن أن نكمل حتى نتأكد

من أن جميع المعادلات

$x \equiv b \pmod{n}$

وهذه المعادلة الوحيدة

$x \equiv -1 \pmod{6}$ ... ①

التي لم تحقق المعادلة السابقة

$7x \equiv 4 \pmod{11}$

11 لايقبل القسمة على 7 وعلى لايكون أولي

$\Rightarrow 2x - 4 \equiv 0 \pmod{11}$ (لايكون مضاعف 11 مباشرة)

أي x هو العدد الذي يجعل الفرق بين 2x و 4 هي (0)

$\Rightarrow \boxed{x = 2}$

$\Rightarrow \boxed{x \equiv 2 \pmod{11}} \ldots (3)$

+ معادلة ثالثة

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

(لايكون مضاعف 17)

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

$\Rightarrow x = 6$

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

الآن المعادلات أصبحت هي

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

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

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

الآن نحلل معادلتين من 1 و 2

$\gcd(6, 11) = 1$

$11 = 1.6 + 5$

$6 = 1.5 + 1$

$\Rightarrow \gcd(6, 11) = 1$

$1 = 6 - 1(5)$

$= 6 - 1(11 - 1(6))$

$= 6 - 1(11) + 1(6)$

$1 = 2(6) - 1(11)$

$\Rightarrow [x] = (2)(2)(6) + (-1)(-1)(11)$

$= 24 + 11$

$= [35] \in \mathbb{Z}/66\mathbb{Z}$

$= 11 \times 6$

$\Rightarrow x \equiv 35 \pmod{66}$ ... (4)

نحل بالمثل (3) و (4) لأن

$\gcd(66, 17) = 1$

$66 = 3.17 + 15$

$17 = 1.15 + 2$

$15 = 7.2 + 1$

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

وصلنا لنهاية الحل نعيد

$1 = 15 - 7(2)$

~~$= 15 - 7(17 - 1(15))$~~

$= 15 - 7(17 - 1.15)$

$= 15 - 7(17) + 7(15)$

$= 8(15) - 7(17)$

$= 8(66 - 3.17) - 7(17)$

$= 8(66) - 24(17) - 7(17)$

$= 8(66) - 31(17)$

$\Rightarrow [x] = (6)(8)(66) + (-31)(17)$

Alnour

$[x] = [-15277]$

$66 \times 17 = 1122$))

$[x] = [-15277]$

$= [-13 \times 1122 - 961]$

$= [-961]$

$= [-961 + 1122]$

$= [431] \in \mathbb{Z}/1122\mathbb{Z}$

ما فعلناه هو

15277- عدد كبير وأكبر من 1122

ولذلك يجب أن نكتبه على شكل $ab+9$

حتى نتمكن. هكذا $[1122 \times (-13)] = [0]$

لأنه مضاعف لـ 1122 وصفة

بقي $[-961]$ لإيجاد الحل الكوخي

المطلوب. لإيجاد الحل الموجب وصفة وهي

1122. نجد لدينا الحل المطلوب.

// انتهت الإضافة التوضيحية في المحاضرة

الخاصة //

---

③. المعادلات غير الخطية

أولاً: حالة البسيط

$$f(x) \equiv 0 \bmod (m).$$

ونرمز بالرمز: $N_f Sol(m)$

لعدد الحلول للمعادلة $f(x)$ في $\mathbb{Z}/m\mathbb{Z}$

مبرهنة:

$$N_f Sol(m.n) = N_f Sol(m) . N_f Sol(n)$$

مثال تطبيقي:

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

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

$$\Rightarrow f(x) = x^2 - 1 \equiv 0 \pmod{5 \times 3}$$

$$\Rightarrow N_f Sol(15) = N_f Sol(5) \times N_f Sol(3)$$

حيث المعادلة $x^2 - 1 = 0$ حلها

$$\Rightarrow N_f Sol(15) = 2 \times 2 = 4$$

أعداد حلول.

$$x^2 - 1 \equiv 0 \bmod (5)$$

بالتعويض بـ $0, 1, 2, 3, 4$

نجد أن الحلين هما (1) و (3)

بنا

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

هما $0, 1, 2$ نجد (1) و (2)

أي حلول

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

عددها 4 وهي $(1)(1)$ و $(2)(2)$ و $(1)(2)$ و $(2)(1)$

ثانيا: حل معادلات قرجرجانية..

بطريقة هنسل..

مبرهنة هنسل: بحيث نستفيد من الحالة

ونبنا هنا سنختصر حالتها على..

إذا وجد حل ما x_0 لمعادلة

$f(x) \equiv 0 \pmod{p}$ بحيث

$f'(x_0) \not\equiv 0 \pmod{p}$ ..

فإن هناك حل لـ:

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

$\forall x \geq 1$ متشكل

$$x = x_0 + p^x \cdot t$$

مثال توضيحي

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

$f(x) = x^2 - 1$ حيث

نتحقق أن

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

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

نتحقق الشروط:

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

وهو الشرط يحقق أي الحالات

وجود حل $x_0 = 1 \pmod{3}$

$x = x_0 + p^x t$

لنجد t حالات ترضينا.

الآن: نعوض الحل بالحالة

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

$\Rightarrow x = 1 + 3t$

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

$f(1+3t) \equiv 0 \pmod{9}$

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

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

$\underbrace{9t^2}_{\equiv 0} + 6t \equiv 0 \pmod{9}$

بما أن

$\mathbb{Z}/9\mathbb{Z} \quad [9] = [0]$

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

~~نوجد مضاعف مشترك~~

~~وحيد~~

$9 \wedge d(6, 9) \neq 1 = 3$ ~~وحيد~~

وبما أن $3 \nmid 9$ و $3 \mid 6$

$2t \equiv 0 \pmod{3}$

$\Rightarrow \boxed{t = 3}$

$\Rightarrow x = 1 + 3(3) = 10 \; (\mathbb{Z}/10\mathbb{Z})$

$\Rightarrow [10] = [1]$

الحالة 2 نضع t من المعادلة:

$b + a_1 t \equiv 0 \pmod{p^2}$.

$b = \frac{f(x_0)}{p}$ حيث

$a_1 = f'(x_0)$

أي:

$b = 0 , a_1 = 2$

$2t \equiv 0 \pmod 3$

$\Rightarrow \boxed{t = 3}$

و هكذا

سادساً ... التوابع الحسابية

$f: \mathbb{N} \longrightarrow \mathbb{C}$

* التابع الحسابي الضربي "المجالي" نقول عن f إنه تابع ضربي إذا كان

$gcd(n,m) = 1$

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

أي إذا الأعداد أولية فيما بينها فإن صورة الجداء هو جداء الصور

* نقول عنه ضربي تام أو جدائي تام إذا حققت العلاقة $f(n.m) = f(n).f(m)$ لكل أي عددين n, m

---

@ تابع أويلر Euler هو تابع عدد الأعداد التي لا تقل عن n في $\mathbb{Z}/n\mathbb{Z}$

أي هو

$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$

* تابع أويلر تابع ضربي وليس تابع ضربي تام.

* تابع أويلر يحقق العلاقة

$a^{\varphi(n)} = 1 \pmod n$

شرط $gcd(a,n) = 1$

* ملاحظة

في حال كان n عدد أولي فإن

$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = n-1$

أمثلة توضيحية:

$\varphi(7) = |(\mathbb{Z}/7\mathbb{Z})^*|$

$= |\{1, 2, 3, 4, 5, 6\}|$

$= 6$

$\varphi(6) = |(\mathbb{Z}/6\mathbb{Z})^*|$

$= |\{1, 5\}| = 2$

حيث $\begin{cases} gcd(6,1) = 1 \\ gcd(5,6) = 1 \end{cases}$

$$\sigma(n) = \prod_k \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$$

$$\tau(n) = \prod_k (\alpha_k + 1)$$

35 ... $3^{\text{لانهاية}}$ ... أوجد باقي القسمة على 35

$\varphi(35) = \varphi(7) \times \varphi(5)$

$\gcd(7,5) = 1$ لأن

لأن 5, 7 أعداد أولية فيما بينها

$\varphi(35) = 6 \times 4 = 24$

$\gcd(3, 35) = 1$

$\Rightarrow 3^{\varphi(35)} \equiv 1 \pmod{35}$

$3^{24} \equiv 1 \pmod{35}$

$(3^{24})^{4166} \equiv 1 \pmod{35}$ وأيضاً

$3^{24 \cdot 4166} \times 3^{16} \equiv 11 \pmod{35}$

أي 3^{16} باقي قسمته على 35 هو 11

$\Rightarrow 3^{\text{لانهاية}} \equiv 11 \pmod{35}$

⊕ التابع دالة الترتيب ..

نقول عن تابع إنه دالة الترتيب إذا لم يكن هناك قاسم رئيسي أ:

$6 = 3^1 \times 2^1$ دالة الترتيب

$49 = 7^2$ ليس دالة الترتيب

$8 = 2^2 \times 2^1$ " " "

Mobius تابع ⓒ

$\mu(n)$: $n = 1$ ← 1

ليس دالة الترتيب ← 0

دالة الترتيب عدد ← $(-1)^r$

$n = p_1 \cdot p_2 \cdot p_3 \cdots p_r$

⊕ ملاحظة $\sum_{d|n} \mu(d) = 0$

إذا كان مجموع توابع موبيوس لقواسم عدد ما هي (0) "

ⓑ .. التابعان $\sigma(n)$ و $\tau(n)$

$\sigma(n)$: تابع مجموع قواسم n

$\tau(n)$: عدد قواسم n

⊕ إن $\sigma(n)$ و $\tau(n)$ توابع ضربية .. وليست ضربية تماماً

مثال توضيحي:

$n = 14$

قواسم العدد 14 هي $1, 2, 7, 14$

$$\Rightarrow \sum_{d \mid 14} \mu(d) =$$

$2 = 2\times 1 \quad 7 = 7\times 1 \quad 14 = 7\times 2$

$$= \mu(1) + \mu(2) + \mu(7) + \mu(14)$$
$$= 1 + (-1)^1 + (-1)^1 + (-1)^2$$
$$= 1 - 1 - 1 + 1$$
$$= 0$$

سابعاً: الأعداد: $1\ldots111$ (n مرة)

* $\underbrace{11\ldots1}_{n \text{ مرة}} = \dfrac{10^n - 1}{9}$

* ملاحظة: إذا كان $n = \alpha k$

$$\Rightarrow \underbrace{11\ldots1}_{n=\alpha k \text{ مرة}} = \underbrace{1\ldots1}_{\alpha \text{ مرة}} \times \underbrace{1\underbrace{0\ldots0}_{\alpha-1}1\,0\ldots0\,1\ldots0\ldots01}_{k-1 \text{ مرة}}$$

مثال توضيحي:

$$\underbrace{111111}_{6 \text{ مرات} = 3\times 2} = \overbrace{111}^{3 \text{ مرة}} \times \underbrace{1\overbrace{00}^{3-1 \text{ مرة}}1}_{2-1 \text{ مرة}}$$

$6 = 2\times 3$

أو بالعكس

$$\underbrace{111111}_{2\times 3} = \overbrace{11}^{2 \text{ مرة}} \times \underbrace{1\overbrace{0}^{2-1 \text{ مرة}}1\overbrace{0}{}1}_{3-1 \text{ مرة}}$$

- نضع $11\ldots1$ α مرة
- ثم نضع 1 ونضيف أمامها $[0\ldots0]$ $(\alpha-1)$ مرة
- ونكرر الخطوة الثانية $[k-1]$ مرة

لهذه الأعداد مسائل هامة جداً بالمحاضرة الثالثة عشر...

ثامناً: المعادلات التربيعية

$$x^2 \equiv a \pmod{p}$$

p عدد أولي

رمز لوجاندر Legendre

p عدد أولي فردي: $\left(\dfrac{a}{p}\right)$

⇕

$$x^2 \equiv a \pmod{p} \quad \ldots (*)$$

نميز الحالات

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \text{ يقسم } a \\ 1 & p \text{ لا يقسم } a \text{ و } (*) \text{ تقبل الحل} \\ -1 & p \text{ لا يقسم } a \text{ و } (*) \text{ لا تقبل الحل} \end{cases}$$

ه مجموعة من المبرهنات الهامة في التمارين " صيغ سنعتمدها إذا كان المعادلة حل أو لا "

[1]. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ حيث $a \equiv b \pmod p$

" أي b باقي قسمة a على p "

[2]. $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p$

[3]. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{إذا كان } p \text{ باقي قسمة على 4 يساوي 1} \\ -1 & \text{إذا كان } p \text{ باقي قسمة على 4 يساوي } -1 \end{cases}$

$p \equiv 1 \pmod 4$ إذا كان : 1

$p \equiv 3 \pmod 4$ " " " : -1

[4]. $\left(\frac{a.b}{p}\right) = \left(\frac{a}{p}\right) . \left(\frac{b}{p}\right)$

[5]. $\left[\frac{2}{p}\right] = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 \\ -1 \end{cases}$

[6]. $\left(\frac{p}{q}\right).\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$

$= \begin{cases} 1 \\ -1 \end{cases}$

$p \equiv 1 \pmod 4$ أو $q \equiv 1 \pmod 4$: 1

إذا p أو q تحقق إحداهما

$p \equiv 3 \pmod 4$ و $q \equiv 3 \pmod 4$: -1

تمارين محلولة

حل المعادلة $x^2 \equiv 44 \pmod{47}$

حل 1 :

إذا السؤال يكون إيجاد $\left(\frac{44}{47}\right)$

$\left(\frac{a}{p}\right) = \left(\frac{44}{47}\right) = \left(\frac{11 \times 4}{47}\right)$

[4]. $= \left(\frac{11}{47}\right) . \left(\frac{4}{47}\right)$

$= \left(\frac{11}{47}\right) . \left(\frac{2}{47}\right) . \left(\frac{2}{47}\right)$

$\left(\frac{2}{47}\right)$

سيكون حسب [5] إما (1) أو (-1)

لكن الحالة سيكون تابع حمار

$\left(\frac{2}{47}\right)\left(\frac{2}{47}\right) = 1$

$\Rightarrow \left(\frac{44}{47}\right) = 1 \cdot \left(\frac{11}{47}\right)$

$\left(\frac{11}{47}\right)\cdot\left(\frac{47}{11}\right) = -1$

$11 \equiv 3 \bmod 4$ بما

$\Rightarrow \left(\frac{11}{47}\right) = -1\left(\frac{47}{11}\right)$

$\Rightarrow \left(\frac{44}{47}\right) = -1\left(\frac{47}{11}\right)$

11 عدد أولي وصفه دفت [1]

$47 \equiv 3 \pmod{11}$

$\Rightarrow \left(\frac{47}{11}\right) = \left(\frac{3}{11}\right)$

$\Rightarrow \left(\frac{44}{47}\right) = -1\left(\frac{3}{11}\right)$

$\left(\frac{3}{11}\right)\left(\frac{11}{3}\right) = -1$

$11 \equiv 3 \bmod 4$

$\Rightarrow \left(\frac{3}{11}\right) = -1\left(\frac{11}{3}\right)$

$\Rightarrow \left(\frac{44}{47}\right) = (-1)(-1)\left(\frac{11}{3}\right)$

$= \left(\frac{11}{3}\right)$

3 أولي وصفه دفت [1]

$\left(\frac{44}{47}\right) = \left(\frac{2}{3}\right)$

حسب [3]

$= (-1)$

وصلنا لا يوجد للعادلة حل

// للمزيد من الشارحين الصفحة 15

تابعنا ... وصلنا لمفهوم

دفت //

هذه الخصائص مطلوبة نصاً ودفت

للحد ...

① مبرهنة Wilson

اذا كان P عدد اولي فإن

$(P-1)! \equiv -1 \pmod{P}$

[P ≠ 2]

والعكس صحيح

② اذا كان P عدد اولي فردي فإن

$\left(\left(\frac{P-1}{2}\right)!\right)^2 \equiv (-1)(-1)^{\frac{P-1}{4}} \pmod{P}$

③ مبرهنة Fermat الصغرى

إذا كان p عدد أولي و a عدد صحيح بحيث a و p أوليان فيما بينهما ($p \times a$)

$$a^{p-1} \equiv 1 \pmod{p}$$

ملاحظة

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

④

إذا كان P عدد أولي فإن زمرة الضرب $(\mathbb{Z}/P\mathbb{Z})^*$ تكون زمرة دورية من المرتبة $(P-1)$

$$(\mathbb{Z}/P\mathbb{Z})^* = \langle g \rangle$$

إعداد: محمد الخوني