٢٠١٦/٥/٩

المحاضرة التاسعة

مجموعة البواقي المختزلة

تعريف: لتكن المجموعة $A(m)=\{0,1,2,\dots,m-1\}$ مجموعة البواقي التامة بالمقاس m فتكون مجموعة البواقي المختزلة هي:

$$T(m)=\{a\in A \;;\; (a,m)=1\}$$

مثال: $m=6 \leftarrow A(6)=\{1,2,3,4,5,6\}$

$a\in A$, $(a,m)=1 \rightarrow T(6)=\{1,5\}$

القاسم المشترك لـ 6, 5 هو 1.

مثال: $m=12 \leftarrow A(12)=\{0,\pm1,\pm2,\pm3,\pm4,\pm5,6\}$

مجموعة البواقي المختزلة هي $\{\pm1,\pm5\}$

$$T(12)=\{1,5,7,11\}$$

دالة أولر: φ

هي دالة عددية قيمتها عند العدد m ; $\varphi(m)$ تساوي عدد الأعداد التي هي اصغر من m وأولية نسبياً مع m

$\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$

$\varphi(6)=2$, ...

مبرهنة: دالة أولر $\varphi(m)$ هي دالة ضربية. أي تحقق: ① $\varphi(1)=1$

② $\varphi(m.n)=\varphi(m).\varphi(n)$ حيث $m,n\in\mathbb{Z}^+$, $(n,m)=1$

مبرهنة: إذا كان P عدداً أولياً فإن $\varphi(P)=P-1$

مجموعة البواقي التامة $A(P)=\{0,1,2,\dots,P-1\}$

هي مجموعة البواقي المختزلة $T(P)=\{1,2,\dots,P-1\}$

أي $\varphi(P)=P-1$ عددها $P-1$

مبرهنة: إذا كان P عدداً أولياً فإن $\varphi(P^\alpha)=P^{\alpha-1}(P-1)$

الإثبات: مجموعة البواقي التامة بالمقاس P^α

عدد العناصر هو $m=P^\alpha$

$A=\{0,1,\dots,P^\alpha-1\}$

$=\{1,2,P,\dots,P^2,\dots,P.P^{\alpha-1}\}$

نجد العناصر التي لها عامل مشترك مع p^α في A هي :

$$p, 2p, 3p, \dots, p^{\alpha-1}.p$$

عدد هذه العناصر هو $p^{\alpha-1}$ فيكون عدد العناصر من المجموعة البواقي التامة التي هي أولية مع p^α هي :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$
$$= p^\alpha\left(1-\frac{1}{p}\right)$$
$$= p^{\alpha-1}(p-1)$$

مبرهنة : إذا كان $n = p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_r^{\alpha_r}$, p_i أوليات مختلفة فإن :

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)$$

الإثبات :

بما أن الدالة φ ضربية فإن :

$$\varphi(n) = \varphi(p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1}).\varphi(p_2^{\alpha_2})\dots\varphi(p_r^{\alpha_r})$$
$$= p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_r^{\alpha_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)$$
$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)$$

* $\varphi(360) = \varphi(2^3.3^2.5)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$
$= 2^3.3^2.5\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 96$

مبرهنة أويلر :

إذا كان $(a,m)=1$ فإن $a^{\varphi(m)} \equiv 1 \pmod m$

الإثبات : نأخذ مجموعة البواقي المختزلة بالقاس m وهي $T = \{a_1, a_2, \dots, a_{\varphi(m)}\}$

كذلك تكون المجموعة $T_1 = \{aa_1, aa_2, \dots, aa_{\varphi(m)}\}$

أيضاً مجموعة بواقي مختزلة بالمقاس m لذ أن عناصر T_1 أولية مع m وعناصر T_1 غير متطابقة بالمقاس m لنفرض عكس ذلك أي لوجد اعداد من T_1 متطابقة. $aa_i \equiv aa_j \pmod m$

بما أن $(a,m)=1 \Longleftarrow a_i \equiv a_j \pmod m$

$\{1 \le i < j \le \varphi(m)\}$ وهذا تناقض

بما أن كل عنصر من T يطابق عنصر من T_1 بالمقاس m ومنه جداء عناصر T يطابق جداء عناصر T_1 بالمقاس m

$a.a_1.a.a_2.\dots.a\varphi(m)\equiv a_1.a_2\dots a_{\varphi(m)}$

$a^{\varphi(m)}.a_1a_2\dots a_{\varphi(m)}\equiv a_1.a_2\dots a_{\varphi(m)} \pmod m$

بما أن $(a_1.a_2\dots a_{\varphi(m)}, m)=1$

نجد أنه $a^{\varphi(m)}\equiv 1 \pmod m$

* نجد أن مبرهنة فيرما الصغرى هي حالة خاصة عندما $m=p$ من مبرهنة أولر $a^{p-1}\equiv 1 \pmod p$

مثال: أوجد رقمي الآحاد والعشرات للعدد 3^{256} (رقمي الآحاد والعشرات في العدد 3^{256} هو باقي قسمته على 100)

$3^{\varphi(100)}\equiv 1 \pmod{100}$, $\varphi(100)=\varphi(2^2.5^2)$

$=2^2.5^2\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$

$=2^2.5^2\left(\frac{1}{2}\right)\left(\frac{4}{5}\right)=40$

$\Rightarrow 3^{40}\equiv 1 \pmod{100}$

$3^{256}=(3^{40})^6.3^{16}\equiv 3^{16}\equiv(81)^4\equiv(-19)^4\equiv(19)^4\equiv(361)^2\equiv(61)^2$

$\equiv(3721)\equiv 21 \pmod{100}$

مثال: حل المطابقة $6x\equiv 15 \pmod{21}$

$(6,21)=3 \nmid 15$ إذاً للمطابقة ثلاث حلول مختلفة بالقاسم m

$2x\equiv 5 \pmod 7$

$(2,7)=1$; $2^{\varphi(7)}\equiv 1 \pmod 7$, $2^6\equiv 1 \pmod 7$

$2^6x\equiv 5.2^6 \pmod 7$

$x\equiv 5.4 \pmod 7$

$\therefore x\equiv 6 \pmod 7 \Rightarrow x\equiv 6+7t \quad t=0,1,2$

$x\equiv 6,13,20 \pmod 7$

$x\equiv 6,13,20 \pmod{21}$

نتيجة: إذا أقسم القاسم d جميع قواسم العدد n فإن $\frac{n}{d}$ يقسم كذلك جميع قواسم العدد n

الموضوع : .....

$n=12$

$d=\{1,2,3,4,6,12\}$

$\frac{n}{d}=\{12,6,4,3,2,1\}$

$d_1=\frac{n}{d}$ ، $n=d.d_1$ ، $d \setminus n$ ، $d_1 \setminus n$

الدالة τ: هي الدالة العددية قيمتها عند العدد n تساوي عدد القواسم الموجبة للعدد n.

$$\tau(n)=\sum_{d \setminus n} 1$$

$\tau(1)=1$ ، $\tau(2)=2$ ، $\tau(3)=2$ ، $\tau(4)=3$ ، $\tau(5)=2$ ، $\tau(7)=2$

$\tau(11)=\tau(13)=2$

بشكل عام: p عدد أولي $\tau(p)=2$

$n=p^\alpha$ تكون قواسم العدد $n=p^\alpha$ هي $1, p, p^2, \dots, p^\alpha$

عددهم هو $\alpha+1$ أي $\tau(p^\alpha)=\alpha+1$

إذا كان $n>1$ الشكل القانوني لـ $n=p_1^{\alpha_1} \dots p_r^{\alpha_r}$

فإن $\tau(n)=\tau(p_1^{\alpha_1}) \dots \tau(p_r^{\alpha_r})$

كون τ دالة ضربية.

$$= (\alpha_1+1)(\alpha_2+1) \dots (\alpha_r+1)$$

* τ دالة ضربية لأنها تحقق:

* $\tau(1)=1$

كذلك $\tau(d_1.d_2) = \tau(d_1).\tau(d_2)$

عددية $\rightarrow$ $F(n)=\sum_{d \setminus n} f(d)$ $\rightarrow$ عددية

$f(d)=1 \Longleftarrow f(1)=1$

$f(d_1.d_2)=1$

$$f(d_1.d_2)=\sum_{d \setminus d_1.d_2} 1 = f(d_1).f(d_2)$$

ثم استنتج أن τ دالة ضربية.

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1)$$
$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

$$\tau(360) = \tau(2^3 \cdot 3^2 \cdot 5) = 4 \times 3 \times 2 = 24$$

الدالة $\sigma(n)$ هي دالة عددية تعطيها كل العدد n يساوي مجموع القواسم الموجبة للعدد n

$$\sigma(n) = \sum_{d \mid n} d$$

$\sigma(1) = 1$ ، $\sigma(2) = 3$ ، $\sigma(3) = 4$ ، $\sigma(4) = 7$ ، $\sigma(5) = 6$
$\sigma(6) = 12$ ، $\sigma(7) = 8$

مبرهنة: الدالة σ هي دالة ضربية:

1) $\sigma(1) = 1$

2) $\sigma(n.m) = \sigma(n)\sigma(m)$ ، $(n,m) = 1$

حسب الصيغة f دالة ضربية فإن $F(n) = \sum_{d \mid n} f(d)$ الدالة ضربية

$f(d) = d$ نثبت أن $f(d) = d$ دالة ضربية فإن $\sigma(n) = \sum_{d \mid n} d$ دالة ضربية.

1) $f(1) = 1$

2) $(d_1, d_2) = 1$; $f(d_1 d_2) = d_1 d_2 = f(d_1) \cdot f(d_2)$

$f(d) = d$ دالة ضربية ومنه $\sigma(n) = \sum_{d \mid n} d$ هي دالة ضربية.

إذا كان $n = p$ $\Leftarrow$ $\sigma(p) = p + 1$

إذا كان $n = p^\alpha$ $\Leftarrow$ قواسم العدد p^α هي: $1, p, p^2, \dots, p^\alpha$

$$\sigma(p^\alpha) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$$

إذا كان $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

$$\sigma(n) = \sigma(p_1^{\alpha_1} \cdots p_r^{\alpha_r})$$
$$= \sigma(p_1^{\alpha_1}) \cdot \sigma(p_2^{\alpha_2}) \cdots \sigma(p_r^{\alpha_r})$$
$$= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}$$
$$= \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

$$\sigma(360) = \sigma(2^3 \cdot 3^2 \cdot 5) \cdot \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1}$$

$$\sigma(360) = 15 \cdot 13 \cdot 6 = 1170$$

★ الدالتان τ ، σ ليستا ضربيتين تماماً.

$$\tau(20) = \tau(2^2 \cdot 5) = 6$$

$$\tau(2) \cdot \tau(10) = 2 \cdot 4 = 8 \qquad (2,10) = 2$$

ملاحظة:

$$\tau(20) = 6 \neq 8 = \tau(2) \cdot \tau(10)$$

τ ليست ضربية تماماً.

$$\sigma(20) = \sigma(2^2 \cdot 5) = \frac{2^3-1}{2-1} \cdot \frac{5^2-1}{5-1} = 7 \cdot 6 = 42$$

$$\sigma(2) \cdot \sigma(10) = 3 \cdot 18 = 54$$

$$\sigma(20) = 42 \neq \sigma(2) \cdot \sigma(10) = 54$$

σ ليست ضربية تماماً.

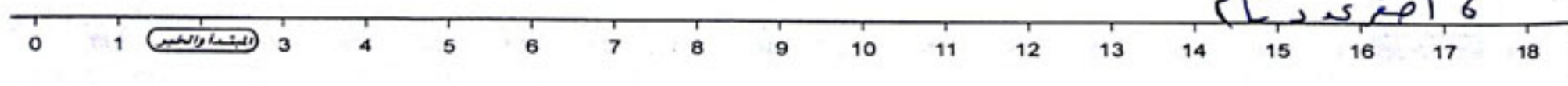
الأعداد التامة (الكاملة): تقول عن العدد n أنه تام (كامل) إذا كان $\sigma(n) = 2n$

ونقول أن العدد n هو عدد ناقص التام إذا كان: $\sigma(n) < 2n$

ويسمى فوق التام إذا كان: $\sigma(n) > 2n$

$$\sigma(6) = \sigma(2) \cdot \sigma(3) = 3 \cdot 4 = 2 \cdot 6 = 12$$

6 أصغر عدد تام



$\sigma(28) = \sigma(2^2 \cdot 7) = \frac{2^3-1}{2-1} \cdot \frac{7^2-1}{7-1} = 7 \cdot 8 = 56 = 2 \cdot 28$

28 هو عدد تام

مثال عن العدد الناقص (الغير التام):

$\sigma(8) = \sigma(2^3) = 15 < 2 \cdot 8 = 16$

وبكون 8 عدد ناقص.

مثال عن العدد فوق التام (زائد):

$\sigma(12) = \sigma(2^2 \cdot 3) = 7 \cdot 4 = 28 > 2 \cdot 12$

12 هو عدد زائد.

العددين التوأمين: هما عددين اوليان الفرق بينهما 2

$(3,5)$ ، $(5,7)$ ، $(11,13)$ ، $(17,19)$ ، ...

الأعداد المتحابة: نقول عن العددين انهما متحابان n و m.
إذا حققت مايلي:

$\sigma(n) - n = m$

$\sigma(m) - m = n$

بالرموز: $\sigma(n) = \sigma(m) = n+m$

مثال: $(220, 284)$

$\sigma(220) = \sigma(2^2 \cdot 5 \cdot 11) = 7 \cdot 6 \cdot 12 = 504$

$\sigma(220) - 220 = 504 - 220 = 284$

$\sigma(284) = \sigma(2^2 \times 71) = 7 \cdot 72 = 504$

$\sigma(284) - 284 = 504 - 284 = 220$

لا يوجد عدد تام فردي

الصيغة : $1 + 2 + 2^2 + \dots + 2^{k-1} = 2^k - 1 = p$

تعطي اعداد أولية واعداد غير اولية:

$k = 2 \Rightarrow 1 + 2 = 3$

$k = 3 \Rightarrow 1 + 2 + 2^2 = 7$

$k = 4 \Rightarrow 1 + 2 + 2^2 + 2^3 = 15$ غير أولي

خاصة: إذا كان العدد $2^k - 1$ اولياً , $k > 1$

فإن : $n = 2^{k-1}(2^k - 1)$

هو عدد تام (كامل) وكل عدد تام (كامل) زوجي هو من الشكل

الـــبات:

كذلك العدد الناقص هو : $A = 2^{k-2}(2^k - 1)$

والعدد الزائد هو: $B = 2^k(2^k - 1)$

امثلة:

1) $k = 2 \Rightarrow 2^k - 1 = 3$ اولي $\Rightarrow n = 2.3 = 6$

$k = 3 \Rightarrow 2^3 - 1 = 7$ اولي $\Rightarrow n = 4.7 = 28$

2) $k = 2 \Rightarrow 2^2 - 1 = 3$ اولي $\Rightarrow A = 3$ عدد ناقص

$k = 3 \Rightarrow 2^3 - 1 = 7$ اولي $\Rightarrow A = 27 = 14$ عدد ناقص

العدد الزائد: $B = 2^k(2^k - 1)$

$k = 2 \Rightarrow 2^2 - 1 = 3$ اولي $\Rightarrow B = 4.3 = 12$

$k = 3 \Rightarrow 2^3 - 1 = 7$ اولي $\Rightarrow B = 8.7 = 56$

الموضوع : .....

برهنة: إذا كان العدد $a^k - 1$ أولياً
$k \geq 2$ ، $a > 0$ فإن $a = 2$ و k عدد أولي
تسمى الأعداد $M_k = 2^k - 1$ ، $k \geq 2$
أعداد ميرسين

الأعداد $M_p = 2^p - 1$ هي أعداد أوليّة، سميت أعداد ميرسين الأوليّة.
وتكون أوليّة عندما p يأخذ القيم:
$p = 2, 3, 5, 7, 13, 17, 19, 31, 127, 257$.

دالة موبياس: نعرّف دالة موبياس μ قيمتها عند n تساوي:

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & p^2 \mid n \quad p \text{ أولي} \\ (-1)^r & n = p_1 \cdot p_2 \cdots p_r \end{cases}$$

$\mu(1) = 1$
$\mu(2) = \mu(3) = -1$
$\mu(4) = \mu(9) = 0$
$\mu(5) = -1$
$\mu(6) = 1$

* μ هي دالة ضربية
1) $\mu(1) = 1$
2) $\mu(n.m) = \mu(n).\mu(m)$
$(n, m) = 1$

صيغة موبياس للتعاكس: إذا كانت F ، f دالتين عدديتين
وكان $F(n) = \sum_{d \mid n} f(d)$

ملاحظة :

$$f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

تعريف : دالة ليوفيل

$$\lambda(n) = \begin{cases} 1 & n = 1 \\ (-1)^{\alpha_1+\alpha_2+\dots+\alpha_r} & ; \ n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \end{cases}$$

وهي دالة ضربية.

$\lambda(1) = 1$ ، $\lambda(2) = \lambda(3) = -1$

$\lambda(4) = 1$ ، ...

دالة ما نجولد : تعرف كالتالي :

$$\Lambda(n) = \begin{cases} \log p & n = p^k \text{ ، } p \text{ اولي} \\ & 1 \le k \\ 0 & \text{فيما عدا ذلك} \end{cases}$$

خواص :

1) $\sum_{d|n} \Lambda(d) = \log n$

2) $\Lambda(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log d$