٣,١ نظرية الدوال العددية

Theory of Arithmetic Functions

٣,١,١ الـدوال الـعـدديـة Arithmetic Functions

يطلق على الدوال مثل دالة أويلر مسمى الدوال العددية. والدالة العددية عموما هي الدالة التي مجالها $\mathbb{Z}^+$ ومجالها المقابل مجموعة جزئية من الأعداد المركبة.

تسمى الدالة العددية غير الصفرية

❖ **ضربية**

إذا كان $\mathrm{f}(m \cdot n) = \mathrm{f}(m) \cdot \mathrm{f}(n)$ لكل $m,n \in \mathbb{Z}^+$ حيث $(m,n) = 1$.

❖ **ضربية تماما**

إذا كان $\mathrm{f}(m \cdot n) = \mathrm{f}(m) \cdot \mathrm{f}(n)$ لكل $m,n \in \mathbb{Z}^+$.

مبرهنة ٣,١ إذا كانت f دالة ضربية فإن $\mathrm{f}(1) = 1$.

البرهان. لأن f ضربية فإن $\mathrm{f}(n) = \mathrm{f}(n) \cdot \mathrm{f}(1)$ لكل $n \in \mathbb{Z}^+$. ولأنها غير صفرية فإنه يوجد عدد n بحيث $\mathrm{f}(n) \neq 0$ وبالتالي فإن $\mathrm{f}(1) = 1$.

تعريف

نعرف الدالتان

- عدد قواسم n $\qquad \sigma(n) = \sum_{d|n} d$
- مجموع قواسم n $\qquad \tau(n) = \sum_{d|n} 1$

مبرهنة ٣,٢ إذا كانت g دالة ضربية فإن الدالة: $\mathrm{f}(n) = \sum_{d|n} \mathrm{g}(d)$ هي أيضا ضربية.

البرهان. لنعتبر $m_1, m_2 \in \mathbb{Z}^+$ بحيث $(m_1, m_2) = 1$. لكل قاسم d للعدد $m = m_1 m_2$ يوجد عددان وحيدان $d_1 \mid m_1$ و $d_2 \mid m_2$ بحيث $d = d_1 d_2$. لذا

$$\begin{aligned}
\mathrm{f}(m_1 m_2) &= \sum_{d|m_1 m_2} \mathrm{g}(d) = \sum_{d_1|m_1} \sum_{d_2|m_2} \mathrm{g}(d_1 d_2) \\
&= \sum_{d_1|m_1} \sum_{d_2|m_2} \mathrm{g}(d_1)\mathrm{g}(d_2) && \text{لأن g ضربية} \\
&= \left(\sum_{d_1|m_1} \mathrm{g}(d_1)\right)\left(\sum_{d_2|m_2} \mathrm{g}(d_2)\right) \\
&= \mathrm{f}(m_1)\mathrm{f}(m_2)
\end{aligned}$$

مبرهنة٣,٣ الدالتان τ و σ ضربيتان.

البرهان. حيث أن $\mathrm{g}(n) = 1$ و $\mathrm{h}(n) = n$ دالتان ضربيتان، باستخدام المبرهنة السابقة نجد أن الدالتان

$$\sum_{d|n} \mathrm{g}(n) = \sum_{d|n} 1 = \tau(n)$$
$$\sum_{d|n} \mathrm{h}(n) = \sum_{d|n} n = \sigma(n)$$

ضربيتان.

بواسطة الاستقراء الرياضي يمكن إثبات

مبرهنة٣,٤ إذا كانت f دالة ضربية وكانت $n_1, n_2, \ldots, n_k \in \mathbb{Z}^+$ أولية نسبيا مثنى مثنى فإن

$$\mathrm{f}(n_1 \cdot n_2 \cdot \ldots \cdot n_k) = \mathrm{f}(n_1) \cdot \mathrm{f}(n_2) \cdot \ldots \cdot \mathrm{f}(n_k)$$

مبرهنة٣,٥ إذا كان $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ فإن

$$\tau(n) = \sum_{i=1}^{r} (k_i + 1)$$
$$\sigma(n) = \prod_{i=1}^{r} \left(\frac{p_i^{k_i+1} - 1}{p_i - 1} \right)$$

البرهان. لاحظ أن قواسم العدد $p_i^{k_i}$ هي: $1, p_i, p_i^2, \ldots, p_i^{k_i}$

عددها: $\tau\left(p_i^{k_i}\right) = (k_i + 1)$

مجموعها: $\sigma\left(p_i^{k_i}\right) = \frac{p_i^{k_i+1} - 1}{p_i - 1}$ (متتالية هندسية حدها الأول 1 وحدها الأخير $p_i^{k_i}$)

وبما أن τ و σ ضربيتان فمن المبرهنة السابقة ينتج المطلوب.

٣,١,٢ الأعداد التامة Perfect Numbers

تعريف

نقول إن العدد $n \in \mathbb{Z}^+$:

- **عددا تاما**: إذا كان $\sigma(n) = 2n$ مثل 6 و 28
- **عددا ناقصا**: إذا كان $\sigma(n) < 2n$ مثل 14
- **عددا زائدا**: إذا كان $\sigma(n) > 2n$ مثل 12

المبرهنة التالية تقدم قاعدة للأعداد التامة الزوجية.

مبرهنة٣,٦ ليكن m زوجيا موجبا. m عدد تام $\Leftrightarrow$ $m = 2^n\left(2^{n+1} - 1\right)$ حيث $2^{n+1} - 1$ عدد أولي.

البرهان. لنفرض أن $m = 2^n\left(2^{n+1} - 1\right)$ بحيث $2^{n+1} - 1$ أولي.

$$\sigma(m) = \sigma\left(2^n\left(2^{n+1}-1\right)\right) = \sigma(2^n)\sigma\left(2^{n+1}-1\right) = \left(2^{n+1}-1\right)\left[\left(2^{n+1}-1\right)+1\right] = 2m$$

لبرهان العكس نفرض أن m تام. لنكتب $m = 2^n b$ حيث $n > 1$ و b عدد فردي. بما أن m تام لدينا

$$2^{n+1}b = 2m = \sigma(m) = \sigma(2^n)\sigma(b) = \left(2^{n+1}-1\right)\sigma(b)$$

وحيث أن $\left(2^n, 2^{n+1}-1\right) = 1$ لابد أن $2^{n+1} \mid \sigma(b)$ أي يوجد c بحيث $\sigma(b) = 2^{n+1}c$. هذا يعني أن

$$b = \left(2^{n+1}-1\right)c \text{ ، } m = 2^n\left(2^{n+1}-1\right)c$$

نثبت الآن أن $c = 1$. لو فرضنا أن $c \neq 1$ فإن b له على الأقل 3 قواسم 1 و c و b. هذا يعني أن

$$\sigma(b) \geq 1 + c + b = 1 + c + c\left(2^{n+1}-1\right) = 1 + c2^{n+1} > \sigma(b)$$

وهذا تناقض. إذن $b = \left(2^{n+1}-1\right)$ ، $\sigma(b) = 2^{n+1}$ ، $m = 2^n\left(2^{n+1}-1\right)$

ويبقى إثبات أن $2^{n+1}-1$ أولي. لو فرضنا أن $k \mid 2^{n+1}-1$ حيث $1 < k < 2^{n+1}-1$ لأصبح

$$2^{n+1} = \sigma\left(2^{n+1}-1\right) \geq 1 + k + 2^{n+1} - 1 = k + 2^{n+1} > 2^{n+1}$$

وهذا تناقض.

- تسمى الأعداد $2^k - 1$ ، $k \in \mathbb{Z}^+$ أعداد مرسين.
- إذا كان العدد $2^k - 1$ أولي فإن k أولي. أما فليس صحيحا فمثلا $2^{11} - 1 = 23 \cdot 89$.
- يوجد تقابل بين الأعداد الزوجية التامة وأعداد مرسين الأولية.
- من المحتمل أن أعداد مرسين الأولية غير منتهية ولكن لا يوجد برهان حتى الآن.
- هناك العديد من طرق اختبار أولية عدد مرسين $2^p - 1$. منها المبرهنة التالية:

مبرهنة٣,٧ ليكن p أوليا فرديا. إذا كان q قاسما أوليا للعدد $2^p - 1$ فإن $q = 2kp + 1$ حيث $k \in \mathbb{Z}^+$.

البرهان. بما أن $q \mid 2^{q-1} - 1$ (مبرهنة فيرما الصغرى) فإن

$$\left(2^{q-1}-1, 2^p-1\right) > 1 \Leftrightarrow 2^{(q-1,p)} - 1 > 1 \Leftrightarrow (q-1,p) > 1 \Leftrightarrow (q-1,p) = p \Leftrightarrow p \mid q-1$$

وبالتالي يوجد $m \in \mathbb{Z}^+$ بحيث $q = mp + 1$ ، ولأن q فردي فلابد أن m زوجي أي $m = 2k$ و $k \in \mathbb{Z}^+$.

مثال١ أثبت أن $M_{13} = 8191$ أولي.

الحــل حيث $\sqrt{8191} < 91$ ، من المبرهنة السابقة يكفي التحقق من قابلية القسمة على الأعداد الأولية من الصورة $q = 26k + 1$ وهي 53 و 79. بما أن $53 \nmid 8191$ و $79 \nmid 8191$ فإن M_{13} أولي.

٣,١,٣ د الــة أو يــلـر Euler's φ-Function

ندرس الآن دالة أويلر بتفصيل أكثر. رأينا فيما سبق تحقق الخواص

- ❖ لأي $n \in \mathbb{Z}^+$: $\varphi(n) = |\{k \in \{1,2,\dots,n-1\} : (k,n) = 1\}|$
- ❖ n أولي $\Leftrightarrow \varphi(n) = n-1$.

تمهيدية(١) الدالة φ ضربية.

البرهان. ليكن $m,n \in \mathbb{Z}^+$ حيث $(m,n) = 1$. لنعتبر نظام الرواسب التام المعتاد قياس كل من m و n و mn:

$$A' = \{0,1,\dots,m-1\}, \qquad B' = \{0,1,\dots,n-1\}, \qquad C' = \{0,1,\dots,mn-1\}$$

ولنرمز لأنظمة الرواسب المختزلة قياس هذه الأعداد $A \subseteq A'$ ، $B \subseteq B'$ ، $C \subseteq C'$. من التعريف

$$|A| = \varphi(m) \qquad |B| = \varphi(n) \qquad |C| = \varphi(mn)$$

لإثبات $\varphi(mn) = \varphi(m)\varphi(n)$ سوف ننشئ تقابلا بين $A \times B$ و C. لنفرض $c \in C'$ يطابق $a \pmod m$ a ويطابق b قياس n، لاحظ أن

$$c \in C \Leftrightarrow (c,mn) = 1 \Leftrightarrow (c,m) = 1,(c,n) = 1 \Leftrightarrow (a,m) = 1,(b,n) = 1 \Leftrightarrow a \in A, b \in B$$

وعليه نعرف التطبيق

$$f : C \to A \times B$$
$$f(c) = (a,b) \Leftrightarrow c \equiv a \pmod m, c \equiv b \pmod n$$

- ❖ f أحادية: لنفرض أن $c_1,c_2 \in C$ بحيث $f(c_1) = f(c_2)$. هذا يعني أن

$$c_1 \equiv c_2 \pmod m, c_1 \equiv c_2 \pmod n \Leftrightarrow c_1 \equiv c_2 \pmod{mn} \Leftrightarrow c_1 = c_2$$

- ❖ f شامل: لنفرض أن $(a,b) \in A \times B$. بما أن $(m,n) = 1$ فمن مبرهنة الباقي الصينية النظام

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

له حل وحيد قياس mn وليكن c. إضافة لذلك، لابد أن $c \in C$ (لماذا؟).

تمهيدية(٢) ليكن p أوليا، $\varphi\left(p^k\right) = p^k - p^{k-1}$.

البرهان. أولا نحسب عدد الأعداد m حيث $1 \le m \le p^k$ و $\left(m,p^k\right) > 1$.

$$\left(m,p^k\right) > 1 \Leftrightarrow p \mid m \Leftrightarrow m = rp, 1 \le r \le p^{k-1} \Leftrightarrow m \in \left\{p,2p,3p,\dots,p^{k-1}p\right\}$$

وهذه عددها p^{k-1}. نطرح هذا من العدد الإجمالي p^k (الأعداد من 1 إلى p^k) لنجد أن

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

مبرهنة٣,٢ إذا كان $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ تحليل n إلى قوى عوامله الأولية فإن

$$\begin{aligned}\varphi(n) &= \prod_{i=1}^{r} p_i^{k_i} - p_i^{k_i-1} \\ &= \prod_{i=1}^{r} p_i^{k_i-1}(p_i - 1) \\ &= \prod_{i=1}^{r} p_i^{k_i}\left(1-\frac{1}{p_i}\right) = n\cdot\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)\end{aligned}$$

مثال٢ جد أول خمس خانات عشرية في العدد $23145!$.

نحتاج $\varphi(100,000)$ وحيث

$$100,000 = 10^5 = 2^5\cdot 5^5 \Rightarrow \varphi(100,000) = \varphi\left(2^5\right)\varphi\left(5^5\right) = 2^5(2-1)\cdot 5^5(5-1)$$

مبرهنة٣,٩

$$n = \sum_{d|n}\varphi(d)$$

البرهان. لنضع $\mathrm{f}(n) = \sum_{d|n}\varphi(d)$. نعلم أن f ضربية ولذلك نحسب أولا

$$\mathrm{f}\left(p^k\right) = \sum_{d|p^k}\varphi(d) = \sum_{i=0}^{k}\varphi\left(p^i\right) = 1+\sum_{i=1}^{k}\left(p^i - p^{i-1}\right) = 1+(p-1)+\left(p^k-1\right) = p^k$$

ومن ضربية الدالة ينتج أن $\mathrm{f}(n) = n$.

الطريقة الثانية مبنية على محاولة تصنيف الأعداد 1 إلى n بواسطة القواسم كما يلي:

- خذ قاسما لـ n وليكن d مجموعة الأعداد c، $c \le n$ التي تشترك مع n في d بالضبط. أي تحقق $(c,n) = d$ ومنه $c = i\cdot d$ حيث $\left(i,\frac{n}{d}\right) = 1$.

$$A_d = \{1\le c\le n : (c,n) = d\} = \left\{c : c = i\cdot d, \left(i,\tfrac{n}{d}\right) = 1\right\}$$

ونلحظ التقابل $c \leftrightarrow i$ بين A_d والأوليات مع $\frac{n}{d}$ لذا فإن $|A_d| = \varphi\left(\frac{n}{d}\right)$، والآن

$$n = \sum_{d|n}|A_d| = \sum_{d|n}\varphi\left(\tfrac{n}{d}\right)$$

مع تغير d $\varphi\left(\frac{n}{d}\right)$

$$C = \left\{c_1, c_2, \ldots, c_{\varphi(mn)}\right\} \qquad B = \left\{b_1, b_2, \ldots, b_{\varphi(n)}\right\} \qquad A = \left\{a_1, a_2, \ldots, a_{\varphi(m)}\right\}$$

٣,١,٤ صيغة موبياس للتعاكس

لنعرف الدالة $\omega(n)$ عدد القواسم الأولية لـ n.

دالة موبياس μ :

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & , \quad \text{خالية مــن المربعــات} \quad n \\ 0 & , \quad \text{ما عدا ذلك} \end{cases}$$

مبرهنة١٠,٣ الدالة μ ضربية، كما أنها تحقق $\sum_{d|n} \mu(d) = \begin{cases} 1 & , n = 1 \\ 0 & n > 1 \end{cases}$.