الأربعاء 13/5/2015

المحاضرة السادسة عشرة

تعريف مجموعة البواقي المختزلة

إذا كانت مجموعة البواقي التامة بالقياس m هي:

$$A = \{0, 1, 2, \ldots, m-1\}$$

فإن مجموعة البواقي المختزلة بالقياس m هي المجموعة الجزئية T من A التي تحوي الأعداد الأولية نسبياً مع m.

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

مثال:

إذا كانت $m = 6 \Leftarrow A = \{0, 1, 2, 3, 4, 5\}$

$(0, 6) = 6$; مجموعة البواقي المختزلة بالقياس 6 $T = \{1, 5\}$

مثال:

$$A(12) = \{0, \mp 1, \mp 2, \mp 3, \mp 4, \mp 5, \mp 6\}$$

هي مجموعة بواقي تامة بالقياس 12.

فإن مجموعة البواقي المختزلة بالقياس 12 هي:

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

دالة أويلر:

تعريف:

من أجل أي عدد صحيح موجب m فإن قيمة $\varphi(m)$ تساوي عدد الأعداد الصحيحة الأولية مع m والتي لا تتجاوز m

أي $\varphi(m)$ تساوي عدد عناصر مجموعة البواقي المختزلة بالقياس m

مثال:

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

$\varphi(5)=4$, $\varphi(6)=2$, $\varphi(12)=4$

- إنّ دالة أولر $\varphi(n)$ هي دالة ضربية أي تحقق:

1) $\varphi(1)=1$

2) إذا كان $(n,m)=1$ فإنّ:

$$\varphi(n.m)=\varphi(n).\varphi(m)$$

مثال:

$$\varphi(12)=\varphi(4.3)=\varphi(3).\varphi(4)=2.2=4$$

وهي ليست ضربية تماماً.

مبرهنة:

إذا كان p عدداً أولياً فإنّ:

$$\varphi(p)=p-1$$

لذلك:

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

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

مبرهنة:

إذا كان p عدداً أولياً فإنّ:

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

البرهان:

إنّ مجموعة البواقي التامة للعدد p^a:

$$A=\{1,2,3,\dots,p,\dots,2p,\dots,p.p^{a-1}\}$$

عدد عناصر A هو p^a

فإن الأعداد التي ليست أولية مع p^a هي:

$$p, 2p, 3p, \ldots, p^{a-1}\cdot p$$

وعددها p^{a-1} نحذفها من المجموعة A، فيكون عدد الأعداد الأولية مع p^a في A هي:

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

مبرهنة:

إذا كان n عدداً صحيحاً موجباً $n>1$ وكان:

$$n = p_1^{a_1}\, p_2^{a_2} \cdots p_r^{a_r}$$

حيث p_i أعداد أولية مختلفة ; $a_i \in Z^+$ $(i=1,2,\ldots,r)$

فإن:

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

$$= n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$$

الإثبات: تحقق كون $\varphi(n)$ ضربية

مثال:

$$\varphi(360) = \varphi(2^3 . 3^2 . 5)$$

$$= 2^3 . 3^2 . 5\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 2^3 . 3^2 . 5\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$$

$$= 2^2 . 3 . 8 = 96$$

مبرهنة أويلر:

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

البرهان:

نأخذ مجموعة البواقي المختزلة بالقياس m:

$$T = \{a_1, a_2, \dots, a_{\varphi(m)}\}$$

كذلك تكون المجموعة:

$$T_1 = \{aa_1, aa_2, \dots, a.a_{\varphi(m)}\}$$

مجموعة بواقي مختزلة بالقياس m.

إن كل عنصر من T_1 أولي مع m كذلك يكون عناصر T_1 غير متطابقة بالقياس m لأنه لو كان لدينا عددين متطابقين بالقياس m

$$a.a_i \equiv aa_j \pmod m \quad ; \quad 1 \leq i < j \leq \varphi(m)$$

وبما أن $(a,m)=1$

$$\Rightarrow a_i \equiv a_j \pmod m$$

هذا تناقض كون a_i, a_j من T.

كل عنصر من T يطابق عنصر من T_1 بالقياس m كذلك جداء عناصر T تطابق جداء عناصر T_1 بالقياس m.

$$a_1 a_2 \cdots a_{\varphi(m)} \equiv a_1 . a_2 \cdots a_{\varphi(m)} \pmod m$$

ولما كان $(a_1, a_2, \dots, a_{\varphi(m)}, m) = 1$ حيث أن $(a,m)=1$

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

نتيجة:

إن مبرهنة فيرما الصغرى حالة خاصة من مبرهنة أويلر حيث $m = p$

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

تمرين:

أوجد رقمي الآحاد والعشرات للعدد 3^{256}

الحل:

إن العدد المؤلف من رقمي الآحاد والعشرات يساوي باقي قسمة 3^{256} على العدد 100

ملاحظة: لما كان $(3,100)=1$ فإن $3^{\varphi(100)} \equiv 1 \pmod{100}$

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 2^2 \cdot 5^2 \left(\frac{1}{2}\right)\left(\frac{4}{5}\right)$$
$$= 2 \cdot 4 \cdot 5 = 40$$
$$3^{40} \equiv 1 \pmod{100}$$

ولدينا $256 = (40)(6) + 16$ لذلك

$$3^{256} \equiv (3^{40})^6 \cdot 3^{16} \equiv (-19)^4 \pmod{100}$$
$$\equiv (361)^2 \equiv (61)^2 \equiv 3721 \equiv 21 \pmod{100}$$

الباقي هو 21 والرقمان الطرفيان يعطيان 21

تعريف:

إذا قسم العدد d جميع قواسم n فإن $\frac{n}{d}$ يقسم أيضاً جميع قواسم n لأنه من أجل كل $d \mid n$ نجد $n = d \cdot d_1$ و $d_1 = \frac{n}{d} \mid n$

مثال:

إن قواسم العدد 12 هي:

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

وقيم $\frac{n}{d}$ المقابلة لهذه القواسم هي:

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

الدالة الضربية τ:

تعريف:

الدالة τ دالة عددية قيمتها عند العدد $n \ni \mathbb{Z}^+$ هي عدد الأعداد التي تقسم n يمكن أن نكتب

$$\tau(n) = \sum_{d \mid n} 1 \qquad \text{(مجموع لما } d \mid n\text{)}$$

مثال:

$$\tau(12) = 6 \quad , \tau(1) = 1 \quad \tau(2) = 2 \quad , \tau(3) = 2$$
$$\tau(4) = 3 \quad , \quad \tau(5) = 2$$

مرهصة:

الدالة τ دالة ضربية.

البرهان

$$\tau(1) = 1$$

ونعلم أنه إذا كانت f دالة ضربية فإن الدالة المعرفة بـ $F(n) = \sum_{d|n} f(d)$ هي دالة ضربية

وإن الدالة $f(d) = 1$ أيًا كانت $d \geq 1$ دالة ضربية تمامًا لأن:

$$f(1) = 1$$

$$f(d_1 . d_2) = f(d_1) . f(d_2) . = 1 . 1 = 1$$

$\Rightarrow f(d) = 1$ ضربية $\Rightarrow$ $\tau(n) = \sum_{d|n} 1$ دالة ضربية

تعيين الدالة τ:

1) $\tau(p) = 2$ حيث p عدد أولي.

2) $\tau(p^a) = a+1$; مقاسم p^a هي $1, p, p^2, p^3, \dots, p^a$ عددهم هو $a+1$

3) $\tau(p_1^{a_1} . p_2^{a_2} \dots p_r^{a_r}) = (a_1+1)(a_2+1)\dots(a_r+1) = \prod_{i=1}^{r} (a_i+1)$

مثال:

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

24 مقاسم للعدد 360

انتهت المحاضرة ..