دالة فاي لأويلر ونظرية الباقي الصينية

Euler's Phi Function and the Chinese Remainder Theorem

إن صيغة أويلر :

$$a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$$

نتيجة جميلة وقوية، ولكن فائدتها ستكون محدودة بالنسبة لنا إلا إذا أوجدنا طريقة فعالة لحساب قيمة $\phi(m)$. طبعاً نحن لا نريد سرد جميع الأعداد من 1 إلى $m-1$ ومن ثم نتحقق من أن كل عدد أولي نسبياً مع m. هذا سيكون إضاعة كبيرة للوقت إذا كانت $m \approx 1000$ مثلاً، وسيكون مستحيلاً لـ $m \approx 10^{100}$. كما لاحظنا في الفصل الماضي، إحدى الحالات التي يمكن فيها حساب $\phi(m)$ بسهولة هي عندما يكون $m = p$ عدداً أوليًّا؛ لأنه عند ذلك فإن كل عدد صحيح $1 \le a \le p-1$ هو عدد أولي نسبياً مع m. لذلك؛ فإن $\phi(m) = p-1$.

يمكننا بسهولة اشتقاق صيغة مناسبة لـ $\phi\left(p^k\right)$ عندما $m = p^k$ قوة لعدد أولي. بدلاً من محاولة عد الأعداد بين 1 , p^k والتي تكون أولية نسبياً مع p^k ، سنبدأ بجميع الأعداد $1 \le a \le p^k$ ، وبعد ذلك نحذف الأعداد التي ليست أولية نسبياً مع p^k.

متى يكون عدد a ليس أولياً نسبياً مع p^k ؟ إن العوامل الوحيدة لـ p^k هي

عبارة عن قوى لـ p ؛ وعليه فإن a ليس أولياً نسبياً مع p^k تحديداً عندما يقبل a القسمة على p . بمعنى آخر،

$$\phi\left(p^k\right) = p^k - \#\left\{a : 1 \le a \le p^k \text{ and } p \mid a\right\}$$

وعليه ؛ فعلينا عد كم عدد صحيح بين 1 , p^k يقبل القسمة على p . إن هذا سهل، إنهم مضاعفات p :

$$p, 2p, 3p, 4p, \ldots, \left(p^{k-1} - 2\right)p, \left(p^{k-1} - 1\right)p, p^k$$

يوجد p^{k-1} من هذه الأعداد ، والتي تعطينا الصيغة :

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

مثلاً،

$$\phi\left(2401\right) = \phi\left(7^4\right) = 7^4 - 7^3 = 2058$$

p^j	q^k	$p^j q^k$	$\phi(p^j)$	$\phi(q^k)$	$\phi\left(p^j q^k\right)$
2	3	6	1	2	2
4	5	20	2	4	8
3	7	21	2	6	12
8	9	72	4	6	24
9	25	225	6	20	120

هذا يعني أنه يوجد 2058 عدد صحيح بين 1 , 2401 أولي نسبياً مع 2401.

عرفنا الآن كيف نحسب $\phi(m)$ عندما يكون m قوة لعدد أولي. سنفرض الآن أن m هو حاصل ضرب عددين كل منهما قوة لعدد أولي، $m = p^j q^k$. لنصيغ تخميناً، سنحسب $\phi(p^j q^k)$ لبعض القيم الصغيرة ونقارنها مع القيمتين $\phi(p^j)$ و $\phi(q^k)$.

من الجدول السابق نستطيع أن نخمن أن:

$$\phi(p^j q^k) = \phi(p^j)\phi(q^k)$$

بالإمكان أيضاً طرح بعض الأمثلة بأعداد ليست قوى أولية مثل:

$$\phi(14) = 6 \quad , \quad \phi(15) = 8 \quad , \quad \phi(210) = \phi(14 \cdot 15) = 48$$

كل ذلك يقود إلى التوقع بأن الادعاء التالي صحيح:

إذا كان $\gcd(m,n) = 1$ ، فإن $\phi(mn) = \phi(m)\phi(n)$.

قبل محاولة إثبات صحة قاعدة الضرب هذه، سنوضح كيف يمكن استخدامها لتسهيل حساب $\phi(m)$ لأي m ، أو بدقة أكثر، لأي m تستطيع تحليلها إلى حاصل ضرب أعداد أولية.

افرض أننا أُعطينا عدد m ، وافرض أننا حللنا m إلى حاصل ضرب أعداد أولية، ولنقل:

$$m = p_1^{k_1}, p_2^{k_2}, \ldots, p_r^{k_r}$$

حيث $p_1, p_2, \ldots, p_r$ جميعها أعداد مختلفة. أولاً سنستخدم قاعدة الضرب لحساب:

$$\phi\left(m\right)=\phi\left(p_1^{k_1}\right)\cdot\phi\left(p_2^{k_2}\right)\ldots\phi\left(p_r^{k_r}\right)$$

ثم نستخدم قاعدة القوة الأولية $\phi\left(p^k\right)=p^k\cdot p^{k-1}$ لنحصل على :

$$\phi\left(m\right)=\left(p_1^{k_1}-p_1^{k_1-1}\right)\cdot\left(p_2^{k_2}-p_2^{k_2-1}\right)\ldots\left(p_r^{k_r}-p_r^{k_r-1}\right)$$

هذه القاعدة تبدو معقدة، لكن الإجراء المستخدم لحساب $\phi\left(m\right)$ بسيط جداً. مثلاً،

$$\begin{aligned}\phi\left(1512\right)&=\phi\left(2^3\cdot3^3\cdot7\right)=\phi\left(2^3\right)\cdot\phi\left(3^3\right)\cdot\phi\left(7\right)\\&=\left(2^3-2^2\right)\cdot\left(3^3-3^2\right)\cdot\left(7-1\right)\\&=4\cdot18\cdot6\\&=432\end{aligned}$$

وعليه ؛ فإن هناك 432 عدد بين 1 , 1512 أولي نسبياً مع 1512.

أصبحنا الآن جاهزين لإثبات قاعدة الضرب لدالة فاي لأويلر. كما أننا سنعيد كتابة نص صيغة القوى الأولية لأنه من المناسب صياغتهما مع بعضهما البعض.

نظرية (١١,١) (صيغ دالة فاي)

a. *إذا كان* p *عدداً أولياً و* $k\geq1$ *؛ فإن* $\phi\left(p^k\right)=p^k-p^{k-1}$

b. *إذا كان* $\gcd\left(m,n\right)=1$ *؛ فإن* $\phi\left(mn\right)=\phi\left(m\right)\phi\left(n\right)$

البرهان

لقد أثبتنا صحة صيغة القوة الأولية (a) في بداية هذا الفصل، وعليه سنتحقق من صحة صيغة الضرب (b). سنفعل ذلك باستخدام واحدة من أقوى الأدوات المتاحة في نظرية الأعداد:

العـــــدّ

باختصار، سنهدف إلى إيجاد مجموعة تضم $\phi(mn)$ عنصراً ، وإيجاد مجموعة ثانية تضم $\phi(m)\phi(n)$ عنصراً. ثم سنثبت أن كلتا المجموعتين تضم نفس العدد من العناصر.

المجموعة الأولى هي :

$$\{a : 1 \le a \le mn \ \text{ and } \ \gcd(a, mn) = 1\}$$

من الواضح أن هذه المجموعة تضم $\phi(mn)$ عنصراً ؛ لأن هذه المجموعة ليست إلا تعريف

$\phi(mn)$. المجموعة الثانية هي :

$$\{(b,c) : 1 \le b \le m \ \text{ and } \ \gcd(b,m) = 1 \ \text{ and } 1 \le c \le n \ \text{ and } \ \gcd(c,n) = 1\}$$

كم زوج (b,c) يوجد في المجموعة الثانية؟حسناً، هناك $\phi(m)$ من الخيارات لاختيار b ؛ لأن هذا هو تعريف $\phi(m)$ ، وهناك $\phi(n)$ من الخيارات لاختيار c ؛ لأن هذا هو تعريف $\phi(n)$. لذا يوجد $\phi(m)$ خياراً لاختيار الإحداثي الأول b و $\phi(n)$ خياراً لاختيار الإحداثي الثاني c ، إذن يوجد $\phi(m)\phi(n)$ خياراً لاختيار الزوج (b,c).

على سبيل المثال، إذا أخذنا $m = 4 \ , \ n = 5$ ؛ فإن المجموعة الأولى ستضم الأعداد :

$$\{1,3,7,9,11,13,17,19\}$$

وهي الأعداد الأولية نسبياً مع 20. أما المجموعة الثانية ستضم :

$$\{(1,1),(1,2),(1,3),(1,4),(3,1),(3,2),(3,3),(3,4)\}$$

حيث العدد الأول من كل زوج أولي نسبياً مع 4 والعدد الثاني أولي نسبياً مع 5.

نعود الآن إلى الحالة العامة، سنقوم بأخذ كل عنصر من المجموعة الأولى ونربطه بزوج من المجموعة الثانية بالطريقة التالية :

$$\left\{ a : \begin{array}{l} 1 \le a \le mn \\ \\ \gcd(a, mn) = 1 \end{array} \right\} \to \left\{ (b,c) : \begin{array}{l} 1 \le b \le m, \ \gcd(b,m) = 1 \\ \\ 1 \le c \le n, \quad \gcd(c,n) = 1 \end{array} \right.$$

$$a \bmod mn \qquad \mapsto \qquad \big(a \bmod m, \ a \bmod n\big)$$

وهذا يعني أننا أخذنا عدداً صحيحاً a من المجموعة الأولى وربطناه بالزوج (b,c) بالعلاقة :

$$a \equiv b \big(\bmod m\big) \quad , \quad a \equiv c \big(\bmod n\big)$$

لنفهم ما سبق بوضوح سنعود إلى مثالنا السابق، حيث $m = 4$ و $n = 5$ ، فمثلاً، العدد 13 في المجموعة الأولى مرتبط بالزوج $(1,3)$ من المجموعة الثانية لأن :

$$13 \equiv 1 (\bmod 4) \quad , \quad 13 \equiv 3 (\bmod 5)$$

ونفعل ذلك مع كل عنصر من عناصر المجموعة الأولى لنحصل على :

$$\{1,3,7,9,11,13,17,19\} \rightarrow \{(1,1),(1,2),(1,3),(1,4),(3,1),(3,2),(3,3),(3,4)\}$$

$1 \mapsto (1,1)$ $\quad$ $11 \mapsto (3,3)$

$3 \mapsto (3,3)$ $\quad$ $13 \mapsto (1,3)$

$7 \mapsto (3,2)$ $\quad$ $17 \mapsto (1,2)$

$9 \mapsto (1,4)$ $\quad$ $19 \mapsto (3,4)$

في هذا المثال يمكنك أن ترى أننا قمنا بربط كل زوج في المجموعة الثانية بعدد واحد فقط في المجموعة الأولى. هذا يعني أن المجموعتين لهما نفس العدد من العناصر. نريد التأكد الآن أن هذا الربط يبقى صحيحاً في الحالة العامة.

نحتاج إلى التحقق من أن الجملتين التاليتين صحيحتان:

١- الأعداد المختلفة في المجموعة الأولى ترتبط مع أزواج مختلفة في المجموعة الثانية.

٢- كل زوج من المجموعة الثانية ارتبط بعدد من المجموعة الأولى.

عندما نتأكد من صحة هاتين الجملتين نكون قد تحققنا أن كلتا المجموعتين تضم نفس العدد من العناصر. ولكننا نعلم أن المجموعة الأولى تضم $\phi(mn)$ عنصراً والمجموعة الثانية تضم $\phi(m)\phi(n)$ عنصر. ولكي ننهي إثبات أن $\phi(mn)=\phi(m)\phi(n)$، علينا فقط التحقق من (1) و (2).

للتحقق من صحة (1)، لنأخذ العددين a_1 , a_2 من المجموعة الأولى، ولنفرض أن للعددين نفس الصورة في المجموعة الثانية. هذا يعني أن:

$$a_1 \equiv a_2 \pmod{m} \quad , \quad a_1 \equiv a_2 \pmod{n}$$

لـذلك، $a_1 - a_2$ يقبـل القسـمة علـى كـل مـن n, m. علـى أي حـال n, m عددان أوليان نسبياً؛ وعليه فإن $a_1 - a_2$ يقبل القسمة على mn. بكلمات أخرى،

$$a_1 \equiv a_2 \pmod{mn}$$

وهذا يعني أن a_2, a_1 هما نفس العنصر في المجموعة الأولى. وهذا ينهي التحقق من صحة العبارة (1).

للتحقق من صحة العبارة (2)، نحتاج إلى إثبات أن لأي قيمتين c, b يمكننا إيجاد -على الأقل- عدد صحيح واحد a يحقق

$$a \equiv b \pmod{m} \quad , \quad a \equiv c \pmod{n}$$

حقيقة أن هذين التطابقين المتزامنين(الآنيين) لهما حل، لها من الأهمية ما يبرر إعطاءها اسماً.

نظرية (٢, ١١) (نظرية الباقي الصينية)

ليكن m و n عددين صحيحين بحيث أن $\gcd(m,n) = 1$، وليكن b و c أي عددين صحيحين. عندئذ فإن التطابقين المتزامنين:

$$x \equiv b \pmod{m} \text{ و } x \equiv c \pmod{n}$$

لهما حل واحد فقط، بحيث $0 \le x < mn$.

البرهان

دعنا نبدأ، كما جرت العادة، بمثال. افرض أننا نريد حل :

$$x \equiv 8 \pmod{11} \text{ و } x \equiv 3 \pmod{19}$$

حل التطابق الأول يتكون من جميع الأعداد التي على الشكل $x = 11y + 8$. نعوض ذلك في التطابق الثاني ونبسط ونحاول الحل. لذلك:

$$11y + 8 \equiv 3 \pmod{19}$$
$$11y \equiv 14 \pmod{19}$$

نحن نعرف حل التطابق الخطي من هذا النوع (انظر نظرية التطابق الخطي في الفصل الثامن). الحل هو $y_1 \equiv 3 \pmod{19}$ ، بعد ذلك يمكننا إيجاد حل التطابق الأصلي باستخدام

$$x_1 = 11y_1 + 8 = 11 \cdot 3 + 8 = 41$$

أخيراً، للتحقق من صحة الحل:

$(41 - 8)/11 = 3$ و $(41 - 3)/19 = 2$. صح.

بالعودة إلى الحالة العامة، سنبدأ أيضاً بحل التطابق الأول $x \equiv b \pmod{m}$. الحل يتكون من جميع الأعداد التي على الصورة $x = my + b$. نعوض ذلك في التطابق الثاني فينتج أن :

$$my \equiv c - b \pmod{n}$$

ومعطى أن $\gcd(m, n) = 1$ ، إذن تخبرنا نظرية التطابق الخطي في الفصل الثامن أنه يوجد حل واحد فقط y_1 ، حيث $0 \leq y_1 < n$. فيكون حل التطابقين الأصليين هو :

$$x_1 = my_1 + b$$

وهذا الحل سيكون وحيداً بحيث $0 \le x_1 < mn$ ؛ لأنه يوجد y_1 واحدة فقط بين 0 , n ، وضربنا y_1 بـ m لنحصل على x_1. هذا يُكمل برهاننا لنظرية الباقي الصينية، وبالتالي ينهي برهان الصيغة $\phi(mn) = \phi(m)\phi(n)$.

فاصل تاريخي

إن أول تأريخ لنظرية الباقي الصينية يعود إلى أواخر القرن الثالث أو أوائل القرن الرابع الميلادي، عندما ظهرت في أحد الأعمال الرياضية الصينية. ما يثير الدهشة، أن هذه النظرية تعاملت مع أصعب مسألة بثلاثة تطابقات آنية.

" لدينا عدد من الأشياء، ولكن لا نعلم بالضبط كم عددها.إذا عددناها ثلاثة ثلاثة، سيتبقى اثنان. إذا عددناها خمسة خمسة، سيتبقى ثلاثة. إذا عددناها سبعة سبعة، سيتبقى اثنان. كم عدد هذه الأشياء؟"

Sun Tzu Suan Ching (Master Sun's Mathematical Manual)
Circa AD 300, volume 3, problem 26.

تمارين

(١١,١) (a) أوجد قيمة $\phi(97)$.

(b) أوجد قيمة $\phi(8800)$.

(١١,٢) (a) إذا كان $m \ge 3$ ، اشرح لماذا $\phi(m)$ دائماً عدد زوجي.

(b) $\phi(m)$ " عادة " ما يقبل القسمة على 4. صف جميع قيم m التي يكون عندها $\phi(m)$ لا يقبل القسمة على 4.

(١١,٣) افرض أن $p_1, p_2, \ldots, p_r$ أعداد أولية مختلفة تقسم m. بين أن الصيغة التالية لـ $\phi(m)$ صحيحة.

$$\phi\left(m\right)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right)$$

استخدم هذه الصيغة لحساب $\phi\left(1000000\right)$.

(١١,٤) اكتب برنامجاً لحساب $\phi\left(n\right)$ (قيمة دالة فاي لأويلر). يجب أن تحسب $\phi\left(n\right)$ بتحليل n إلى عواملها الأولية، وليس بإيجاد جميع قيم a الواقعة بين $1, n$ والتي تكون أولية نسبياً مع n.

(١١,٥) في كل فقرة مما يلي، أوجد x التي تمثل حلاً لنظام التطابقات(التطابقات الآنية) المعطاة:

(a) $x\equiv 5\left(\mathrm{mod}\,9\right)$ و $x\equiv 3\left(\mathrm{mod}\,7\right)$

(b) $x\equiv 1\left(\mathrm{mod}\,87\right)$ و $x\equiv 3\left(\mathrm{mod}\,37\right)$

(c) $x\equiv 8\left(\mathrm{mod}\,13\right)$ و $x\equiv 2\left(\mathrm{mod}\,12\right)$ و $x\equiv 5\left(\mathrm{mod}\,7\right)$

(١١,٦) حل مسألة الباقي الصينية الواردة قبل 1700 عام (التي أوردناها في الفاصل التاريخي).

(١١,٧) ذات يوم كان أحد المزارعين في طريقه إلى السوق ليبيع إنتاج مزرعته من البيض عندما سقط أحد النيازك على العربة وحطم كامل المحصول. ومن أجل تقديم طلب لشركة التأمين لتقوم بتعويضه عن خسارته، كان بحاجة إلى أن يعرف عدد البيض الذي تحطم. ولكنه كان يعرف أنه عندما عَدَّ البيض بيضتين بيضتين، بقيت عنده بيضه واحدة، عندما عده ثلاثاً ثلاثاً، بقيت عنده واحدة، عندما عده أربعاً أربعاً، بقيت عنده واحدة، عندما عده خمساً خمساً، بقيت عنده واحدة، عندما عده ستًّا ستًّا، بقيت عنده واحدة، ولكن عندما عده سبعاً سبعاً، لم يتبق عنده ولا بيضة. كم أقل عدد من البيض كان في العربة؟

(١١,٨) اكتب برنامجاً يأخذ كمدخل أربعة أعداد صحيحة (b,m,c,n) ، حيث $\gcd(m,n)=1$ ، ويوجد عدد صحيح x ، حيث $0 \le x \le mn$ يحقق

$$x \equiv b \pmod{m} \quad , \quad x \equiv c \pmod{n}$$

(١١,٩) في هذا التمرين سوف نبرهن إحدى نتائج نظرية الباقي الصينية لثلاثة تطابقات. ليكن m_1, m_2, m_3 أعداداً صحيحة موجبة، بحيث أن كل اثنين منها أوليان نسبياً. أي :

$$\gcd(m_1,m_2)=1 \quad , \quad \gcd(m_1,m_3)=1 \quad , \quad \gcd(m_2,m_3)=1$$

ليكن a_1, a_2, a_3 أي ثلاثة أعداد صحيحة. بيّن أنه يوجد عدد صحيح واحد فقط x في الفترة $0 \le x < m_1m_2m_3$ هو حل لنظام التطابقات الثلاثة التالية :

$$x \equiv a_1 \pmod{m_1} \quad , \quad x \equiv a_2 \pmod{m_2} \quad , \quad x \equiv a_3 \pmod{m_3}$$

هل تستطيع أن تكتشف كيف يمكن تعميم هذه المسألة بحيث تتعامل مع العديد من التطابقات

$$x \equiv a_1 \pmod{m_1} \ , \ x \equiv a_2 \pmod{m_2}, \ldots , \ x \equiv a_r \pmod{m_r} \ ؟$$

بشكل خاص، ما هي الشروط التي نحتاج تحققها على $m_1, m_2, \ldots, m_r$ ؟

(١١,١٠) ماذا تستطيع أن تقول عن n إذا كانت قيمة $\phi(n)$ عدداً أوليًّا؟ ماذا لو كانت مربع عدد أولي ؟

(١١,١١) (a) أوجد على الأقل خمسة أعداد صحيحة مختلفة n ، بحيث $\phi(n)=160$. كم عدداً آخر يمكن أن تجد؟

(b) افرض أن العدد الصحيح n يحقق $\phi(n)=1000$. اعمل قائمة بجميع الأعداد الأولية التي من المحتمل أنها تقسم n.

(c) استخدم المعلومة التي حصلت عليها من الفقرة (b) لإيجاد جميع الأعداد

الصحيحة n التي تحقق $\phi\left(n\right)=1000$.

(١١,١٢) أوجد جميع قيم n التي تمثل حلاً لكل معادلة من المعادلات التالية:

$$(a)\ \ \phi\left(n\right)=n/2 \qquad (b)\ \ \phi\left(n\right)=n/3 \qquad (c)\ \ \phi\left(n\right)=n/6$$

(مساعدة: الصيغة الواردة في التمرين 11.3 قد تكون مفيدة).

(١١,١٣) (a) لكل عدد صحيح $2\leq a\leq 10$ ، أوجد آخر أربع خانات للعدد a^{1000}.

(b) اعتماداً على خبراتك من الفقرة (a)، وخبراتك الأخرى إن استدعى الأمر، أعط معياراً بسيطاً يُمَكنُكَ من التنبؤ بآخر أربع خانات للعدد a^{1000} إذا علمت قيمة a.

(c) برهن أن معيارك الوارد في حل الفقرة (b) صحيح.