الفصل العاشر

التطابقات، القوى، وصيغة أويلر
Congruences, Powers, and Euler's Formula

في الفصل السابق قمنا بإثبات نظرية فيرما الصغرى والتي تنص على:

إذا كان p عدداً أولياً و $a \not| p$ ؛ فإن $a^{p-1} \equiv 1 \pmod{p}$. هذه القاعدة ليست صحيحة إذا استبدلنا p بعدد غير أولي. على سبيل المثال، $2^8 \equiv 4 \pmod{9}$ و $5^5 \equiv 5 \pmod{6}$.

هذا يدفعنا إلى التساؤل عن فيما إذا كان هناك بعض القوى قياس m بحيث $a^{???} \equiv 1 \pmod{m}$.

ملاحظتنا الأولى أن هذا مستحيل إذا كان $\gcd(a,m) > 1$. لنرى السبب، افرض أن $a^k \equiv 1 \pmod{m}$. فإن $a^k = 1 + my$ ، حيث y عدد صحيح ؛ وعليه فإن $\gcd(a,m)$ يقسم $a^k - my = 1$. بمعني، إذا وجدت قوة لـ a تطابق 1 قياس m ، فيجب أن يكون $\gcd(a,m) = 1$. نستنتج من النقاش السابق أننا نبحث عن مجموعة الأعداد التي تكون أولية نسبياً مع m ،

$$\left\{a : 1 \le a \le m \ , \ \gcd(a,m) = 1\right\}$$

على سبيل المثال :

m	$\{a : 1 \le a \le m \quad and \quad \gcd(a,m)=1\}$
1	$\{1\}$
2	$\{1\}$
3	$\{1,2\}$
4	$\{1,3\}$
5	$\{1,2,3,4\}$
6	$\{1,5\}$
7	$\{1,2,3,4,5,6\}$
8	$\{1,3,5,7\}$
9	$\{1,2,4,5,7,8\}$
10	$\{1,3,7,9\}$

عدد الأعداد الصحيحة بين 1 , m والتي هي أولية نسبياً مع m هو عدد مهم ؛ ولهذا سوف نعطي هذا المقدار اسماً :

$$\phi(m) = \# \left\{a : 1 \le a \le m \ , \ \gcd(a,m) = 1\right\}$$

الدالة ϕ تسمى "دالة فاي لأويلر" (*Euler's phi function*) . من خلال الجدول يمكننا قراءة قيم $\phi(m)$ حيث $1 \le m \le 10$.

m	1	2	3	4	5	6	7	8	9	10
$\phi(m)$	1	1	2	2	4	2	6	4	6	4

لاحظ أنه إذا كان p عدداً أوليًّا فإن أي عدد صحيح $1 \leq a < p$ هو عدد أولي نسبياً مع p. وعليه للأعداد الأولية لدينا الصيغة.

$$\phi\left(p\right) = p - 1$$

سنحاول محاكاة البرهان الذي استخدمناه لإثبات نظرية فيرما الصغرى. افرض مثلاً أننا نريد إيجاد قوة العدد 7 المطابقة لـ 1 قياس 10. بدلاً من أخذ جميع الأعداد $1 \leq a < 10$ ، سنقوم فقط بأخذ الأعداد الأولية نسبياً مع العدد 10. وهي :

$$1,3,7,9\left(\bmod 10\right)$$

إذا ضربنا كل واحد منهم بـ 7 ، نحصل على :

$$7 \cdot 1 \equiv 7 \,(\bmod 10), \qquad 7 \cdot 3 \equiv 1 (\bmod 10),$$
$$7 \cdot 7 \equiv 9 \,(\bmod 10), \qquad 7 \cdot 9 \equiv 3 \,(\bmod 10).$$

لاحظ أننا حصلنا مرة أخرى على نفس الأعداد ولكن بترتيب مختلف. وبالتالي إذا ضربناها مع بعضها سنحصل على نفس النتيجة.

$$\left(7 \cdot 1\right)\left(7 \cdot 3\right)\left(7 \cdot 7\right)\left(7 \cdot 9\right) \equiv 1 \cdot 3 \cdot 7 \cdot 9 \left(\bmod 10\right)$$
$$7^4 \left(1 \cdot 3 \cdot 7 \cdot 9\right) \equiv 1 \cdot 3 \cdot 7 \cdot 9 \left(\bmod 10\right)$$

الآن بالإمكان اختصار $1 \cdot 3 \cdot 7 \cdot 9$ من طرفي التطابق لنحصل على $7^4 \equiv 1\left(\bmod 10\right)$.

من أين أتى الأس 4 ؟ إنه يساوي عدد الأعداد الصحيحة بين 0 و 10 والتي تكون أولية نسبياً مع 10 ; بمعنى، أن الأس يساوي 4 ؛ لأن $4 = \phi\left(10\right)$. وهذا يوضح صحة الصيغة التالية.

نظرية (١٠,١) (صيغة أويلر)

إذا كان $\gcd(a,m)=1$ *؛ فإن :*

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

البرهان

الآن وقد حددنا المجموعة الصحيحة من الأعداد التي سنتعامل معها ، فإن برهان صيغة أويلر تقريباً يطابق برهان نظرية فيرما الصغرى. لذلك سنجعل :

$$1 \le b_1 < b_2 < \ldots < b_{\phi(m)} < m$$

هي الأعداد التي عددها $\phi(m)$ الواقعة بين 0 , m والتي تكون أولية نسبياً مع m .

نتيجة (١٠,٢)

إذا كان $\gcd(a,m)=1$ *؛ فإن الأعداد :*

$$b_1a, b_2a, b_3a, \ldots, b_{\phi(m)}a \pmod{m}$$

هي نفس الأعداد :

$$b_1, b_2, b_3, \ldots, b_{\phi(m)} \pmod{m}$$

على الرغم من أنها قد تختلف في الترتيب.

البرهان

نلاحظ أنه إذا كان b أوليًّا نسبياً مع m ؛ فإن ab أيضاً أولي نسبياً مع m . لذا فإن كل عدد في القائمة :

$$b_1a, b_2a, b_3a, \ldots, b_{\phi(m)}a \pmod{m}$$

مطابق لأحد الأعداد في القائمة :

$$b_1, b_2, b_3, \ldots, b_{\phi(m)} \pmod{m}$$

علاوة على ذلك يوجد $\phi(m)$ من الأعداد في كل قائمة. لذلك إذا استطعنا إثبات أن الأعداد في القائمة الأولى جميعها مختلفة قياس m ، إن هذا يعني أن القائمتين هما نفس القائمة (بعد إعادة الترتيب).

افرض أننا أخذنا عددين b_ja و b_ka من القائمة الأولى، وافرض أنهما متطابقان :

$$b_ja \equiv b_ka \pmod{m}$$

فيكون $m \mid (b_j - b_k)a$. ولكن a, m عددان أوليان نسبياً ؛ وعليه فإن $m \mid (b_j - b_k)a$. من ناحية أخرى، b_k , b_j يقعان بين 1 , m ، وهذا يعني أن $|b_j - b_k| \le m - 1$. يوجد عدد واحد فقط القيمة المطلقة له أقل من m ويقبل القسمة على m ، إن هذا الرقم هو الصفر.

لذلك ؛ فإن $b_j = b_k$. هذا يثبت أن الأعداد في القائمة :

$$b_1a, b_2a, b_3a, \ldots, b_{\phi(m)}a \pmod{m}$$

جميعها مختلفة قياس m ، وهذا ينهي إثبات صحة النتيجة.

باستخدام النتيجة السابقة بالإمكان بسهولة إتمام إثبات صيغة أويلر. النتيجة نصت على أن قائمتي الأعداد :

$$b_1a, b_2a, b_3a, \ldots, b_{\phi(m)}a \pmod{m}$$

و :

$$b_1, b_2, b_3, \ldots, b_{\phi(m)} \pmod m$$

هما نفس القائمة ، وعليه فإن حاصل ضرب الأعداد في القائمة الأولى هو نفس حاصل ضرب الأعداد في القائمة الثانية :

$$(b_1 a)\cdot(b_2 a)\cdot(b_3 a)\ldots\left(b_{\phi(m)} a\right) \equiv b_1 \cdot b_2 \cdot b_3 \ldots b_{\phi(m)} \pmod m$$

بالإمكان أخذ a كعامل مشترك من الطرف الأيسر للتطابق (عددهم $\phi(m)$) لنحصل على :

$a^{\phi(m)} B \equiv B \pmod m$ حيث $B = b_1 b_2 b_3 \ldots b_{\phi(m)}$.

أخيراً ، نلاحظ أن B أولي نسبياً مع m ؛ لأن كل واحد من $\left\{b_i, i = 1,\ldots,\phi(m)\right\}$ أولي نسبياً مع m . هذا يعني أننا نستطيع اختصار B من طرفي التطابق لنحصل على قاعدة أويلر :

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

تمارين

(١٠,١) ليكن $b_1 < b_2 < \cdots < b_{\phi(m)}$ أعداداً صحيحة بين $1, m$ وأولية نسبياً مع m (تتضمن العدد 1) ، وليكن $B = b_1 b_2 b_3 \cdots b_{\phi(m)}$ حاصل ضربهم . المقدار B ورد خلال برهان صيغة أويلر.

(a) بين أنه إما $B \equiv 1 \pmod m$ وإما $B \equiv -1 \pmod m$.

(b) احسب قيمة B عند بعض قيم m الصغيرة وحاول إيجاد نمط عندما يكون B مساوياً $+1 \pmod m$ وعندما يكون مساوياً $-1 \pmod m$.

(١٠,٢) العدد 3750 يحقق $\phi\left(3750\right)=1000$. (في الفصل القادم سوف نرى كيف نحسب $\phi\left(3750\right)$ بخطوات قصيرة جداً). أوجد عدد a له الخصائص الثلاث التالية:

(i) $a\equiv 7^{3003}\left(\bmod 3750\right)$

(ii) $1\le a\le 5000$

(iii) a لا يقبل القسمة على 7.

(١٠,٣) العدد غير الأولي m يسمى عدد كارمايكل (*Carmichael number*) إذا كان التطابق $a^{m-1}\equiv 1\left(\bmod m\right)$ صحيحاً لكل عدد a ، حيث $\gcd\left(a,m\right)=1$.

(a) تحقق من أن $m=561=3\cdot 11\cdot 17$ هو عدد كارمايكل. [مساعدة: ليس من الضروري أن تحسب قيمة $a^{m-1}\left(\bmod m\right)$ لجميع قيم a الـ 320 . بدلاً من ذلك، استخدم نظرية فيرما الصغرى لتتأكد من أن $a^{m-1}\equiv 1\left(\bmod p\right)$ لكل عدد أولي p يقسم m ، ومن ثم اشرح لماذا هذا يقتضي أن $a^{m-1}\equiv 1\left(\bmod m\right)$.]

(b) حاول إيجاد عدد كارمايكل آخر. هل تَظُن أن هناك عدداً لا نهائيًّا منها؟