الفصل التاسع

التطابقات، القوى، ونظرية فيرما الصغرى

Congruences, Powers, and Fermat's Little Theorem

خذ عدد a ، وانظر إلى قوى هذا العدد $a, a^2, a^3, \ldots\ldots$ قياس m.

هل يوجد نمط معين في هذه القوى؟ سنبدأ مع مقياس أولي $m = p$ ؛ لأن اكتشاف النمط يكون أسهل مع الأعداد الأولية. هذه حالة شائعة عند دراسة نظرية الأعداد، وخاصة عند دراسة التطابقات؛ لذلك عندما نريد اكتشاف نمط تطابق، فإنه من الطبيعي أن نبدأ بمقياس أولي.

a	a^2	a^3	a^4	a^5	a^6
0	0	0	0	0	0
1	1	1	1	1	1
2	4	3	1	2	4
3	4	2	1	3	4
4	1	4	1	4	1

a^k modulo 5

a	a^2	a^3	a^4
0	0	0	0
1	1	1	1
2	1	2	1

a^k modulo 3

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	1	2	4	1	2	4
3	2	6	4	5	1	3	2
4	2	1	4	2	1	4	2
5	4	6	2	3	1	5	4
6	1	6	1	6	1	6	1

a^k modulo 7

لكل من الأعداد الأولية $p = 7$, $p = 5$, $p = 3$ ، قمنا بعمل قائمة للأعداد الصحيحة $a = 0,1,2,\ldots$ وبعض قواها قياس p . قبل أن تسهب في القراءة، عليك أن تتوقف، اختبر تلك الجداول، وحاول تخمين بعض الأنماط. بعد ذلك تحقق من تخمينك بعمل جدول مشابه لـ $p = 11$ ، وتحقق من أن أنماطك ما زالت صحيحة.

عدد من الأنماط المثيرة يمكن رؤيتها في هذه الجداول. أحد هذه الأنماط والذي سوف ندرسه في هذا الفصل يمكن رؤيته في الأعمدة:

$$a^2 \pmod 3 \quad , \quad a^4 \pmod 5 \quad , \quad a^6 \pmod 7$$

كل مدخل من مدخلات هذه الأعمدة (بعيداً عن رأس العمود) يساوي 1. هل هذا النمط يظل متحققاً مع أعداد أولية أكبر؟ بإمكانك التحقق من ذلك باختبار الجدول الذي صنعته لـ $p = 11$ ، وستجد أن

$$1^{10} \equiv 1\big(\mathrm{mod}\,11\big) \ , \ 2^{10} \equiv 1\big(\mathrm{mod}\,11\big) \ , \ 3^{10} \equiv 1\big(\mathrm{mod}\,11\big) \ldots$$
$$9^{10} \equiv 1\big(\mathrm{mod}\,11\big) \ , \ 10^{10} \equiv 1\big(\mathrm{mod}\,11\big)$$

وهذا يقود إلى وضع التخمين التالي :

$$a^{p-1} \equiv 1 \pmod{p} \quad , \quad \forall \ 1 \leq a < p$$

بالطبع لسنا بحاجة لحصر a لتكون بين a و $p-1$. إذا كان الفرق بين a_1 , a_2 أحد مضاعفات p فإن قواها ستكون نفسها قياس p. وعليه فإن الشرط الحقيقي الذي يجب وضعه على a هو ألا يكون أحد مضاعفات p. أول من وضع هذه النتيجة هو "بيير دي فيرما" (Pierre de Fermat) في رسالة إلى (Frenicle de Bessy) عام 1640، ولكن فيرما لم يُشر إلى البرهان. أول برهان معروف لهذه النتيجة وضع من قبل "جوتفريد ليبنيز" (Gottfried Leibniz).[١]

نظرية (١, ٩) (نظرية فيرما الصغرى)

إذا كان p عدداً أولياً، و a أي عدد حيث $a \not\equiv 0 \pmod{p}$ ؛ فإن $a^{p-1} \equiv 1 \pmod{p}$.

قبل إعطاء البرهان لنظرية فيرما الصغرى، نود أن نوضح مدى أهميتها وكيف يمكن استخدامها لتبسيط الحسابات. وكمثال خاص لنأخذ التطابق :

$$6^{22} \equiv 1 \pmod{23}$$

هذا التطابق يقول إن العدد $6^{22} - 1$ أحد مضاعفات 23. إذا أردنا أن نتحقق من صحة هذه الحقيقة دون استخدام نظرية فيرما الصغرى، علينا أن نجد حاصل

---

(١) جوتفريد ليبنيز (1646-1716) هو أكثر من اشتهر باكتشافه لعلم التفاضل والتكامل.هو وإسحاق نيوتن عملا بشكل مستقل على النظريات الأساسية في التفاضل والتكامل وفي نفس الوقت. ولقد أمضى الرياضيون الألمان والإنجليز القرنين اللاحقين بالجدل حول لمن تعود أولوية الاكتشاف. الإجماع الحالي هو أن كل من ليبنيز ونيوتن يجب أن يعطى لقب مكتشف (مستقل) علم التفاضل والتكامل.

الضرب 6^{22} ، ونطرح منه 1 ، ونقسم الناتج على 23. وهذا ما ينتج لدينا :

$$6^{22}-1=23\cdot 5722682775750745$$

بالمثل إذا أردنا أن نثبت مباشرة أن $73^{100}\equiv 1\pmod{101}$ علينا أن نحسب $73^{100}-1$. لسوء الحظ، فإن العدد $73^{100}-1$ يتكون من 187 خانة! مع ملاحظة أننا في هذا المثال استخدمنا $p=101$ ، والذي يعتبر نسبياً عدداً أولياً صغيراً. إن نظرية فيرما الصغرى قدمت حقيقة مدهشة جداً حول الأعداد الكبيرة.

يمكننا استخدام نظرية فيرما الصغرى لتبسيط الحسابات. فمثلاً ، لحساب $2^{35}\pmod 7$ ، بإمكاننا استخدام حقيقة أن $2^6\equiv 1\pmod 7$. فنكتب $35=6\cdot 5+5$ ، ونستخدم قوانين الأسس لحساب :

$$2^{35}=2^{6\cdot 5+5}=\left(2^6\right)^5\cdot 2^5\equiv 1^5\cdot 2^5\equiv 32\equiv 4\pmod 7$$

بطريقة مشابهة افرض أننا نريد حل التطابق $x^{103}\equiv 4\pmod{11}$. بالتأكيد، $x\not\equiv 0\pmod{11}$ ؛ وعليه فإن نظرية فيرما الصغرى تخبرنا أن :

$$x^{10}\equiv 1\pmod{11}$$

برفع الطرفين للقوة العاشرة نحصل على :

$$x^{100}\equiv 1\pmod{11}$$

بضرب الطرفين بـ x^3 نحصل على :

$$x^{103}\equiv x^3\pmod{11}$$

وعليه لحل التطابق الأصلي يكفي أن نحل :

$$x^3 \equiv 4 \pmod{11}$$

وهذا تطابق يمكن حله بالمحاولة مرة بعد أخرى مع القيم $x = 1, x = 2, \ldots\ldots$

لذلك،

$x \pmod{11}$	0	1	2	3	4	5	6	7	8	9	10
$x^3 \pmod{11}$	0	1	8	5	9	4	7	2	6	3	10

وعليه؛ فإن $x \equiv 5 \pmod{11}$ هو حل التطابق $x^{103} \equiv 4 \pmod{11}$.

أصبحنا الآن جاهزين لتقديم الإثبات لنظرية فيرما الصغرى. لتوضيح طريقة البرهان، سنقوم أولاً بإثبات أن $3^6 \equiv 1 \pmod{7}$. طبعاً، لسنا مضطرين لإعطاء برهان ممتاز لهذه الحقيقة، حيث إن $3^6 - 1 = 728 = 7 \cdot 104$. مع ذلك، عند محاولة فهم برهان أو عند محاولة بناء برهان، فإنه غالباً ما يكون من المفيد استخدام أعداد محددة. طبعاً، الفكرة هي إنشاء برهان لا يعتمد على أعداد محددة ليكون البرهان صحيح بشكل عام.

لإثبات أن $3^6 \equiv 1 \pmod{7}$، سنبدأ بالأعداد:

$$1, 2, 3, 4, 5, 6,$$

اضرب كل واحد منها بالعدد 3، واختزل قياس 7. النتائج تظهر في الجدول التالي:

$x \pmod{7}$	1	2	3	4	5	6
$3x \pmod{7}$	3	6	2	5	1	4

لاحظ أن الأعداد $1,2,3,4,5,6$ تظهر مجدداً مرة واحدة بالضبط في الصف الثاني. وعليه إذا ضربنا جميع الأعداد في الصف الثاني مع بعضها، سنحصل على نفس النتيجة فيما لو ضربنا جميع أعداد الصف الأول مع بعضها. طبعاً يجب علينا العمل قياس 7. لذلك:

$$(3.1)\ (3.2)\ (3.3)\ (3.4)\ (3.5)\ (3.6) = 1.\ 2.\ 3.\ 4.\ 5.\ 6 \pmod 7$$

الأعداد في الصف الأول **الأعداد في الصف الثاني**

لتوفير الفراغ سنستخدم الرمز $n!$ والذي هو حاصل ضرب الأعداد $1,2,\ldots,n$، بمعنى آخر،

$$n! = 1\cdot 2\cdot 3\cdots\big(n-1\big)\cdot n$$

بأخذ 3 كعامل مشترك في العوامل الستة الموجودة في الطرف الأيسر من التطابق نحصل على:

$$3^6\cdot 6! \equiv 6! \big(\mathrm{mod}\, 7\big)$$

لاحظ أن $6!$ و 7 أوليان نسبياً، وبالتالي يمكننا اختصار $6!$ من طرفي التطابق. هذا يعطي $3^6 \equiv 1\big(\mathrm{mod}\, 7\big)$، وهذا بالضبط ما تنص عليه نظرية فيرما الصغرى.

نحن الآن جاهزون لإثبات نظرية فيرما الصغرى بشكل عام. إن أهم ملاحظة أثناء إثباتنا أن $3^6 \big(\mathrm{mod}\, 7\big)$ هي أن الضرب بـ 3 أدى إلى إعادة ترتيب الأعداد $1,2,3,4,5,6\big(\mathrm{mod}\, 7\big)$. وعليه سنقوم أولاً بإثبات الادعاء التالي:

الادعاء (٩,٢)

ليكن p عدداً أولياً وليكن a أي عدد بحيث $a \not\equiv 0\big(\mathrm{mod}\, p\big)$. عندئذ فإن الأعداد:

$$a, 2a, 3a, \ldots, (p-1)a \pmod{p}$$

هي نفس الأعداد :

$$1, 2, 3, \ldots, (p-1) \pmod{p}$$

مع إمكانية اختلافهم بالترتيب.

البرهان

القائمة $a, 2a, 3a, \ldots, (p-1)a$ تضم $(p-1)$ عدداً، وواضح أنه لا يوجد عدد فيها يقبل القسمة على p. افرض أننا أخذنا العددين ja , ka من هذه القائمة، وافرض أننا وجدنا أن هذين العددين متطابقان.

$$ja \equiv ka \pmod{p}$$

نستنتج من ذلك أن $p \mid (j-k)a$ ؛ وعليه فإن $p \mid (j-k)$ ، لأننا فرضنا أن p لا يقسم a. لاحظ أننا استخدمنا نظرية خاصية قابلية القسمة الأولية المبرهنة في الفصل السابع، والتي تنص على أنه إذا كان عدد أولي يقسم حاصل ضرب فإنه يقسم أحد عوامله. من جهة أخرى، نعرف أن $1 \le j, k \le p-1$ ؛ وعليه فإن $|j-k| < p-1$. يوجد هناك عدد واحد فقط يقبل القسمة على p ؛ حيث القيمة المطلقة له أقل من $p-1$ وهذا العدد هو الصفر. لذلك فإن $j = k$. هذا يبين أن مضاعفات العدد a في القائمة $a, 2a, 3a, \ldots, (p-1)a$ مختلفة قياس p.

لذلك أصبحنا نعرف الآن أن القائمة $a, 2a, 3a, \ldots, (p-1)a$ تضم $(p-1)$ عدداً مختلفاً غير صفري قياس p.

لكن نعرف أنه لا يوجد إلا $(p-1)$ عدد مختلف غير صفري قياس p وهي الأعداد $1,2,3,\ldots,(p-1)$. وعليه ؛ فإن القائمة $a,2a,3a,\ldots,(p-1)a$ والقائمة $1,2,3,\ldots,(p-1)$ يجب أن يكون لهما نفس الأعداد قياس p ، على الرغم من أنه قد يكون هناك اختلاف في الترتيب ، وهذا ينهي برهان الادعاء السابق.

باستخدام الادعاء ، من السهل إنهاء برهان نظرية فيرما الصغرى. نص الادعاء على أن قائمتي الأعداد :

$$a,2a,3a,\ldots,(p-1)a \pmod p \quad \text{و} \quad 1,2,3,\ldots,(p-1) \pmod p$$

هي نفس القائمة ؛ وعليه فإن حاصل الضرب في القائمة الأولى يساوي حاصل الضرب في القائمة الثانية :

$$a\cdot(2a)\cdot(3a)\ldots((p-1)a)\equiv 1\cdot 2\cdot 3\ldots(p-1)\pmod p$$

وعليه ؛ فإن

$$a^{p-1}\cdot(p-1)!\equiv(p-1)!\pmod p$$

أخيراً ، نلاحظ أن $(p-1)!$ أولي نسبياً مع p ، لذلك نستطيع اختصاره من طرفي المعادلة لنحصل على نظرية فيرما الصغرى.

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

يمكن استخدام نظرية فيرما الصغرى لإثبات أن عدداً ما هو عدد مؤلف دون أن نضطر إلى تحليله. فمثلاً :

$$2^{1234566}\equiv 899557\pmod{1234567}$$

وهذا يعني أن 1234567 لا يمكن أن يكون عدداً أولياً ؛ لأنه لو كان كذلك فإن نظرية فيرما الصغرى تخبرنا أن $2^{1234566}$ يطابق 1 قياس 1234567.[إذا كنت مندهشاً كيف أننا حسبنا $2^{1234566} \pmod{1234567}$ ، فلا تغضب ؛ سوف نشرح كيف فعلنا ذلك في الفصل السادس عشر] .يظهر من ذلك أن $1234567 = 127 \cdot 9721$ ؛ وعليه فإننا استطعنا في هذه الحالة إيجاد عامل. ولكن إذا أخذنا العدد $m = 10^{100} + 37$.

فعندما نحسب $2^{m-1} \pmod{m}$ سنحصل على :

$$2^{m-1} \equiv 362636032754586106248776019963358391083687325301915138012832082409112485946357945905973007023184439 7 \pmod{m}$$

مرة أخرى، نستنتج من نظرية فيرما الصغرى أن $10^{100} + 37$ ليس عدداً أولياً، ولكن ليس واضحاً تماماً كيف يمكن إيجاد عامل. سيكشف الكمبيوتر بشكل سريع أنه لا يوجد عوامل أولية أقل من 200,000. إنه من المدهش إلى حد ما أننا نستطيع بسهولة أن نعرف أن أعداداً ما هي أعداد مؤلفة وفي نفس الوقت نكون غير قادرين على إيجاد أي من عواملها.

تمارين

(٩,١) استخدم نظرية فيرما الصغرى لإنجاز المهام التالية :

(a) أوجد عدد $0 \leq a < 73$ حيث $a \equiv 9^{794} \pmod{73}$

(b) حل $x^{86} \equiv 6 \pmod{29}$

(c) حل $x^{39} \equiv 3 \pmod{13}$

(٩,٢) المقدار $(p-1)!\pmod p$ ظهر في برهاننا لنظرية فيرما الصغرى ، على الرغم من أننا لم نحتَج معرفة قيمته.

(a) إحسب $(p-1)!\pmod p$ عند بعض القيم الصغيرة لـ p ، أوجد نمطاً، واعمل تخميناً.

(b) برهن أن تخمينك صحيح. [حاول أن تكتشف لماذا للمقدار $(p-1)!\pmod p$ قيمة نفس قيمة p عندما تأخذ p قيماً صغيرة ، ومن ثم عمم ملاحظتك لإثبات هذه الصيغة لجميع قيم p].

(٩,٣) طلب منك التمرين 9.2 أن تحدد قيمة $(p-1)!\pmod p$ عندما يكون p عدداً أولياً .

(a) احسب قيمة $(m-1)!\pmod p$ عند بعض القيم الصغيرة غير الأولية لـ m. هل تجد نفس النمط الذي وجدته على الأعداد الأولية؟

(b) إذا كنت تعلم قيمة المقدار $(n-1)!\pmod p$ ، كيف تستطيع استخدام هذه القيمة لتحدد تماماً فيما إذا كان n أوليًّا أم لا ؟

(٩,٤) إذا كان p عدداً أولياً، وإذا كان $a \not\equiv 0 \pmod p$ ؛ فإن نظرية فيرما الصغرى تخبرنا أن $a^{p-1} \equiv 1 \pmod p$.

(a) التطابق $7^{1734250} \equiv 1660565 \pmod{1734251}$ صحيح، هل تستطيع أن تستنتج أن 1734251 عدد مؤلَف ؟

(b) التطابق $129^{64026} \equiv 15179 \pmod{64027}$ صحيح . هل تستطيع أن تستنتج أن 64027 عدد مؤلَف؟

(c) التطابق $2^{52632} \equiv 1 \pmod{52633}$ صحيح . هل تستطيع أن تستنتج أن 52633 عدد أولي ؟