الفصل السادس عشر

القوى قياس m والتربيعات المتعاقبة
Powers Modulo m and Successive Squaring

كيف يمكنك حساب $5^{100000000000000} \pmod{12830603}$ ؟

إذا كان 12830603 عدداً أوليًّا، فإنك قد تحاول استخدام نظرية فيرما الصغرى، وحتى لو لم يكن أوليًّا، فإنه يمكنك تطبيق صيغة أويلر (الفصل 10). في الحقيقة ؛ فإن $12830603 = 3571 \cdot 3593$

و

$$\begin{aligned}\phi(12830603) &= \phi(3571 \cdot 3593) \\ &= 3570 \cdot 3592 \\ &= 12823440\end{aligned}$$

وتخبرنا صيغة أويلر أن :

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

لأي a , m عندما $\gcd(a,m) = 1$ ، وعليه يمكننا الاعتماد على حقيقة أن :

$$100000000000000 = 7798219 \cdot 12823440 + 6546640$$

ولتبسيط مسألتنا فإن :

$$5^{100000000000000} = \left(5^{12823440}\right)^{7798219} \cdot 5^{6546640}$$
$$\equiv 5^{6546640} \left(\mathrm{mod}\ 12830603\right)$$

الآن بقي علينا حساب القوة 6546640 للعدد 5 ؛ ومن ثم حساب $5^{6546640} \left(\mathrm{mod}\ 12830603\right)$. لسوء الحظ فإن العدد $5^{6546640}$ له أكثر من 4 ملايين خانة، وعليه سيكون من الصعب علينا، إجراء هذه الحسبة حتى من خلال الكمبيوتر. وفيما بعد سوف نحتاج حساب $a^k \left(\mathrm{mod}\, m\right)$ لأعداد a , k و m لها مئات الخانات، وفي هذه الحالة فإن عدد خانات a^k أكبر من عدد جسيمات أجزاء الذرة في الكون المعروف! نحن بحاجة إلى إيجاد طريقة أفضل.

قد تتساءل عزيزي القارئ عن سر وجود الرغبة لحساب قوى كبيرة من هذا النوع.

أحد الجوانب الجوهرية لهذا الاهتمام هو القدرة على إنجاز عمليات حسابية تحوي أرقاماً كبيرة[1]، وهناك أسباب تطبيقية عديدة. كما سنرى لاحقاً، فإنه يمكن استخدام حساب $a^k \left(\mathrm{mod}\, m\right)$ لكتابة الرسائل بالشيفرة وحل هذه الشيفرة. ومن المثير للدهشة أن الشيفرات الناتجة عالية الفاعلية، ذلك أنها لا تُفَك حتى مع أكثر تقنيات فك الشيفرات تعقيداً المعروفة في وقتنا الحالي ؛ ولإثارة الفضول، سوف نركز فيما بقي من هذا الفصل على مناقشة كيفية حساب القوى الكبيرة والجذور الكبيرة بالنسبة لعدد m . بعد ذلك سوف نبين في الفصل الثامن عشر، كيف نستخدم مثل هذه الحسابات لتوليد شيفرات لا تُفَك (unbreakable codes).

---

(١) سؤال من الصف الرابع : "ماذا يفعل الرياضيون عند ضرب أعداد كبيرة؟".

إن الفكـرة الذكيـة المسـتخدمة في حسـاب $a^k \pmod m$ تسـمى "طريقـة التربيعـات المتعاقبـة" (*Method of Successive squaring*). وقبـل وصـف هـذه الطريقـة بشكل عام، سوف نقدم لها من خلال حساب:

$$7^{327} \pmod{853}$$

الخطـوة الأولى، هـي إنشـاء جـدول يعطـي قـيم $7, 7^2, 7^4, 7^8, 7^{16}, \ldots$ قيـاس العدد 853. لاحظ أنه للحصول على كل رقـم لاحـق في هـذه القائمـة، فإننـا نحتـاج إلى تربيـع العـدد السـابق. عـلاوة علـى ذلـك، بمـا أننـا دائمـاً نختـزل قيـاس العـدد 853 قبـل التربيع، فإننا لن نتعامل مـع أي عـدد أكبر مـن 852^2. الجـدول التـالي يـبين القـوى 2^k للعدد 7 قياس العدد 853.

$$\begin{aligned}
7^1 &\equiv 7 \equiv 7 \pmod{853}\\
7^2 \equiv (7^1)^2 &\equiv 7^2 \equiv 49 \equiv 49 \pmod{853}\\
7^4 \equiv (7^2)^2 &\equiv 49^2 \equiv 2401 \equiv 695 \pmod{853}\\
7^8 \equiv (7^4)^2 &\equiv 695^2 \equiv 483025 \equiv 227 \pmod{853}\\
7^{16} \equiv (7^8)^2 &\equiv 227^2 \equiv 51529 \equiv 349 \pmod{853}\\
7^{32} \equiv (7^{16})^2 &\equiv 349^2 \equiv 121801 \equiv 675 \pmod{853}\\
7^{64} \equiv (7^{32})^2 &\equiv 675^2 \equiv 455625 \equiv 123 \pmod{853}\\
7^{128} \equiv (7^{64})^2 &\equiv 123^2 \equiv 15129 \equiv 628 \pmod{853}\\
7^{256} \equiv (7^{128})^2 &\equiv 628^2 \equiv 394384 \equiv 298 \pmod{853}
\end{aligned}$$

الخطوة التالية، هي كتابة الأس 327 كمجموع قوى للعدد 2. هـذا الأسـلوب يسـمى "المفكـوك الثنـائي" (*binary expansion*) للعـدد 327. أكـبر قـوة للعـدد 2 أقـل من 327 هي $2^8 = 256$ ؛ لـذلك نكتب $327 = 256 + 71$. ومـن ثـم؛ فإن أكبر قوة للعدد 2 أقل من 71 هي $2^6 = 64$ ؛ لذلك $327 = 256 + 64 + 7$. وهكذا:

$$\begin{aligned} 327 &= 256+71 \\ &= 256+64+7 \\ &= 256+64+4+3 \\ &= 256+64+4+2+1 \end{aligned}$$

الآن، سوف نستخدم المفكوك الثنائي للعدد 327 لحساب:

$$\begin{aligned} 7^{327} &= 7^{256+64+4+2+1} \\ &= 7^{256}\cdot 7^{64}\cdot 7^{4}\cdot 7^{2}\cdot 7^{1} \\ &= 298\cdot 123\cdot 695\cdot 49\cdot 7 \pmod{853} \end{aligned}$$

الأرقام في السطر الأخير أخذت من جدول قوى العدد التي حسبت سابقاً.

لإتمام حساب $7^{327} \pmod{853}$ ، نحتاج فقط لإيجاد ناتج ضرب الأرقام الخمسة $298\cdot 123\cdot 695\cdot 49\cdot 7$ ومن ثم نختزلهم قياس 853. وإذا كان ناتج ضرب الأعداد الخمسة كبيراً جداً، فإننا يمكن أن نقوم بضرب أول عددين فقط مختزلة قياس 853 ، ثم تُضرب بالعدد الثالث ومن ثم تختزل قياس 853 ، وهكذا.عندما نستمر بهذا الأسلوب فإننا لا نحتاج أبداً للتعامل مع أي رقم أكبر من 852^2 . لذلك،

$$\begin{aligned} 298\cdot 123\cdot 695\cdot 49\cdot 7 &\equiv 828\cdot 695\cdot 49\cdot 7 \equiv 538\cdot 49\cdot 7 \\ &\equiv 772\cdot 7 \equiv 286 \pmod{853} \end{aligned}$$

وهو المطلوب!

هذا يبدو بالعمل المرهق، ولكن افترض بدلاً من ذلك أننا حاولنا حساب $7^{327} \pmod{853}$ مباشرة من خلال حساب 7^{327} أولاً ثم القسمة على 853 وأخذ الباقي. من الممكن أن يقوم كمبيوتر صغير بإنجاز هذا العمل، حيث :

$$7^{327} = 22236123868955180582 \underbrace{\ldots\ldots\ldots}_{237\ digits\ omitted} 32584937995509879543$$
$$\equiv 286 \pmod{853}$$

ولكن، كما ترى، فإننا حصلنا على أرقام ضخمة. وبذلك يكون من غير الممكن حساب a^k خصوصاً عندما يكون للعدد k ، مثلاً، 20 خانة، ناهيك عن كون العدد k له مئات الخانات لإنشاء شيفرات سرية.

من جهة أخرى، طريقة التربيعات المتعاقبة يمكن استخدامها لحساب $a^k \pmod{m}$ حتى لو كان للعدد k مئات أو ألوف الخانات، لأن تحليلاً متأنيًّا لهذه الطريقة يبين أنها تحتاج $\log_2(k)$ خطوة تقريباً لحساب $a^k \pmod{m}$. لن نتطرق لهذا التحليل هنا، ولكن سنلاحظ أن $\log_2(k)$ أكبر أو أقل من $3 \cdot 322$ مرة عدد خانات k. لذلك؛ إذا كان للعدد k 1000 خانة، مثلاً، فإننا بحاجة 3322 خطوة لحساب $a^k \pmod{m}$. واضح أن هذا العدد من الخطوات كبير جداً إذا ما أردنا إنجازه يدوياً، ولكن هذا عمل مقدور عليه حتى مع أبسط أجهزة الكمبيوتر. ولإعطائك فكرة عن الوقت اللازم لإنجاز هذه الخطوات، فإن كمبيوتري المحمول (بالمواصفات Pentium chip $1500\ MHz$ ، لهؤلاء الميالين لاستخدام التقنية) يستخدم التربيعات المتعاقبة لحساب:

$$7^{10^{200,000}} \equiv 787 \pmod{853}$$ في 0.36 ثانية

و

$$7^{10^{2,000,000}} \equiv 303 \pmod{853}$$ في 4.48 ثانية.

سنعرض الآن الطريقة العامة لحساب القوى باستخدام التربيعات المتعاقبة.

خوارزمية (١٦,١). (التربيعات المتعاقبة لحساب $a^k \pmod{m}$)

الخطوات التالية تحسب قيمة $a^k \pmod{m}$:

1. نكتب k كمجموع قوى للعدد 2

$$k = u_0 + u_1 \cdot 2 + u_2 \cdot 4 + u_3 \cdot 8 + \cdots + u_r \cdot 2^r \ ,$$

حيث أي u_i إما تساوي 0 وإما تساوي 1. (هذا يسمى المفكوك الثنائي للعدد k).

2. أنشئ جدولاً لقوى العدد a قياس m باستخدام التربيعات المتعاقبة.

$$\begin{aligned}
a^1 &\equiv A_0 \pmod m \\
a^2 \equiv \left(a^1\right)^2 &\equiv A_0^2 \equiv A_1 \pmod m \\
a^4 \equiv \left(a^2\right)^2 &\equiv A_1^2 \equiv A_2 \pmod m \\
a^8 \equiv \left(a^4\right)^2 &\equiv A_2^2 \equiv A_3 \pmod m \\
&\vdots \qquad \vdots \\
a^{2^r} \equiv \left(a^{2^{r-1}}\right)^2 &\equiv A_{r-1}^2 \equiv A_r \pmod m
\end{aligned}$$

لاحظ أنه لحساب أي سطر من الجدول فإنك تحتاج فقط لأخذ آخر عدد في السطر السابق، ثم تربيعه، وبعد ذلك اختزاله قياس m . أيضاً لاحظ أن الجدول يحوي $r+1$ سطراً، حيث r هو أعلى أس للعدد 2 ظهر في المفكوك الثنائي للعدد k في الخطوة1.

3. الضرب

$$A_0^{u_0} \cdot A_1^{u_1} \cdot A_2^{u_2} \ldots A_r^{u_r} \pmod m$$

سيطابق $a^k \pmod m$. لاحظ أن أي u_i إما تساوي 0 وإما تساوي 1 ؛ وعليه فإن ذلك الرقم هو حاصل ضرب كل A_i لها u_i يساوي 1.

التحقق. نحسب:

$$a^k = a^{u_0+u_1\cdot 2+u_2\cdot 4+u_3\cdot 8+\cdots+u_r\cdot 2^r} \quad \text{باستخدام الخطوة1}$$

$$= a^{u_0}\cdot\left(a^2\right)^{u_1}\cdot\left(a^4\right)^{u_2}\ldots\left(a^{2^r}\right)^{u_r}$$

$$\equiv A_0^{u_0}\cdot A_1^{u_1}\cdot A_2^{u_2}\ldots A_r^{u_r} \pmod m \quad \text{باستخدام الجدول من الخطوة2.}$$

كما أشرنا سابقاً، حساب قوى كبيرة $a^k \pmod m$ يستخدم لإنشاء شيفرات سرية. لإيجاد هذه الشيفرات، فإنه من الضروري إيجاد بعض الأرقام الأولية الكبيرة، مثلاً الأعداد الأولية التي عدد خاناتها بين 100 و 200 خانة. هذا يطرح سؤالاً عن كيفية معرفتنا لعدد ما m فيما إذا كان أولياً أم لا. من الطرق المؤكدة ولكنها غير فعاله، هي محاولة قسمة m على كل عدد أصغر من أو يساوي $\sqrt{m}$ ، بعد ذلك نرى فيما إذا حصلنا على أي عوامل للعدد m. إذا لم نحصل على عوامل، فإن m عدد أولي.لسوء الحظ، هذه الطريقة غير عملية حتى مع الأرقام المعتدلة الحجم.

باستخدام التربيعات المتعاقبة ونظرية فيرما الصغرى (الفصل التاسع)، فإننا غالباً ما نستطيع أن نعرف أن عدد m يمكن تحليله إلى عوامل دون إيجاد أي من هذه العوامل! ولكن كيف. خذ أي رقم a أقل من m. في البداية احسب $\gcd(a,m)$. إذا كان أكبر من 1، عندها تكون قد أوجدت عاملاً من عوامل m، عندئذ m يمكن تحليله إلى عوامل وبذلك تم المطلوب. أما إذا كان $\gcd(a,m)=1$ ، فاستخدم التربيعات المتعاقبة لحساب $a^{m-1} \pmod m$.

نظرية فيرما الصغرى تقول إنه إذا كان m عدداً أوليًا؛ فإن الجواب سيكون 1 ، لذلك إذا كان الجواب أي عدد غير 1، فإنك تستنتج أن m يحلل إلى عوامل دون الحاجة لمعرفة أي منها.

إليك المثال التالي. باستخدام التربيعات المتعاقبة نحسب:

$$2^{283976710803262} \equiv 280196559097287 \pmod{283976710803263},$$

وعليه ؛ فإننا نستنتج أن 283976710803263 عدد غير أولي. في الحقيقة، فإن عوامله الأولية هي :

$$283976710803263 = 104623 \cdot 90437 \cdot 30013$$

الآن، افرض أن $m = 630249099481$. باستخدام التربيعات المتعاقبة نجد أن :

$$2^{630249099480} \equiv 1 \pmod{630249099481}$$

و

$$3^{630249099480} \equiv 1 \pmod{630249099481}$$

هل هذا يعني أن 630249099481 عدد أولي؟ ليس بالضرورة، لكن من المؤكد أنه يبدو كذلك. وإذا اختبرنا $a^{m-1} \pmod{m}$ لقيم a تساوي $11,7,3$ وحصلنا أيضاً على 1 ، عندئذ ستزيد قناعتنا بأن 630249099481 عدد أولي. باستخدام نظرية فيرما الصغرى بهذا الاتجاه، فإنه من غير الممكن البرهان بشكل قاطع أن عدد ما هو عدد أولي، لكن إذا كان $a^{m-1} \equiv 1 \pmod{m}$ لكثير من قيم a ، فإننا نتوقع بشكل كبير أن m في الحقيقة هو عدد أولي. إن هذا يبين كيف أن نظرية فيرما الصغرى والتربيعات المتعاقبة يمكن استخدامها لإثبات أن بعض الأرقام تحلل وكذلك كيف أننا يمكن أن نتوقع بشكل كبير أن البعض الآخر هو أعداد أولية.لسوء الحظ ، هناك بعض الأرقام m غير أولية و $a^{m-1} \equiv 1 \pmod{m}$ لجميع قيم a ، حيث $\gcd(a,m) = 1$. مثل هذه الأرقام m تسمى " أعداد كارميشيل" (*Carmichael*

numbers). أصغر عدد كارميشيل هو 561 ، وذلك كما رأينا في تمرين10.3 .سوف نبحث أكثر في أرقام كارميشيل واختبار الأولية في الفصل التاسع عشر.

تمارين

(١٦,١) استخدم طريقة التربيعات المتعاقبة لحساب القوى التالية :

$$(a)\ 5^{13} \pmod{23} \qquad (b)\ 28^{749} \pmod{1147}$$

(١٦,٢) دائماً ما عرضنا لك، خلال هذا الفصل، طريقة التربيعات المتعاقبة بهدف حساب $a^k \pmod{m}$ بفاعلية عالية، لكن هذه الطريقة تتضمن إنشاء جدول لقوى a قياس m .

(a) بين أن الخوارزمية التالية تعمل أيضاً على حساب $a^k \pmod{m}$. إن هذه الخوارزمية أكثر فاعلية من طريقة التربيعات المتعاقبة، وهي مناسبة جداً لتطبيقها من خلال الكمبيوتر.

(b) طبق الخوارزمية أعلاه على كمبيوترك باستخدام لغة كمبيوتر من اختيارك.

(c) استخدام برنامجك لحساب :

$$2^{1000} \pmod{2379} \quad \text{(i)}$$

$$567^{1234} \pmod{4321} \quad \text{(ii)}$$

$$47^{258008} \pmod{1315171} \quad \text{(iii)}$$

(١٦,٣) (a) احسب $7^{7386} \pmod{7387}$ باستخدام طريقة التربيعات المتعاقبة. هل العدد 7387 عدد أولي؟

(b) احسب $7^{7392} \pmod{7393}$ باستخدام طريقة التربيعات المتعاقبة. هل العدد 7393 عدد أولي؟

(١٦.٤) اكتب برنامجاً يفحص فيما إذا كان عدد n قابلاً للتحليل إلى عوامل أو أنه من المحتمل أن يكون أولياً كما يلي. اختر 10 أرقام عشوائياً $a_1, a_2, \ldots, a_{10}$ بين 2 و $n-1$ واحسب $a_i^{n-1} \pmod{m}$ لكل a_i. إذا كان $a_i^{n-1} \not\equiv 1 \pmod{n}$ لأي a_i ، اطبع الرسالة "n يحلل إلى عوامل". إذا كان $a_i^{n-1} \pmod{n}$ لكل a_i ، اطبع الرسالة "من المحتمل أن يكون n أوليًّا"

ادمج هذا البرنامج في برنامج التحليل إلى عوامل خاصتك (تمرين7.6) كطريقة لاختبار فيما إذا كان عدداً كبيراً أوليًّا أم لا.

(١٦.٥) احسب $2^{9990} \pmod{9991}$ باستخدام طريقة التربيعات المتعاقبة، واعتمد على إجابتك لتقول فيما إذا كنت تعتقد أن 9991 عدد أولي أم لا.