الفصل السابع عشر

حساب الجذور النونية (k^{th}) قياس m
Computing k^{th} Roots Modulo m

تعلمنا في الفصل السابق كيف نحسب القوى النونية قياس m عندما يكون k و m عددين كبيرين جداً. الآن سوف نتجه بالاتجاه المعاكس، حيث سنحاول حساب الجذور النونية قياس m. بمعنى آخر، افرض أننا أعطينا عدداً b، وطلب منا إيجاد حل التطابق:

$$x^k \equiv b \pmod{m}$$

قد نلجأ للتعويض $x = 0,1,2,\ldots$ حتى نجد الحل، لكن إذا كان m عدداً كبيراً، فإن هذا سيستغرق وقتاً طويلاً. لكن إذا عرفنا قيمة $\phi(m)$ فإننا نستطيع حساب الجذر k^{th} للعدد b قياس m ببساطة شديدة. كالعادة، سنقوم أولاً بشرح الطريقة بمثال.

لنبحث في حل التطابق:

$$x^{131} \equiv 758 \pmod{1073}$$

الخطوة الأولى، هي حساب $\phi(1073)$. يمكننا عمل ذلك باستخدام صيغ ϕ الواردة في الفصل الحادي عشر، وذلك من خلال تحليل 1073 إلى عوامله الأولية.

وهذا عمل بسيط ، حيث $1073 = 29.37$ ؛ وعليه :

$$\phi(1073) = \phi(29)\phi(37) = 28 \cdot 36 = 1008$$

الخطوة الثانية ، هي إيجاد حل صحيح (موجب) للمعادلة

$ku - \phi(m)v = 1$ ، أي للمعادلة $131u - 1008v = 1$.

نعلم أن حل هذه المعادلة موجود ، حيث :

$$\gcd(k, \phi(m)) = \gcd(131, 1008) = 1$$

ومن الطريقة الواردة في الفصل السادس فإننا نستطيع إيجاد الحل $u = 731$ و $v = 95$. بشكل أكثر دقة ، الطريقة المشروحة في الفصل السادس تعطي الحل :

$$131 \cdot (-277) + 1008 \cdot 36 = 1$$

لنحصل على قيم موجبة للمجهولين ، u , v سنصيغ الحل على الشكل :

$$u = -277 + 1008 = 731 \qquad , \qquad v = -36 + 131 = 95$$

المعادلة :

$$131 \cdot 731 - 1008 \cdot 95 = 1$$

تزودنا بمفتاح الحل للمسألة الأصلية.

سنأخذ الآن x^{131} ونرفعه إلى القوة u^{th} ، أي إلى القوة 731. لاحظ أن :

$$\left(x^{131}\right)^{731} = x^{131 \cdot 731} = x^{1+1008 \cdot 95} = x \cdot \left(x^{1008}\right)^{95}$$

لكن $\phi(1073) = 1008$ ، وصيغة أويلر (الفصل العاشر) تخبرنا أن :

$$x^{1008} \equiv 1 \pmod{1073}$$

وهـذا يعـني أن $\left(x^{131}\right)^{1008} \equiv x \pmod{1073}$. لـذلك إذا رفعنـا طـرفي التطابق $x^{131} \equiv 758 \pmod{1073}$ إلى القوة 731 ، سنحصل على :

$$x \equiv \left(x^{131}\right)^{731} \equiv 758^{731} \pmod{1073}$$

الآن نحن نحتاج فقط إلى استخدام طريقة التربيعات المتعاقبة (الفصل 16) لحساب العدد $758^{731} \pmod{1073}$. الجواب الذي توصلنا إليه هو $x \equiv 905 \pmod{1073}$.

أخيراً ، يمكننا استخدام التربيعات المتعاقبة للتحقق من أن 905^{131} هو في الحقيقة يطابق 758 قياس 1073.

سنعطي الآن الطريقة العامة لحساب الجذور قياس m .

خوارزمية (١٧,١). (**كيف نحسب الجذور النونية قياس m**)

ليكن b , k , m أعداداً صحيحة معطاة تحقق :

$$\gcd(b,m)=1 \qquad , \qquad \gcd\left(k,\phi(m)\right)=1$$

الخطوات التالية تعطي حل التطابق :

$$x^k \equiv b \pmod{m}$$

١- احسب $\phi(m)$ (انظر الفصل الحادي عشر).

٢- أوجد عددين صحيحين موجبين u , v يحققان المعادلة $ku - \phi(m)v = 1$. (انظر الفصل السادس). طريقة أخرى لعمل ذلك هي أن u عدد صحيح موجب يحقق $ku \equiv 1 \pmod{\phi(m)}$ ؛ وعليه فإن u هو معكوس k قياس $\phi(m)$.

3. احسب $b^u \pmod m$ باستخدام التربيعات المتعاقبة. (انظر الفصل السادس عشر). القيمة التي نحصل عليها تعطي الحل x.

لماذا؟ للإجابة، نحتاج فقط لاختبار فيما إذا كان $x=b^u$ يمثل حل للتطابق $x^k \equiv b \pmod m$.

$$
\begin{aligned}
x^k &= \left(b^u\right)^k && \left(\text{بتعويض } x=b^u \text{ في } x^k\right)\\
&= b^{uk}\\
&= b^{1+\Phi(m)v} && \left(\text{لأن } ku-\phi(m)v=1 \text{ من الخطوة } 2\right)\\
&= b\cdot\left(b^{\Phi(m)}\right)^v\\
&\equiv b \pmod m && \left(\text{لأن } b^{\Phi(m)} \equiv 1 \pmod m \text{ من صيغة أويلر (الفصل } 10)\right)
\end{aligned}
$$

وهذا تأكيد كامل على أن $x=b^u$ هو الحل المطلوب للتطابق $x^k \equiv b \pmod m$.

إن طريقة التربيعات المتعاقبة المشروحة في الفصل 16 يمكن تطبيقها دائماً لحساب قوى $a^k \pmod m$، حتى مع الأرقام الكبيرة جداً k, m. هل طريقتنا لإيجاد الجذور النونية قياس m لها نفس الفاعلية؟ بمعنى، ما مدى صعوبة تطبيقها لحل $x^k \equiv b \pmod m$؟ لنراجع الخطوات الثلاث بترتيب عكسي. الخطوة 3 تقول بحساب $b^u \pmod m$ باستخدام التربيعات المتعاقبة، ولهذا فهي لا تسبب أي مشكلة. الخطوة 2 تطلب منا حل $ku-\phi(m)v=1$. الطريقة المشروحة في الفصل6 لحل مثل هذه المعادلات هي أيضاً سهلة التطبيق، حتى مع القيم الكبيرة للعددين k و $\phi(m)$؛ لأنها تقوم على الخوارزمية الإقليدية.

أخيراً، نأتي إلى الخطوة 1 والتي تبدو بسيطة، والتي تهدف إلى إيجاد قيمة $\phi(m)$. إذا علمنا تحليل m إلى عواملها الأولية، عندئذ فمن السهل حساب $\phi(m)$ باستخدام الصيغ الواردة في الفصل الحادي عشر. على كل حال، إذا كان m عدد كبيراً جداً، فإنه من الصعب جداً، إن لم يكن مستحيلاً، تحليل m في مدة معقولة من الزمن. على سبيل المثال، لو طلب منك حل التطابق:

$$x^{3968039} \equiv 34781 \pmod{27040397}$$

إذا لم يكن لديك كمبيوتر، فإن هذا سيستغرق منك وقتاً ليس بالقصير لتكتشف أن العدد 27040397 يحلل إلى حاصل ضرب عددين أوليين: $27040397 = 4409.6133$ وعليه:

$$\phi(27040397) = 4408 \cdot 6132 = 27029856$$

بعد حساب $\phi(m)$، يمكننا تطبيق الخطوة 2،

$$3968039 \cdot 17881559 - 27029856 \cdot 2625050 = 1$$

بعد ذلك، ومن الخطوة 3:

$$x \equiv 34781^{17881559} \equiv 22929826 \pmod{27040397}$$

لتوجد بذلك الحل.

تخيل الآن لو أنني بدلاً من اختيار عدد m له 8 خانات، اخترت عددين أوليين p , q كل منهما له 100 خانة، واخترت m على أن يكون $m = pq$. عندئذ سيكون من المستحيل عليك حل التطابق $x^k \equiv b \pmod{m}$ إلا إذا قمت بإخبارك عن قيمة كل من p , q ؛ لأنك إذا لم تعلم بقيمة كل من p , q فإنك يجب أن تكون قادراً على إيجاد قيمة $\phi(m)$.

باختصار، فإن هذا الفصل يحوي طريقة عملية وفعالة لحل:

$$x^k \equiv b \pmod m$$

بشرط أن نكون قادرين على حساب $\phi(m)$. قد يبدو أن من سوء الحظ أن هذه الطريقة لا تعمل إذا لم نكن قادرين على حساب $\phi(m)$ ، لكن نقطة الضعف هذه هي بالتحديد ما سَيُستغل في الفصل القادم لبناء شيفرات سرية غاية في الإتقان.

تماريـــــــن

(١٧,١) حل التطابق $x^{329} \equiv 452 \pmod{1147}$. (مساعدة: 1147 عدد غير أولي)

(١٧,٢) (a) حل التطابق $x^{113} \equiv 347 \pmod{463}$.

(b) حل التطابق $x^{275} \equiv 139 \pmod{588}$.

(١٧,٣) في هذا الفصل بينا كيف نحسب الجذر النوني للعدد b قياس m ، لكن ربما تكون قد سألت نفسك فيما إذا كان للعدد b أكثر من جذر نوني. في الحقيقة فإن هذا ممكن! على سبيل المثال، إذا كان a جذراً تربيعيًّا للعدد b قياس m ، فمن الواضح أن $-a$ هو جذر تربيعي للعدد b قياس m .

(a) ليكن b , k , m أعداداً صحيحة بحيث:

$$\gcd(b,m)=1 \qquad , \qquad \gcd(k,\phi(m))=1$$

بين أن b لها جذر نوني وحيد قياس m .

(b) لو فرضنا أن $\gcd(k,\phi(m))>1$. بيّن أنه إما b ليس له جذر نوني قياس m ، وإما أن له جذرين نونيين على الأقل قياس m . (هذا سؤال صعب بالنسبة للمادة العلمية التي تلقيتها حتى الآن).

(c) إذا كان $m = p$ أوليًّا، انظر إلى بعض الأمثلة وحاول إيجاد صيغة لعدد الجذور النونية للعدد b قياس p (إعتبر أن له على الأقل جذراً واحداً).

(١٧,٤) طريقتنا في حل $x^k \equiv b \pmod m$ تقوم أولاً على إيجاد عددين صحيحين u , v يحققان المعادلة $ku - \phi(m)v = 1$ ، عندئذ يكون الحل هو $x \equiv b^u \pmod m$. على كل حال، نحن بينا فقط أن هذه الطريقة تعمل عندما يكون $\gcd(b,m) = 1$ ؛ لذلك استخدمنا صيغة أويلر $b^{\Phi(m)} \equiv 1 \pmod m$.

(a) إذا كان m هو حاصل ضرب أعداد أولية مختلفة، بين أن $x \equiv b^u \pmod m$ دائماً حل للتطابق $x^k \equiv b \pmod m$ ، حتى إذا كان $\gcd(b,m) > 1$.

(b) بيّن أن طريقتنا لا تجدي في حل التطابق $x^5 \equiv 6 \pmod 9$.

(١٧,٥) (a) حاول استخدام الطرق الواردة في هذا الفصل لحساب الجذر التربيعي للعدد 23 قياس 1279 . (1279 عدد أولي). ما هو الخطأ؟

(b) بشكل أكثر عمومية، إذا كان p عدداً أوليًّا فرديًّا، اشرح لماذا الطرق الواردة في هذا الفصل لا يمكن استخدامها لإيجاد جذور تربيعية قياس p . سوف نبحث في مسألة الجذور التربيعية قياس p في فصول لاحقة.

(c) بشكل أعم، اشرح لماذا طريقتنا في حساب الجذور النونية قياس m لا تعمل إذا كان $\gcd(k,\phi(m))$ أكبر من 1.

(١٧,٦) اكتب برنامجًا لحل $x^k \equiv b \pmod m$. أعط المستخدم ميزة تزويد البرنامج لعوامل m ليستخدمها في حساب $\phi(m)$.