الفصل الحادي عشر

موضوعات في الجبر ونظرية الأعداد
Topics in Algebra and Number Theory

يعتمد أمن أنظمة التعمية ذوات المفتاح المعلن على بعض مسائل نظرية الأعداد التي يعتقد أنها صعبة الحل. من هذه المسائل المشهورة مسألة تحليل الأعداد الصحيحة (FACTOR) ومسألة اللوغارتيم المنفصل (DLP):

FACTOR: جد تحليل العدد الصحيح الموجب n إلى عوامله الأولية.

DLP: ليكن p عدداً أولياً وليكن $\alpha \in \mathbb{Z}_p^*$ مولداً. إذا علمت $\alpha^x \pmod p$ فجد x.

وبتفصيل أكثر، تتطلب أي خطة تعمية للأنظمة ذوات المفتاح المعلن إلى مسألتين مترابطتين، إحداهما سهلة الحساب (التنفيذ) وأما الثانية فصعبة الحساب. على سبيل المثال، في مسألة تحليل الأعداد الصحيحة يكون من السهل نسبياً إيجاد حاصل الضرب $n = pq$ حيث p و q عددان أوليان ولكن المسألة العكسية وهي تحليل العدد n لإيجاد العددين الأوليين p و q فهي من المسائل غير المحلولة ويعتقد أنها صعبة حسابياً بصورة عامة.

نقدم في البنود التالية أربعة موضوعات هي الرواسب التربيعية، واختبار الأوليات، وتحليل الأعداد الصحيحة، واللوغاريتمات المنفصلة. هدفنا هو تقديم مادة

كافية من الجبر ونظرية الأعداد (وأيضاً خوارزميات نظرية الأعداد) لتكون أساساً لخطط تعمية أنظمة ذوات مفتاح معلن، ولذا لن يكون شرحنا لهذه المادة مفصلاً.

(١١,١) الخوارزميات، تعقد الحسابات، حساب التطابقات

Algorithms, Complexity, and Modular Arithmetic

نقدم في هذا البند عدداً من الخوارزميات لتنفيذ العمليات الحسابية على الأعداد الصحيحة حيث تقاس فعالية هذه الخوارزميات بدلالة عدد العمليات الثنائية اللازمة لتنفيذ الخوارزمية. على سبيل المثال، إذا كان x و y عددين، عدد المراتب الثنائية لكل منهما يساوي k فنحتاج لتنفيذ $x+y$ إلى عدد من المراتب الثنائية لا يزيد عن k ونحتاج عدد من المراتب لا يزيد عن k^2 لتنفيذ xy (يوجد على الأكثر $k-1$ عملية جمع كل منها تحتاج إلى عدد k من العمليات الثنائية على الأكثر). وهذا العدد من العمليات الثنائية هو الأسوأ الذي نحصل عليه لجميع الأعداد الصحيحة التي عدد مراتبها الثنائية لا يزيد عن k. نستخدم عدد العمليات الثنائية ليكون المقياس للزمن اللازم لتنفيذ الخوارزمية على مدخل طوله k. يعتمد في العادة حساب الزمن اللازم على سعة المدخل وغالباً ما يعبر عن ذلك باستخدام رمز O الكبير (big-oh). لتكن f و g متتاليتين معرفتين على الأعداد الصحيحة الموجبة. نقول إن $f = O(g)$ إذا وجد عددان c و n_0. بحيث يكون:

$$\text{لكل } n \geq n_0 \text{ لكل } \big|f(n)\big| \leq c\big|g(n)\big|.$$

على سبيل المثال، $f(n) = 3n^4 + 7n - 1 = O(n^4)$ ، $\log n = O(n^t)$ لكل $t > 0$. العبارة $f = O(1)$ تعني أن $|f|$ محدودة من الأعلى بثابت. في حالتي جمع وضرب عددين طول كل منهما k مرتبة ثنائية، يكون التعقد الحسابي هو $O(k)$ و $O(k^2)$

على التوالي. لاحظ أن العبارة $f(n) = O(2^n)$ لا تستبعد أن يكون $f(n) = O(n^2)$ وهي دالة تزايدها أبطأ بكثير من الدالة السابقة.

نقول إن خوارزمية لحساب عددين x و y طول كل منهما k هي خوارزمية حدودية (Polynomial time algorithm) إذا كان تعقدها الحسابي هو $O(k^t)$ حيث $t \in \mathbb{Z}$. سنعتبر الخوارزمية الحدودية على أنها خوارزمية فعالة (efficient) ولكن من المهم التنبيه أنه في بعض الأحيان تكون خوارزمية حدودية أبطأ من خوارزمية أسية لجميع قيم المدخلات المهمة.

لنفرض أن x و y عددان صحيحان حيث $0 \leq x, y \leq n$. عندئذ، يكون طول مدخل الخوارزمية هو عدد العمليات الثنائية $k = \lfloor \log_2 n \rfloor + 1$ في التمثيل الثنائي للعدد n. على وجه الخصوص، تكون الخوارزمية فعالة إذا كان زمن تنفيذها $O(k^t)$ وليس $O(n^t)$.

الأعداد الصحيحة

لنفرض أن $a, b \in \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$. نقول إن a يقسم b (a divides b) ونكتب $a \mid b$ إذا وجد عدد صحيح $c \in \mathbb{Z}$ حيث $b = ac$. على سبيل المثال، $-3 \mid 15$ لأن $15 = (-3)(-5)$، كما أن أي عدد صحيح يقسم العدد 0. إذا وجد قاسماً $a \notin \{\pm 1, \pm b\}$ للعدد b فنقول إن القاسم a غير تافه. نقول إن العدد الصحيح $a \geq 2$ عدد أولي (prime) إذا كانت جميع قواسمه تافهة، ويسمى العدد غير الأولي عدداً مؤلفاً (composite)، تقدم مبرهنة الأعداد الأولية (prime number theorem) تقريباً لعدد الأعداد الأولية $\pi(x)$ في الفترة $[2, x]$ وهذا التقريب هو $\pi(x) \sim x / \log x$. في الحقيقة هذا التقريب هو حد أدنى، على سبيل المثال، إذا كان $x = 10^3$ فيكون:

$$\pi(x) = 168 > x / \log x \approx 144 \cdot 8.$$

من السهل التحقق من صحة الخواص التالية (تمرين (١١,١,٩)):

١- إذا كان $a \mid b$ و $b \mid c$ فإن $a \mid c$.

٢- إذا كان $c \mid a$ و $c \mid b$ (أي c قاسم مشترك للعددين a وb) فإن $c \mid (ax + by)$ لكل $x, y \in \mathbb{Z}$.

٣- إذا كان $p \mid ab$ حيث p عدد أولي فإن $p \mid a$ أو $p \mid b$.

نقول إن العدد $d \geq 0$ هو القاسم المشترك الأكبر (greatest common divisor) للعددين a و b ويكتب $d = \gcd(a,b)$ أو $d = (a,b)$ إذا كان $c \mid d$ لجميع القواسم المشتركة c للعددين a و b. تضمن لنا خوارزمية إقليدس (Euclidean algorithm) التي نقدمها لاحقاً وجود القاسم المشترك الأكبر دائماً. من الممكن استخدام المبرهنة الأساسية في الحساب (يمكن كتابة أي عدد صحيح $a \geq 2$ بطريقة وحيدة باستثناء الترتيب كحاصل ضرب أعداداً أولية) لإيجاد القاسم المشترك الأكبر. فمثلاً، إذا كان $36 = 2^2 \cdot 3^2$ و $24 = 2^3 \cdot 3$ فنرى أن $(36,24) = 2^2 \cdot 3$.

إن مسألة تحليل العدد إلى حاصل ضرب عوامله الأولية تعدُّ من المسائل الصعبة ومع ذلك فمن الممكن إيجاد القاسم المشترك الأكبر دون الحاجة إلى التحليل. ولرؤية ذلك دعنا نقدم أولاً خوارزمية القسمة (division algorithm):

إذا كان $a, b \in \mathbb{Z}$ حيث $b \geq 1$ فمن الممكن استخدام القسمة المطولة لكتابة:

$$a = qb + r \quad \text{حيث} \quad 0 \leq r < b$$

العددان الصحيحان q (خارج القسمة) و r (الباقي ويكتب أحياناً $r = a \pmod b$) هما عددان وحيدان. تستخدم خوارزمية إقليدس الحقيقة $(a,b) = (b, a \pmod b)$ حيث $a > b > 0$ لإيجاد القاسم المشترك الأكبر.

خوارزمية (١١,١,١) خوارزمية إقليدس

المدخل: عددان صحيحان $a \geq b \geq 0$.

المخرج: القاسم المشترك الأكبر (a,b) للعددين a و b.

(١) ضع $r_0 = a$ و $r_1 = b$.

(٢) جد أول عدد صحيح $n \geq 0$ يحقق $r_{n+1} = 0$ حيث $r_{i+1} = r_{i-1} \pmod{r_i}$. أي أن r_{i+1} هو الذي نحصل عليه من خوارزمية القسمة $r_{i-1} = q_{i+1}r_i + r_{i+1}$.

(٣) $r_n = (a,b)$.

من الواضح أن خوارزمية إقليدس تتوقف دائماً لأن $0 \leq r_{i+1} < r_i$ لكل $i > 0$. في الحقيقة، $r_{i+2} < r_i / 2$ ومن ثم لا يمكن أن يزيد عدد عمليات القسمة عن $1 + 2\log_2 a$. عدد العمليات الثنائية لكل عملية قسمة هو $O(\log_2^2 a)$ ومن ثم يكون الزمن اللازم لتنفيذ خوارزمية إقليدس هو $O(\log_2^3 a)$ عملية ثنائية. ومن الممكن إثبات أن الزمن اللازم هو في الحقيقة $O(\log_2^2 a)$. وآيا كان الزمن المستخدم فخوارزمية إقليدس هي خوارزمية فعالة. التمرين (**١١,١,١١**) يثبت أن r_n هو بالفعل (a,b).

مثال (١١,١,٢)

في هذا المثال نستخدم خوارزمية إقليدس لحساب $(299,221)$ فنحصل على:

$$\begin{aligned} (q_2 = 1, r_2 = 78) \quad & 299 = 1 \cdot 221 + 78 \\ (q_3 = 2, r_3 = 65) \quad & 221 = 2 \cdot 78 + 65 \\ (q_4 = 1, r_4 = 13) \quad & 78 = 1 \cdot 65 + 13 \\ (q_5 = 5, r_5 = 0) \quad & 65 = 5 \cdot 13 + 0 \end{aligned}$$

وبهذا يكون $(299,221) = r_4 = 13$. ▲

من الممكن استخدام خوارزمية إقليدس لكتابة (a,b) كتركيب خطي للعددين a و b. أي إيجاد عددين $x,y \in \mathbb{Z}$ بحيث يكون $(a,b) = ax + by$. يتم ذلك بخطوات ارجاعية لخوارزمية إقليدس (انظر الملحق A للاطلاع على التفاصيل). أول خطوتان هما:

$$\begin{aligned} (a,b) = r_n &= r_{n-2} - q_n r_{n-1} \\ &= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\ &= (1 + q_n q_{n-1})r_{n-2} - q_n r_{n-3} \end{aligned}$$

ونحصل على (a,b) كتركيب خطي للعددين r_{n-2} و r_{n-3}.

تسمى هذه الطريقة خوارزمية إقليدس الموسعة حيث في الخطوة النهائية نحصل على (a,b) كتركيب خطي للعددين $r_0 = a$ و $r_1 = b$. وبتطبيق ذلك على المثال **(١١,١,٢)** نجد أن:

$$\begin{aligned}(299,221) = 13 &= 78 - 65\\ &= 78 - (221 - 2\cdot 78) = 3\cdot 78 - 221\\ &= 3(299 - 1\cdot 221) - 211 = 3\cdot 299 - 4\cdot 221\\ &= 3a - 4b\end{aligned}$$

حيث $a = 299$ و $b = 221$.

إذا كان $(a,b) = 1$ فنقول إن العددين a و b أوليان نسبياً (relatively prime). إذا كان $n \geq 1$ فعدد الأعداد الأولية نسبياً مع n في الفترة $[1,n]$ يرمز له بالرمز $\varphi(n)$ ويسمى دالة أويلر (Euler function). فمثلاً، $\varphi(6) = 2$ و $\varphi(p^i) = p^{i-1}(p-1)$ لكل عدد أولي p. دالة أويلر دالة ضربية. أي أن:

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ لكل } a,b \text{ حيث } (a,b) = 1.$$

على وجه الخصوص، $\varphi(pq) = (p-1)(q-1)$ لكل عددين أوليين p و q حيث $p \neq q$.

الأعداد الصحيحة قياس n

ليكن n عدد صحيح موجب. نقول إن a يطابق b قياس n ونكتب $a \equiv b \pmod n$ إذا كان $n \mid (a-b)$. فمثلاً، $14 \equiv 9 \pmod 5$، $-11 \equiv 3 \pmod 7$، $-1 \equiv n-1 \pmod n$. التطابق هو علاقة تكافؤ على مجموعة الأعداد الصحيحة $\mathbb{Z}$. أي أن العلاقة:

- انعكاسية: $a \equiv a \pmod n$ لكل $a \in \mathbb{Z}$.
- تناظرية: إذا كان $a \equiv b \pmod n$ فإن $b \equiv a \pmod n$.
- متعدية: إذا كان $a \equiv b \pmod n$ و $b \equiv c \pmod n$ فإن $a \equiv c \pmod n$.

إذا كان $a = qn + r$ حيث $0 \le r < n$ فنرى أن $a \equiv r \pmod{n}$. من ذلك نجد أن كل $a \in \mathbb{Z}$ يطابق عدداً وحيداً في الفترة $[0, n-1]$. يحتوي فصل التكافؤ أو فصل التطابق أو نظام الرواسب التام $[a]$ على جميع الأعداد الصحيحة التي تطابق a قياس n. سنرمز لجميع فصول التطابق المختلفة قياس n بالرمز $\mathbb{Z}_n$.

من السهل أن نرى أن عمليتي الجمع والضرب على $\mathbb{Z}_n$ المعرفتين على النحو التالي:

$$[a] + [b] = [a + b]$$
$$[a][b] = [ab]$$

حسنتا التعريف، أي إذا كان $a \equiv a' \pmod{n}$ و $b \equiv b' \pmod{n}$ فإن $a + b \equiv a' + b' \pmod{n}$ و $ab \equiv a'b' \pmod{n}$. يكون النظام $(\mathbb{Z}_n, +, \cdot)$ حلقة تحت عمليتي الجمع والضرب (تمرين (١١,١,١٢)). في العادة نكتب $\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$ عوضًا عن $\mathbb{Z}_n = \{[0],[1],\ldots,[n-1]\}$ حيث قابلنا بين العنصر a وفصل التكافؤ $[a]$.

ليكن $a \in \mathbb{Z}_n$. إذا وجد $x \in \mathbb{Z}_n$ حيث $ax \equiv 1 \pmod{n}$ فنقول إن a قابل للعكس (invertible) وأن x هو معكوس (نظير ضربي) للعدد a ونكتب $x = a^{-1}$. فمثلاً $2^{-1} = 5$ في الحلقة $\mathbb{Z}_9$ لأن $2 \cdot 5 \equiv 1 \pmod{9}$، أما الأعداد $\{0,3,6\}$ فليس لها معكوسات. إذا كان $a \in \mathbb{Z}_n$ قابلاً للعكس فنرى أن $ax \equiv 1 \pmod{n}$. أي أن $n \mid (ax - 1)$. ومن ذلك يكون $ax - ny = 1$ حيث $y \in \mathbb{Z}$. وبهذا يكون $(a,n) = 1$. وبالعكس، إذا كان $(a,n) = 1$ فيوجد $x, y \in \mathbb{Z}$ حيث $ax + ny = 1$. ومن ثم يكون $ax \equiv 1 \pmod{n}$. إذن، $a \in \mathbb{Z}_n$ قابل للعكس إذا وفقط إذا كان $(a,n) = 1$. وبهذه الحالة نستطيع استخدام خوارزمية إقليدس الموسعة لإيجاد معكوس a.

مثال (١١,١,٣)

لنفرض أن $a = 7$ و $n = 9$. العمود الأول من الجدول التالي يستخدم خوارزمية إقليدس ليبين أن $(7,9) = 1$ ومن ثم فللعدد a معكوس في الحلقة $\mathbb{Z}_9$. أما العمود الثاني فيجد $x, y \in \mathbb{Z}$ حيث $ax + ny = (a,n)$.

خوارزمية اقليدس الموسعة لكتابة $(a,n) = ax + ny$	خوارزمية اقليدس لإيجاد (a,n)
$1 = 7 - 3 \cdot 2$	$9 = 1 \cdot 7 + 2$
$= 7 - 3(9 - 1 \cdot 7)$	$7 = 3 \cdot 2 + 1$
$= 4 \cdot 7 - 3 \cdot 9$	$2 = 2 \cdot 1 + 0$

إذن، $7^{-1} = 4$ ومن السهل التحقق من أن $7 \cdot 4 \equiv 28 \equiv 1 (\mathrm{mod}\, 9)$. ▲

مجموعة جميع أعداد $\mathbb{Z}_n$ القابلة للعكس $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : (a,n) = 1\}$ زمرة تحت عملية الضرب عدد عناصرها يساوي $\varphi(n)$. فمثلاً، $\mathbb{Z}_{12}^* = \{1,5,7,11\}$، $\mathbb{Z}_p^* = \{1,2,\ldots p-1\}$ حيث p أولي. إذا كان p عدداً أولياً وكان $a \in \mathbb{Z}_p^*$ فتنص مبرهنة فيرما الصغرى (Fermat's little theorem) على أن $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ أما تعميم هذه المبرهنة فتسمى مبرهنة أويلر (Euler theorem) وهي $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$ لكل عدد صحيح $n \geq 2$ ولكل $a \in \mathbb{Z}_n^*$.

تعرف رتبة (order) العدد $a \in \mathbb{Z}^*$ وتكتب $ord(a)$ على أنه أصغر عدد صحيح موجب t يحقق $a^t \equiv 1 (\mathrm{mod}\, n)$. يقدم التمرين **(١١,١,٢١)** بعض الخصائص الأساسية التي تتحقق في الزمرة $\mathbb{Z}_n^*$، إحدى هذه الخصائص هي أن $\mathrm{ord}(a) \mid \varphi(n)$ لكل $a \in \mathbb{Z}_n^*$.

إذا كانت رتبة $a \in \mathbb{Z}_n^*$ هي $\mathrm{ord}(a) = \left|\mathbb{Z}_n^*\right| = \varphi(n)$ فنقول إن a مولِّداً (generator) للزمرة $\mathbb{Z}_n^*$. وفي هذه الحالة يكون $\mathbb{Z}_n^* = \{a^j : a \leq i < \varphi(n)\}$. من

المعلوم وجود مولدات للزمرة $\mathbb{Z}_p^*$ حيث p عدد أولي، فمثلاً من السهل التحقق من أن 2 مولّداً للزمرة $\mathbb{Z}_{13}^*$.

مثال (١١,١,٤)

اعتبر الزمرة $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$. عدد عناصر $\mathbb{Z}_{15}^*$ هو $\varphi(15) = \varphi(3)\varphi(5) = (3-1)(5-1) = 8$. رُتب هذه العناصر مبينة في الجدول التالي:

$a \in \mathbb{Z}_{15}^*$	1	2	4	7	8	11	13	14
$\mathrm{ord}(a)$	1	4	2	4	4	2	4	2

لاحظ أن $\mathrm{ord}(a)$ يقسم $\varphi(n) = 8$ لكل $a \in \mathbb{Z}_{15}^*$. لاحظ أيضاً عدم وجود مولّد للزمرة $\mathbb{Z}_{15}^*$؛ وذلك لعدم وجود عنصر من الرتبة 8. ▲

مبرهنة (١١,١,٥) مبرهنة الباقي الصينية

إذا كانت الأعداد الصحيحة $n_1, n_2, \ldots n_k$ أولية نسبياً مثنى مثنى فيكون لنظام التطابقات:

$$\begin{aligned} x &\equiv a_1 (\mathrm{mod}\, n_1) \\ x &\equiv a_2 (\mathrm{mod}\, n_2) \\ &\vdots \\ x &\equiv a_k (\mathrm{mod}\, n_k) \end{aligned}$$

حلاً وحيداً قياس $n = n_1 n_2 \ldots n_k$.

لنفرض أن $k = 2$ في مبرهنة الباقي الصينية. بما أن $(n_1, n_2) = 1$ فيوجد $s,t \in \mathbb{Z}$ حيث $sn_1 + tn_2 = 1$. التمرين **(١١,١,١٨)** يطلب التحقق من أن $x = (sn_1a_2 + tn_2a_1)(\mathrm{mod}\, n)$ هو الحل الوحيد للنظام. وكمثال على ذلك، نأخذ النظام:

$$\begin{aligned} x &\equiv 3 (\mathrm{mod}\, 7) \\ x &\equiv 6 (\mathrm{mod}\, 13) \end{aligned}$$

باستخدام خوارزمية إقليدس الموسعة نجد أن $(7,13) = 1 = 2 \cdot 7 - 1 \cdot 13$.
وبهذا فإن الحل الوحيد للنظام قياس $n = 7 \cdot 13 = 91$ هو $2 \cdot 7 \cdot 6 - 1 \cdot 13 \cdot 3 = 45$
. خوارزمية جاوس (Gauss) التالية تعمم لنا ذلك.

خوارزمية (١١,١,٦) جاوس

يمكن حساب الحل x لنظام تطابقات مبرهنة الباقي الصينية على النحو التالي:

$$x \equiv \sum_{i=1}^{k} a_i N_i M_i (\bmod n)$$

حيث $N_i = \dfrac{n}{n_i}$ و $M_i \equiv N_i^{-1} (\bmod n)$.

إن حساب $a^k (\bmod n)$ بطريقة فعالة مهم للعديد من خطط التعمية. من الممكن إنجاز ذلك بطريقة بدائية بحساب a^k ومن ثم قسمة الناتج على n أو بحساب $a^i (\bmod n)$ ، $i \le i \le k$ بعمليات ضرب متتالية. ولكن كل من هاتين الطريقتين غير فعالة سواء من ناحية سعة التخزين اللازمة أو عدد عمليات الضرب اللازمة. أما طريقة التربيع والضرب (Square-and-multiply) فهي طريقة فعالة لإجراء هذه الحسابات. ولاستخدام هذه الطريقة نقوم بإيجاد التمثيل الثنائي للعدد k وهو:

$$t = \lfloor \log_2 k \rfloor \quad \text{حيث} \quad k = \sum_{i=0}^{t} k_i 2^i$$

وبعد ذلك نجد:

$$a^k = \prod_{i=0}^{t} a^{k_i 2^i} = \left(a^{2^0}\right)^{k_0} \left(a^{2^1}\right)^{k_1} \ldots \left(a^{2^t}\right)^{k_t} = \prod_{k_i=1} a^{2^i}.$$

لاحظ أن $a^{2^t} = \left(a^{2^{t-1}}\right)^2$. ولذا نحتاج لحساب $a^k (\bmod n)$ عدد t من التربيعات قياس n وعلى الأكثر t من عمليات الضرب قياس n. الخوارزمية التي نقدمها لحساب $a^k (\bmod n)$ يتم تنفيذها بعمليات ضرب جزئية. يمكن أيضاً الرجوع إلى [63] حيث توجد خوارزميات تربيع وضرب أخرى.

خوارزميات (١١,١,٧) خوارزمية التربيع والضرب

المـدخلات: $0 \neq a \in \mathbb{Z}_n$ وعـدد صـحيح $0 \leq k < n$ والتمثيـل الثنـائي $k = \sum_{i=0}^{t} k_i 2^i$.

المخرج: $a^k \pmod n$.

(١) ضع $A \leftarrow a$ و $b \leftarrow 1$.

(٢) لكل i من 0 إلى t نفذ التالي:

(أ) إذا كان $i > 0$ فضع $A \leftarrow A^2 \pmod n$.

(ب) إذا كان $k_i = 1$ فضع $b \leftarrow bA \pmod n$.

(٣) توقف (b).

مثال (١١,١,٨)

نستخدم الخوارزمية لحساب $3^{26} \pmod{35}$. أي أن $a = 3$ وأن $n = 35$ وأن:

$$k = 26 = \sum_{i=0}^{4} k_i 2^i = 11010_2.$$

الجدول التالي يبين حسابات الخوارزمية:

i	0	1	2	3	4
k_i	0	1	0	1	1
A	3	$3^2 \pmod n = 9$	$9^2 \pmod n = 11$	$11^2 \pmod n = 16$	$16^2 \pmod n = 11$
b	1	$1 \cdot 9 \pmod n = 9$	9	$9 \cdot 16 \pmod n = 4$	$4 \cdot 11 \pmod n = 9$

إذن $3^{26} \pmod{35} = 9$. في هـذا المثـال البسـيط، يمكـن التحقـق وبسهـولة مـن صـواب الخوارزميـة بحسـاب القـوة قيـاس $\varphi(n) = \varphi(5 \cdot 7) = 24$ لنحصـل علـى $3^k \pmod n = 3^2$. ▲

يلخص الجدول (١١,١) تعقد الحسابات للعمليات الأساسية في الزمرة $\mathbb{Z}_n$:

الجدول (١١,١). تحقق الحسابات في $\mathbb{Z}_n$ للعمليات الأساسية.

العملية قياس n	عدد العمليات الثنائية
الجمع : $a+b \pmod n$	$O(\log_2 n)$
الضرب : $ab \pmod n$	$O\left((\log_2 n)^2\right)$
المعكوس : $a^{-1} \pmod n$	$O\left((\log_2 n)^2\right)$
القوة : $a^k \pmod n$ حيث $k < n$	$O\left((\log_2 n)^3\right)$

تمارين

(١١,١,٩) أثبت خواص قابلية القسمة التالية :

(أ) $a \mid a$

(ب) إذا كان $a \mid b$ و $b \mid c$ فإن $a \mid c$.

(ج) إذا كان $a \mid b$ و $b \mid a$ فإن $a = \pm b$.

(د) إذا كان $c \mid a$ و $c \mid b$ فإن $c \mid (ax+by)$ لكل $x, y \in \mathbb{Z}$.

(١١,١,١٠) يُعرف المضاعف المشترك الأصغر (Least common multiple) ويكتب $\operatorname{lcm}(a,b)$ للعددين الصحيحين الموجبين a و b على النحو التالي :

$$\operatorname{lcm}(a,b) = \frac{ab}{(a,b)}$$

إذا كان $a \mid c$ و $b \mid c$ فأثبت أن $\operatorname{lcm}(a,b) \mid c$.

(١١,١,١١) هذا التمرين يتعلق بخوارزمية إقليدس **(١١,١,١)**.

(أ) أثبت أن البواقي تحقق $r_{i+2} < r_i / 2$.

(ب) أثبت أن مخرج الخوارزمية هو بالفعل (a,b).

(١١,١,١٢) يناقش هذا التمرين بعض الخواص الأساسية للحلقة $\mathbb{Z}_n$.

(أ) أثبت أن عمليتي الجمع والضرب على $\mathbb{Z}_n$ معرفتان تعريفاً حسناً.

(ب) أثبت أن $(\mathbb{Z}_n,+,\cdot)$ حلقة، استخدم خواص الحلقة $\mathbb{Z}$ لإثبات ذلك، على سبيل المثال تحقق من أن الضرب يتوزع على الجمع. أي أثبت أن:

$$\big([a]+[b]\big)[c]=[a][c]+[b][c].$$

(١١,١,١٣) استخدم خوارزمية إقليدس لإيجاد $d=(105,180)$ ثم جد $x,y\in\mathbb{Z}$ بحيث يكون $105x+180y=d$.

(١١,١,١٤) استخدم خوارزمية التربيع والضرب لحساب $47^{332}(\mathrm{mod}\,576)$.

(١١,١,١٥) أعط مثالاً مناقضاً لكل من العبارات الخاطئة التالية:

(أ) إذا كان $a,b,n\in\mathbb{Z}$ حيث $n\mid ab$ فإن $n\mid a$ أو $n\mid b$.

(ب) إذا كان $p\in\mathbb{Z}^+$ و $a\in\mathbb{Z}$ حيث $(a,p)=1$ فإن $a^{p-1}\equiv 1(\mathrm{mod}\,p)$.

(ج) إذا كان $a,b,c\in\mathbb{Z}$ فإن $(ab,c)=(a,c)(b,c)$.

(١١,١,١٦) جد رتبة كل عنصر من عناصر $\mathbb{Z}_{11}^*$ ثم حدد مولدات $\mathbb{Z}_{11}^*$.

(١١,١,١٧) لنفرض أن $a\in\mathbb{Z}_n^*$. أثبت أن جميع الأعداد $a^i(\mathrm{mod}\,n)$ حيث $0\le i<\mathrm{ord}(a)$ مختلفة.

(١١,١,١٨) أثبت الادعاء المذكور بعد مبرهنة الباقي الصينية **(١١,١,٥)** وهو أن $x\equiv(sn_1a_2+tn_2a_1)(\mathrm{mod}\,n)$ حيث $sn_1+tn_2=1$ حل للنظام المكون من التطابقين.

(١١,١,١٩) بين فيما إذا كان للنظام:

$$x\equiv 15(\mathrm{mod}\,70)$$
$$x\equiv 104(\mathrm{mod}\,151)$$

حلولاً أم لا. وبحالة وجود حلولاً للنظام فجد جميع هذه الحلول باستخدام خوارزمية إقليدس الموسعة.

(١١,١,٢٠) أثبت أن التطابق $ax\equiv b(\mathrm{mod}\,n)$ قابلاً للحل إذا وفقط إذا كان $(a,n)\mid b$. وإذا وجد حلول فعددها (a,n).

(١١,١,٢١) إذا كان $a \in \mathbb{Z}_n^*$ فأثبت صواب كل من العبارات التالية:

(أ) $a^x \equiv 1 (\mathrm{mod}\, n)$ إذا وفقط إذا كان $\mathrm{ord}(a) \mid x$. على وجه الخصوص $\mathrm{ord}(a) \mid \varphi(n)$.

(ب) $a^x \equiv a^y (\mathrm{mod}\, n)$ إذا وفقط إذا كان $x \equiv y (\mathrm{mod}\, \mathrm{ord}(a))$.

(ج) $a^x (\mathrm{mod}\, n) = a^{x(\mathrm{mod}\, \mathrm{ord}(a))} (\mathrm{mod}\, n)$.

(١١,١,٢٢) ليكن p عدداً أولياً و $a \in \mathbb{Z}^+$. أثبت أن عدد حلول التطابق $x^a \equiv 1 (\mathrm{mod}\, p)$ في الحقل $\mathbb{Z}_p$ يساوي $(a, p-1)$.

(١١,١,٢٣) إذا كان p عدداً أولياً فأثبت أن جميع العناصر غير الصفرية في $\mathbb{Z}_p$ قابلة للعكس وأن $\mathbb{Z}_p$ حقلاً. تنص مبرهنة فيرما الصغرى على أن $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ حيث $a \in \mathbb{Z}_p^*$ ويمكن برهانها على النحو التالي:

(أ) افرض أن $T = \{a, 2a, \ldots, (p-1)a\} \subseteq \mathbb{Z}_p$. أثبت أن جميع عناصر T غير صفرية ومختلفة.

(ب) استخدم الفقرة (أ) لإثبات أن $T = \mathbb{Z}_p^*$. من ذلك يكون:

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a(2a) \cdots (p-1)(a) (\mathrm{mod}\, p)$$

الآن، أكمل البرهان باستخدام خوارزمية القسمة.

(١١,٢) الرواسب التربيعية
Quadratic Residues

افرض أن $a \in \mathbb{Z}_n^*$. نقول إن العدد a راسباً تربيعياً قياس العدد n (quadratic residue modulo) إذا وجد $x \in \mathbb{Z}_n^*$ حيث $x^2 \equiv a (\mathrm{mod}\, n)$. وفي هذه الحالة نقول إن x هو جذر تربيعي للعدد a قياس n. إذا لم يكن a راسباً تربيعياً قياس n فنقول إنه ليس راسباً تربيعياً قياس n (quadratic nonresidue modulo n). سنرمز لمجموعة الرواسب التربيعية قياس n بالرمز Q_n ولمجموعة الرواسب غير التربيعية

قياس n بالرمز $\overline{Q_n}$. لاحظ أن $\mathbb{Z}_n^* = Q_n \cup \overline{Q_n}$. لاحظ إمكانية وجود عناصر $a \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$ بحيث يكون التطابق $x^2 \equiv a(\mathrm{mod}\, n)$ قابلاً للحل ولكن a ليس راسباً تربيعياً قياس n، على سبيل المثال، بأخذ $4 \in \mathbb{Z}_6$ وملاحظة أن $2^2 \equiv 4(\mathrm{mod}\, 6)$ نجد أن 2 حل للتطابق $x^2 \equiv 4(\mathrm{mod}\, 6)$ ولكن $2 \notin Q_6$ (لأن $4 \notin \mathbb{Z}_6^*$).

مبرهنة (١١,٢,١)

لنفرض أن $p > 2$ عدد أولي وأن α مولِّد للزمرة $\mathbb{Z}_p^*$. عندئذ، يكون $a \in \mathbb{Z}_p^*$ راسباً تربيعياً قياس p إذا وفقط إذا وجد $i \in \mathbb{Z}$ بحيث يكون $a \equiv \alpha^{2i}(\mathrm{mod}\, p)$.

البرهان

إذا كان $a \equiv \alpha^{2i}(\mathrm{mod}\, p)$ حيث $i \in \mathbb{Z}$ فنرى أن $x = \alpha^i$ يحقق $x^2 \equiv a(\mathrm{mod}\, p)$ ومن ثم يكون a راسباً تربيعياً قياس p. ولبرهان العكس، نفرض أن $a \in Q_p$. عندئذ، يوجد $i \in \mathbb{Z}$ حيث $x \equiv \alpha^i(\mathrm{mod}\, p)$ حل للتطابق $x^2 \equiv a(\mathrm{mod}\, p)$ ومن ثم يكون $\alpha^{2i} \equiv a(\mathrm{mod}\, p)$. ■

نتيجة (١١,٢,٢)

لنفرض أن $p > 2$ عدد أولي وأن α مولِّد للحقل $\mathbb{Z}_p^*$. عندئذ،

(١) $Q_p = \{\alpha^i(\mathrm{mod}\, p) : 0 \le i \le p-2$ و i زوجي$\}$ و

$\overline{Q_p} = \{\alpha^i(\mathrm{mod}\, p) : 0 \le i \le p-2$ و i فردي$\}$.

(٢) $\left|Q_p\right| = \left|\overline{Q_p}\right| = \dfrac{p-1}{2}$.

(٣) إذا كان $a \in Q_p$ فيكون للتطابق $x^2 \equiv a(\mathrm{mod}\, p)$ حلان غير متطابقين فقط.

(٤) $\alpha^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\, p)$.

البرهان

نحصل على الفقرتين (١) و (٢) مباشرة من المبرهنة.

أما بالنسبة للفقرة الثالثة فلاحظ أولاً أن $\pm x$ حلان للتطابق وأن $x \not\equiv -x \pmod p$ (لأن $2x \not\equiv 0 \pmod p$ وأن p فردي و لا يقسم x)(*). ولبرهان الفقرة (٤)، لاحظ أولاً أن $\alpha^{\frac{p-1}{2}}$ حل للتطابق $x^2 \equiv 1 \pmod p$ لأن α من الرتبة $p-1$ وأن:

$$\left(\alpha^{\frac{p-1}{2}}\right)^2 = \alpha^{p-1} \equiv 1 \pmod p$$

وذلك استناداً إلى مبرهنة فيرما الصغرى. من ذلك نرى أن $\alpha^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$. وبما أن $ord(\alpha) = p-1$ فنرى أن $\alpha^{\frac{p-1}{2}} = -1 \pmod p$. ■

لنفرض أن $a \in \mathbb{Z}_p^*$. عندئذ، بتجريب عناصر المجموعة $\left\{x^2 \pmod p : x \in \mathbb{Z}_p^*\right\}$ يكون بمقدورنا معرفة فيما إذا كان $a \in Q_p$ أم لا. ولكن هذه الطريقة ليست فعالة حيث الزمن اللازم (في أسوأ الأحوال) لإنجاز ذلك يحتاج إلى $O(p)$ عملية ضرب. نستعين بالنتيجة السابقة للحصول على اختبار أكثر فعالية. يُعرف رمز ليجندر (Legendre symbol) ويرمز له بالرمز $\left(\frac{a}{p}\right)$ حيث $a \in \mathbb{Z}$ و $p > 2$ عدد أولي على النحو التالي:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & , p \mid a \\ 1 & , a \pmod p \in Q_p \\ -1 & , a \pmod p \not\in Q_p \end{cases}$$

مبرهنة (١١,٢,٣) معيار أويلر

لنفرض أن $p > 2$ عدد أولي وأن $a \in \mathbb{Z}$. عندئذ،

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

(*) المترجمان: ولبرهان عدم وجود حلول أخرى غير متطابقة قياس p نفرض أن y_1 و y_2 حلان للتطابق. عندئذ، $p \mid (y_2^2 - y_1^2)$. أي أن $p \mid (y_2 - y_1)$ أو أن $p \mid (y_2 + y_1)$. إذن $y_2 \equiv y_1 \pmod p$ أو أن $y_2 \equiv -y_1 \pmod p$.

البرهان

سنبرهن الحالة $a \in Q_p$ ونترك الحالتين $a \in \overline{Q_p}$ و $p \mid a$ للتمرين (**١١,٢,١٠**).

لنفرض أن α مولِّد للمجموعة $\mathbb{Z}_p^*$. عندئذ، يوجد $i \in \mathbb{Z}$ حيث $\alpha^{2i} \equiv a(\bmod p)$ وذلك استناداً إلى المبرهنة (**١١,٢,١**) وبهذا يكون:

$$a^{\frac{p-1}{2}} \equiv (\alpha^{2i})^{\frac{p-1}{2}} \equiv (\alpha^{p-1})^i \equiv 1(\bmod p) \equiv \left(\frac{a}{p}\right)(\bmod p)$$

وذلك لأن $\left(\frac{a}{p}\right) = 1$. ■

إذا استخدمنا معيار أويلر لاختبار فيما إذا كان $a \in Q_p$ فنحتاج لحساب $a^{\frac{p-1}{2}}$ ويمكن إنجاز ذلك بعدد $O(\log_2^3 p)$ من العمليات الثنائية وذلك باستخدام خوارزمية التربيع والضرب، وهذه طريقة فعالة. لاحظ أن استخدام معيار أويلر يبين فقط فيما إذا كان $a \in Q_p$ أم لا ولكنه لا يجد الجذر التربيعي (على عكس عملية التجريب) للعدد a.

مثال (١١,٢,٤)

نستخدم معيار أويلر لاختبار فيما إذا كان $3 \in Q_p$ حيث $p = 23$. لحساب $3^{\frac{p-1}{2}} (\bmod p)$ لاحظ أن:

$$\frac{p-1}{2} = 11 = 1011_2 = \sum_{i=0}^{3} k_i 2^i$$

وباستخدام الخوارزمية (**١١,١,٧**) نجد أن الحسابات هي:

i	0	1	2	3
k_i	1	1	0	1
A	3	$3^2 = 9$	$9^2(\bmod p) = 12$	$12^2(\bmod p) = 6$
b	3	$3 \cdot 9(\bmod p) = 4$	4	$4 \cdot 6(\bmod p) = 1$

إذن، $\left(\frac{3}{p}\right) = 3^{\frac{p-1}{2}} \pmod p = 1$. وبهذا يكون $3 \in Q_{23}$ ويوجد x حيث $x^2 \equiv 3 \pmod{23}$. سنقدم لاحقاً خوارزمية فعالة لإيجاد x. ولكن في هذا المثال السهل نرى وبسهولة أن $16^2 \equiv 3 \pmod{23}$. ▲

من الممكن أيضاً استخدام خصائص رمز ليجندر لحساب $\left(\frac{a}{p}\right)$ بطريقة أكثر فعالية من الطريقة المستخدمة في المثال (**١١,٢,٤**)، وسنوضح ذلك بعد تقديم تعميم لرمز ليجندر.

ليكن $n \geq 3$ عدداً صحيحاً فردياً حيث $n = p_1^{e_1} \dots p_k^{e_k}$ هو تحليل n إلى قوى عوامله الأولية ولنفرض أن $a \in \mathbb{Z}$. يرمز لرمز جاكوبي (Jacobi symbol) بالرمز $\left(\frac{a}{n}\right)$ ويعرف بدلالة رمز ليجندر على النحو التالي:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \dots \left(\frac{a}{p_k}\right)^{e_k}.$$

خواص رمز جاكوبي

نفرض أن $m, n \geq 3$ عددان صحيحان فرديان وأن $a, b \in \mathbb{Z}$. عندئذ:

(١) $\left(\frac{a}{n}\right) \in \{-1, 0, 1\}$ وأن $\left(\frac{a}{n}\right) = 0$ إذا وفقط إذا كان $(a, n) \neq 1$.

(٢) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ و $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

(٣) إذا كان $a \equiv b \pmod n$ فإن $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

(٤) $\left(\frac{1}{n}\right) = 1$ و $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & , n \equiv 1 \pmod 4 \\ -1 & , n \equiv 3 \pmod 4 \end{cases}$.

(٥) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & , n \equiv \pm 1 \pmod 8 \\ -1 & , n \equiv \pm 3 \pmod 8 \end{cases}$.

(٦) قانون المقلوب التربيعي (Low of quadratic reciprocity) :

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

باستخدام هذه الخواص لحساب $\left(\frac{3}{23}\right)$ المقدم في المثال (**١١,٢,٤**) نحصل على :

$$\left(\frac{3}{23}\right) = \left(\frac{23}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{23-1}{2}} = \left(\frac{2}{3}\right)(-1)^{1\cdot 11} = -\left(\frac{2}{3}\right) = -(-1) = 1$$

وذلك لأن 23 أولي. وبهذا يكون $3 \in Q_{23}$ وهذا يتفق مع ما وجدناه باستخدام معيار أويلر.

إذا تمحصنا في تعريف رمز جاكوبي $\left(\frac{a}{n}\right)$ فنرى أننا نحتاج إلى تحليل n وهذه مسألة يعتقد أنها صعبة ومع ذلك فمن الممكن استخدام خواص رمز جاكوبي لحسابه دون اللجوء إلى التحليل.

مثال (١١,٢,٥)

باستخدام خواص رمز جاكوبي لحساب $\left(\frac{28}{55}\right)$ نحصل على :

$$\left(\frac{28}{55}\right) = \left(\frac{2}{55}\right)^2\left(\frac{7}{55}\right) \qquad \text{(خاصية ٢)}$$

$$= \left(\frac{55}{7}\right)(-1)^{\frac{55-1}{2}\cdot\frac{7-1}{2}} \qquad \text{(خاصية ٦)}$$

$$= -\left(\frac{55}{7}\right) = -\left(\frac{6}{7}\right) \qquad \text{(خاصية ٣)}$$

$$= -\left(\frac{-1}{7}\right) - (-1)^{\frac{7-1}{2}} = 1 \qquad \text{(خاصية ٤)}$$

ومع أن قيمة رمز جاكوبي يساوي 1 ، إلا أننا لا نستطيع الاستنتاج بأن 28 راسب تربيعي قياس 55 (في الحقيقة هو راسب غير تربيعي). وبملاحظة $28^{(55-1)/2} \equiv 52 \pmod{55}$

نرى أن معيار أويلر لا يتحقق للأعداد المؤلفة. وأخيراً، تذكر أن للراسب التربيعي قياس عدد أولي جذران. هنا $n = 55$ عدد مؤلف وأن الجذور التربيعية للعدد 1 قياس 55 هي ± 1 و ± 21 (سنناقش ذلك في البند (**١١,٤**)). ▲

كما رأينا في المثال السابق نجد أن $\left(\frac{a}{n}\right) = 1$ لا يحسم مسألة أن a راسب تربيعي أو راسب غير تربيعي قياس العدد المؤلف n. ومع ذلك إذا كان $a \in Q_n$ فيوجد $x \in \mathbb{Z}_n^*$ بحيث يكون $x^2 \equiv a (\mathrm{mod}\, n)$ ومن ثم نجد أن $\left(\frac{a}{n}\right) = \left(\frac{x^2}{n}\right) = \left(\frac{x}{n}\right)^2 = 1$. وهذا يعني أنه إذا كان $\left(\frac{a}{n}\right) = -1$ فإن a راسب غير تربيعي قياس n. ولهذا السبب، إذا كان $n \geq 3$ عدداً صحيحاً فردياً نعرف المجموعة J_n على أنها:

$$J_n = \left\{ a \in \mathbb{Z}_n^* : \left(\frac{a}{n}\right) = 1 \right\}$$

تسمى عناصر $\widetilde{Q_n} = J_n \setminus Q_n$ أشباه المربعات قياس n (pseudosquares module n).

لاحظ أن $Q_n \subseteq J_n$ وأن $Q_n = J_n$ عندما يكون n أولياً.

مثال (١١,٢,٦)

سنجد في هذا المثال الرواسب التربيعية وأشباه المربعات قياس العدد $n = 15$.

لاحظ أن $\left(\frac{a}{15}\right) = \left(\frac{a}{3}\right)\left(\frac{a}{5}\right)$ وأن:

$$\left(\frac{a}{3}\right) = \begin{cases} 1 & , a \equiv 1 (\mathrm{mod}\, 3) \\ -1 & , a \equiv 2 (\mathrm{mod}\, 3) \end{cases}$$

$$\left(\frac{a}{5}\right) = \begin{cases} 1 & , a \equiv \pm 1 (\mathrm{mod}\, 5) \\ -1 & , a \equiv \pm 2 (\mathrm{mod}\, 5) \end{cases}$$

الجدول التالي يبين قيم رمز جاكوبي $\left(\frac{a}{n}\right)$:

$a \in \mathbb{Z}_{15}^*$	1	2	4	7	8	11	13	14
$\left(\frac{a}{3}\right)$	1	-1	1	1	-1	-1	1	-1
$\left(\frac{a}{5}\right)$	1	-1	1	-1	-1	1	-1	1
$\left(\frac{a}{15}\right)$	1	1	1	-1	1	-1	-1	-1

إذن $J_{15} = \{1,2,4,8\}$. ومن السهل أن نجد أن $Q_{15} = \{1,14\}$. ولذا فإن أشباه المربعات هي $\widetilde{Q_{15}} = J_{15} \setminus Q_{15} = \{2,8\}$. ▲

ليكن $a \in J_n$. إن مسألة تحديد فيما إذا كان a راسباً تربيعياً أو شبه مربع قياس n ، تدعى مسألة الرواسب التربيعية (quadratic residuosity problem)، اختصاراً QRP. لنأخذ الحالة الخاصة $n = pq$ حيث p و q عددان أوليان مختلفان. سنطلب في التمارين إثبات أن $a \in J_{pq}$ راسب تربيعي إذا وفقط إذا كان $a \in Q_p$ و $a \in Q_q$ وأن :

$$\left|Q_{pq}\right| = \left|\widetilde{Q_{pq}}\right| = \frac{(p-1)(q-1)}{4}.$$

وبتطبيق ذلك على المثال (**١١,٢,٦**) نجد أن $\left(\frac{a}{3}\right) = 1 = \left(\frac{a}{5}\right)$ إذا وفقط إذا كان $a \in \{1,4\}$. وبهذا نجد أن $Q_{15} = \{1,4\}$ وأن $\left|Q_{15}\right| = 2 = \frac{(3-1)(5-1)}{4}$.

تمارين

(**١١,٢,٧**) جد كل من Q_{30} و $\widetilde{Q_{30}}$.

(**١١,٢,٨**) جد قيمة رمزي جاكوبي $\left(\frac{156}{235}\right)$ و $\left(\frac{1833}{587}\right)$. هل $156 \in Q_{235}$ ؟

(**١١,٢,٩**) جد الرواسب التربيعية وأشباه المربعات قياس العدد $n = 21$.

(**١١,٢,١٠**) أحد الزملاء غير الدقيقين ادعى أن "36 راسب تربيعي قياس n لكل $n > 36$ لأن $6^2 = 36$". صحح هذا الادعاء وحدد فيما إذا كان $36 \in Q_{745}$.

(**١١,٢,١١**) لنفرض أن لدينا الخواص التالية لرمز ليجندر:

- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ و $\left(\frac{-2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}$ لكل عدد أولي فردي.
- إذا كان p و q عددين أوليين فرديين فإن:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}.$$

لنفرض أن $n \geq 3$ عدد صحيح فردي. أثبت خواص رمز جاكوبي التالية:

(أ) إذا كان n_1 و n_2 عددين صحيحين فرديين فأثبت أن:

$$\frac{n_1 n_2 - 1}{2} \equiv \frac{n_1 - 1}{2} + \frac{n_2 - 1}{2} (\mathrm{mod}\, 2).$$

استنتج أن $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

(ب) إذا كان n_1 و n_2 عددين صحيحين فرديين فأثبت أن:

$$\frac{n_1^2 n_2^2 - 1}{8} \equiv \frac{n_1^2 - 1}{8} + \frac{n_2^2 - 1}{8} (\mathrm{mod}\, 2).$$

استنتج أن $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

(ج) إذا كان $a \geq 3$ عدداً صحيحاً فردياً فأثبت أن:

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)(-1)^{(a-1)(n-1)/4}.$$

(**١١,٢,١٢**) افرض أن p عدد أولي فردي. أثبت أن $-3 \in Q_p$ إذا وفقط إذا كان $p \equiv 1 (\mathrm{mod}\, 3)$.

(**١١,٢,١٣**) أثبت استحالة أن يكون الراسب التربيعي مولّداً للمجموعة $\mathbb{Z}_p^*$.

(**١١,٢,١٤**) ليكن $n = pq$ حيث p و q عددان أوليان فرديان مختلفان.

(أ) أثبت أن $a \in Q_n$ إذا وفقط إذا كان $\left(\frac{a}{p}\right) = 1 = \left(\frac{a}{q}\right)$.

(ب) أثبت أن $|Q_n| = \frac{(p-1)(q-1)}{4}$. ارشاد: أثبت أن الدالة $f : Q_n \to Q_p \times Q_q$ المعرفة بالقاعدة $f(a) = (a \bmod p, a \bmod q)$ تقابل.

(**١١,٢,١٥**) أكمل برهان معيار أويلر (مبرهنة (**١١,٢,٣**)).

(١١,٣) اختبار الأوليات

Primality Testing

أحد المتطلبات الأساسية للعديد من أنظمة التعمية ذوات المفاتيح المعلنة هي توليد أعداد أولية كبيرة. ولذا فإحدى المسائل المطروحة هي اختبار فيما إذا كان العدد الصحيح $n > 2$ عدداً أولياً أم عدداً مؤلفاً. وبقسمة العدد على جميع الأعداد الأولية بين 2 و $\sqrt{n}$ يحدد فيما إذا كان العدد أولياً أم لا. كما أن هذه الطريقة تزودنا بعامل غير تافه إذا كان العدد مؤلفاً. ولكن هذه الطريقة ليست فعالة؛ لأنها تحتاج إلى $O(\sqrt{n})$ من عمليات القسمة.

في هذا البند نقدم اختباران احتماليان لأولية العدد هما اختبار سولوفي وستراسن (Solovay-Strassen test) واختبار ميلر ورابن (Miller-Rabin test). هذان الاختباران احتماليان؛ لأنه لو كان المخرج "مؤلف" يكون العدد n هو بالفعل مؤلف وإذا كان المخرج "أولي" فمن المحتمل أن يكون العدد مؤلفاً. ولهذا السبب فالتسمية الصحيحة لهذان الاختباران يجب أن تكون اختبارات أن يكون العدد مؤلفاً.

يعتمد اختبار سولوفي وستراسن على معيار أويلر (مبرهنة (**١١,٢,٣**)) والذي ينص على:

إذا كان n أولياً فإن $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) (\mathrm{mod}\, n)$. ويقترح علينا هذا المعيار التعريف التالي.

تعريف (١١,٣,١)

لنفرض أن n عدد صحيح فردي مؤلف وأن $1 \leq a < n$. إذا كان $(a,n) \neq 1$ أو كان $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) (\mathrm{mod}\, n)$ فنقول إن a شاهد أويلر على أن العدد n مؤلف (Euler witness to compositeness of n).

مبرهنة (١١,٣,٢)

ليكن n عدداً صحيحاً فردياً مؤلفاً وليكن $a \in \mathbb{Z}_n^*$ شاهد أويلر على أن العدد n مؤلف. عندئذ، على الأقل نصف عناصر $\mathbb{Z}_n^*$ هي شهود أويلر على n مؤلف.

البرهان

مجموعة غير الشهود $G = \left\{ x \in \mathbb{Z}_n^* : x^{(n-1)/2} \equiv \left(\frac{x}{n}\right) (\mathrm{mod}\, n) \right\}$ مغلقة تحت عملية الضرب في الزمرة المنتهية $\mathbb{Z}_n^*$. ولذا فهي زمرة جزئية من $\mathbb{Z}_n^*$. واستناداً إلى مبرهنة لاجرانج نرى أن $|G|$ يقسم $|\mathbb{Z}_n^*|$. وبما أن $a \in \mathbb{Z}_n^* \setminus G$ فنجد أن $|G| \leq |\mathbb{Z}_n^*| / 2$. ومن الممكن برهان المبرهنة بإثبات أن ab شاهد أويلر على أن العدد n مؤلف عندما يكون $b \in \mathbb{Z}_n^*$ ليس شاهدًا. وبهذا فعدد غير الشهود في $\mathbb{Z}_n^*$ هو على الأكثر $|\mathbb{Z}_n^*| / 2$. ■

مبرهنة (١١,٣,٣)

إذا كان n عدداً صحيحاً فردياً مؤلفاً فيوجد شاهد أويلر على أن العدد n مؤلف في $\mathbb{Z}_n^*$.

البرهان

لنفرض أولاً أن n ليس خالياً من المربعات. أي يوجد عدد أولي p حيث $p^2 \mid n$. ولنفرض أن $a = 1 + \frac{n}{p}$. عندئذ، $a \in \mathbb{Z}_n^*$ وأن:

$$\left(\frac{a}{n}\right) = \left(\frac{1+n\,/\,p}{(n\,/\,p)p}\right)$$

$$= \left(\frac{1+n\,/\,p}{n\,/\,p}\right)\left(\frac{1+n\,/\,p}{p}\right)$$
$$= \left(\frac{1}{n\,/\,p}\right)\left(\frac{1}{p}\right) = 1$$

أيضاً، لدينا:

$$a^p \equiv \big(1+n\,/\,p\big)^p \equiv 1 + \sum_{i=1}^{p}\binom{p}{i}\big(n\,/\,p\big)^i \equiv 1(\mathrm{mod}\, n).$$

إذن، $ord(a) = p$ ؛ لأن $a \equiv 1(\mathrm{mod}\, n)$. وبما أن $p \nmid (n-1)$ فنجد أن $a^{(n-1)/2} \not\equiv 1(\mathrm{mod}\, n)$. وبهذا يكون a شاهد أويلر على أن n مؤلف في هذه الحالة.

لنفرض الآن أن n حاصل ضرب أعداد أولية مختلفة. وليكن p قاسماً أولياً للعدد n و b راسب غير تربيعي قياس العدد p. باستخدام مبرهنة الباقي الصينية نستطيع إيجاد عدد a يحقق:

$$a \equiv b(\mathrm{mod}\, p)$$
$$a \equiv 1(\mathrm{mod}\, n\,/\,p)$$

وباستخدام خواص رمز جاكوبي نجد أن:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p(n\,/\,p)}\right)$$

$$= \left(\frac{a}{p}\right)\left(\frac{a}{n\,/\,p}\right)$$

$$= \left(\frac{b}{p}\right)\left(\frac{1}{n\,/\,p}\right) = -1$$

لأن b راسب غير تربيعي قياس p (لاحظ أن $a \in \mathbb{Z}_n^*$). الآن، من تعريف a نحصل على $a^{(n-1)/2} \equiv 1(\mathrm{mod}\, n\,/\,p)$ ومن ثم $a^{(n-1)/2} \not\equiv -1(\mathrm{mod}\, n\,/\,p)$.

إذن، $a^{(n-1)/2} \not\equiv -1 \pmod{n}$ ويكون a شاهد أويلر على أن n مؤلف في هذه الحالة أيضاً. ■

يمكن النظر إلى اختبار سولوفي وستراسن على أنه الاختبار الذي يبحث عن شاهد أويلر على n مؤلف وإذا لم يجد مثل هذا الشاهد فإنه يستنتج أن من المحتمل أن يكون n أولياً. ويستخدم عدد شواهد أويلر على أن n مؤلف للحصول على حد للخطأ.

خوارزمية (١١,٣,٤) اختبار سولوفي وستراسن

المدخل: عدد فردي $n > 2$ ووسيط $t \geq 1$.

المخرج: الإجابة "مؤلف" أو الإجابة "احتمال أولي".

(١) نفذ التالي على الأكثر t مرة:

(أ) اختار عدداً عشوائياً a حيث $1 < a < n$.

(ب) إذا كان $(a, n) \neq 1$ توقف "مؤلف".

(ج) إذا كان $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$ توقف "مؤلف".

(٢) توقف "احتمال أولي".

الزمن اللازم لتنفيذ العروة الداخلية يساوي $O(\log_2^3 n)$ عملية ثنائية. كتبنا خطوات الخوارزمية لأجل التوضيح مع ملاحظة أنه يمكن استبدال الخطوة (١,٢) بمقارنة $a^{(n-1)/2} \pmod{n}$ حيث نتوقف "مؤلف" إذا كانت القيمة لا تساوي 1 أو $n - 1$.

إذا كان مخرج الاختبار "مؤلف" فتمنح شهادة (certificate) تسمح من التحقق بطريقة فعالة على أن n هو بالفعل مؤلف. الشهادة في اختبار سولوفي وستراسن هي شاهد أويلر على أن n مؤلف وخوارزمية التحقق من ذلك هي التحقق من أن $(a, n) \not\equiv 1$ أو أن $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$. احتمال أن يكون مخرج الاختبار "احتمال أولي" عندما يكون n مؤلفاً لا يزيد عن 2^{-t}.

يمكن استخدام اختبار سولوفي وستراسن (أو اختبار ميلر ورابن المقدم في التمارين) لتوليد أعداد احتمال أن تكون أولية كبيرة جداً على النحو التالي: اختار عدداً عشوائياً n من الكبر المناسب حتى يكون مخرج الخوارزمية "احتمال n أولي". عند التطبيق العملي، من الممكن اختبار قابلية قسمة n على أعداد أولية صغيرة ومن الممكن أيضاً فرض شروط أخرى وذلك يعتمد على الغرض من التطبيق.

تمارين

(١١,٣,٥) افرض أن n عدد صحيح فردي مؤلف وأن $1 \leq a < n$. إذا كان $a^{n-1} \not\equiv 1 (\mathrm{mod}\, n)$ فنقول إن a شاهد فيرما على أن n مؤلف (Fermat witness to compositeness of n). إذا كان a شاهد فيرما على أن n مؤلف فأثبت أن a شاهد أويلر على أن n مؤلف.

(١١,٣,٦) نفذ اختبار سولوفي وستراسن على العدد $n = 91$. اختار $a = 74$ كأول قيمة "عشوائية" للعدد a. إذا لم تكن سيء الحظ فالاختيار العشوائي الثاني للعدد a سيثبت أن n مؤلف.

(١١,٣,٧) (اختبار ميلر ورابن) ليكن n عدداً صحيحاً فردياً وليكن $n - 1 = 2^s r$ حيث r عدد فردي ولنفرض أن $a \in \mathbb{Z}_n^*$.

حقيقة: إذا كان n عدداً أولياً فإما أن يكون $a^r \equiv 1 (\mathrm{mod}\, n)$ أو يوجد j ، $0 \leq j < s$ بحيث يكون $a^{2^j r} \equiv -1 (\mathrm{mod}\, n)$.

تعريف: افرض أن n مؤلف. إذا كان $a^r \not\equiv 1 (\mathrm{mod}\, n)$ وكان $a^{2^j r} \not\equiv -1 (\mathrm{mod}\, n)$ لكل j ، $0 \leq j < s$ فنقول إن a شاهد قوي على أن n مؤلف (Strong witness to compositeness of n).

حقيقة: إذا كان $n \not= 9$ عدداً فردياً مؤلفاً فعدد الشواهد القوية $a \in \mathbb{Z}_n^*$ على أن n مؤلف يزيد عن ثلاثة أرباع عناصر $\mathbb{Z}_n^*$.

(أ) استخدم المفاهيم والحقائق السابقة لتصميم اختبار لأولية العدد n.

(ب) ما هو الزمن اللازم (عدد العمليات الثنائية) لتنفيذ الخوارزمية.

(ج) ناقش صواب النتائج التي تحصل عليها من هذا الاختبار.

(١١,٤) التحليل والجذور التربيعية
Factoring and Square Roots

إن مسألة كتابة عدد مؤلف n كحاصل ضرب عوامله الأولية تعدت كونها مسألة أكاديمية فقط حيث عديد من أنظمة التعمية ذات الانتشار الواسع (مثل نظام RSA الذي نقدمه في الفصل الثاني عشر) تعتمد تماماً على صعوبة تحليل عدد مؤلف n. من المؤكد أن تحليل مثل هذا العدد سيؤدي إلى شهرة من ينجح بذلك:

خصصت صحيفة نيويورك تايمز في العام ١٩٨٨م الصفحة الأولى عن استخدام طريقة المرشح التربيعي (نناقشه في البند (**١١,٤,٢**)) لتحليل عدد مكون من 100 مرتبة بالاستعانة بشبكة حاسبات مؤلفة من 400 حاسب.

لا توجد لحد الآن خوارزمية فعالة لتحليل عدد n دون وضع قيود عليه، ولكن توجد بعض الخوارزميات الفعالة عند وضع شروط مقيدة على n. على سبيل المثال، من الممكن تجريب القسمة على أعداد أولية للحصول على عامل صغير، كما أن طريقة بولارد رو (التي سنقدمها لاحقاً) هي طريقة فعالة للحصول على قواسم صغيرة نسبياً للعدد n. التحدي الذي ناقشه مقال مجلة نيويورك تايمز يتعلق بالعدد $n = pq$ حيث p و q عددان أوليان مكونان من 41 و 60 مرتبة على التوالي وتم اختيارهما بعناية لاختبار خوارزمية مصممة لأغراض خاصة. وفي مثل هذه الحالات تم اختيار خوارزمية عامة من عائلة المربعات العشوائية[١].

---

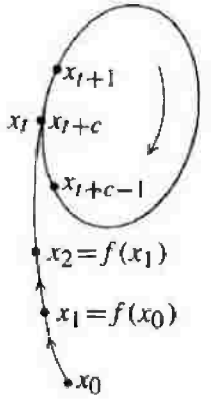
(١) في الثاني عشر من أكتوبر ١٩٨٨م كتب مالكم براوني "التغلب على مسألة رياضية شديدة الصعوبة". ولكن براوني كان أقل حماسة من محرري مجلة نيويورك تايم حيث كتبوا العنوان الدراماتيكي "تم التغلب على أصعب مسألة رياضية باستخدام مئات الحاسبات".

فيما يلي نفترض أن للعدد n على الأقل قاسمين أوليين مختلفين؛ لأن العدد الذي يكون على الصورة $n = x^k$ حيث $x \in \mathbb{Z}$ و $k > 1$ يسهل التعرف عليه ومن ثم بسهل الحصول على قاسم غير تافه (تمرين (١١,٤,٩)).

(١١,٤,١) طريقة رو لبولارد

لدينا المسألة التالية: نفرض أن X مجموعة منتهية وأن $f : X \to X$ وأن $x_0 \in X$. من الممكن تعريف المتتالية $(x_i) \subseteq X$ على النحو التالي: $x_1 = f(x_0)$، $x_2 = f(x_1)$ وهكذا. أي أن $x_i = f(x_{i-1})$ لكل عدد صحيح موجب i. بما أن X منتهية فحدود المتتالية ستتكرر بعد قيمة معينة. أي يوجد $i < j$ بحيث يكون $x_i = x_j$. والمسألة هي إيجاد هذا الزوج (i, j).

للمساعدة على فهم هذه المسألة نقوم بإنشاء شكل رو (rho-diagram) للمتتالية f ببذرة x_0 (انظر الشكل أدناه).



يبين الشكل الرؤوس x_i لجميع قيم x_i المختلفة ويوجد ضلع موجه من x_i إلى $x_{i+1} = f(x_i)$ لكل i. جاءت تسمية الشكل من كونه يشبه حرف الهجائية اليونانية ρ.

لنفرض أن c هو عدد الأضلاع الموجهة في دورة الشكل وأن t هو عدد الأضلاع الموجهة في ذيل الشكل. ولذا فعدد الأضلاع الموجهة في الشكل يساوي $k = t + c$

حيث k عدد الرؤوس. الرأس الذي يلتقي عنده الذيل بالدورة هو $x_t = x_{t+c}$. لاحظ أنه إذا كان i و j عددين صحيحين غير سالبين فيكون $x_i = x_j$ إذا وفقط إذا كان $i = j$ أو $i \equiv j (\mathrm{mod}\, c)$ في حالة $t \leq i$ و $t \leq j$.

إحدى الطرق لحل هذه المسألة هي حساب x_i بالتتالي وتخزينها ثم مقارنة كل x_i جديدة مع جميع القيم التي تم تخزينها إلى أن نحصل على المساواة المطلوبة. ولكن هذه الطريقة تحتاج إلى تخزين جميع قيم x_i (عددها k) في شكل رو، وبهذا فهي طريقة غير عملية؛ لأن k عادة ما يكون كبير جداً. وأما إذا اتبعنا طريقة رو لبولارد فنحتاج فقط إلى تخزين متغيرين x و y. نبدأ أولاً بوضع $x = x_0$ و $y = y_0$. ثم نكرر حساب:

$$x \leftarrow f(x) \qquad \text{و} \qquad y \leftarrow f(f(y))$$

(أي أننا نستبدل x بالمقدار $f(x)$ ونستبدل y بالمقدار $f(f(y))$) إلى أن نحصل على $x = y$. بعد الخطوة i يكون $x = x_i$ و $y = x_{2i}$. إذا توقفت الطريقة بعد الخطوة m حيث:

$$x_m = x = y = x_{2m}$$

فيكون الزوج المرتب $(m, 2m)$ هو الحل المنشود لمسألتنا.

من السهل إثبات أن m هو أصغر عدد صحيح موجب يحقق $m \geq t$ و $c \mid m$. تتوقف هذه الطريقة بعد $m < k$ من الخطوات وتستخدم عدد $3m < 3k$ من العمليات على f. إذا كانت f عشوائية وكان $|X| = n$ عدداً كبيراً فمن الممكن إثبات أن كل من t و c يساوي تقريباً $\sqrt{\pi n / 8}$. ومن ثم $k = c + t$ يساوي تقريباً $\sqrt{\pi n / 2} \approx 1.253\sqrt{n}$ [٢].

---

(٢) تقدير k يرتبط مع محيرة تاريخ الولادة: إذا كان لدينا مجموعة أشخاص عددها 23 فإن احتمال أن يكون تاريخ ميلاد شخصان منهم على الأقل في اليوم نفسه يساوي $\frac{1}{2}$ على الأقل. إن مثل هذا الاعتبار شائع الاستخدام في الخطط المصممة للهجوم التي تعتمد على تقصي عشوائي لإيجاد تضاربات تؤدي إلى "جذر تربيعي" للحدود الدنيا على عدد عناصر مجموعات معينة (تعرف هذه الطريقة بهجوم تاريخ الولادة).

نعود الآن إلى مسألة تحليل عدد مؤلف معطى n لنفرض أن $p < \sqrt{n}$ قاسم أولي (غير معلوم) للعدد n. هدفنا هو إيجاد عددين صحيحين x و y حيث $x \equiv y(\mathrm{mod}\, p)$ ولكن $x \not\equiv y(\mathrm{mod}\, n)$. عندئذ، يكون $d = (x-y, n)$ قاسماً غير تافه للعدد n. إذا كان d أو $\frac{n}{d}$ مؤلفاً فنكرر العملية إلى أن نحصل على قاسم أولي للعدد n.

الفكرة الأساسية هنا هي تنفيذ طريقة رو على دالة f معرفة على $\mathbb{Z}_n$ مع التظاهر على أن خطوات التنفيذ تتم على $\mathbb{Z}_p$ مع أن p غير معلوم. ولكي نضمن نجاح هذا التظاهر فيجب أن تحقق f الخاصية التالية:

لكل $a, b \in \mathbb{Z}_n$ ، إذا كان $a \equiv b(\mathrm{mod}\, p)$ فإن $f(a) \equiv f(b)(\mathrm{mod}\, p)$. كثيرات الحدود تحقق هذه الخاصية، ولذا يكون من المناسب اختيار f على أنها كثيرة حدود. ومن المستحسن أن تشابه f دالة معرفة على $\mathbb{Z}_p$ ، وذلك لتحسين فرص النجاح. إحدى هذه الدوال هي $f(x) = x^2 + 1$ حيث البذرة $x_0 = 2$ (من الممكن اختيار دالة أخرى ولكن بالتأكيد ليست دالة خطية).

وبهذا تكون تفاصيل الطريقة على النحو التالي لكثيرة حدود f بمعاملات صحيحة و $x_0 \in \mathbb{Z}_n$: نبدأ بوضع $x = x_0$ و $y = y_0$ ونكرر الخطوتين:

$$x \leftarrow f(x)(\mathrm{mod}\, n)$$
$$y \leftarrow f(f(y))(\mathrm{mod}\, n)$$

إلى أن نحصل على $d = (x-y, n) > 1$. إذا كان $d < n$ فنكون قد نجحنا في تحليل n. أما إذا كان $d = n$ فالطريقة تفشل وفي هذه الحالة نجرب دالة أخرى f وبذرة أخرى x_0.

بما أن $p \leq \sqrt{n}$ فمن المتوقع أن يكون الزمن اللازم لحساب f هو على الأكثر $3\sqrt{\pi p\,/\,2} = O(\sqrt{p}) = O(n^{1/4})$. ومع أن هذه الطريقة لا تعدُّ فعالة من الناحية

النظرية، إلا أنها أفضل من تجريب جميع d حيث $1 < d \leq \sqrt{n}$ لنرى فيما إذا كان $d \mid n$ ، حيث الزمن الذي تحتاجه هذه الطريقة يساوي $O\left(n^{1/2}\right)$ عملية قسمة.

وكمثال، دعنا نستخدم طريقة رو لتحليل $n = 551$ حيث $f(x) = x^2 + 1 (\mathrm{mod}\, 551)$ و $x_0 = 2$. الجدول التالي يبين خطوات حساب x ، y ، $d = (x - y, n)$.

$x \leftarrow f(x)$	$y \leftarrow f(f(y))$	$d = (x - y, 551)$
5	26	1
26	449	1
126	240	19

لاحظ أن كلا العددين 19 و $\frac{551}{19} = 29$ هو عدد أولي. وبهذا نكون قد حصلنا على تحليل العدد $551 = 19 \cdot 29$.

(١١,٤,٢) المربعات العشوائية

من أفضل طرق تحليل أعداد عامة هي عائلة المربعات العشوائية حيث استخدمت طريقة المرشح التربيعي (quadratic sieve) في العام ١٩٩٤م لتحليل أعداد عدد مراتبها العشرية بين 100 إلى 129 مرتبة. واستخدمت طريقة أكثر تعقيداً من هذه العائلة تدعى مرشح الحقل العددي (number field sieve) في العام ١٩٩٦م لتحليل عدد مكون من 130 مرتبة عشرية، وفي العام ١٩٩٩م لتحليل عددين عدد مراتبهما العشرية هو 140 و 155 مرتبة، وهذه الأعداد هي الأعداد التي اقترحتها مختبرات RSA. والتي أطلق عليها تحدي RSA.

لنفرض أن n عدد مؤلف. المطلوب هنا هو إيجاد $x, y \in \mathbb{Z}_n$ حيث $x^2 \equiv y^2 (\mathrm{mod}\, n)$. فإذا كان $x \not\equiv \pm y (\mathrm{mod}\, n)$ فإن $(x + y, n)$ هو قاسم غير تافه للعدد n ؛ لأن n يقسم $x^2 - y^2 = (x - y)(x + y)$ ولكن n لا يقسم أي من العددين

$x-y$ و $x+y$. وكحالة خاصة، إذا كان $n=pq$ حيث p و q عددان أوليان مختلفان فعندئذ يكون عدد حلول التطابق $x^2 \equiv a^2 (\mathrm{mod}\, n)$ يساوي أربعة حلول ($a \in \mathbb{Z}_n^*$ معطى) ويمكن إيجاد هذه الحلول باستخدام مبرهنة الباقي الصينية. على سبيل المثال، إذا كان $n=15$ واستطعنا بطريقة أو بأخرى الحصول على $x=2$ و $y=7$ تحقق التطابق $x^2 \equiv y^2 (\mathrm{mod}\, 15)$ فنجد أن $(x+y,n)=(9,15)=3$ وهذا قاسم غير تافه للعدد 15.

إحدى الطرق المتبعة لإيجاد x و y مناسبين هي حساب مجموعة الأزواج المرتبة $\left(a_i, b_i \equiv a_i^2 (\mathrm{mod}\, n)\right)$ حيث a_i عدد عشوائي ومحاولة إيجاد مجموعة جزئية S بحيث يكون $\prod_{i \in S} b_i$ مربعاً كاملاً. في هذه الحالة، $x = \prod_{i \in S} a_i$ والجذر التربيعي y للعدد $\prod_{i \in S} b_i$ يحققان $x^2 \equiv y^2 (\mathrm{mod}\, n)$. وإضافة إلى ذلك، إذا كان $x \not\equiv \pm y (\mathrm{mod}\, n)$ فنكون قد نجحنا في تحليل n، وإذا كان $x \equiv \pm y (\mathrm{mod}\, n)$ فنقوم باختيار مجموعة S مختلفة (من الممكن أن نحتاج لتوليد المزيد من الأزواج المرتبة $\left(a_i, b_i\right)$).

بصورة أدق نقوم باختيار أساس للتحليل $B = \{p_1, p_2, \ldots, p_t\}$ تحتوي على أول t من الأعداد الأولية. إذا استطعنا تحليل b على B فنأخذ الزوج المرتب $\left(a, b \equiv a^2 (\mathrm{mod}\, n)\right)$ ويسمى b في هذه الحالة عدد ناعم من النوع p_t (p_t-smooth). لنفرض أننا حصلنا على الأزواج المرتبة $\left(a_i, b_i\right)$ حيث $1 \le i \le t+1$، $b_i = \prod_{j=1}^{t} p_j^{e_{ij}}$ هو تحليل b_i. الآن، نقوم باختيار المجموعة S بحيث تظهر القوى الزوجية فقط للأعداد الأولية في العدد $\prod_{i \in S} b_i$. لاحظ أن أي $t+1$ متجهاً $e_i = \left(e_{i1}, \ldots, e_{it}\right) (\mathrm{mod}\, 2)$ يجب أن تكون مرتبطة خطياً على $\mathbb{Z}_2$ وتوجد مجموعة S يكون $\sum_{i \in S} e_i$ هو المتجه الصفري. عندئذ، يكون العدد $\prod_{i \in S} b_i$ على الشكل المطلوب.

مثال (١١,٤,١)

نوظف الطريقة لتحليل $n = 10057$. لنفرض أن $t = 5$. عندئذ، أساس التحليل هو المجموعة $B = \{2,3,5,7,11\}$ الجدول التالي يبين خيارات a_i حيث يحتفظ فقط بالخيارات التي تؤدي إلى تحليل $b_i \equiv a_i^2$ على أساس التحليل.

i	a_i	$b_i \equiv a_i^2 (\bmod n)$	التحليل
1	7231	1018	$2 \cdot 509$
1	105	968	$2^3 \cdot 11^2$
2	115	3168	$2^5 \cdot 3^2 \cdot 11$
3	1006	6336	$2^6 \cdot 3^2 \cdot 11$
4	3010	8800	$2^5 \cdot 5^2 \cdot 11$
5	4014	882	$2 \cdot 3^2 \cdot 7^2$
6	4023	2816	$2^8 \cdot 11$

لاحظ إهمال الخيار $a = 7231$ ؛ لأن $a^2 (\bmod n)$ لا يتحلل تماماً على أساس التحليل. وفي هذه الحالة التحليل المقابل في العمود الأخير هو فقط تحليل جزئي.

يوجد عدد $t + 1 = 6$ من الأزواج المرتبة (a_i, b_i). ومن ثم توجد مجموعة S بحيث يكون $\prod_{i \in S} b_i$ مربعاً كاملاً. وبالتجريب نجد أن $S = \{4,5,6\}$ تؤدي إلى $x^2 \equiv y^2 (\bmod n)$ حيث $x = 3010 \cdot 4014 \cdot 4023 \equiv 2748 (\bmod n)$ و $y = 2^7 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \equiv 7042 (\bmod n)$. وبما أن $x \not\equiv \pm y (\bmod n)$ فنحصل على القاسم غير التافه $(x + y, n) = 89$ ويكون $n = 10057 = 89 \cdot 113$.

من الممكن أيضاً الحصول على مربع كامل باختيار $S = \{1,5\}$. والقيم المقابلة لذلك هي $x = 105 \cdot 4014 \equiv 9133 (\bmod n)$ و $y = 2^2 \cdot 3 \cdot 7 \cdot 11 = 924$. ولكن $x \equiv -y (\bmod n)$. وبهذا لا نحصل على معلومات مفيدة من هذا الخيار. ▲

لاحظ أن اختيار أساس تحليل أكبر يزيد من فرصة أن يكون b_i ناعم من النوع p_t ولكن هذا يحتاج إلى المزيد من العلاقات. إذا كان t معطى فإحدى الإستراتيجيات المتبعة لزيادة فرص الحصول على أعداد ناعمة من النوع p_t هي اختيار a بحيث يكون $b \equiv a^2 (\mathrm{mod}\, n)$ صغيراً نسبياً. ومثال مشهور على ذلك هي طريقة المرشح التربيعي.

لنفرض أن n معطى وأن $m = \left\lfloor \sqrt{n} \right\rfloor$. نعرف الدالة $q : \mathbb{Z} \to \mathbb{Z}$ بالقاعدة $q(z) = (z+m)^2 - n$. لاحظ أن $q(z) \approx z^2 + 2zm$ وإذا كان $|z|$ صغيراً فإن $|q(z)|$ صغير بالنسبة إلى n. في خوارزمية المرشح التربيعي نضع $a = z + m$ و $b = q(z) = a^2 - n$ حيث $z = 0, \pm 1, \ldots$. بما أنه من الممكن أن يكون b سالباً فإننا نضيف -1 إلى أساس التحليل. إضافة إلى ذلك، لاحظ أنه إذا كن p قاسماً أولياً للعدد b فإن $a^2 \equiv n (\mathrm{mod}\, p)$. وبهذا يكون n راسباً تربيعياً قياس p (إلا إذا كان $p \mid n$). ولذا فأساس التحليل يحتاج فقط احتواء الأعداد الأولية p التي تحقق $\left(\frac{n}{p}\right) = 1$.

مثال (١١,٤,٢)

سنحلل العدد $n = 10057$ المقدم في المثال السابق. ضع $m = \left\lfloor \sqrt{n} \right\rfloor = 100$ و $q(z) = (z+100)^2 - 10057$. لنفرض أن أساس التحليل هو $B = \{-1\} \cup \{2, 3, 11, 19\}$ (B تحتوي على الأعداد الأولية $p \leq 19$ التي تحقق $\left(\frac{n}{p}\right) = 1$). الجدول التالي يبين بعض قيم z التي تجعل $q(z)$ يتحلل على أساس التحليل:

z	$a = z + m$	$b = q(z)$	التحليل
0	100	-57	$-3 \cdot 19$
-1	99	-256	-2^8
1	101	144	$2^4 \cdot 3^2$
-3	97	-648	$-2^3 \cdot 3^4$
5	105	968	$2^3 \cdot 11^2$

من العلاقات للعدد $z \in \{-1,-3,5\}$ نجد أن $x^2 \equiv y^2 (\mathrm{mod}\, n)$ حيث $x = 99 \cdot 97 \cdot 105$ و $y = 2^7 \cdot 3^2 \cdot 11$. ولكن $x \equiv y (\mathrm{mod}\, n)$ في هذه الحالة ومن ثم فالطريقة تفشل في تحليل n. وإذا اخترنا $z = 1$ فنجد أن $101^2 \equiv 2^4 \cdot 3^2$. وبملاحظة أن $x = 101$ و $y = 2^2 \cdot 3$ يحققان $x \not\equiv \pm y (\mathrm{mod}\, n)$ فإننا نحصل على قاسم غير تافه $(x + y, n) = 133$ للعدد 10057. ▲

تحتاج عملية اختيار الأزواج المرتبة المناسبة (a,b) إلى جهد كبير، ويستعاض عن طريقة تجريب القواسم بطريقة المرشح الأكثر فعالية لاختبار النعومة. على سبيل المثال، في العام ١٩٩٤م احتاج تحليل العدد المشهور المكون من 129 مرتبة إلى 600 شخص و 1600 آلة للحصول على أكثر من 8 ملايين علاقة خلال سبعة أشهر حيث كان عدد عناصر أساس التحليل يساوي 524339 (انظر [1]). ومنذ العام ١٩٩٩م تبين أن محاولة تحليل عدد مختار جيداً n عدد مراتبه الثنائية يساوي 1024 (308 مرتبة عشرية) هي محاولة مستحيلة حتى مع استخدام طريقة مرشح الحقل العددي المطورة.

(١١,٤,٣) الجذور التربيعية

يبين البند السابق وجود علاقة بين مسألتي التحليل والجذور التربيعية. في الحقيقة هاتان المسألتان متكافئتان وهذا ما سنبينه في هذا البند.

تذكر أن طريقة تحليل المربعات العشوائية تتم بمحاولة إيجاد x و y حيث $x^2 \equiv y^2 (\mathrm{mod}\, n)$. فإذا كان $x \not\equiv \pm y (\mathrm{mod}\, n)$ فإننا نحصل على قاسم غير تافه $(x + y, n)$ للعدد n. وبهذا يكون من الواضح أننا لو استطعنا إيجاد جميع الجذور التربيعية لراسب تربيعي $x^2 \in \mathbb{Z}_n^*$ فإننا سنحصل على قاسم غير تافه للعدد n. من المعلوم عدم وجود طريقة فعالة عامة لإيجاد الجذور التربيعية ومع ذلك سنناقش ما ستؤديه مثل هذه الخوارزمية.

سندرس الطريقة للمثال $n = pq$ حيث p و q عددان أوليان فرديان مختلفان (يمكن تعميم هذه الطريقة على الحالة العامة). استناداً إلى النتيجة (**١١,٢,٢**) نرى وجود جذران تربيعان بالضبط لراسب تربيعي قياس عدد أولي. ويمكن اللجوء إلى مبرهنة الباقي الصينية لإثبات وجود أربعة جذور تربيعية للتطابق $x^2 \equiv a(\mathrm{mod}\, pq)$ حيث $a \in Q_{pq}$.

لنفرض الآن وجود خوارزمية يكون مخرجها جذراً تربيعياً للعدد $a \in Q_{pq}$. لتحليل العدد pq ، نقوم باختيار عشوائي لعدد $x \in \mathbb{Z}_n^*$ وإدخال $x^2(\mathrm{mod}\, n)$ إلى الخوارزمية. لكل من الأعداد المختارة x نجد باحتمال يساري $\frac{1}{2}$ أن $y \not\equiv \pm x(\mathrm{mod}\, n)$ حيث y هو الجذر التربيعي الناتج عن تنفيذ الخوارزمية. أي من المتوقع الحصول على قاسم غير تافه $(x+y,n)$ للعدد n بمحاولتين فقط.

نقول إن مسألة تحليل n تختزل إلى مسألة إيجاد الجذور التربيعية. وبدقة أكثر، إذا كانت A و B مسألتين حسابيتين فنكتب $A \leq B$ ، إذا استطعنا حل المسألة A بزمن حدودي (بدلالة حجم البيانات المدخلة) بوجود خوارزمية حدودية لحل المسألة B. أي أن $A \leq B$ تعني أن المسألة A ليست أصعب من المسألة B. ونقول إن المسألتين A و B متكافئتان حسابياً إذا كان $A \leq B$ و $B \leq A$. ونستخدم المفهوم نفسه في حالة الخوارزميات العشوائية التي تحتاج لزمن تنفيذ حدودي بدلالة سعة المدخلات. على وجه الخصوص FACTOR $\leq$ SQROOT.

سنبين الآن كيفية إيجاد الجذور التربيعية لراسب تربيعي $a \in Q_n$ إذا علمنا تحليل n (أي سنبرهن أن SQROOT $\leq$ FACTOR). لنفرض أن لدينا الجذور التربيعية قياس كل من العددين الأوليين p و q. عندئذ، نستطيع إيجاد الجذور التربيعية الأربعة للعدد a قياس $n = pq$ وذلك بإيجاد x و y اللذان يحققان التطابقات:

$$\left\{\begin{matrix} x \equiv a_p(\mathrm{mod}\, p) \\ x \equiv a_q(\mathrm{mod}\, q) \end{matrix}\right\} \quad \text{و} \quad \left\{\begin{matrix} y \equiv -a_p(\mathrm{mod}\, p) \\ y \equiv a_q(\mathrm{mod}\, q) \end{matrix}\right\}$$

حيث a_r هو جذر تربيعي للعدد a قياس r. عندئذ، الجذور الأربعة هي $\pm x$ و $\pm y$. وبهذا نكون قد وجدنا خوارزمية فعالة لمسألة SQROOT على فرض وجود خوارزمية فعالة لإيجاد الجذور التربيعية قياس عدد أولي.

لنفرض أولاً الحالة التي يكون فيها العدد الأولي p على الصورة $p \equiv 3(\mathrm{mod}\, 4)$. عندئذ، استناداً إلى معيار أويلر نجد أن:

$$a^{(p-1)/2} \equiv 1(\mathrm{mod}\, p)$$

حيث $a \in Q_p$. ومن ثم فإن:

$$\left(a^{(p+1)/4}\right)^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2}a \equiv a(\mathrm{mod}\, p)$$

إذن، الجذران التربيعيان للعدد a قياس العدد p هما $\pm a^{(p+1)/4}$. الآن، إذا كان كل من العددين الأوليين p و q على الصورة $4k+3$ (يسمى العدد $n = pq$ في هذه الحالة، عدد بلم Blum integer) فنكون قد وجدنا خوارزمية فعالة لإيجاد الجذور التربيعية للعدد a قياس n.

في الحقيقة، توجد خوارزمية سهلة نسبياً لإيجاد الجذور التربيعية قياس عدد أولي إذا علمنا راسب غير تربيعي (على وجه الخصوص، إذا كان $p \equiv 5(\mathrm{mod}\, 8)$ فإن $2 \in \overline{Q_p}$، انظر [63]). ولكن لا توجد خوارزمية فعالة غير احتمالية لإيجاد راسب غير تربيعي قياس عدد أولي. وبما أن نصف عناصر $\mathbb{Z}_p^*$ هي رواسب غير تربيعية فتوجد خوارزمية فعالة احتمالية لإيجاد الجذور التربيعية قياس عدد أولي وذلك باختيار أعداد عشوائية x حتى الحصول على عدد يحقق $\left(\frac{x}{p}\right) = -1$.

مما سبق نستطيع ضمان طرق فعالة لإيجاد الجذور التربيعية قياس عدد أولي. وبهذا يكون SQROOT $\leq$ FACTOR ونخلص إلى تكافؤ المسألتين حسابياً. سنناقش ذلك لاحقاً في البند (**١٢,٣**) مرة أخرى عند دراستنا لبرهان أمن أنظمة التعمية.

تمارين

(**١١,٤,٣**) يوضح هذا التمرين طريقة رو لبولارد لتحليل العدد $n = 391 = 17 \cdot 23$:

(أ) نفذ طريقة رو لبولارد حيث $x_0 = 2$ و $x_{i+1} = f(x_i) = x_i^2 + 1 (\mathrm{mod}\, n)$ (تذكر أن الخوارزمية تتوقف عندما يكون $1 < \left(x_{2i} - x_i, n\right) < n$. سنحصل على قاسم غير تافه عندما يكون $i = 4$).

(ب) أكمل الجدول التالي :

i	0	1	2	3	4	5	6	7	8
$x_i (\mathrm{mod}\, 17)$	2	5	9	14	10	16	2		
$x_i (\mathrm{mod}\, 23)$	2								

ارسم مخطط رو لكل صف من صفوف الجدول موضحاً الذيل والدورة.

(ج) بين كيفية اختيار عدد مؤلف n يؤدي إلى فشل طريقة رو لبولارد لتحليل هذا العدد.

(**١١,٤,٤**) حلل العدد $n = 5141$ بطريقة رو لبولارد مستخدماً $x_0 = 1$ و $x_{i+1} \equiv x_i^2 + 2 (\mathrm{mod}\, n)$ ، $i \geq 0$.

(**١١,٤,٥**) حلل العدد $n = 1081$ بطريقة المرشح التربيعي (كما في المثال (**١١,٤,٢**)) مستخدماً أساس تحليل مناسب يحتوي على جميع الأعداد الصحيحة التي لا يزيد عن العدد 11.

(**١١,٤,٦**) حلل العدد $n = 24961$ بطريقة المرشح التربيعي (كما في المثال (**١١,٤,٢**)) مستخدماً أساس تحليل مناسب يحتوي على جميع الأعداد الصحيحة التي لا تزيد عن العدد 23.

(**١١,٤,٧**) إذا كان $n = ab$ حيث $|a - b|$ صغير نسبياً فمن الممكن تحليل العدد بخطوات قليلة باستخدام طريقة فيرما للتحليل التي يمكن وصفها على النحو التالي :

- لنفرض أن n عدد فردي. يوجد تقابل بين تحليل n على الصورة $n = ab$ حيث $0 < a \leq b$ والتمثيل $n = t^2 - s^2$ حيث t و s عددان صحيحان غير سالبين. هذا التقابل هو:

$$ab = t^2 - s^2 = (t - s)(t + s)$$

حيث $t = \dfrac{a+b}{2}$ و $s = \dfrac{a-b}{2}$.

- إذا كان العددان a و b قريبان من بعضهما فإن $s = \dfrac{a-b}{2}$ عدد صغير ويكون $t \approx \sqrt{n}$.
- لتحليل n ، نقوم بتجريب قيم متتالية للعدد t مبتدئين بالقيمة $\lceil \sqrt{n} \rceil$ حتى نحصل على مربع كامل $t^2 - n$.

حلل العدد $n = 2881$ بطريقة فيرما للتحليل. لمعرفة تفاصيل طريقة فيرما للتحليل (انظر [50] و [74]).

(**١١,٤,٨**) بين كيفية الحصول على الجذور التربيعية للعدد $179 \in \mathbb{Z}_{187}$ مستخدماً التحليل $187 = 11 \cdot 17$.

(**١١,٤,٩**) صمم اختبار فعال لمعرفة فيما إذا كان n قوة كاملة (أي أن $n = x^k$ حيث x عدد صحيح و $k > 1$). إذا كان n قوة كاملة فجد تحليل جزئي للعدد n.

(**١١,٤,١٠**) لنفرض أن $n = pq$ حيث $p \neq q$ عددان أوليان ولنفرض أن $\varphi = \varphi(n) = (p-1)(q-1)$. مسألة حساب φ يرمز لها بالرمز COMPUTE Φ وهي مسألة إيجاد φ بمعرفة n. صمم خوارزمية فعالة لمسألة FACTOR بمعرفة خوارزمية لحساب COMPUTE Φ.

(١١,٥) اللوغاريتمات المنفصلة
Discrete Logarithms

لنفرض أن p عدد أولي فردي وأن α مولداً للزمرة $\mathbb{Z}_p^*$. لنفرض أن $\beta \in \mathbb{Z}_p^*$. اللوغاريتم المنفصل للعدد β للأساس α (the discrete logarithm of β to the base α) ويكتب $\log_\alpha \beta$ هو العدد الصحيح الوحيد x حيث $0 \le x \le p-2$ الذي يحقق $\beta \equiv \alpha^x \pmod n$. على سبيل المثال، $\alpha = 3$ مولداً للزمرة $\mathbb{Z}_5^*$ وأن $\log_3 4 = 2$ لأن $4 \equiv 3^2 \pmod 5$.

مسألة اللوغاريتيم المنفصل أو اختصاراً DLP تنص على:

جد x إذا علمت (p, α, β).

كما هو الحال في مسألة تحليل العدد فإن مسألة اللوغاريتم المنفصل مسألة تافهة من الناحية النظرية وذلك بالقيام بحساب α^x بتجريب قيم $x \ge 0$ حتى نجد β. ولكن هذه الطريقة غير فعالة؛ لأنها تحتاج إلى $O(p)$ عملية ضرب قياس p. لا توجد خوارزمية فعالة لحساب مسألة اللوغاريتم المنفصل ولهذا يعتمد أمن العديد من أنظمة التعمية على فرضية عدم وجود خوارزمية فعالة لحل مسألة DLP. سنقدم هنا خوارزميتان لحساب DLP وكلاهما ليست حدودية ولكنهما أفضل من طريقة الاستنفاد.

(١١,٥,١) الخطوة الصغيرة والخطوة الكبيرة

تشبه خوارزمية الخطوة الصغيرة والخطوة الكبيرة إلى حد ما هجوم اللقاء في المنتصف على النظام DES المضاعف حيث يكون عدد عمليات الضرب قياس العدد أصغر من عدد العمليات باستخدام طريقة الاستنفاد ولكن ذلك يكون على حساب سعة التخزين اللازمة.

لنفرض أن $m = \left\lfloor \sqrt{p-1} \right\rfloor$. إذا كان $\beta \equiv \alpha^x \pmod p$ فحينئذ نكتب $x = im + j$ حيث $0 \le i, j < m$ و $\beta \equiv \alpha^x \equiv \alpha^{im}\alpha^j$ أو $\beta\alpha^{-im} \equiv \alpha^j$. نشكل الآن جدولاً مدخلاته $\left(j, \alpha^j \pmod p\right)$ حيث $0 \le j < m$. لكل i،

$0 \le i < m$. نقوم بحساب $\beta\alpha^{-im} \pmod p$ ونبحث عن قيمة مساوية لهذا العدد في الجدول. وعند وجود هذه القيمة يكون لدينا:

$$\beta\alpha^{-im} \equiv \alpha^j \pmod p .$$

ومن ثم نحصل على:

$$\log_\alpha \beta = im + j .$$

مثال (١١,٥,١)

لنفرض أن $p = 41$ ، $\alpha = 6$ ، $\beta = 2$. سنقوم بتطبيق الخوارزمية لحساب $\log_6 2 \in \mathbb{Z}_{41}$.

بوضع $m = \left\lfloor \sqrt{40} \right\rfloor = 7$ وإنشاء جدول مدخلاته (j, α^j) حيث $0 \le j < 7$ نحصل على:

j	0	1	2	3	4	5	6
$\alpha^j \pmod p$	1	6	36	11	25	27	39

عندئذ، $\alpha^{-1} \equiv 7 \pmod p$ و $\alpha^{-m} \equiv 7^7 \equiv 17 \pmod{41}$. الآن، نقوم بحساب $\beta(\alpha^{-m})^i \pmod p$ حتى نحصل على المدخل المطلوب:

$$\begin{aligned}
\beta\left(\alpha^{-m}\right)^0 &\equiv \beta \equiv 2 && : \quad i = 0 \\
\beta\left(\alpha^{-m}\right)^1 &\equiv 2 \cdot 17 \equiv 34 && : \quad i = 1 \\
\beta\left(\alpha^{-m}\right)^2 &\equiv 34 \cdot 17 \equiv 4 && : \quad i = 2 \\
\beta\left(\alpha^{-m}\right)^3 &\equiv 4 \cdot 17 \equiv 27 && : \quad i = 3
\end{aligned}$$

وبهذا نحصل على قيمة من قيم الجدول عند $i = 3$ و $j = 5$ مما يؤدي إلى أن $\beta\alpha^{-3m} = \alpha^5$. أي أن $\beta \equiv \alpha^{21+5} \pmod p$ ويكون $\log_6 2 = 26 \in \mathbb{Z}_{41}$. ▲

يحتاج إنشاء الجدول إلى عدد $m - 1$ من عمليات الضرب قياس عدد. والخطوة الكبيرة تحتاج إلى أخذ المعكوس وعدد $O(m)$ من عمليات الضرب قياس عدد. ولذا

فالزمن اللازم لتنفيذ الخوارزمية يحتاج إلى $O\left(\sqrt{p-1}\right)$ من عمليات الضرب قياس عدد، وهذا أفضل من طريقة الاستنفاد ولكنه أسوأ بكثير من زمن حدودي.

(١١,٥,٢) حساب الدليل

إن أفضل الطرق لحساب اللوغاريتم المنفصل هي طرق معدلة من خوارزمية حساب الدليل وبعض من هذه الطرق يشبه خوارزميات المربعات العشوائية للتحليل. الخطوة الحسابية الأولى (غالية التكاليف) تجد لوغاريتمات عناصر أساس تحليل مختار B (ليس بالضرورة أن يعتمد على أعداد معينة β لحساب $\log_\alpha \beta$). أما الخطوة الثانية فتجد لنا عدد صحيح k حيث $\alpha^k\beta$ يتحلل على B. وبحالة نجاح الخطوتين يكون $\log_\alpha \beta$ سهل الحساب.

نقوم باختيار أساس التحليل $B=\{p_1,\ldots,p_t\}$ المكون من أول t عدد أولي. ولنفرض أن الحسابات هي قياس العدد الأولي p. في الخطوة الأولى نقوم باختيار أعداد عشوائية k لمحاولة إيجاد قيم $\alpha^k \pmod p$ بحيث تتحلل على B. وبهذا يكون:

$$\alpha^k \pmod p = p_1^{e_1}\ldots p_t^{e_t} \quad \text{حيث} \quad e_i \geq 0 .$$

ومن ذلك نجد أن:

$$k \equiv e_1 \log_\alpha p_1 + \ldots + e_t \log_\alpha p_i \pmod{p-1}$$

عادة نجد أكثر من t من هذه التطابقات على أمل نحصل على نظام معادلات خطية في المتغيرات $\log_\alpha p_i$ يكون له حل وحيد.

في الخطوة الثانية نبحث عن قيمة k بحيث يتحلل $\alpha^k\beta \pmod p$ على B. وإذا نجحنا في ذلك يكون $\alpha^k\beta \pmod p = p_1^{e_1}\ldots p_t^{e_t}$ حيث $e_i \geq 0$. ومن ذلك نرى أن:

$$k + \log_\alpha \beta \equiv e_1 \log_\alpha p_1 + \cdots + e_t \log_\alpha p_t \pmod{p-1}$$

ويكون:

$$\log_\alpha \beta = \left(e_1 \log_\alpha p_1 + \cdots + e_t \log_\alpha p_t - k\right) \pmod{p-1} .$$

مثال (١١,٥,٢)

لنفرض أن $p = 19$ ، $\alpha = 2$. سنجد $\log_\alpha 17$. لنفرض أن أساس التحليل هو $B = \{2,3,5\}$. في هذا المثال، $\alpha \in B$ ونحصل مباشرة على $\log_\alpha 2 = 1$. لإيجاد لوغاريتمات العنصرين الآخرين من عناصر B نقوم بحساب $\alpha^k \pmod p$ لعدد عشوائي k بحيث نحصل على قيمتين على الأقل كل منهما تتحلل على B :

$$2^9 \pmod p = 2 \times 3^2$$
$$2^7 \pmod p = 14$$
$$2^{11} \pmod p = 3 \times 5$$

يهمل السطر الثاني ؛ لأن 14 لا يتحلل على B . ومن ذلك نحصل على نظام التطابقات :

$$9 \equiv \log_\alpha 2 + 2\log_\alpha 3 \pmod{p-1}$$
$$11 \equiv \log_\alpha 3 + \log_\alpha 5 \pmod{p-1}$$

في المجهولين $\log_\alpha 3$ و $\log_\alpha 5$.

هذا النظام له أكثر من حل. ولذا فمن الممكن أن نحصل على إجابات خاطئة مثل $\log_\alpha 3 = 4$ و $\log_\alpha 5 = 7$. لهذا نقوم بإضافة علاقة أخرى مثل $\alpha^{14} \pmod p = 6$ لنحصل على تطابق جديد $14 \equiv \log_\alpha 2 + \log_\alpha 3 \pmod{p-1}$. ومن ثم يكون للنظام الجديد حل وحيد هو :

$$\log_\alpha 3 = 13 \text{ و } \log_\alpha 5 = 16 .$$

الآن، لإيجاد $\log_\alpha 17$ نبحث عن k بحيث يتحلل $\alpha^k \times 17 \pmod p$ على B . على سبيل المثال، إذا كان $k = 5$ فنجد أن $\alpha^5 \times 17 \pmod p = 2^2 \cdot 3$. وبهذا يكون :

$$\log_\alpha 17 \equiv \left(2\log_\alpha 2 + \log_\alpha 3 - 5\right) \equiv 10 \pmod{p-1} .$$ ▲

إن عملية حساب اللوغاريتمات لعناصر أساس التحليل مكلفة جداً على الرغم من إمكانية توزيع عمليات إيجاد العلاقات المناسبة. يمكن استخدام نتائج الخطوة الأولى

لحساب لوغاريتم أي β معطى بعد إيجاد قيمة k يتحلل $\alpha^k\beta$ على أساس التحليل. إن اختيار أساس تحليل أكبر يسمح بتمثيل عناصر أكثر من $\mathbb{Z}_p^*$ كحاصل ضرب عناصر B ولكن هذا يؤدي إلى حل نظام تطابقات أكبر.

استخدمت هذه الطريقة في العام ١٩٩٠م لحساب لوغاريتمات قياس أعداد أولية عدد مراتبها يقع بين 50 و 100 مرتبة عشرية. على سبيل المثال، قام كل من لاماتشايا (La Macchia) وأدليكو (Odlyzko) (انظر [54]) في العام ١٩٩٠م بحساب لوغاريتمات قياس عدد أولي مكون من 192 مرتبة ثنائية (58 مرتبة عشرية) بزمن معقول باستخدام طريقة معدلة لحساب الدليل تعرف بطريقة أعداد جاوس الصحيحة حيث استطاعوا باختصار نظام مكون من 288017 علاقة بعدد من المجاهيل يساوي 96321 إلى نظام مكون من 7262 علاقة وعدد من المجاهيل يساوي 6006 ومن ثم حل هذا النظام. ثم استخدمت هذه البيانات لحساب لوغاريتمات معينة بجهد بسيط نسبياً. كان لهذا الجهد أهمية عملية حيث يعتمد أمن خطط إثبات الهوية المقترح من قبل أنظمة الميكرو على صعوبة حل مسألة اللوغاريتمات المنفصلة قياس عدد أولي (انظر [88]).

قام كل من جو (Joux) وليرسير (Lercier) في العام ١٩٩٨م بحساب لوغاريتمات منفصلة في الزمرة $\mathbb{Z}_p^*$ حيث p عدد أولي مكون من 90 مرتبة باستخدام طريقة أعداد جاوس الصحيحة مستخدمين لهذا الغرض شبكة مكونة من أربعة حاسبات استطاعت خلال شهر واحد من الحصول على $6 \cdot 7$ مليون معادلة ومن ذلك حصلوا على 976062 معادلة ظهر فيها كل من المتغيرات على الأقل مرتين. بعد ذلك استطاعوا خلال ثلاثة أسابيع من اختصار النظام الخطي وحله. احتاج حساب لوغاريتمات مختارة إلى 9 ساعات في المتوسط باستخدام حاسب آلي واحد.

لقد استخدم مرشح الحقل العددي لتحليل الأعداد في حساب مسألة اللوغاريتمات المنفصلة، حيث استخدم كل من جو وليرسر في العام ١٩٩٩م طريقة مرشح معدلة

لحساب لوغاريتمات في الزمرة $\mathbb{Z}_p^*$ حيث عدد مراتب p يساوي 100. استخدموا لذلك حاسب آلي من نوع بنتيوم II جمعت خلال ثمانية شهور $2 \cdot 8$ مليون معادلة ثم استخدموا بعد ذلك معالج (DES Alpha 500 MHZ) لحل نظام المعادلات الخطي خلال ثلاثة أسابيع. احتاج حساب لوغاريتمات مختارة إلى يوم واحد. وبهذا استنتجوا أن طريقة مرشح الحقل العددي أفضل من طريقة أعداد جاوس الصحيحة لحساب اللوغاريتمات المنفصلة قياس أعداد أولية مكونة من أكثر من 100 مرتبة (انظر [46]).

تمارين

(١١,٥,٣) إذا علمت أن $\alpha = 5$ مولّداً للزمرة $\mathbb{Z}_{97}^*$ فاستخدم طريقة الخطوة الصغيرة والخطوة الكبيرة لحساب $\log_5 4 \in \mathbb{Z}_{97}$.

(١١,٥,٤) لنفرض أن $p = 41$ وأن $\alpha = 6$ مولّداً للزمرة $\mathbb{Z}_p^*$. وضح طريقة حساب الدليل لحساب $\log_6 13$ وذلك بإكمال الخطوات التالية:

(أ) اختار $B = \{2,3,5\}$ أساساً للتحليل. افرض أنه تم حساب $\alpha^k \pmod p$ حيث $k \in \{8,20,16\}$ وكانت نتيجة الحسابات هي:

$$\alpha^8 \pmod p = 10 \Rightarrow 8 \equiv \log_\alpha 2 + \log_\alpha 5 \pmod{p-1}$$
$$\alpha^{20} \pmod p = 40 \Rightarrow 20 \equiv 3\log_\alpha 2 + \log_\alpha 5 \pmod{p-1}$$
$$\alpha^{16} \pmod p = 18 \Rightarrow 16 \equiv \log_\alpha 2 + 2\log_\alpha 3 \pmod{p-1}$$

تحقق من أن نظام التطابقات ليس له حل وحيد $\left(\log_\alpha 2, \log_\alpha 3, \log_\alpha 5\right)$.

(ب) أضف التطابق الذي تحصل عليه من $\alpha^1 \pmod p = 2 \cdot 3$ ومن ثم حل النظام (قيمة $\log_\alpha 2$ يجب أن تكون مساوية للقيمة التي حصلنا عليها في المثال **(١١,٥,١)**).

(ج) جد $\log_\alpha 13$ بتطبيق (ب) على $\alpha^k \cdot 13 \pmod p$ حيث $k = 11$.

(١١,٥,٥) ليكن p عدداً أولياً و α مولّداً للزمرة $\mathbb{Z}_p^*$. بين أن المرتبة الثنائية الأقل أهمية للعدد x يمكن حسابها بفعالية من $\alpha^x \pmod p$.

(**١١,٥,٦**) ناقش باخ (انظر [2]) العلاقة بين تحليل الأعداد وحساب اللوغاريتمات. على وجه الخصوص يبين هذا التمرين أن وجود خوارزمية لحساب x حيث $a^x \equiv b(\mathrm{mod}\, n)$ يؤدي إلى خوارزمية احتمالية لتحليل عدد مؤلف n. لنفرض أن $n = pq$ حيث $p \neq q$ عددان أوليان فرديان. ولنفرض أن $\lambda = lcm\big(\varphi(p), \varphi(p)\big)$.

(أ) أثبت أن $K = \left\{ z \in \mathbb{Z}_n^* : z^{\lambda/2} \equiv \pm 1(\mathrm{mod}\, n) \right\}$ هي زمرة جزئية فعلية من $\mathbb{Z}_n^*$. استنتج أن على الأقل نصف عناصر $\mathbb{Z}_n^*$ لا تنتمي إلى K.

(ب) لنفرض أن $a \in \mathbb{Z}_n^* \setminus K$ وأن $a^x \equiv 1(\mathrm{mod}\, n)$ حيث $x \neq 0$ (يسمى قوة a). أثبت وجود k حيث $0 < k < \log_2 x$ جذر تربيعي غير تافه للعدد 1 (أي أن $a^{x/2^k} \not\equiv \pm 1$ وأن $\left(a^{x/2^k}\right)^2 \equiv 1$).

(ج) استنتج أن $\left(a^{x/2^k} + 1, n\right)$ قاسم غير تافه للعدد n.

نحصل الآن على خوارزمية التحليل التالية التي تستخدم الخوارزمية $a^x \equiv b(\mathrm{mod}\, n)$ لإيجاد قوة للعدد a. على الرغم من أن $\varphi(n)$ غير معلوم، إلا أنه يوجد r من بين أول $\log_2 n$ عدد أولي حيث $(r, \varphi(n)) = 1$. لهذا العدد r تقدم الخوارزمية حلاً y للتطابق $\left(a^r\right)^y \equiv a(\mathrm{mod}\, n)$ وقوة $x = ry - 1$ للعدد a.

(١١,٦) حواشي
Notes

معظم المادة التي قدمت في هذا الفصل هي مادة تقليدية يمكن إيجادها في عديد من الكتب الجيدة. على سبيل المثال (انظر [74] و [50]). الفصلان الثاني والثالث من [63] يغطيان بعض المادة المهمة ويحتوي على عديد من المراجع. يقدم [50] عديد من الأمثلة لحساب الزمن اللازم (بدلالة عدد العمليات الثنائية) للعمليات الحسابية وهو موضوع نادراً ما تجده في كتب نظرية الأعداد.