حول خوارزمية احتمالية

ناجي هرماس
أستاذ بقسم الرياضيات، جامعة زيان عاشور، الجلفة
nadjihermas@gmail.com

1. خواص شائعة للأعداد الأولية

الأعداد الأولية لها أهمية مركزية في نظرية الأعداد، وتعتبر الجواهر الفردية في عالم الأعداد، حيث إنها تدخل في تركيب بقية الأعداد الطبيعية، وبذلك تُماثل في العالم المادي الذرات التي تتكون منها كل عناصر المادة في الكون. وقد برهن أقليدس وجود ما لا نهاية منها. ونظرًا لأن لهذه الأعداد أهمية في بعض التطبيقات الملموسة مثل استخدامها الحاسم في علم التعمية (Cryptography)، فإنه تجري في الوقت الحالي عمليات حسابية هائلة مستندة إلى الحاسبات الحديثة لاكتشاف أكبر عدد ممكن منها. نشير مثلا إلى أن العدد الميرسيني $2^{1398269}-1$، والذي يتكوّن من أكثر من 400 ألف رقم عشري، هو أحد أكبر الأعداد الأولية المكتشفة حديثا، وقد تم الوصول إلى هذه النتيجة في شهر نوفمبر من عام 1996. وللعلم فإن الأعداد الميرسينية المنسوبة إلى عالم الرياضيات الفرنسي ميرسين (Mersenne) هي الأعداد ذات الشكل 2^n-1، حيث n عدد طبيعي.

فيما يلي نعرض بعض الخواص البسيطة للأعداد الأولية.

ليكن n عددًا طبيعيًا معطى غير معدوم. نعرّف على مجموعة الأعداد الصحيحة $\mathbb{Z}$ علاقة تكافؤ كما يلي:

$$\forall_{a\in\mathbb{Z}}, \forall_{b\in\mathbb{Z}}: a \equiv b \bmod n \Leftrightarrow a-b \in n\mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z}: a-b=kn.$$

إن صف تكافؤ العدد الصحيح a وفق هذه العلاقة هو "تعريفًا" المجموعة

$$\bar{a}=\{a+kn: k\in\mathbb{Z}\}.$$

ويوجد عدد طبيعي وحيد $r\in\{0,1,\dots,n-1\}$ ينتمي إلى هذا الصف، أي يحقق $a\equiv r \bmod n$. وكما يمكن الملاحظة بسهولة، فإن هذا العدد يمثّل في الحقيقة باقي القسمة الإقليدية للعدد a على n، لذلك فإنه يتحدد عمليا بإجراء الخوارزمية المرافقة لهذه القسمة.

يُرمز غالبًا لمجموعة حاصل القسمة الناتجة عن علاقة التكافؤ المشار إليها آنفا بالرمز $\mathbb{Z}/n\mathbb{Z}$، وعليه يأتي:

$$\mathbb{Z}/n\mathbb{Z}=\{\bar{a}: a\in\mathbb{Z}\}=\{\bar{r}: 0\le r\le n-1\}.$$

فيما يخص هذه المجموعة، لدينا النتيجة التالية:

مبرهنة 1. ليكن n عددًا طبيعيًا معطى أكبر من أو يساوي 2.

1- $\mathbb{Z}/n\mathbb{Z}$ حلقة واحدية وتبديلية؛

2- $\bar{a}$ قابل للقلب في $\mathbb{Z}/n\mathbb{Z}$ إذا، وإذا فقط، كان $a\wedge n=1$، أي إذا كان n وَ a أوليين فيما بينهما؛

3- n عدد أولي إذا، وإذا فقط، كانت $\mathbb{Z}/n\mathbb{Z}$ حقلًا إذا، وإذا فقط، كانت $\mathbb{Z}/n\mathbb{Z}$ حلقة تامة.

من أجل $2\le n$، نرمز بـ$\mathbb{U}_n$ إلى مجموعة العناصر القابلة للقلب في الحلقة $\mathbb{Z}/n\mathbb{Z}$ وبـ$\varphi(n)$ إلى عدد عناصرها، والذي يُعرف في أبجديات نظرية الحساب باسم دليل أويلر (Euler's indicator) لـn. إنه يساوي حسب النتيجة رقم 2 من المبرهنة السابقة عدد كل الأعداد الأولية مع n والأصغر منه. وحسب النتيجة رقم 3 من المبرهنة ذاتها، فإنه إذا كان n أوليًا، فإن $\mathbb{U}_n=\mathbb{Z}/n\mathbb{Z}-\{\bar{0}\}$، وعليه $\varphi(n)=n-1$. ويصعب في الحالة العامة تحديد $\varphi(n)$، لأن ذلك يتطلب تفكيك n إلى جداء عوامل أولية.

لدينا المبرهنة التالية، والتي تعرف تاريخيًا باسم مبرهنة أويلر.

مبرهنة 2. ليكن $2 \leq n$. من أجل كل عدد صحيح $a \in \mathbb{Z}$ أولي مع n، $a^{\varphi(n)} \equiv 1 \bmod n$.

البرهان. نعلم من نظرية الزمر أنه إذا كانت G زمرة منتهية (Finite group) رتبتها (يعني عدد عناصرها) تساوي m، فإن $x^m = e$ من أجل كل $x \in G$، حيث يشير e إلى العنصر الحيادي لـG.

الآن ليكن a عددًا صحيحًا أوليًا مع n. من الخاصية رقم 2 الواردة في المبرهنة رقم 1 نستخلص بأن $\bar{a}$ ينتمي إلى الزمرة المنتهية $\mathbb{U}_n$ ذات الرتبة $\varphi(n)$، ومنه المساواة $\bar{a}^{\varphi(n)} = \bar{1}$، والتي تعني بالضبط أن $a^{\varphi(n)} \equiv 1 \bmod n$. ■

نستخلص سريعًا من المبرهنة رقم 2 النتيجة التالية والتي تحمل الاسم المبرهنة الصغرى لفيرما (Fermat's little theorem).

مبرهنة 3. من أجل كل عدد أولي p، لدينا

$$\forall_{a\in\mathbb{Z}}: a \wedge p = 1 \Rightarrow a^{p-1} \equiv 1 \bmod p,$$

أو أيضا

$$\forall_{a\in\mathbb{Z}}: a^p \equiv a \bmod p.$$

لقد تم التأكد حديثا من أنه يوجد ما لا نهاية من الأعداد الطبيعية غير الأولية n بحيث:

$$\forall_{a\in\mathbb{Z}}: a \wedge n = 1 \Rightarrow a^{n-1} \equiv 1 \bmod n.$$

تدعى هذه الأعداد بأعداد كارمايكل (Carmichael)، وأصغرها هو 561.

إن مبرهنة فيرما الصغرى تعطي شرطًا ضروريًا فحسب لأن يكون عدد طبيعي معطى أوليًا، بيد أن مبرهنة ويلسون (Wilson) التالية تعطي شرطًا ضروريًا وكافيًا للمسألة ذاتها.

مبرهنة 4. ليكن $2 \leq p$. يكون p أوليًا إذا، وإذا فقط، كان $(p-1)! \equiv -1 \bmod p$.

البرهان. لدينا $(2-1)! = 1 = 2 - 1 = -1 + 2$، وعليه $(2-1)! \equiv -1 \bmod 2$، وهذا يعني أن العلاقة الواردة في المبرهنة صحيحة من أجل $p = 2$. ليكن إذن p عددًا أوليًا بحيث $3 \leq p$. حسب الخاصية رقم 3 من المبرهنة رقم 1 فإن $\mathbb{Z}/p\mathbb{Z}$ حقل، وبالتالي فهي حلقة تامة. ويُستخلص من هذا بأن كثير الحدود $X^2 - \bar{1}$ يقبل بالضبط جذرين تربيعيين في $\mathbb{Z}/p\mathbb{Z}$ هما $\bar{1}$ وَ$-\bar{1}$، وبعبارة أخرى فإن $\overline{p-1} = -\bar{1}$ هما العددان الوحيدان مقلوبا نفسيهما في $\mathbb{Z}/p\mathbb{Z}$. لذلك إذا كان $x \in M = \{\bar{2}, \dots, \overline{p-2}\}$، فإن حتمًا $x \neq x^{-1}$ وَ$x^{-1} \in M$، وبالتالي يمكن كتابة هذه المجموعة على النحو الآتي $M = \{x_1, x_1^{-1}, \dots, x_m, x_m^{-1}\}$، حيث $m = (p-3)/2$. ومنه:

$$\bar{2} \times \cdots \times \overline{p-2} = x_1 \times x_1^{-1} \times \cdots \times x_m \times x_m^{-1} = \bar{1} \times \cdots \times \bar{1} = \bar{1},$$

وَ

$$\overline{(p-1)!} = \bar{1} \times \bar{2} \times \cdots \times \overline{p-2} \times \overline{p-1} = \bar{1} \times \overline{-1} = \overline{-1}.$$

وعليه يأتي $(p-1)! \equiv -1 \bmod p$.

بالعكس لنفرض أن $(p-1)! \equiv -1 \bmod p$. إذا لم يكن p أوليًا، فإنه يوجد عدد طبيعي q قاسم لـp بحيث $1 < q < p$. إن q يقسم أيضا $(p-1)!$، لذلك نستنتج من العلاقة المفروضة آنفًا أن q يقسم 1، وهذا مستحيل، لذلك فإن p حتمًا أولي. ■

ونظرًا لأن حساب $(p-1)!$ يتطلب عددًا هائلًا من العمليات الحسابية من أجل قيم كبيرة قليلا لـp، فإن الاستخدام المباشر لنتيجة المبرهنة 4 من أجل معرفة إن كان p أوليًا أم لا هو أمر بلا جدوى عمليًا لكونه يفرض إنجاز حسابات مكلفة للغاية. ومع ذلك توجد مخارج مناسبة تؤدي إلى استخدامات ذات قيمة للنتيجة المشار إليها، منها على سبيل المثال المزاوجة بين عمليات حسابية سهلة الإنجاز واختيارات عشوائية مناسبة لتحديد أولية p من عدمها على ضوء المبرهنة 3. تدعى الخوارزميات الحسابية المنشأة وفق هذه الطريقة بالخوارزميات الاحتمالية (Probabilistic algorithms)، وهي تلقى رواجًا متزايدًا في الحساب.

ليكن $3 \leq n$ عددًا فرديًا معطى. لدينا:

$$(n-1)! = \frac{n-1}{2}! \times \left(\frac{n-1}{2}+1\right) \times \cdots \times (n-1)$$
$$= \left(\frac{n-1}{2}\right)! \times \prod_{k=\frac{n-1}{2}+1}^{n-1} k = \frac{n-1}{2}! \times \prod_{j=1}^{\frac{n-1}{2}} (n-j).$$

ومنه نحصل على

$$(n-1)! \equiv \frac{n-1}{2}! \times \prod_{j=1}^{\frac{n-1}{2}} (-j) \bmod n \equiv (-1)^{\frac{n-1}{2}} \left(\frac{n-1}{2}!\right)^2 \bmod n.$$

وبالتالي إذا كان $n \equiv 1 \bmod 4$ فإن

$$(n-1)! \equiv \left(\frac{n-1}{2}!\right)^2 \bmod n.$$

من هذه العلاقة ومن المبرهنة رقم 4 نحصل على النتيجة التالية:

نتيجة 5. ليكن p عددًا طبيعيًا بحيث $p \equiv 1 \bmod 4$. يكون p أوليًا إذا، وإذا فقط، كان

$$-1 \equiv \left(\frac{p-1}{2}!\right)^2 \bmod p.$$

وهكذا فإذا كان p عددًا أوليًا بحيث $p \equiv 1 \bmod 4$، فإن $-\bar{1}$ هو مربع في الحقل $\mathbb{Z}/p\mathbb{Z}$، ويمثّل $(p-1/2)!$ أحد جذريه التربيعيين. ويصعب حساب هذا الجذر إن كان p كبيرًا قليلًا، لكن توجد مع ذلك خوارزمية احتمالية، سنتحدث عنها فيما يلي، أكثر فاعلية لحسابه.

من ناحية أخرى يُبرهن كتمرين بسيط أنه من أجل كل عدد أولي p، إذا كان $-\bar{1}$ مربعًا في الحقل $\mathbb{Z}/p\mathbb{Z}$، فإن $p \equiv 1 \bmod 4$. ومنه النتيجة:

نتيجة 6. من أجل كل عدد طبيعي p، الدعوتان التاليتان متكافئتان:

1- p يحقق الشرطين $p \equiv 1 \bmod 4$ وَ

$$-1 \equiv \left(\frac{p-1}{2}!\right)^2 \bmod p.$$

2- p عدد أولي وَ $-\bar{1}$ مربع في الحقل $\mathbb{Z}/p\mathbb{Z}$.

فيما يلي نعطي نص مبرهنة العناصر الأصلية (Theorem of primitive elements)، والتي يعتبر برهانها تمرينًا جيدًا في الحساب.

مبرهنة 7. ليكن p عددًا أوليًا. يوجد على الأقل عنصر $\xi \in \mathbb{Z}/n\mathbb{Z} - \{\bar{0}\}$ رتبته $p-1$، وبالتالي $\xi^{p-1} = \bar{1}$ وَ $\mathbb{Z}/n\mathbb{Z} - \{\bar{0}\} = \{\bar{1}, \xi, \xi^2, \dots, \xi^{p-2}\}$. يدعى ξ عنصرًا أصليًا في الزمرة $\mathbb{Z}/n\mathbb{Z} - \{\bar{0}\}$.

2. خوارزمية احتمالية لحساب جذر تربيعي

ليكن p عددًا أوليًا بحيث $p \equiv 1 \bmod 4$. وبالتالي $p-1 = 2^k q$ حيث $2 \leq k$ وَ q عدد طبيعي فردي.

لنضع

$$\mathcal{G} = \{x \in \mathbb{U}_p : x^{2q} = \bar{1}\}, \mathcal{E} = \mathbb{U}_p - \mathcal{G} = \{x \in \mathbb{U}_p : x^{2q} \neq \bar{1}\}.$$

فيما يخص هاتين المجموعتين لدينا التوطئة التالية:

توطئة 1. لدينا $\operatorname{card}\mathcal{G}=2q$، وبالتالي $\operatorname{card}\mathcal{E}=\operatorname{card}\mathbb{U}_p-\operatorname{card}\mathcal{G}=2q(2^{k-1}-1)$.

البرهان. حسب المبرهنة رقم 7، يمكننا اختيار عنصر $\xi\in\mathbb{Z}/n\mathbb{Z}-\{\bar{0}\}$ رتبته $p-1$. وبالتالي إذا كان $x\in\mathcal{G}$، فإنه يوجد $i\in\{0,1,\dots,p-2\}$ بحيث $x=\xi^i$، وعليه $\bar{1}=x^{2q}=\xi^{2iq}$، الأمر الذي يعني أن $p-1$ قاسم لـ$2iq$، ونكتب ذلك رمزيًا كما يلي $p-1|2iq$، وتأتي صحة هذا الاستنتاج من حقيقة أن رتبة ξ هي $p-1$. بالعكس إذا كان $x=\xi^i$ بحيث $i\in\{0,1,\dots,p-2\}$ وَ$2iq=\alpha(p-1)$ مع α عدد طبيعي، فإن

$$x^{2q}=\xi^{2iq}=\xi^{\alpha(p-1)}=(\xi^{p-1})^{\alpha}=(\bar{1})^{\alpha}=\bar{1},$$

وبالتالي $x\in\mathcal{G}$. إذن يمكننا أن نكتب $\mathcal{G}=\{x=\xi^i:i\in I\}$ حيث $I=\{i:0\le i\le p-2\wedge p-1|2iq\}$.

لنلاحظ أن التطبيق $i\mapsto\xi^i$ هو تقابل من I إلى $\mathcal{G}$، ويعود ذلك دائما إلى كون رتبة ξ هي $p-1$، ومنه نستنتج بأن للمجموعتين I وَ$\mathcal{G}$ عدد العناصر ذاته. من ناحية أخرى بما أن $p-1|2iq\Leftrightarrow 2^{k-1}|i$، فإن لدينا

$$I=\left\{i=2^{k-1}\alpha:0\le\alpha\le\frac{p-2}{2^{k-1}}\right\}=\left\{i=2^{k-1}\alpha:0\le\alpha\le\left[\frac{p-2}{2^{k-1}}\right]\right\},$$

حيث يشير $\left[\frac{p-2}{2^{k-1}}\right]$ إلى الجزء الصحيح لـ$\frac{p-2}{2^{k-1}}$، وهو تعريفًا العدد الصحيح الوحيد β الذي يحقق

$$\beta\le\frac{p-2}{2^{k-1}}<\beta+1.$$

وعليه فإن عدد عناصر I يساوي $\left[\frac{p-2}{2^{k-1}}\right]+1$. لكن

$$\frac{p-2}{2^{k-1}}=\frac{p-1}{2^{k-1}}-\frac{1}{2^{k-1}}=2q-\frac{1}{2^{k-1}}.$$

لذلك بما أن $2\le k$، فإن $2q-1<\frac{p-2}{2^{k-1}}<2q$، ومن ثمة يأتي $\left[\frac{p-2}{2^{k-1}}\right]=2q-1$ وَ$\left[\frac{p-2}{2^{k-1}}\right]+1=2q$. انتهى البرهان. ■

لنسحب بصورة عشوائية عددًا من المجموعة $\mathbb{U}_p$. إن احتمال أن يكون هذا العدد من المجموعة الجزئية $\mathcal{G}$ هو

$$\frac{\operatorname{card}\mathcal{G}}{\operatorname{card}\mathbb{U}_p}=\frac{2q}{2^kq}=\frac{1}{2^{k-1}}\le\frac{1}{2}.$$

وبالتالي إذا كررنا عملية السحب n مرة (مع الإرجاع)، فإن احتمال أن نحصل في كل سحب من هذه السحوبات على عدد من $\mathcal{G}$ هو

$$\frac{1}{2^{n(k-1)}}.$$

وعليه فإن احتمال أن نحصل في أحد السحوبات على عدد من $\mathcal{E}$ هو

$$1-\frac{1}{2^{n(k-1)}}.$$

وبما أن $2\le k$، فإن هذا الاحتمال أكبر من أو يساوي

$$1-\frac{1}{2^n}.$$

وهكذا يمكن التأكد على سبيل المثال من أنه بعد إجراء عشرين عملية سحب عشوائية مثلما أشير إليها آنفًا، فإن احتمال أن نحصل في واحدة منها على عدد من $\mathcal{E}$ يساوي أو أكبر من 0.9999990463، أي يساوي تقريبا 1، وهذا معناه حصولنا فعلا على عدد من $\mathcal{E}$ بعد إنجاز عشرين سحبًا متتابعًا.

ويمكن زيادة التأكيد على هذه النتيجة باستخدام مبدأ الاحتمالات العملية لبوريل (Borel)، والذي نصه "إن أية حادثة عشوائية ذات احتمال أقل من 10^{-50} لا تتحقق أبدا". وكما أشير آنفًا، فإن احتمال ألا نحصل على عدد من $\mathcal{E}$ بعد إجراء n سحبًا متتابعًا هو أقل من

$$\frac{1}{2^n}.$$

وبما أنه لدينا

$$\frac{1}{2^n} \leq 10^{-50} \Leftrightarrow 10^{50} \leq 2^n \Leftrightarrow 50\frac{\operatorname{lin} 10}{\operatorname{lin} 2} \leq n.$$

فإننا سنحصل حتمًا على عدد من $\mathcal{E}$ إن أجرينا عددًا من السحوبات المتتابعة يفوق العدد الحقيقي

$$50\frac{\operatorname{lin} 10}{\operatorname{lin} 2} \approx 166.10,$$

والذي هو ليس كبيرًا.

تمثّل عملية إنجاز السحوبات الموصوفة آنفًا الخطوة الأولى من الخوارزمية الاحتمالية التي نرغب في تقديمها هنا، ونمر الآن إلى شرح الخطوة الثانية للخوارزمية ذاتها.

لنفترض بأن لدينا عددًا x من المجموعة $\mathcal{E}$. إن المجموعة $\mathcal{I} = \left\{i \geq 1: x^{2^i q} = \bar{1}\right\}$ ليست خالية لأن $k \in \mathcal{I}$ حسب المبرهنة الصغرى لفيرما، ولا تحتوي على 1 لأن $x^{2q} \neq \bar{1}$ بسبب انتماء x إلى $\mathcal{E}$. لذلك فإن عنصرها الأصغر $\min \mathcal{I}$ محصور بين 2 وَk. لنضع $\alpha = \min \mathcal{I} - 2$. من تعريف $\min \mathcal{I}$ نستخلص أن $y = x^{2^{\alpha+1}q} \neq \bar{1}$، بالإضافة إلى ذلك لدينا $y^2 = x^{2^{\alpha+2}q} = x^{2^{\min \mathcal{I}}q} = \bar{1}$، وبالتالي $y = x^{2^{\alpha+1}q} = -\bar{1}$، تأتي هذه النتيجة من حقيقة أن كثير الحدود $X^2 - \bar{1}$ يقبل بالضبط جذرين تربيعيين هما $\bar{1}$ وَ$-\bar{1}$ في الحلقة التامة $\mathbb{Z}/p\mathbb{Z}$. وهكذا حصلنا على جذر تربيعي للعدد $-\bar{1}$ هو $x^{2^\alpha q}$. إن الخطوة الثانية في الخوارزمية المنشودة أصبحت واضحة، وهي: بعد العثور عشوائيًا على عدد من $\mathcal{E}$ نقوم بحساب المربعات المتتابعة للمقدار x^q حتى نحصل على جذر تربيعي لـ$-\bar{1}$.

والآن بمقدورنا عرض خوارزميتنا بواسطة كلمات اللغة العربية، وهي ليست بحاجة إلا لصياغتها بلغات البرمجة الحديثة من أجل تنفيذها واختبار فعاليتها.

"الخطوة الأولى: قم بالسحب العشوائي المتتابع (مع الإرجاع) لأعداد من المجموعة $\mathbb{U}_p$، وتوقّف عن السحب عند العثور على عدد x يحقق $x^{2q} \neq \bar{1}$.

الخطوة الثانية: قم بحساب المربعات المتتابعة للعدد x^q، وتوقّف عن الحساب عند الحصول على مربع منها مساوٍ للعدد $-\bar{1}$."

وكما تم توضيح ذلك فإن هذه الخوارزمية قابلة للتنفيذ، بل ويُتحقق من أنها أقل تكلفة حسابية من خوارزمية الضرب المباشرة لحساب المقدار $((p-1)/2)!$.

في الختام نقدّم بالاستناد إلى مبدأ الاحتمالات العملية لبوريل النتيجة التالية:

نتيجة 8. ليكن p عددًا طبيعيًا بحيث $p \equiv 1 \bmod 4$. إن لم نحصل على عنصر من $\mathcal{E}$ بعد إجراء أكثر من 167 سحب عشوائي متتابع، فإن p ليس أوليًا.