الفصل الرابع عشر

أعداد ميرسن الأولية

Mersenne Primes

في هذا الفصل سوف ندرس الأعداد الأولية التي يمكن كتابتها على الشكل $a^n - 1$ عندما $n \geq 2$. فعلى سبيل المثال، العدد 31 هو مثال على هذا النوع من الأعداد الأولية، حيث $31 = 2^5 - 1$. وكخطوة أولى في هذه الدراسة انظر إلى الجدول التالي:

$2^2 - 1 = 3$	$2^3 - 1 = 7$	$2^4 - 1 = 3 \cdot 5$	$2^5 - 1 = 31$
$3^2 - 1 = 2^3$	$3^3 - 1 = 2 \cdot 13$	$3^4 - 1 = 2^4 \cdot 5$	$3^5 - 1 = 2.11^2$
$4^2 - 1 = 3.5$	$4^3 - 1 = 3^2.7$	$4^4 - 1 = 3.5.17$	$4^5 - 1 = 3.11.13$
$5^2 - 1 = 2^3.3$	$5^3 - 1 = 2^2.31$	$5^4 - 1 = 2^4.3.13$	$5^5 - 1 = 2^2.11.71$
$6^2 - 1 = 5.7$	$6^3 - 1 = 5.43$	$6^4 - 1 = 5.7.37$	$6^5 - 1 = 5^2.311$
$7^2 - 1 = 2^4.3$	$7^3 - 1 = 2.3^2.19$	$7^4 - 1 = 2^5.3.5^2$	$7^5 - 1 = 2.3.2801$
$8^2 - 1 = 3^2.7$	$8^3 - 1 = 7.73$	$8^4 - 1 = 3^2.5.7.13$	$8^5 - 1 = 7.31.151$

من السهل ملاحظة أنه إذا كان a فردياً ؛ فإن $a^n - 1$ زوجي ، وعليه لا يمكن أن يكون أولي. بالنظر إلى الجدول فإننا نلاحظ أيضاً أن $a^n - 1$ يقبل القسمة على $a-1$ دائماً. وفي الحقيقة ، فإن هذه الملاحظة صحيحة. ويمكننا إثبات أنّ ذلك صحيح باستخدام الصيغة المشهورة لمجموع المتسلسلة الهندسية :

المتسلسلة الهندسية

$$x^n - 1 = (x-1)\left(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1\right)$$

ولفحص صحة هذه الصيغة للمتسلسلة الهندسية سوف نقوم بإيجاد مفكوك الضرب في الحد الأيمن.

$$\begin{aligned}
(x-1)&\left(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1\right) \\
&= x.\left(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1\right) \\
&\qquad -1.\left(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1\right) \\
&= \left(x^n + x^{n-1} + \cdots + x^3 + x^2 + x\right) \\
&\qquad -\left(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1\right) \\
&= x^n - 1
\end{aligned}$$

باستخدام المتسلسلة الهندسية عندما $x = a$ ، سنلاحظ مباشرة أن $(a^n - 1)$ دائماً يقبل القسمة على $(a-1)$. لذلك فإن المقدار $(a^n - 1)$ سيحلل إلى عوامل إلا إذا كان $a - 1 = 1$ ، أي أن $a = 2$.

على كل حال، حتى إذا كان $a = 2$ ، فإن العدد $2^n - 1$ مؤلَف بشكل متكرر. مرة أخرى فلننظر إلى البيانات التالية :

n	2	3	4	5	6	7	8	9	10
2^n-1	3	7	3.5	31	$3^2.7$	127	3.5.17	7.73	3.11.31

من هذا الجدول الصغير نلاحظ ما يلي :

عندما n عدد زوجي ؛ فإن (2^n-1) يقبل القسمة على $3=2^2-1$

عندما n يقبل القسمة على 3 ، فإن (2^n-1) يقبل القسمة على $7=2^3-1$

عندما n يقبل القسمة على 5 ، فإن (2^n-1) يقبل القسمة على $31=2^5-1$

وعليه ؛ فإننا نتوقع أنه إذا كان n يقبل القسمة على m ؛ فإن (2^n-1) يقبل القسمة على (2^m-1) .

من السهل التحقق من صحت الملاحظة السابقة. لذلك افرض أن n تُحلل على أنها $n=mk$. عندئذ $2^n=2^{mk}=\left(2^m\right)^k$. سوف نستخدم صيغة المتسلسلة الهندسية عندما $x=2^m$ لنحصل على :

$$2^n-1=\left(2^m\right)^k-1=\left(2^m-1\right)\left(\left(2^m\right)^{k-1}+\left(2^m\right)^{k-2}+\cdots+\left(2^m\right)^2+\left(2^m\right)+1\right)$$

هذا يبرهن أنه إذا كانت n تحلل إلى عوامل ؛ فإن (2^n-1) تحلل إلى عوامل أيضاً. سنعرض الآن للنظرية التالية والتي تحققنا من صحتها سابقاً.

نظرية (١٤,١)

إذا كان a^n-1 عدداً أوليًا عند بعض القيم $a\geq 2$ و $n\geq 2$ ، فإن a يجب أن تساوي 2 و n يجب أن يكون عدداً أوليًا.

هذا يعني أنه إذا كنا مهتمين بالأعداد الأولية التي على الشكل $a^n - 1$ فإننا نحتاج فقط لدراسة الحالة التي يكون فيها $a = 2$ و n عدد أولي. الأعداد الأولية التي على الشكل $2^p - 1$ تسمى أعداد "ميرسن" الأولية (*Mersenne primes*). أولى الأعداد الأولية لميرسن هي :

$$2^2 - 1 = 3 \, , \, 2^3 - 1 = 7 \, , \, 2^5 - 1 = 31 \, , \, 2^7 - 1 = 127 \, , \, 2^{13} - 1 = 8191$$

بالطبع ليس كل عدد على الشكل $\left(2^p - 1\right)$ هو عدد أولي. فمثلاً :

$$2^{11} - 1 = 2047 = 23.89$$

و

$$2^{29} - 1 = 536870911 = 233.1103.2089$$

سميت أعداد ميرسن الأولية بهذا الاسم نسبة إلى الأب مارين ميرسن (١٥٨٨- ١٦٤٨)، والذي أكد عام 1644 أن $\left(2^p - 1\right)$ عدد أولي عندما :

$$p = 2,3,5,7,13,17,19,31,67,127,257$$

وهذه فقط هي الأعداد الأولية الأقل من 258 والتي تجعل المقدار $\left(2^p - 1\right)$ عدداً أوليًّا. إنه من غير المعروف كيف اكتشف ميرسن هذه "الحقائق"، خصوصاً إذا كانت قائمته هذه ليست صحيحة. والقائمة الكاملة للأعداد الأولية p الأقل من 10000 والتي تجعل المقدار $\left(2^p - 1\right)$ عدداً أوليًّا هي(١) :

$$p = 2,3,5,7,13,17,19,31,61,89,107,127,521,607,1279$$
$$2203,2281,3217,4253,4423,9689,9941$$

---

(١) لاحظ أن الأب ميرسن ارتكب خمسة أخطاء، ثلاثة منها عندما حذف الأعداد $(61,89,107)$ ، واثنين منها عندما ضم العددين $(67,257)$.

لقد أصبح من الممكن وبظهور الآلات الحاسبة فحص الأعداد التي لها مئات الخانات فيما إذا كانت أعداداً أولية أم لا. وفي الحقيقة، فإنه لم يبرهن على أن العدد $\left(2^{127}-1\right)$ هو عدد أولي إلا على يد (E.Lucas) وذلك سنة 1876 ، وظل عدد لوكاس الأولي هو أكبر عدد أولي معروف حتى خمسينيات القرن العشرين (1950s)! الجدول 14.1 يبين أعداد ميرسن الأولية التي اكتشفت فيما بعد باستخدام الكمبيوتر، مقرونة بأسماء الذين اكتشفوها.

إن أحدث أعداد ميرسن الأولية الواردة في الجدول رقم (١٤,١) اكتشفت من خلال مشروع بحثي متخصص يسمى Woltman's Great Internet Mersenne Prime Search. أنت أيضاً، عزيزي القارئ ، يمكنك المشاركة في البحث لتدوين اسمك في عالم الأعداد الأولية[١] من خلال تحميل برنامج من الموقع الإلكتروني GIMPS :
www.mersenne.org/prime.htm

كذلك يمكنك عزيزي القارئ زيارة الموقع :
www.utm.edu/research/primes/mersenne.shtm1
لتتعرف أكثر على أعداد ميرسن الأولية على الصعيدين الموضوعي والتاريخي.

بالطبع، فعلى الرغم من أهمية مشاهدة قائمة أكبر الأعداد الأولية المعروفة، فإنه لا توجد أهمية رياضية عظيمة في إيجاد أعداد ميرسن أولية أخرى. والأكثر أهمية من وجهة نظر رياضية هو السؤال التالي. وإجابته غير معروفة.

سؤال رقم (١٤,٢). هل أعداد ميرسن الأولية لا نهائية، أو هل انتهت قائمة أعداد ميرسن الأولية؟

(١) آندي وارول"Andy Warhol" قالت إن أي شخص في المستقبل سيصبح مشهوراً خلال دقيقة. إحدى طرق الحصول على مثل هذه الشهرة يكون من خلال إيجاد أكبر عدد ميرسن أولي. ومازال البحث عن أكبر وأفضل أعداد أولية مستمر.

p	Discovered by	Date
521, 607, 1279, 2203, 2281	Robinson	1952
3217	Riesel	1957
4253, 4423	Hurwitz	1961
9689, 9941, 11213	Gillies	1963
19937	Tuckerman	1971
21707	Noll, Nickel	1978
23209	Noll	1979
44497	Noll, Slowinski	1979
86243	Slowinski	1982
110503	Colquitt, Welsch	1988

p	Discovered by	Date
132049	Slowinski	1983
216091	Slowinski	1985
756839	Slowinski, Gage	1992
859433	Slowinski, Gage	1994
1257787	Slowinski, Gage	1996
1398269*	Armengaud	1996
2976221*	Spence	1997
3021377*	Clarkson	1998
6972593*	Hajratwala	1999
13466917*	Cameron	2001
20996011*	Shafer	2003
24036583*	Findley	2004
25964951*	Nowak	2005
30402457*	Boone, Cooper	2005
32582657*	Boone, Cooper	2006

الجدول رقم (١٤,١). الأعداد الأولية $P \geq 500$ التي تجعل المقدار $\left(2^p - 1\right)$ عدداً أوليًّا. الأعـــداد الأولية p الواردة في الجدول بجانبها علامة ★ اكتشفت من خـــلال **GIMPS** **(Woltman, Kurokowski, …)**

تمارين

(١٤،١) إذا كان (a^n+1) عدداً أوليًّا عند بعض الأعداد $a \geq 2$ و $n \geq 1$ ، بين أن العدد n يجب أن يكون من قوى العدد 2.

(١٤،٢) ليكن $F_k = 2^{2^k}+1$. مثال،

$$F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

العالم الرياضي "فيرما" Fermat اعتقد أن كل الأعداد F_k هي أعداد أولية، لكن الرياضي "أويلر" Euler برهن في سنة 1732 أن $F_5 = (641)(6700417)$ ، وفي سنة 1880 بين "لاندري" Landry أن F_6 يحلل إلى عوامل. الأعداد الأولية التي على الشكل F_k تسمى أعداد فيرما الأولية Fermat prime . بين أنه إذا كان $k \neq m$ ، فإن العددين F_k و F_m ليس لهما قاسم مشترك غير العدد 1، أي بين أن $\gcd(F_k, F_m) = 1$. (مساعدة: إذا كان $k > m$ ، بين أن F_m تقسم $F_k - 2$).

(١٤،٣). الأعداد (3^n-1) ليست أعداد أولية عندما $(n \geq 2)$ ؛ لأنها دائماً أعداد زوجية. على كل حال، يحدث أحياناً أن يكون $(3^n-1)/2$ عدداً أوليًّا. فمثلاً $(3^3-1)/2 = 13$ هو عدد أولي.

(a) أوجد عدداً أوليًّا آخر على الشكل $(3^n-1)/2$.

(b) إذا كان n عدداً زوجيًّا، بين أن $(3^n-1)/2$ يقبل القسمة على 4 دائماً، وعليه لا يمكن أن يكون عدداً أولياً.

(c) استخدم فكرة مشابهة لتبرهن أنه إذا كان n من مضاعفات العدد 5 ؛ فإن $(3^n-1)/2$ لا يمكن أن يكون عدداً أولياً.

(d) هل تعتقد أنه يوجد عدد لا نهائي من الأعداد الأولية تكتب على الشكل $(3^n-1)/2$ ؟