الفصل التاسع عشر

اختبار الأولية وأعداد كارمايكل
Primality Testing and Carmichael Numbers

إن الأعداد الأولية تمثل حجر الأساس للأعداد الصحيحة. ومن خلال لا نهائية الأعداد الأولية نشاهد بعضاً أعمق وأجمل النماذج في كل نظرية الأعداد، وفي الحقيقة في كل الرياضيات. والأعداد الأولية، وخصوصاً الكبيرة منها، لها جانب تطبيقي كما رأينا عندما أنشأنا نظام التعمية RSA في الفصل الثامن عشر. إن هذا يقودنا إلى طرح السؤال الصعب التالي:

- **كيف نستطيع أن نعرف فيما إذا كان عدد (كبير) أوليًّا أم لا؟**

لأعداد صغيرة n مثل:

$$8641 \quad , \quad 8633 \quad , \quad 8629$$

فإننا نستطيع ببساطة اختبار كل القواسم (الأولية) المحتملة حتى $\sqrt{n}$ ، وإما أن نجد قاسماً وإما نعلم أن n عدد أولي. لذلك نجد أن 8641 , 8629 عددين أوليين، بينما 8633 يحلل إلى $89 \cdot 97$ وعليه فإنه ليس أوليًّا.

للأعداد الكبيرة مثل:

$$m = 1137369476253104052311779730283443758629640 01$$

و :

$$n = 1137369476253104052311779730283443758629536 03$$

نحتاج إلى عمل شاق حتى مع وجود الكمبيوتر، لاختبار جميع القواسم المحتملة وصولاً إلى الجذر التربيعي. على كل حال، رأينا في الفصل السادس عشر أنه ليس من الصعب جداً (على الكمبيوتر) رفع الأعداد إلى قوى كبيرة جداً قياس أعداد كبيرة جداً. فعلى سبيل المثال، يحتاج الكمبيوتر وقتاً قليلاً جداً لحساب :

$$2^m = 2^{1137369476253104052311779730283443758629640 01}$$

$$\equiv 3924197081539349906012004369263061596179002 0 \pmod m$$

للوهلة الأولى، يبدو أن حساب هذا التطابق عديم الفائدة، ولكن في الحقيقة فإن له أهمية تطبيقية بالغة لتوضيح ذلك، دعنا نتذكر نظرية فيرما الصغرى (انظر الفصل التاسع)، والتي تنص على أنه إذا كان p عدداً أوليًّا فإن : $a^p \equiv a \pmod p$ لأي عدد صحيح a.

لذلك فإن حقيقة أن 2^m لا يطابق 2 قياس m تخبرنا أن m لا يمكن أن يكون عدداً أوليًّا. لذلك يمكننا القول إن اللاتطابق $2^m \not\equiv 2 \pmod m$ تمثل برهاناً على أن m ليس أولياً. إن هذا يعكس الأهمية البالغة لنتيجتنا. لقد أثبتنا أن m ليس أوليًّا، على الرغم من أننا لا نعرف عوامل m ، وفي الحقيقة فإن برهاننا، على أن m يحلل إلى عوامل، لا يزودنا بأي معلومة تساعدنا في إيجاد هذه العوامل[1]. إن

---

(١) العدد m هو حاصل ضرب عددين أوليين كبيرين هما :

2836061511010998317 , 4010383667058247049513965 3 .

الدرس الذي تعلمناه هو أنه بالإمكان غالباً أن نعرف أن عدداً معيناً يحلل إلى عوامل دون أن نكون قادرين على معرفة هذه العوامل.

لنناقش الآن الرقم الآخر:

$$n = 1137369476253104052311779730283443758629536 03$$

إذا قمنا بعمل نفس الحسابات سنجد أن:

$$2^n = 2^{1137369476253104052311779730283443758629536 03} \equiv 2 \pmod{n}$$

هل يمكننا استخدام نظرية فيرما الصغرى لاستنتاج أن n أولي؟ والجواب هو قطعاً لا، إن نظرية فيرما الصغرى لا تعمل في ذلك الاتجاه. لذلك سنحاول مع أرقام أخرى، وليكن حتى $a = 100$، وسنجد أن:

$$3^n \equiv 3 \pmod{n} \quad , \quad 4^n \equiv 4 \pmod{n},$$
$$5^n \equiv 5 \pmod{n} \quad , \quad \ldots \quad , \quad 100^n \equiv 100 \pmod{n}$$

ما زلنا لا نستطيع استخدام نظرية فيرما الصغرى لنستنتج أن n عدد أولي، ولكن حقيقة إن $a^n \equiv a \pmod{m}$ متحققة على 99 قيمة مختلفة من a يفرض علينا القول إن n "من المحتمل" أن يكون أوليًّا.

هذه العبارة غريبة، كيف يمكن أن يكون عدد "من المحتمل أولي"؟ فإما أن يكون أولي وإما لا، فهو لا يمكن أن يكون أوليًّا يومي الثلاثاء والخميس وغير أولي في باقي أيام الأسبوع.

افرض أننا نفكر في العدد n على أنه ظاهرة طبيعية، وأننا ندرس n بروح العالم الخبير. إننا سوف نقوم بإجراء تجاربنا باختيار قيم مختلفة للعدد a ومن ثم حساب قيمة:

$$a^n \pmod n$$

لو أن تجربة واحدة أنتجت عدداً غير a ، سنستنتج أن n غير أولي. لذلك من المنطقي في كل مرة تنتج التجربة القيمة a أن تزيد قناعتنا بأن n أولي.

إننا نستطيع وضع هذه الاستنتاجات كخطى راسخة من خلال النظر لقيم a التي قواها النونية تختلف عن العدد a. ونقول إن العدد a "شاهد"(*witness*)على n إذا كان:

$$a^n \not\equiv a \pmod n$$

وهذا اسم مناسب جداً للعدد a ؛ لأنه إذا حاول العدد n أن يلعب دور العدد الأولي، فإن النائب العام يمكنه طلب a للشهادة ليثبت أن n قابل للتحليل.

إذا كان n أوليًّا، فمن الواضح أنه لا يمتلك شهوداً. وضعنا في الجدول الوارد في صفحة 126 قائمة بالشهود على كل الأرقام n حتى الرقم 20 ، ويبين هذا الجدول أن الأعداد غير الأولية لها عدد كافٍ من الشهود.

لدعم هذه الملاحظة أكثر، قمنا باختيار بعض الأعداد غير الأولية بشكل عشوائي بين 100 و 1000 ورصدنا عدد الشهود لكل عدد. كذلك قمنا بإعطاء النسبة المئوية لعدد الشهود بالنسبة للعدد n

n	287	190	314	586	935	808	728	291
# الشهود	278	150	310	582	908	804	720	282
% الشهود	96.9%	78.9%	98.7%	99.3%	97.1%	99.5%	98.9%	96.9%

من الواضح أنه إذا كان n غير أولي، فإن معظم قيم a تكون شهوداً. على سبيل المثال:

إذا كان $n = 287$ ، وإذا اخترنا قيمة عشوائية للعدد a ، فإنه يوجد 96.9%

n	شهود n
3	أولي
4	2,3
5	أولي
6	2,5
7	أولي
8	2,3,4,5,6,7
9	2,3,4,5,6,7
10	2,3,4,7,8,9
11	أولي
12	2,3,5,6,7,8,10,11
13	أولي
14	2,3,4,5,6,9,10,11,12,13
15	2,3,7,8,12,13
16	2,3,4,5,6,7,8,9,10,11,12,13,14,15
17	أولي
18	2,3,4,5,6,7,8,11,12,13,14,15,16,17
19	أولي
20	2,3,4,6,7,8,9,10,11,12,13,14,15,17,18,19

فرصة ليكون a شاهداً للعدد غير الأولي n. لذلك لن نحتاج لعمل اختبارات كثيرة لإثبات أن n عدد غير أولي.

إن كل الدلائل وأيضاً الحدس يشير إلى أن الأعداد غير الأولية لها كثير من الشهود. ولكن هل هذا صحيح فعلاً؟ إذا بدأنا بعمل قائمة لكل الأعداد وشهودها، فإننا سنصطدم بالحالة التعيسة عندما $n = 561$. إن هذا عدد غير أولي، حيث $561 = 3 \cdot 11 \cdot 17$ ، ولكن لسوء الحظ فإن 561 ليس له ولا حتى شاهد واحد! إحدى طرق التحقق من أن 561 ليس له أي شاهد هو حساب $a^n \pmod n$ لكل قيم a من 1 إلى 561. سنلجأ إلى طريقة أسهل. لإثبات أن:

$$a^{561} \equiv a \pmod{561}$$

فإنه يكفي أن نبرهن أن:

$$a^{561} \equiv a \pmod 3 \quad , \quad a^{561} \equiv a \pmod{11} \quad , \quad a^{561} \equiv a \pmod{17}$$

لأنه إذا قبل عدد القسمة على 3 ، وعلى 7 ، وعلى 17 ، فإنه سيقبل القسمة على حاصل ضربهم $3 \cdot 11 \cdot 17$. بالنسبة للتطابق الأول، نُلاحظ أنه إذا كانت 3 من قواسم a فإن كلا الطرفين 0 ، بينما إذا لم يكن العدد 3 من قواسم a فإننا نستطيع استخدام نظرية فيرما الصغرى $a^2 \equiv 1 \pmod 3$ لحساب:

$$a^{561} = a^{2.280+1} = \left(a^2\right)^{280} \cdot a \equiv 1 \cdot a \equiv a \pmod 3$$

التطابقان الثاني والثالث يمكن فحصهما بنفس الطريقة. وعليه فإما 11 يقسم a وبالتالي كلا الطرفين 0 قياس 11 ، وإما أننا نستخدم التطابق $a^{10} \equiv 1 \pmod{11}$ لحساب:

$$a^{561} = a^{10.56+1} = \left(a^{10}\right)^{56} \cdot a \equiv 1 \cdot a \equiv a \pmod{11}$$

أخيراً، إما 17 يقسم a وبالتالي كلا الطرفين 0 قياس 17 ، وإما أننا نستخدم التطابق $a^{16} \equiv 1 (\mathrm{mod} 17)$ لحساب :

$$a^{561} = a^{16.35+1} = \left(a^{16}\right)^{35} \cdot a \equiv 1 \cdot a \equiv a (\mathrm{mod} 17)$$

لذلك لا يوجد شهود للعدد غير الأولي 561 .

هذا المثال وأربعة عشر مثالاً غيره لوحظت أول ما لوحظت من قبل ر.د.كارمايكل R.D.Carmichael في سنة 1910 ؛ لذلك سُميت هذه الأعداد باسم مكتشفها.

أعداد كارمايكل هي أعداد غير أولية n لها الخاصية التالية :

$a^n \equiv a (\mathrm{mod}\, n)$ لكل عدد صحيح $1 \le a \le n$.

بعبارة أخرى، عدد كارمايكل هو عدد غير أولي يتنكر بصورة عدد أولي، لعدم وجود شهود له. لقد رأينا أن 561 عدد كارمايكل، وفي الحقيقة هو أصغرها.

هنا قائمة بكل أعداد كارمايكل حتى 10000.

561, 1105, 1729, 2465, 2821, 6601, 8911

وتحليلهم هو :

$561 = 3 \cdot 11 \cdot 17$ $\qquad$ $2821 = 7 \cdot 13 \cdot 31$

$1105 = 5 \cdot 13 \cdot 17$ $\qquad$ $6601 = 7 \cdot 23 \cdot 41$

$1729 = 7 \cdot 13 \cdot 19$ $\qquad$ $8911 = 7 \cdot 19 \cdot 67$

$2465 = 5 \cdot 17 \cdot 29$

نلاحظ مباشرة أن كل عدد في هذه القائمة هو حاصل ضرب ثلاثة أعداد فردية مختلفة.

لذلك يمكن أن نخمن أن أعداد كارمايكل دائماً تنتج من حاصل ضرب ثلاثة أعداد أولية فردية مختلفة.

إن تخميننا لن يصمد طويلاً ؛ لأن $62745 = 3 \cdot 5 \cdot 47.89$ هو عدد كارمايكل ناتج عن حاصل ضرب أربعة أعداد أولية. إن هذا لا يعني أن نتخلى عن تخميننا ، بل يجب علينا عمل بعض التعديلات.

لاحظ أن تخميننا في الحقيقة هو ثلاثة تخمينات :

أن عدد كارمايكل هو حاصل ضرب ثلاثة أعداد أولية فقط ، أن عوامله الأولية مختلفة ، وأن العوامل الأولية فردية. لذلك سنقوم بحذف الجزء الخاطئ من التخمين ونبقي على الجزأين الآخرين كل منهما بنص منفصل عن الآخر :

(A) كل عدد كارمايكل هو عدد فردي.

(B) كل عدد كارمايكل هو حاصل ضرب أعداد أولية مختلفة.

دعنا نبرهن هاتين الحقيقتين.

برهان (A) : نستخدم تطابق كارمايكل :

$$a^n \equiv a \pmod{n}$$

مع : $a = n-1 \equiv -1 \pmod{n}$ لنحصل على :

$$(-1)^n \equiv -1 \pmod{n}$$

وهذا يقتضي أن n فردي (أو $n = 2$).

برهان (B) : افرض أن n عدد كارمايكل.

ليكن p عدداً فرديًّا يقسم n .

p^{e+1} أكبر قوة للعدد p يقسم n .

نريد أن نبرهن أن e يساوي 0 .

بما أن n عدد كارمايكل ؛ فإن $a^n \equiv a \pmod{n}$ لأي قيمة للعدد a . وكحالة خاصة، فإن هذا صحيح عندما $a = p^e$ ، لذلك:

$$p^{en} \equiv p^e \pmod{n}$$

لذلك n يقسم الفرق $p^{en} - p^e$ ، وحيث إن p^{e+1} يقسم n فإن: p^{e+1} يقسم $p^{en} - p^e$ لذلك:

$$\frac{p^{en} - p^e}{p^{e+1}} = \frac{p^{en-e} - 1}{p} \quad \text{عدد صحيح.}$$

وهذا صحيح فقط عندما $e = 0$. وهو المطلوب.

الخاصيتان (A) و (B) لأعداد كارمايكل مفيدتان، ولكن ستكونان مفيدتين أكثر إذا استطعنا استنباط طريقة سهلة لاختبار فيما إذا كان عدد ما هو عدد كارمايكل أم لا.

طريقة فحصنا السابقة والتي عرفنا من خلالها أن 561 هو عدد كارمايكل زودتنا بالمفتاح. فبدلاً من التحقق أن $a^n \equiv a \pmod{n}$ ، فإننا نقوم بفحص فيما إذا كان $a^n \equiv a \pmod{p}$ لكل عدد أولي p يقسم a . بعد ذلك نقارن التطابق قياس p مع نظرية فيرما الصغرى ليزودنا بالعلاقة بين p , n . والناتج يعطينا المعيار الذي من خلاله نحكم على العدد فيما إذا كان عدد كارمايكل أم لا. سنقوم الآن بإعطاء نص هذا المعيار والبرهان عليه.

نظرية (١٩,١) (معيار كورسيلت Korselt لأعداد كارمايكل).

ليكن n عدداً غير أولي. عندئذ فإن n عدد كارمايكل إذا وفقط إذا كان n عدداً فرديًّا وكل عدد أولي p يقسم n يحقق الشرطين التاليين:

(1) p^2 لا يقسم n.

(2) $p-1$ يقسم $n-1$.

البرهان

لنفرض بداية أن n عدد غير أولي، ولنفرض أن كل عدد أولي p يقسم n يحقق الشرطين (1) و (2). الآن نريد أن نبرهن أن n عدد كارمايكل. برهاننا يعتمد نفس الأسلوب الذي استخدمناه عند برهاننا أن 561 عدد كارمايكل.

نحلل n إلى عوامله الأولية:

$$n = p_1 p_2 p_3 \dots p_r$$

من الشرط (1) نعلم أن $p_1, p_2, \dots, p_r$ جميعها مختلفة. كذلك نعلم من الشرط (2) أن كل $p-1$ يقسم $n-1$ ؛ لذلك لكل i نستطيع عمل التحليل التالي:

$n-1=(p_i-1)k_i$ ، حيث k_i عدد صحيح.

الآن خذ أي عدد صحيح a. سنحسب قيمة a^n قياس p_i كما يلي:

أولاً، إذا كان p_i يقسم a فمن الواضح أن:

$$a^n \equiv 0 \equiv a \pmod{p_i}$$

وإلا فإن p_i لا تقسم a وعندها يمكننا استخدام نظرية فيرما الصغرى لحساب:

$$a^n = a^{(p_i-1)k_i+1}$$

(لأن $n-1=(p_i-1)k_i$)، إذاً:

$$= a^{(p_i-1)k_i} \cdot a$$

$$\equiv 1^{k_i} \cdot a \pmod{p_i}$$

(من نظرية فيرما الصغرى، التي تخبرنا أن $a^{k_i-1} \equiv 1 \pmod{p_i}$)

$$\equiv a \pmod{p_i}$$

نكون بذلك قد برهنا أن:

$$a^n \equiv a \pmod{p_i} \text{ لكل } i = 1,2,\ldots,r$$

وبكلمات أخرى، $a^n - a$ تقبل القسمة على كل عدد أولي $p_1, p_2, \ldots, p_r$، ولذلك يقبل القسمة على حاصل ضربهم $n = p_1 p_2 \ldots p_r$ (لاحظ أننا نستخدم ذلك عندما $p_1, p_2, \ldots, p_r$ جميعها مختلفة). لذلك:

$$a^n \equiv a \pmod{n}$$

وحيث إننا بينا أن هذا صحيح لكل عدد صحيح a، نكون بذلك قد برهنا أن n عدد كارمايكل.

حتى الآن نكون قد برهنا نصف معيار كورسيلت، وهو: العدد الأولي الفردي الذي يحقق الشرطين (1) و (2) يكون عدد كارمايكل. بالنسبة للاتجاه الآخر، فقد برهنا سابقاً أن أي عدد كارمايكل يحقق الشرط (1)، وفي التمرين 19.1 نطلب منك أن تبين أن أعداد كارمايكل تحقق أيضاً الشرط (2).

ولنبين قوة وفاعلية معيار كورسيلت، سنقوم بالتحقق من أن المثالين اللذين تطرقنا لهما سابقاً هما فعلاً عددي كارمايكل.

أولاً، معيار كورسيلت يخبرنا أن $1729 = 7 \cdot 13 \cdot 19$ هو عدد كارمايكل، لأن:

$$\frac{1729-1}{7-1}=288 \quad , \quad \frac{1729-1}{13-1}=144 \quad , \quad \frac{1729-1}{19-1}=96$$

ثانياً، $62745=3\cdot 5\cdot 47\cdot 89$ هو عدد كارمايكل، لأن:

$$\frac{62745-1}{3-1}=31372, \qquad \frac{62745-1}{5-1}=15686,$$
$$\frac{62745-1}{47-1}=1364, \qquad \frac{62745-1}{89-1}=713$$

في بحثه المنشور سنة 1910 ، توقع كارمايكل أن هناك عدداً لا نهائيًّا من أعداد كارمايكل. (طبعاً هو لم يسميها أعداد كارمايكل!) هذا التخمين ظل بدون برهان لما يزيد عن 70 سنة. وبُرهن سنة 1994 على يد كل من ألفورد، جرانفيل، وبوميرانس.

إن حقيقة وجود أعداد كارمايكل يعني أننا بحاجة إلى طريقة أفضل لفحص فيما إذا كان العدد أوليًّا أم لا. اختبار رابين – ميلر Rabin-Miller للأعداد غير الأولية يقوم على الحقيقة التالية.

نظرية (٢, ١٩) (خاصية الأعداد الأولية)

ليكن p عدداً أوليًا فرديًا و $p-1=2^k q$ ، حيث q عدد فردي.

ليكن a أي عدد لا يقبل القسمة على p . عندئذ فإن أحد الشرطين التاليين يكون صحيح:

(i) a^q يطابق 1 قياس p .

(ii) أحد الأعداد $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}\cdot q}$ يطابق -1 قياس p .

البرهان

نظرية فيرما الصغرى تخبرنا أن $a^{p-1} \equiv 1 \pmod{p}$. إن هذا يعني أننا عندما ننظر إلى قائمة الأرقام:

$$a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}\cdot q}, a^{2^k q}$$

فإننا سنعلم أن آخر رقم في هذه القائمة يطابق 1 قياس p (لأن $2^k q$ يساوي $p-1$). أيضاً، كل رقم في هذه القائمة هو تربيع الرقم الذي يسبقه. لذلك فإن أحد الاحتمالين التاليين يجب أن يتحقق:

(i) أول رقم في القائمة يطابق 1 قياس p.

(ii) أحد أرقام القائمة لا يطابق 1 قياس p، ولكن عندما نربعه يصبح مطابقاً للعدد 1 قياس p. الرقم الوحيد الذي ينطبق عليه هذا الوصف هو -1 قياس p، لذلك في هذه الحالة فإن القائمة تحوي -1 قياس p. وهو المطلوب.

بالعودة للخاصية السابقة للأعداد الأولية، نستطيع أن نستخلص اختبار لفحص الأعداد غير الأولية يسمى اختبار رابين – ميلر Rabin-Miller test. لذلك، إذا كان n عدداً فرديًّا وإذا لم يكن له خاصية العدد الأولي المذكورة سابقاً، فإننا نعلم أن n من المؤكد عدد غير أولي. كذلك، إذا لم يكن للعدد n خاصية العدد الأولي لكثير من القيم المختلفة للعدد a، فإن n من المحتمل أن يكون أوليًّا.

نظرية (٣, ١٩) (إختبار رابين – ميلر للأعداد غير الأولية)

ليكن n عدداً صحيحاً فرديًّا ونكتب $n-1 = 2^k q$، حيث q عدد فردي. إذا تحقق الشرطان التاليان لبعض قيم a التي لا تقبل القسمة على n، فإن n عدد غير أولي.

$$a^q \not\equiv 1 \pmod{n} \quad (a)$$

$$a^{2^i q} \not\equiv -1 \pmod{n} \quad \text{لكل } i = 0,1,\ldots,k-1 \quad (b)$$

من الواضح أن إختبار رابين – ميلر يعمل ؛ لأنه إذا كان n يحقق الشرطين (a) و (b) ، فإنه لا يحقق خاصية العدد الأولي ، إذاً من المؤكد أن n عدد غير أولي. لاحظ أن اختبار رابين – ميلر سريع جداً ، وسهل التنفيذ على الكمبيوتر ؛ لأنه بعد حساب $a^q \pmod{n}$ ، نقوم بحساب بعض التربيعات قياس n . لأي اختيار محدد لقيمة a ، فإن اختبار رابين – ميلر إما أن يبرهن أن n غير أولي ، وإما أنه قد يكون أوليًّا. شاهد رابين – ميلر على قابلية n للتحليل هو عدد a يجعل اختبار رابين – ميلر يبرهن بنجاح أن n عدد غير أولي. السبب الكامن وراء فاعلية اختبار رابين – ميلر يعود إلى الحقيقة التالية المثبتة في مباحث متقدمة في نظرية الأعداد.

إذا كان n عدداً غير أولي فردي فإن 75% من الأعداد a بين 1 و $n-1$ تمثل شهود رابين – ميلر للعدد n .

بكلمات أخرى ، أي عدد غير أولي له كثير من شهود رابين – ميلر على أنه غير أولي ؛ لذلك لا توجد أي "فئة من أعداد كارمايكل" تصلح لاختبار رابين – ميلر.

على سبيل المثال ، إذا اخترنا بشكل عشوائي 100 قيمة مختلفة للعدد a ، وإذا لم يكن أي منها من شهود رابين – ميلر للعدد n ، فإن احتمال[1] أن يكون n عدد

---

(١) لقد قمنا بخدعة صغيرة. في الحقيقة نحن نحتاج لحساب ما يسمى الاحتمال المشروط ، في هذه الحالة ، احتمالية أن يكون n عدداً غير أولي حصلنا عليها بعد أن فشلت 100 قيمة للعدد a في أن تكون شاهداً. القيمة الصحيحة للاحتمال تساوي تقريباً $\ln(n) \cdot 0.25^{100}$.

غير أولي يكون أقل من 0.25^{100} ، وهذا تقريباً يساوي 6.10^{-16} . وإذا شعرت أن ذلك يتطلب الكثير من المخاطرة، فإنك تستطيع دائماً أن تحول مع مئات القيم القليلة الأخرى للعدد a. ومن ناحية تطبيقية، إذا كان n عدداً غير أولي، فإن مجرد اختبارات قليلة من اختبارات رابين – ميلر توحي دائماً بهذه الحقيقة.

لتوضيح ذلك، سوف نقوم بتطبيق اختبار رابين – ميلر عندما $a=2$ على الرقم $n=561$ ، والذي نتذكر أنه عدد كارمايكل. عندنا $n-1=560=2^4\cdot 35$ ، لذلك نحسب:

$$2^{35}\equiv 263 \pmod{561},$$
$$2^{2.35}\equiv 263^2\equiv 166 \pmod{561},$$
$$2^{4.35}\equiv 166^2\equiv 67 \pmod{561},$$
$$2^{8.35}\equiv 67^2\equiv 1 \pmod{561}$$

العدد الأول $2^{35} \pmod{561}$ ليس 1 ولا -1 ، والأعداد الأخرى ليست -1 ؛ لذلك فإن العدد 2 هو شاهد رابين – ميلر على حقيقة أن 561 عدد غير أولي. وكمثال آخر، سوف نأخذ العدد الكبير $n=172947529$. الآن:

$$n-1=172947528=2^3\cdot 21618441$$

نطبق اختبار رابين – ميلر عندما $a=17$ ، لنحصل من أول خطوة على:

$$17^{21618441}\equiv 1 \pmod{172947529}$$

وعليه؛ فإن 17 ليس شاهد رابين – ميلر على n. ثم نحاول مع $a=3$ ، لكن لسوء الحظ:

$$3^{21618441} \equiv -1 \pmod{172947529}$$

لذلك ؛ فإن العدد 3 ليس شاهد رابين – ميلر أيضاً. قد نتوقع الآن أن n عدد أولي، لكن إذا حاولنا مع قيمة أخرى، مثل $a = 23$ ، سنجد أن :

$$23^{21618441} \equiv 40063806 \pmod{172947529},$$

$$23^{2.21618441} \equiv 2257065 \pmod{172947529},$$

$$23^{4.21618441} \equiv 1 \pmod{172947529}$$

لذلك العدد 23 هو شاهد رابين – ميلر على أن n عدد غير أولي. في الحقيقة، فإن n عدد كارمايكل، ولكن ليس من السهل تحليله يدوياً.

تمارين

(١٩,١) ليكن n عدد كارمايكل وليكن p عدداً أوليًّا يقسم n.

(a) أكمل برهان معيار كورسيلت من خلال إثبات أن $p-1$ يقسم $n-1$.
[مساعدة: سنبرهن في الفصل الواحد والعشرون أنه لأي عدد أولي p يوجد عدد q قواه $q, q^2, q^3, \ldots, q^{p-1}$ جميعها مختلفة قياس p. (مثل هذا الرقم يسمى جذراً أوليًّا). حاول أن تضع $a = q$ في تطابق كارمايكل $a^n \equiv a \pmod{n}$.]

(b) برهن أن $p-1$ يقسم الرقم الأصغر $\frac{n}{p} - 1$.

(١٩,٢) هل توجد أعداد كارمايكل تحلل لعددين أوليين فقط. إما أن تعطي مثالاً وإما أن تثبت أن هذه الأعداد غير موجودة.

(١٩,٣) استخدم معيار كورسيلت لتحدد أي من الأرقام التالية يمثل عدد كارمايكل.

(a) 1105 (b) 1235 (c) 2821 (d) 6601

(e) 8911 (f) 10659 (g) 19747 (h) 105545

(i) 126217 (j) 162401 (k) 172081 (l) 188461

(١٩,٤) افرض أنه تم اختيار k لتكوين الأعداد الثلاثة:

$$6k+1\ ,\ 12k+1\ ,\ 18k+1$$

جميعها أعداد أولية.

(a) برهن أن حاصل ضربهم $n=(6k+1)(12k+1)(18k+1)$ هو عدد كارمايكل.

(b) أوجد أول خمس قيم للعدد k ، بحيث يمكن تطبيق هذه الطريقة وأعط أعداد كارمايكل الناتجة من تطبيقها.

(١٩,٥) أعط عدد كارمايكل يحلل إلى خمسة أعداد أولية.

(١٩,٦) (a) اكتب برنامجاً على الكمبيوتر يستخدم معيار كورسيلت لاختبار فيما إذا كان عدد ما هو عدد كارمايكل أم لا.

(b) قمنا سابقاً بعمل قائمة تعرض جميع أعداد كارمايكل الأقل من 10.000. استخدم برنامجك لتضم القائمة جميع أعداد كارمايكل حتى 100.000.

(c) استخدم برنامجك لإيجاد أصغر عدد كارمايكل أكبر من 100.000 .

(١٩,٧) (a) ليكن $n=1105$ ، إذاً $n-1=2^4\cdot 69$ احسب قيم:

$$2^{69}\pmod{1105}, \qquad 2^{2.69}\pmod{1105},$$
$$2^{4.69}\pmod{1105}, \qquad 2^{8.69}\pmod{1105}$$

واستخدم إختبار رابين – ميلر لتستنتج أن n غير أولي.

(b) استخدم اختبار رابين – ميلر عندما $a=2$ لإثبات أن $n=294409$ غير أولي. ثم حلل n وبين أنه عدد كارمايكل.

(c) أعد حل فقرة (b) عندما $n=118901521$.

(١٩.٨) برمج اختبار رابين – ميلر بأعداد صحيحة دقيقة. واستخدمه لتبحث فيما إذا كانت الأعداد التالية غير أولية أم لا.

(a) 155196355420821961

(b) 155196355420821889

(c) 285707540662569884530199015485750433489

(d) 285707540662569884530199015485751094149