الفصل الثاني عشر

الأعداد الأولية
Prime Numbers

إن الأعداد الأولية هي لبنات البناء الأساسية في نظرية الأعداد. هذا ما تخبرنا به النظرية الأساسية للحساب، التي درسناها في الفصل السابع. فكل عدد يُبنى بطريقة واحدة فقط من خلال ضرب أعداد أولية مع بعضها البعض. هناك حالات مناظرة لذلك في فروع العلم الأخرى، وبدون استثناء، كان لاكتشاف ووصف لبنات البناء التأثير العميق على انضباط هذه العلوم. على سبيل المثال، اكتشاف أن كل مادة كيميائية تتكون من عناصر أساسية قليلة و تصنيف "مينديليف" لهذه العناصر في عائلات لها خصائص مشتركة، قد أحدث ثورة في علم الكيمياء. بعد قليل، سنقوم بعمل شبيه لذلك عندما نُصنف الأعداد الأولية إلى مجموعات مختلفة، على سبيل المثال، مجموعة الأعداد الأولية التي تطابق 1 قياس 4 ومجموعة الأعداد الأولية التي تطابق 3 قياس 4. بشكل مشابه، فقد حدث تقدم هائل في الفيزياء عندما اكتشف العلماء أن الذرات تكون كل العناصر، وأن الذرة تتألف من ثلاثة جُسيمات أساسية هي البروتونات، النيوترونات، و الإلكترونات،[1] وأن كل عدد منها يحدد سمات الذرة الكيميائية

(١) هذا الوصف للذرة هو للتبسيط، لكنه صورة دقيقة إلى حد ما عن النظريات الأساسية للذرة والتي تطورت في أوائل القرن العشرين.

والفيزيائية. فمثلاً، الذرة التي تتألف من 92 بروتوناً وفقط 143 نيوترون لها خصائص تميزها بوضوح عن ابنة عمها الذرة التي لها ثلاثة نيوترونات إضافية.

حقيقة أن الأعداد الأولية هي اللبنات الأساسية في دراسة نظرية الأعداد يعد سبباً كافياً لدراسة خصائص هذه الأعداد. طبعاً هذا لا يعني أن جميع هذه الخصائص ستكون مثيرة للاهتمام. فدراسة تصريفات الأفعال الشاذة عندما نتعلم اللغة، ولكن هذا لا يجعل منها موضوعاً جذباً. لحسن الحظ، فكلما درسنا عن الأعداد الأولية أكثر، تصبح مثيرة للاهتمام أكثر، وتصبح العلاقات التي نكتشفها بين هذه الأعداد أكثر جمالاً ودهشة. في هذا الفصل سيكون لدينا وقت فقط لذكر بعض هذه الخصائص الرائعة والكثيرة للأعداد الأولية.

في البداية دعنا نعمل قائمة بالأعداد الأولية القليلة الأولى:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \ldots$$

ما الذي يمكن ملاحظته من هذه القائمة؟ أولاً، يبدو أن 2 هو العدد الزوجي الأولي الوحيد. وهذا صحيح بالطبع. إذا كان n عدداً زوجياً أكبر من 2 فيمكن تحليله إلى $n = 2 \cdot \left(n/2\right)$. الخاصية السابقة تجعل من 2 عدداً شاذاً في مجموعة الأعداد الأولية، وعليه فإن الناس معها حق عندما تقول إن:

" 2 هو أغرب الأعداد الأولية "

الملاحظة الأكثر أهمية التي يمكن ملاحظتها من قائمتنا للأعداد الأولية، هي النقاط الثلاث الموضوعة في نهاية القائمة (...)، والتي تعني أن القائمة غير مكتملة. مثلاً 67 , 71 هما العددان الأوليان التاليان في القائمة. السؤال الرئيسي هنا هو، هل هذه القائمة ستنتهي أو ستستمر إلى ما لانهاية؟ بمعنى آخر، هل هناك عدد لا نهائي من الأعداد الأولية؟ الجواب هو نعم. سنقدم الآن برهاناً جميلاً ظهر في كتاب الأصول (العناصر) لإقليدس (*Euclid's Elements*) قبل أكثر من ألفي عام.

نظرية (١,١٢). (نظرية لانهائية الأعداد الأولية).

هناك عدد لا نهائي من الأعداد الأولية .

برهان "إقليدس". افرض أن لديك قائمة منتهية من الأعداد الأولية. سأُبين لك كيف تجد عدداً أولياً جديداً ليس من ضمن القائمة. بعد ذلك تستطيع إضافة العدد الأولي الجديد للقائمة ونعيد العملية، هذا يثبت أن لدينا عدداً لا نهائيًّا من الأعداد الأولية.

لذا افرض أنك بدأت بقائمة من أعداد أولية $p_1, p_2, \ldots, p_r$. بضرب هذه الأعداد معاً وإضافة 1 نحصل على العدد:

$$A = p_1 p_2 p_3 \ldots, p_r + 1$$

إذا كان A عدداً أوليًّا فقد انتهى البرهان؛ لأن A كبير جداً ليكون في القائمة الأصلية. أما إذا كان A عدداً غير أولي فسيقبل بالطبع القسمة على عدد أولي ما؛ لأن كل عدد يمكن كتابته على شكل حاصل ضرب أعداد أولية. افرض أن q (أصغر عدد أولي) يقسم A . أنا أدعي أن q ليس موجوداً في القائمة الأصلية، وعليه سيكون العدد الأولي الجديد المطلوب.

لماذا q ليس في القائمة الأصلية؟ نعلم أن q يقسم A ، إذن:

$$q \text{ يقسم } p_1 p_2 \ldots p_r + 1 \text{ .}$$

إذا كان q واحداً من $\left\{p_i : i = 1,2,\ldots,r\right\}$ فيجب أن يقسم 1 ، وهذا ليس ممكناً. هذا يعني أن q عدد أولي جديد يمكن إضافته إلى قائمتنا. إذا كررنا هذه الخطوة، فسنعمل قائمة من الأعداد الأولية بالطول الذي نريده. هذا يوضح أنه يجب أن يكون هناك عدد لا نهائي من الأعداد الأولية.

برهان إقليدس جميل وذكي جداً. سنوضح الأفكار الواردة في برهان إقليدس لاستخدامها في عمل قائمة من الأعداد الأولية. نبدأ بقائمة تتكون من عدد أولي واحد $\{2\}$. تبعاً لإقليدس، نحسب $A = 2 + 1 = 3$. وهذا عدد أولي، لذلك سنضيفه إلى قائمتنا. الآن أصبح لدينا عددان أوليان، $\{2,3\}$. مرة أخرى، نحسب $A = 3 \cdot 2 + 1 = 7$، ومرة أخرى A عدد أولي وبالتالي يمكن إضافته لقائمتنا لتصبح $\{2,3,7\}$. بإعادة العملية نحسب $A = 2 \cdot 3 \cdot 7 + 1 = 43$ وهذا عدد أولي آخر! وعليه أصبحت قائمتنا تضم أربعة أعداد أولية $\{2,3,7,43\}$. مرة أخرى، نحسب $A = 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807$. في هذه المرة A ليس عدداً أولياً، ويمكنك تحليله على الصورة $A = 13 \cdot 139$. وحسب إقليدس نضيف 13 إلى القائمة لتصبح $\{2,3,7,43,13\}$. مرة أخرى نحسب $A = 2 \cdot 3 \cdot 7 \cdot 43 \cdot 13 + 1 = 23479$. A هذا أيضاً يحلل على الصورة $A = 53 \cdot 443$. نضيف 53 إلى القائمة لتصبح $\{2,3,7,43,13,53\}$، وسنتوقف هنا. لكن من حيث المبدأ نستطيع الاستمرار في هذه العملية لإنتاج قائمة من الأعداد الأولية بالطول الذي نريده.

أصبحنا نعرف الآن أن هناك عدداً لا نهائيًّا من الأعداد الأولية، كما لاحظنا أن 2 هو العدد الزوجي الأولي الوحيد. كل عدد فردي يطابق 1 أو 3 قياس 4، وبالتالي يمكننا التساؤل عن أي الأعداد الأولية تطابق 1 قياس 4 وأيها تطابق 3 قياس 4. هذا يقسم مجموعة الأعداد الأولية (الفردية) إلى عائلتين، تماماً كما يقسم الجدول الدوري العناصر إلى عائلات لها خصائص متشابهة. في القائمة التالية، أشرنا بمربع إلى الأعداد الأولية المطابقة لـ 1 قياس 4.

$$3, \boxed{5}, 7, 11, \boxed{13}, \boxed{17}, 19, 23, \boxed{29}, 31, \boxed{37}, \boxed{41}, 43, 47, \boxed{53}, 59,$$
$$\boxed{61}, 67, 71, \boxed{73}, 79, 83, \boxed{89}, \boxed{97}, \boxed{101}, \ldots$$

لا يبدو أن هناك نمطاً واضحاً، على الرغم من وجود وفره في الأعداد من كلا النوعين. هنا قائمة أطول.

$p \equiv 1 \pmod 4$	$5,13,17,29,37,41,53,61,73,89,97,101,109,$ $113,137,149,157,173,181,193,197,\ldots$
$p \equiv 3 \pmod 4$	$3,7,11,19,23,31,43,47,59,67,71,79,83,103,$ $107,127,131,139,151,163,167,179,\ldots$

هل هناك إمكانية لانتهاء أحد الصفوف في القائمة أو أن هناك عدداً لا نهائيًّا من الأعداد الأولية في كل عائلة؟ يبدو أن كل صف يستمر إلى ما لا نهاية. سنستخدم الإجراء المستخدم في برهان إقليدس لإثبات وجود عدد لا نهائي من الأعداد الأولية التي تطابق 3 قياس 4. في الفصل الرابع والعشرين سنقوم باستخدام أسلوب مختلف تماماً للتعامل مع الأعداد الأولية التي تطابق 1 قياس 4.

نظرية (١٢,٢) (نظرية الأعداد الأولية المطابقة لـ 3 قياس 4).

يوجد عدد لا نهائي من الأعداد الأولية المكافئة لـ 3 قياس 4.

البرهان

سنفرض أن لدينا قائمة منتهية من الأعداد الأولية المطابقة لـ 3 قياس 4. المطلوب هو جعل القائمة أطول بإيجاد عدد أولي جديد مطابق لـ 3 قياس 4. بالاستمرار بهذه العملية نحصل على قائمة بالطول الذي نريد. وبالتالي نثبت أن لدينا عدداً لا نهائيًّا من الأعداد الأولية المطابقة لـ 3 قياس 4.

افرض أن قائمتنا الابتدائية من الأعداد الأولية المطابقة لـ 3 قياس 4 هي :

$$3, p_1, p_2, \ldots, p_r$$

لنأخذ العدد :

$$A = 4p_1p_2 \ldots p_r + 3$$

(لاحظ أننا لم نضم العدد الأولي 3 إلى حاصل الضرب). نعرف أن A يمكن تحليله إلى حاصل ضرب أعداد أولية :

$$A = q_1q_2 \ldots q_s$$

أدعي أنه من بين الأعداد الأولية $q_1, q_2, \ldots, q_s$ يوجد على الأقل عدد واحد يطابق 3 قياس 4 . هذه هي أهم خطوة في البرهان. لماذا هذا صحيح؟ حسناً، إذا فرضنا أن ذلك خطأ، فإن $q_1, q_2, \ldots, q_s$ جميعها ستكون مطابقة لـ 1 قياس 4 ، في هذه الحالة حاصل ضربها A سيطابق 1 قياس 4 . لكن واضح من تعريف A أنه يطابق 3 قياس 4 ؛ لذا فإنه يوجد على الأقل عدد واحد من $q_1, q_2, \ldots, q_s$ يجب أن يكون مطابقاً لـ 3 قياس 4 ، ولنقل $q_i \equiv 3 \pmod 4$.

إدعائي الثاني هو أن q_i ليس موجوداً في القائمة الأصلية. لِمَ لا ؟ حسناً، نعرف أن q_i يقسم A . بينما واضح من تعريف A أنه لا يوجد أي عدد من $3, p_1, p_2, \ldots, p_r$ يقسم A . لذلك، q_i ليس في قائمتنا الأصلية ؛ لذا يمكن إضافته إلى القائمة وإعادة العملية. بهذه الطريقة يمكن عمل قائمة من الأعداد الأولية المطابقة لـ 3 قياس 4 بالطول الذي نريده، وهذا يثبت أن هناك عدداً لا نهائيًّا من الأعداد الأولية المطابقة لـ 3 قياس 4 .

يمكننا استخدام الأفكار الواردة في برهان نظرية الأعداد الأولية $3 \pmod 4$ لإنشاء قائمة من الأعداد الأولية تطابق 3 قياس 4 . نحن نحتاج لأن نبدأ بقائمة تضم

على الأقل عدداً واحداً من هذه الأعداد، وتذكر أنه غير مسموح للعدد 3 أن يكون في قائمتنا. لذلك سنبدأ بقائمة تضم فقط العدد الأولي $\{7\}$. نحسب $A = 4 \cdot 7 + 3 = 31$. نفس A هذا عدد أولي؛ لذلك فهو عدد جديد $3 \pmod 4$ لنضيفه إلى قائمتنا. القائمة الآن هي $\{7,31\}$، لذلك نحسب $A = 4 \cdot 7 \cdot 31 + 3 = 871$. A هذا ليس أوليًّا؛ ويحلل على الشكل $A = 13 \cdot 67$. برهان النظرية يخبرنا أن أحد العوامل الأولية على الأقل سيطابق 3 قياس 4. في حالتنا هذه، العدد 67 هو $3 \pmod 4$؛ لذلك نضيفه إلى قائمتنا. بعد ذلك نأخذ $\{7,31,67\}$، ونحسب $A = 4 \cdot 7 \cdot 31 \cdot 67 + 3 = 58159$، ونحلله على الشكل $A = 19 \cdot 3061$. في هذه المرة يكون العامل الأول 19 هو $3 \pmod 4$، لذلك تصبح قائمتنا $\{7,31,67,19\}$. سنكرر الإجراء مرة أخرى. إذن:

$$A = 4 \cdot 7 \cdot 31 \cdot 67 \cdot 19 + 3 = 1104967 = 179 \cdot 6173$$

والذي يعطي العدد الأولي 179 لنضيفه إلى القائمة، $\{7,31,67,19,179\}$.

لماذا لا نطبق نفس فكرة العمل على الأعداد الأولية $1 \pmod 4$؟ هذا السؤال ليس بالسؤال الفارغ; إن أهمية فهم مُحددات البرهان على نفس الدرجة من أهمية فهم لماذا البرهان صحيح. لذلك، لنفرض أننا نحاول إنشاء قائمة للأعداد الأولية $1 \pmod 4$. إذا بدأنا بالقائمة $\{p_1, p_2, \ldots, p_r\}$، فإننا نستطيع أن نحسب العدد $A = 4p_1p_2 \ldots p_r + 1$، ونحلله، ونحاول إيجاد معامل أولي جديد $1 \pmod 4$. ماذا يحدث لو بدأنا بالقائمة $\{5\}$؟ نحسب $A = 4 \cdot 5 + 1 = 21 = 3 \cdot 7$، ونجد أن كل من العاملين $3, 7$ ليس $1 \pmod 4$. إذن توقفنا. المشكلة هي إمكانية ضرب عددين $3 \pmod 4$، مثل 3 و 7، وتحصل على عدد $1 \pmod 4$ مثل $A = 21$. بشكل عام، لا نستطيع استخدام حقيقة أن $A \equiv 1 \pmod 4$ لنستنتج أن أحد عوامل

A الأولية هو $1 \pmod 4$ ، وهذا السبب وراء أن هذا البرهان لا يصلُح مع الأعداد الأولية التي تطابق 1 قياس 4 .

ليس هناك سبب محدد لنتعامل فقط مع التطابقات قياس 4 . على سبيل المثال ، كل عدد يطابق إما $0,1,2,3$ وإما 4 قياس 5 ; وباستثناء العدد 5 نفسه ، كل عدد أولي يطابق أحد الأعداد $1,2,3$ أو 4 قياس 5 . (لماذا؟) لذلك يمكننا تقسيم مجموعة الأعداد الأولية إلى أربع عائلات ، اعتمادا على صف تطابقها قياس 5 . هنا قائمة للأعداد القليلة الأولى من كل عائلة :

$p \equiv 1 \pmod 5$	$11,31,41,61,71,101,131,151,181,191,211,241$
$p \equiv 2 \pmod 5$	$2,7,17,37,47,67,97,107,127,137,157,167,197$
$p \equiv 3 \pmod 5$	$3,13,23,43,53,73,83,103,113,163,173,193,223$
$p \equiv 4 \pmod 5$	$19,29,59,79,89,109,139,149,179,199,229,239$

مرة أخرى ، يظهر أن هناك عدداً وفيراً من الأعداد الأولية في كل عائلة ؛ لذلك نتوقع أن كل منها يضُم عدداً لا نهائيًّا من الأعداد الأولية.

بشكل عام ، إذا ثبّتنا المقياس m وعدد a ، فمتى نتوقع أن هناك عدداً لا نهائيًّا من الأعداد الأولية التي تطابق a قياس m ؟ إن هناك حالة واحدة لا يتحقق فيها ذلك ، وهذا يحدث عندما يكون للعددين a و m عامل مشترك. على سبيل المثال ، افرض أن p عدداً أوليًّا ، وأن $p \equiv 35 \pmod{77}$. هذا يعني أن $p = 35 + 77y = 7(5 + 11y)$ ، إذن الاحتمال الوحيد هو أن $p = 7$ ، وحتى

$p = 7$ ليست حلاً بشكل عام، إذا كان p عدداً أوليًّا يحقق التطابق، فإن $\gcd(a,m)$ يقسم p. إذن إما $\gcd(a,m) = 1$ وإما $\gcd(a,m) = p$، وهذا يعني أن هناك احتمال واحد على الأكثر لقيمة p. لهذا نهتم فقط بالسؤال عن الأعداد الأولية التي تطابق a قياس m إذا افترضنا أن $\gcd(a,m) = 1$. نظرية "ديرشله" (Dirichlet) المشهورة (من عام 1837) تنص على أنه إذا تحقق هذا الفرض؛ فإن هناك دائماً عدداً لا نهائيًّا من الأعداد الأولية تطابق a قياس m.

نظرية (١٢,٣) (نظرية ديرشله للأعداد الأولية في المتتالية الحسابية[١]).

ليكن a و m عددين صحيحين، بحيث $\gcd(a,m) = 1$. عندئذ يوجد عدد لا نهائي من الأعداد الأولية التي تطابق a قياس m. أي أن هناك عدداً لا نهائيًّا من الأعداد الأولية p التي تحقق $p \equiv a \pmod{m}$.

في بدايات هذا الفصل برهنا نظرية ديرشله عندما $(a,m) = (3,4)$، والتمرين 12.2 يطلب منك البرهان عندما $(a,m) = (5,6)$. في الفصل الرابع والعشرين، سوف نتعامل مع الحالة $(a,m) = (1,4)$. لسوء الحظ، إن برهان نظرية ديرشله لجميع قيم (a,m) صعب بما فيه الكفاية، لذلك لن نعرضه في هذا الكتاب. إن البرهان يستخدم طرقاً متقدمة في التفاضل والتكامل، وفي الحقيقة، التفاضل والتكامل بأعداد مركبة!

---

(١) المتتالية الحسابية هي قائمة من الأعداد الفرق بينها ثابت. على سبيل المثال، $2,7,12,17,22,\ldots$ هي متتالية حسابية بفرق ثابت مقداره 5. الأعداد التي تطابق a قياس m تُشكّل متتالية حسابية بفرق ثابت m، وهذا ما يشرح اسم نظرية ديرتشلت.

تمارين

(١٢,١) ابدأ بقائمة تضم فقط العدد الأولي $\{5\}$ ، واستخدم الأفكار الواردة في برهان إقليدس من أن هناك عدداً لا نهائيًّا من الأعداد الأولية لإنشاء قائمة من الأعداد الأولية حتى تحصل على أعداد تكون كبيرة على أن تقوم بتحليلها بسهولة. (يجب أن تكون قادراً على تحليل أي عدد أقل من 1000).

(١٢,٢) (a) بين أن هناك عدد لا نهائي من الأعداد الأولية تطابق 5 قياس 6.

(مساعدة: استخدم $A = 6p_1p_2 \dots p_r + 5$).

(b) حاول استخدام نفس الفكرة (مع $A = 5p_1p_2 \dots p_r + 4$) لتبين أن هناك عدداً لا نهائيًّا من الأعداد الأولية تطابق 4 قياس 5. ما هو الخطأ ؟ بشكل خاص ، ماذا يحدث لو بدأت بالعدد $\{19\}$ وحاولت أن تنشئ قائمة أطول؟

(١٢,٣) ليكن p عدداً أوليًّا فرديًّا. أكتب المقدار:

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{p-1}$$

على شكل كسر A_p/B_p بأبسط صورة.

(a) أوجد قيمة $A_p \pmod p$ وبرهن أن إجابتك صحيحة.

(b) اعمل تخميناً عن قيمة $A_p \pmod{p^2}$.

(c) برهن تخمينك في (b). (إن هذا البرهان صعب).

(١٢,٤) ليكن m عدداً صحيحاً موجباً، ليكن $a_1, a_2, \dots, a_{\Phi(m)}$ الأعداد الصحيحة بين 1 و m التي تكون أولية نسبياً مع m ، واكتب المقدار:

$$\frac{1}{a_1}+\frac{1}{a_2}+\frac{1}{a_3}+\cdots+\frac{1}{a_{\phi(m)}}$$

على شكل كسر A_m/B_m بأبسط صورة.

(a) أوجد قيمة $A_m \pmod m$ وبرهن أن إجابتك صحيحة.

(b) ولّد بعض البيانات للقيمة $A_m \pmod{m^2}$ ، حاول إيجاد أنماط ، ومن ثم حاول أن تبرهن أن هذه الأنماط صحيحة بشكل عام. بشكل خاص ، متى يكون $A_m \equiv 0 \pmod{m^2}$ ؟

(١٢,٥) تذكر أن العدد "n مضروب"، والذي يكتب $n!$ ، يساوي حاصل الضرب :

$$n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-1) \cdot n$$

(a) أوجد أعلى قوة للعدد 2 بحيث يقسم كل من الأعداد

$1!, 2!, 3!, \ldots, 10!$

(b) صِغ قاعدة تعطي أعلى قوة للعدد 2 بحيث يقسم $n!$.

استخدم قاعدتك لحساب أعلى قوة للعدد 2 بحيث يقسم $100!$, $1000!$.

(c) برهن أن قاعدتك في (b) صحيحة.

(d) أعد حل الفقرات (a)، (b)، و (c)، ولكن هذه المرة لإيجاد أكبر قوة للعدد 3 بحيث يقسم $n!$.

(e) حاول أن تُصيغ قاعدة عامة لأعلى قوة لعدد أولي p بحيث يقسم $n!$. استخدم قاعدتك لإيجاد أعلى قوة للعدد 7 بحيث يقسم $1000!$ وأعلى قوة للعدد 11 بحيث يقسم $5000!$.

(f) باستخدام قاعدتك من (e) أو طريقة أخرى، برهن أنه إذا كان p عدداً أوليًّا وإذا كان p^m يقسم $n!$ ، فإن $m < n/(p-1)$. (هذه المتباينة مهمة جداً في العديد من مجالات نظرية الأعداد المتقدمة).

(١٢,٦) (a) أوجد عدداً أوليًّا p يحقق $p \equiv 1338 \pmod{1115}$. هل هناك عدد لا نهائي من هذه الأعداد الأولية ؟

(b) أوجد عدداً أوليًّا يحقق $p \equiv 1438 \pmod{1115}$. هل هناك عدد لا نهائي من هذه الأعداد الأولية ؟