مقدمة الكتاب

مع مرور الوقت لم نعد نعرف على وجه الدقة كيف نشأت الأعداد الطبيعية $1,2,3,4,5,6,\ldots$. ولا نعلم من هو أول من أدرك أن هناك مفهوماً محدداً عن "الثلاثية"، كثلاثة صخور، ثلاثة نجوم، وثلاثة أشخاص. لقد كانت الأعداد ملهمة وساحرة ومستخدمة من بدايات التاريخ، وبالطبع لم يكن المفهوم المجرد للأعداد نفسها هو الذي يثير الاهتمام. إن المثير للاهتمام هو طبيعة العلاقات التي تظهر بين الأعداد أحدها مع الآخر. وفي كثير من الأحيان يجد المرء الجمال في عمق هذه العلاقات ودقتها. وهنا يصف أحد مشاهير فلاسفة القرن العشرين الرياضيات فيقول " الرياضيات ، وبنظرة واقعية صحيحة، لا تمتلك الحقيقة فقط، وإنما تمتلك أعلى مراتب الجمال، جمالاً بارداً قاسياً كجمال فن النحت، فناً لا يتماشى مع ضعفنا الطبيعي، فناً يخلو من زخارف الرسومات ومحسنات الموسيقى، فناً لا يزال نقياً رفيعاً كامل الإتقان كأعظم فن يمكنك أن تراه ". (بيرتراند راسل Bertrand Russel، 1902).

إن نظرية الأعداد هي ذلك الجزء من الرياضيات الذي يهدف إلى اكتشاف العديد من العلاقات العميقة والدقيقة التي تربط بين أنواع مختلفة من الأعداد. وكمثال بسيط، نرى أن كثيراً من الناس في مختلف العصور مهتمون بالأعداد المربعة $1,4,9,16,25,\ldots$. إذا قمنا بتجربة جمع عددين مربعين، سنجد أحياناً أننا نحصل على عدد مربع آخر. أكثر الأمثلة شهرة على هذه الظاهرة هو :

$$3^2 + 4^2 = 5^2$$

ولكن هناك أمثلة كثيرة أخرى، مثل :

$$5^2 + 12^2 = 13^2 \quad , \quad 20^2 + 21^2 = 29^2 \quad , \quad 28^2 + 45^2 = 53^2$$

الثلاثيات مثل $(3,4,5)$, $(5,12,13)$, $(20,21,29)$, $(28,45,53)$ تسمى ثلاثيات فيثاغورية[1]. بناءاً على هذه التجربة، فإن أي شخص لديه فضول في طرح عدة أسئلة، مثل :

" هل هناك عدد لا نهائي من الثلاثيات الفيثاغورية؟ " و " إذا كان هناك عدد لا نهائي منها، فهل يمكننا إيجاد صيغة تصف جميع هذه الثلاثيات؟ " هذه النوعية من الأسئلة تُعالج من خلال نظرية الأعداد.

كمثال آخر، لنعتبر مسألة إيجاد الباقي عندما نقسم العدد الضخم :

$$32478543^{743921429837645}$$

على العدد 54817263. إحدى طرق حل هذه المسألة هي : خذ العدد 32478543 ، واضربه في نفسه 743921429837645 مرة، ثم استخدم القسمة الطويلة لتقسم الناتج على 54817263 ، وبعد ذلك نأخذ الباقي. من ناحية تطبيقية، فإن ذلك سيستغرق وقتاً أطول بكثير من عُمْر من سينفذ هذه الطريقة، حتى وإن استخدام أسرع أجهزة الكمبيوتر. نظرية الأعداد تزودنا بطرق لحل مثل هذه المسائل أيضاً. " انتظر دقيقة "، إني أسمعك تقول، " الثلاثيات الفيثاغورية فيها من الأناقة ما يُدخل السرور إلى العين، ولكن أين الجمال في القسمة الطويلة والبواقي؟ ". الجواب هو أن الجمال ليس في البواقي نفسها ولكن في كيفية استخدام هذه البواقي. لقد بين الرياضيون كيف أن حل مسألة الباقي البسيطة هذه (وعكسها) يقود إلى خلق شيفرات بسيطة غاية في السرية لا تقدر حتى

---

(١) للإنصاف ، يجب الإشارة هنا إلى أن البابليين عملوا جداول كبيرة للثلاثيات " الفيثاغورية " قبل ولادة فيثاغورس بعدة قرون.

وكالـة الأمـن القـومي[1] علـى فكهـا. لـذلك حملـت ملاحظـة G. H. Hardy تنبؤاً خاطئاً تماماً عندما قال " لم يكتشف أحد بعد أي هدف عسكري يمكن أن تخدمه نظرية الأعداد، ويبدو أن أحداً لن يتمكن من ذلك لسنوات عديدة ".

إن أرض نظرية الأعداد مليئة بالكائنات الغريبة المتنوعة. فهناك الأعداد المربعة والأعداد الأولية، والأعداد الفردية والأعداد الكاملة (لكن ليس هناك أعداد مربعة – أولية أو أعداد كاملة – فردية). وهناك معادلات فيرما Fermat و معادلات بِلْ Pell، الثلاثيات الفيثاغورية والمنحنيات الناقصية، أرانب فيبوناتشي Fibonacci ، الشيفرات غير القابلة للفك، والكثير الكثير.

سوف تقابل كل هذه الكائنات ، وكائنات أخرى كثيرة، خلال رحلتنا في نظرية الأعداد.

دليل المُعلم

هذا الكتاب مُعَدٌّ ليستخدم كمقرر لفصل دراسي واحد أو سنة جامعية كاملة لدراسة نظرية الأعداد أو للدراسة المستقلة. إن هذا الكتاب يضم موضوعات غنية تكفي تقريباً لفصلين دراسيين ؛ لذلك فالذي يُدرس هذا المقرر لفصل دراسي واحد سيكون عنده بعض المرونة في اختيار الموضوعات التي سيُدرسها. الفصول الأحد عشر الأولى هي فصول أساسية، وربما سيرغب معظم المدرسين بالاستمرار حتى نظام التعمية RSA الوارد في الفصل الثامن عشر ؛ لأنه حسب خبرتي فإن هذا الموضوع من أكثر الموضوعات التي يُفَضِلُها الطلاب.

---

(١) وكالـة الأمـن القـومي (NSA) هـي ذراع لحكومـة الولايـات المتحـدة تهـتم بجمـع البيانـات، عمـل الشيفرات، وفك الشيفرات. إن ميزانية الـ NSA أكبر من ميزانية الـ CIA، وهي أكبر مؤسسة لتوظيف علماء الرياضيات في العالم.

هناك الآن عدة طرق للمضي قُدُماً. هنا بعض التصورات التي تبدو مناسبة لفصل دراسي واحد، لكن تصرف بحرية في تجزيء الفصول الأخيرة حتى تتلاءم مع رغبتك.

الفصول 32 – 20

الجذور البدائية Primitive roots، التعاكس التربيعي Quadratic reciprocity، مجاميع مربعات Sums of squares، معادلة بَلْ Pell's equation، والتقريب الديوفانتيني Diophantine approximation. (أضف الفصلين 39 و 40 عن الكسور المستمرة Continued fractions إذا أسعفك الوقت).

الفصول 32 – 28 و 48 – 43

معادلة فيرما للأس 4 (Fermat equation for exponent 4)، معادلة بَلْ، التقريب الديوفانتيني، المنحنيات الناقصية Elliptic curves، ونظرية فيرما الأخيرة Fermat's last theorem.

الفصول 37 – 29 و 40 – 39

معادلة بَلْ، التقريب الديوفانتيني، أعداد جاوس الصحيحة Gaussian integers، الأعداد المتسامية Transcendental numbers، معاملات ذو الحدين Binomial coefficients، الصيغ الارجاعية الخطية Linear recurrences، والكسور المستمرة.

الفصول 25 – 19 و 38 – 36

اختبار الأولية Primality test، الجذور البدائية، التعاكس التربيعي، معاملات ذو الحدين، الصيغ الإرجاعية الخطية. رمز O الكبيرة Big-Oh notation (هذا المحتوى مصمم بشكل خاص للطلاب الذين يريدون متابعة الدراسة في علم الكمبيوتر أو التشفير).

وفي جميع الحالات ، من الأفضل أن يقرأ الطلاب بعض الفصول التي لم نوردها ، وأن يقوموا بحل التمارين.

معظم التمارين غير العددية والتي ليس لها علاقة بالبرمجة ، الواردة في هذا الكتاب ، صممت لإثراء المناقشة والتجربة. وليس من الضروري الإجابة عنها بشكل "صحيح" أو "كامل". سيجد معظم الطلبة هذه التمارين صعبة في البداية ؛ لذلك يجب أن تمتاز الدراسة بالجدية. يمكنك جعل طلابك يشعرون أن المادة أسهل من خلال جعل أسئلتك تبدأ بعبارة مثل "أخبرني بقدر ما تستطيع عن ...". أبلغ طلابك أن جمع البيانات وحل حالات خاصة ليست مجرد طريقة مقبولة وإنما ضرورية. من جهة أخرى ، أخبرهم أنه لا يوجد شيء اسمه حل كامل ؛ لأن حل مسألة جيدة دائماً ما يطرح أسئلة جديدة ، لذلك إذا كانوا يستطيعون إعطاء إجابة كاملة عن سؤال ما ، فإن هدفهم القادم هو البحث عن تعميمات وقيود هذه الحلول.

إن التفاضل والتكامل مطلوب فقط في الفصلين 38 (رمز O الكبيرة) و 41 (توليد الدوال Generating functions). إذا لم يكن الطلاب قد درسوا التفاضل والتكامل فمن الممكن حذف هذين الفصلين دون أن يؤثر ذلك على تسلسل المادة.

إن نظرية الأعداد ليست سهلة ، ولهذا لا توجد طريقة لإقناع الطلاب بذلك. لكن بدلاً من ذلك ، فإن هذا الكتاب سيبين لطلابك أنهم راضون تمام الرضى عن طريقتهم في التفكير الاستكشافي. إن مكافأتك كمدرس هي أنك تنير لهم طريقهم وتوجه مساعيهم ومجهوداتهم.

الحواسيب، نظرية الأعداد، وهذا الكتاب

هنا أرغب في قول بعض الكلمات عن استخدام الحواسيب (الكمبيوترات) في هذا الكتاب. أنا لا أتوقع ولا أطلب من القارئ استخدام برامج كمبيوتر ذات مستوى عالٍ مثل Maple ، Mathematica ، PART أو Derive ، وإن معظم التمارين (ما عدا

المشار لها) يمكن الإجابة عنها باستخدام آلة حاسبة بسيطة. لا شك أن الكمبيوترات تمكننا من التعامل مع أعداد كبيرة، لكن هدفنا الأساسي دائماً هو استيعاب المفاهيم والعلاقات. لذلك إذا كان لي أن أُصدر حكماً بقبول أو رفض استخدام أجهزة الكمبيوتر، فلا شك أنني سأمنع استخدامها.

على كل حال، كأي قاعدة جيدة، فإن لها شواذ. أولاً، أن إحدى أفضل الطرق لفهم موضوع معين هي شرحها لشخص آخر؛ لذا إذا كنت تعرف القليل عن كيفية كتابة برامج الكمبيوتر، فسوف تجد أنه من المفيد للغاية أن تشرح للكمبيوتر كيف ينجز الخوارزميات الموصوفة في هذا الكتاب. بتعبير آخر، لا تعتمد على برامج الكمبيوتر الجاهزة، بل اعمل البرنامج بنفسك. أفضل الموضوعات لتنفيذ هذا الأسلوب هي الخوارزمية الإقليدية Euclidean algorithm (الفصلين 5,6)، نظام التعمية RSA (الفصول 18 - 16)، التعاكس التربيعي (الفصل 25)، كتابة الأعداد كمجموع مربعين (الفصلين 26,27)، اختبار الأولية (الفصل 19)، وتوليد نقاط نسبية على منحنيات ناقصية (الفصل 43).

الاستثناء الثاني لقاعدة " لا للكمبيوتر " هو توليد البيانات. الاكتشاف في نظرية الأعداد دائماً ما يعتمد على التجربة، والتي قد تستلزم فحص رزمة من البيانات لاكتشاف أنماط.

إن الكمبيوترات مفيدة جداً في توليد مثل هذه البيانات، وأيضاً تساعد أحياناً في البحث عن أنماط؛ لذلك أنا لا أعارض استخدامها لخدمة هذه الأهداف.

لقد ضَمَّنت التمارين بعدد من التمارين الحاسوبية والمشاريع الحاسوبية لتشجيعك على استخدام الكمبيوتر كأداة لمساعدتك على الفهم ولتبحث في نظرية الأعداد. بعض هذه التمارين يمكن تنفيذها على كمبيوتر صغير (أو حتى على حاسبة قابلة للبرمجة)، بينما الأخرى تتطلب أجهزة متطورة و/أو لغات برمجة.

بالنسبة للكثير من البرامج، لم أقم بإعطاء صياغة دقيقة لها، حيث إن جزءاً من البرنامج هو ماذا يجب على المستخدم أن يقوم بإدخاله بالضبط وما هو الشكل الذي يجب أن يأخذه الناتج بالضبط. لاحظ أن برنامج الكمبيوتر الجيد يجب أن يتضمن الميزات التالية:

- مكتوب بشكل واضح يشرح ماذا يعمل البرنامج، كيفية استخدامه، ما هي مدخلاته، وما هي مخرجاته.
- تعليقات داخلية شاملة تشرح طبيعة عمل البرنامج.
- معالجة الخطأ بشكل كامل مع وجود رسائل معلوماتية عن الخطأ.

على سبيل المثال، إذا كان $a = b = 0$، فإن $\gcd(a,b)$ يجب أن يُعطي رسالة الخطأ "$\gcd(0,0)$ is undefined" ($\gcd(0,0)$ غير مُعَرَّف) بدلاً من أن يَدْخُل البرنامج في حلقة لا نهائية (infinite loop)، أو يُعطي رسالة الخطأ (division by zero) (قسمة على صفر).

عندما تقوم بكتابة برامجك الخاصة، حاول أن تجعلها سهلة ومتعددة الاستخدام قدر الإمكان؛ لأنك سترغب في نهاية المطاف بربط القطع مع بعضها لتشكيل مجموعتك الخاصة بنظرية الأعداد الروتينية.

إن المغزى هو أن الكمبيوتر مفيد كأداة للتجربة، ويمكنك أن تتعلم الكثير بتدريس الكمبيوتر كيف يُنجز حسابات نظرية الأعداد، ولكن عندما تكون قد تعلمت واستوعبت الموضوع أولاً، بينما البرمجيات الجاهزة ما هي إلا مجرد عُكَّاز يمنعك من أن تتعلم المشي بمفردك.

جوزيف سيلفرمان