الفصل السابع والعشرون

أي الاعداد يساوي مجموع مربعين؟
Which Numbers Are Sums of Two Squares?

في الفصل الأخير قمنا بإعطاء إجابة حاسمة لسؤال أي الأعداد ألأولية يمكن كتابتها كمجموع مربعين. سنحاول الآن الإجابة عن نفس السؤال لأي عدد. جزء من إستراتيجيتنا، والتي يمكن تلخيصها بكلمتين، لها تاريخ طويل ورائع:

"اقسم وانتصر"

طبعاً، "اقسم" لا تعني القسمة بحد ذاتها، بالأحرى، هي تعني تجزئ المسألة إلى أجزاء ذات حجم مناسب، ومن ثم "انتصر" تعني أننا نحتاج لحل كل جزء. لكن هاتين الخطوتين، واللتان قد تكونان كافيتين لهذا الصراع، يجب أن تُتبعان بخطوة ثالثة: إعادة تركيب الأجزاء مع بعضها. خطوة التوحيد هذه تستخدم المتطابقة من الفصل الأخير التي تعبر عن حاصل ضرب عددين كل منهما يساوي مجموع مربعين كمجموع مربعين:

$$\left(u^2+v^2\right)\left(A^2+B^2\right)=\left(uA+vB\right)^2+\left(vA-uB\right)^2 \ldots\ldots\ldots\ldots(*)$$

بعد ذلك، تأتي هنا إستراتيجية خطوة بخطوة للتعبير عن عدد m كمجموع مربعين.

"اقسم": حلل m إلى حاصل ضرب عوامله الأولية $p_1 p_2 \dots p_r$

"انتصر": اكتب كل عدد أولي p_i كمجموع مربعين.

"وَحّدْ": استخدم المتطابقة (*) بشكل مكرر لكتابة m كمجموع مربعين.

نحن نعلم من الفصل السابق متى بالضبط تعمل خطوة انتصر، لأننا نعلم أن عدداً أولياً p يساوي مجموع مربعين إذا وفقط إذا كان $p=2$ أو $p \equiv 1 \pmod 4$. فعلى سبيل المثال، لكتابة 10 كمجموع مربعين، فإننا نحلل $10 = 2 \cdot 5$ ، اكتب كلاً من 2 , 5 كمجموع مربعين:

$$5 = 2^2 + 1^2 \quad \text{و} \quad 2 = 1^2 + 1^2$$

واستخدم المتطابقة لإعادة التجميع:

$$10 = 2 \cdot 5 = \left(1^2 + 1^2\right)\left(2^2 + 1^2\right) = (2+1)^2 + (2-1)^2 = 3^2 + 1^2$$

سنعرض الآن مثال معقد أكثر. سنكتب $m = 1105$ كمجموع مربعين.

"اقسم": حلل $m = 1105 = 5 \cdot 13 \cdot 17$

"انتصر": اكتب كل عدد أولي p كمجموع مربعين

$$17 = 4^2 + 1^2, \qquad 13 = 3^2 + 2^2, \qquad 5 = 2^2 + 1^2$$

"وَحّدْ": كرر استخدام المتطابقة (*) لكتابة m كمجموع مربعين.

$$\begin{aligned} m = 1105 &= 5 \cdot 13 \cdot 17 \\ &= \left(2^2 + 1^2\right)\left(3^2 + 2^2\right)\left(4^2 + 1^2\right) \\ &= \left((6+2)^2 + (3-4)^2\right)\left(4^2 + 1^2\right) \end{aligned}$$

$$= \left(8^2 + 1^2\right)\left(4^2 + 1^2\right)$$
$$= (32+1)^2 + (4-8)^2$$
$$= 33^2 + 4^2$$

إستراتيجيتنا اقسم، انتصر، ووَحّدْ هي إستراتيجية ناجحة مع العدد m بشرط أن كل عامل أولي من عوامل m يكون مساوياً لمجموع مربعين. نحن نعلم أي الأعداد الأولية يمكن كتابتها على شكل مجموع مربعين، لذلك لدينا الآن طريقة لكتابة m كمجموع مربعين إذا حللنا m كالتالي:

$$m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

حيث كل عامل أولي من العوامل إما 2 وإما يطابق 1 قياس 4.

على كل حال، إذا رجعت إلى القائمة الواردة في آخر فصل، فإنك سترى وجود قيم أخرى m تساوي مجموع مربعين، مثلاً،

$$9 = 3^2 + 0^2 \quad , \quad 18 = 3^2 + 3^2 \quad , \quad 45 = 6^2 + 3^2$$

ماذا يعني هذا؟ لاحظ أن m في كل حالة تقبل القسمة على 3^2 و $m = a^2 + b^2$ وكل من a و b يقبل القسمة على 3^2. إذا قسمنا هذه الأمثلة الثلاثة على 3^2، نحصل على:

$$1 = \frac{9}{3^2} = \frac{3^2 + 0^2}{3^2} = 1^2 + 0^2,$$
$$2 = \frac{18}{3^2} = \frac{3^2 + 3^2}{3^2} = 1^2 + 1^2,$$
$$5 = \frac{45}{3^2} = \frac{6^2 + 3^2}{3^2} = 2^2 + 1^2$$

بمعنى آخر، هذه الأمثلة الثلاثة أُنشأت بأخذ المعادلات:

$$1=1^2+0^2 \quad , \quad 2=1^2+1^2 \quad , \quad 5=2^2+1^2$$

وضرب الطرفين بالعدد 3^2.

يمكننا عمل ذلك بشكل عام. إذا أعطينا أي $m=a^2+b^2$ ، فيمكننا الضرب بالعدد d^2 لنحصل على:

$$d^2m=(da)^2+(db)^2$$

إذاً، إذا كان m مجموع مربعين؛ فإن d^2m كذلك لأي d. من ناحية أخرى، إذا كان $m=a^2+b^2$ يساوي مجموع مربعين، وإذا كان a , b لهما عامل مشترك، ليكن $a=dA$ و $b=dB$ ؛ إذاً يمكننا أخذ d^2 عاملاً مشتركاً لنحصل على:

$$m=d^2\left(A^2+B^2\right)$$

إذاً؛ m يقبل القسمة على d^2 و m/d^2 يساوي مجموع مربعين.

إن المغزى هو أن المربعات التي تقسم m لا تحسب عندما نحاول كتابة m كمجموع مربعين. أي، إذا أخذنا m وحللناه كما يلي:

$$m=p_1p_2\dots p_rM^2$$

حيث الأعداد الأولية $p_1p_2\dots p_r$ جميعها مختلفة، عندئذ يمكن كتابة m كمجموع مربعين بشرط أن كل من $p_1p_2\dots p_r$ يمكن كتابته كمجموع مربعين. فعلى سبيل المثال، لنعتبر أن $m=252000$ نحلل m كما يلي:

$$m = 252000 = 2^5 \cdot 3^2 \cdot 5^3 \cdot 7$$
$$= 2 \cdot 5 \cdot 7 \cdot \left(2^2 \cdot 3 \cdot 5\right)^2$$
$$= 2 \cdot 5 \cdot 7 \cdot 60^2$$

العدد الأولي 7 لا يساوي مجموع مربعين ؛ إذاً m لا تساوي مجموع مربعين. (انظر تمرين 27.4).

وكمثال آخر، لنأخذ $m = 25798500$ فإن:

$$m = 25798500 = 2^2 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 13$$
$$= 5 \cdot 13 \cdot \left(2 \cdot 3^2 \cdot 5 \cdot 7\right)^2$$
$$= 5 \cdot 13 \cdot 630^2$$

في هذه الحالة، كل من 5 , 13 يساوي مجموع مربعين، وبسهولة نجد أن $65 = 5 \cdot 13 = 8^2 + 1^2$ بضرب الطرفين بالعدد 630^2 نحصل على:

$$m = 65 \cdot 630^2 = (8 \cdot 630)^2 + (1 \cdot 630)^2 = 5040^2 + 630^2$$

في هذا الفصل، قمنا بإعطاء إجابة كاملة عن سؤال أي الأعداد يمكن كتابتها على شكل مجموع مربعين. نلخص نتيجتنا هذه من خلال النظرية التالية، والتي تتضمن أيضاً حقائق مهمة أخرى، وتركنا برهانها كتمرين.

نظرية (٢٧,١) (نظرية مجموع مربعين). *ليكن m عدداً صحيحاً موجباً.*

(a) إذا حللنا m كما يلي:

$$m = p_1 p_2 \ldots p_r M^2$$

حيث $p_1 p_2 \dots p_r$ عوامل أولية مختلفة. عندئذ يمكن كتابة m كمجموع مربعين فقط عندما يكون كل من p_i إما 2 وإما يطابق 1 قياس 4.

(b) يمكن كتابة m كمجموع مربعين $m = a^2 + b^2$ ، حيث $\gcd(a,b)=1$ إذا وفقط إذا تحقق أحد الشرطين التاليين:

(i) m فردي وكل عدد أولي يقسم m يطابق 1 قياس 4.

(ii) m زوجي، $m/2$ فردي ، وكل عدد أولي يقسم $m/2$ يطابق 1 قياس 4.

"العودة إلى الثلاثيات الفيثاغورية"

تذكر أن[1] الثلاثي الفيثاغوري هو ثلاثي من أعداد صحيحة موجبة يحقق المعادلة :

$$a^2 + b^2 = c^2$$

ويسمى الثلاثي أولي إذا كان $\gcd(a,b) = 1$. نحن الآن في وضع يؤهلنا لعمل وصف كامل لكل الأعداد التي يمكن أن تمثل الوتر c في ثلاثيات فيثاغورس الأولية.

نظرية فيثاغورس تقول إن كل ثلاثي فيثاغوري يمكن استخراجه باختيار عددين صحيحين فرديين أوليين نسبياً $s > t \geq 1$ ووضع :

$$a = st \quad , \quad b = \frac{s^2 - t^2}{2} \quad , \quad c = \frac{s^2 + t^2}{2}$$

---

(١) في هذا السياق ، عبارة "تذكر أن ..." هي أسلوب مهذب لقول "حان الوقت الآن لإعادة قراءة الفصل الثاني ومراجعة نظرية الثلاثيات الفيثاغورية الواردة في ذلك الفصل".

لذلك نحن نبحث عن وصف لكل الأعداد c التي يمكننا معها إيجاد s , t بحيث $c=\left(s^2+t^2\right)/2$. بكلمات أخرى، c هو الوتر في ثلاثي فيثاغورس الأولي فقط عندما يكون للمعادلة :

$$2c=s^2+t^2$$

حل بعددين صحيحين فرديين أوليين نسبيًّا s و t.

لاحظ أولاً أن c يجب أن يكون فردي. (اختبرنا هذا في الفصل الثاني). إذاً نبحث عن أي الأعداد $2c$ حيث c فردي يمكن كتابتها كمجموع مربعين لعددين صحيحين أوليين نسبيًّا. إن نظرية مجموع مربعين تقول إنه يمكن عمل ذلك إذا وفقط إذا كان كل عدد أولي يقسم c يطابق 1 قياس 4 . النظرية التالية توثق ما قمنا ببرهانه.

نظرية (٢٧,٢) (نظرية وتر فيثاغورس)

العدد c يمثل الوتر في ثلاثي فيثاغورس الأولي (a,b,c) إذا وفقط إذا كان c يساوي حاصل ضرب أعداد أولية كل منها يطابق 1 قياس 4.

على سبيل المثال، العدد $c=1479$ لا يمكن أن يكون وتراً في ثلاثي فيثاغوري أولي ؛ لأن $1479=3\cdot17\cdot29$. من جهة أخرى، $c=1105$ يمكن أن يكون وتراً، لأن $1105=5\cdot13\cdot17$. إضافة إلى ذلك، يمكن حل المعادلة $s^2+t^2=2c$ لإيجاد القيمتين s , t ومن ثم استخدامهما لإيجاد القيمتين المقابلتين a , b. لذلك، من دراستنا لهذا الفصل $1105=33^2+4^2$ ، وعليه :

$$2c=2\cdot1105=\left(1^2+1^2\right)\cdot\left(33^2+4^2\right)=37^2+29^2$$

الآن $s=37$ و $t=29$ إذاً :

$$a = st = 1073 \quad \text{و} \quad b = \left(s^2 - t^2\right)/2 = 264$$

هذا يعطي ثلاثي فيثاغورس الأولي المطلوب $\left(1105\ ,\ 264\ ,\ 1073\right)$ بوتر يساوي 1105.

تمارين

(٢٧,١) لكل عدد m من الأعداد التالية، إما أن تكتب m كمجموع مربعين وإما أن تشرح لماذا لا يمكن عمل ذلك.

$(a)\ 4370 \qquad (b)\ 1885 \qquad (c)\ 1189 \qquad (d)\ 3185$

(٢٧,٢) لكل عدد c من الأعداد التالية، إما أن تجد ثلاثي فيثاغوري أوليًّا وتره c وإما أن تشرح لماذا لا يمكن عمل ذلك.

$(a)\ 4370 \qquad (b)\ 1885 \qquad (c)\ 1189 \qquad (d)\ 3185$

(٢٧,٣) أوجد زوجين كل منهما يتألف من عددين صحيحين موجبين أوليين نسبيًّا (a,c) بحيث $a^2 + 5929 = c^2$. هل يمكنك إيجاد زوج آخر بحيث $\gcd(a,c) > 1$؟

(٢٧,٤) في هذا التمرين سوف تكمل برهان الجزء الأول من نظرية مجموع مربعين.

ليكن m عدداً صحيحاً موجباً وَحُلَلْ كما يلي: $m = p_1 p_2 \dots p_r M^2$

حيث $p_1 p_2 \dots p_r$ عوامل أولية مختلفة، إذا كان بعض p_i يطابق 3 قياس 4، برهن أن m لا يمكن كتابتها على شكل مجموع مربعين.

(٢٧,٥) في هذا التمرين سوف تبرهن الجزء الثاني من نظرية مجموع مربعين. ليكن m عدداً صحيحاً موجباً.

(a) إذا كان m فرديًّا وكل عدد أولي يقسم m يطابق 1 قياس 4، برهن

أن m لا يمكن كتابته على شكل مجموع مربعين $m=a^2+b^2$ ، حيث $\gcd(a,b)=1$.

(b) إذا كان m زوجيًّا و $m/2$ فرديًّا، وإذا كان كل عدد أولي يقسم $m/2$ يطابق 1 قياس 4 ، برهن أن m يمكن كتابته على شكل مجموع مربعين حيث $\gcd(a,b)=1$.

(c) إذا أمكن كتابة m كمجموع مربعين $m=a^2+b^2$ ، حيث $\gcd(a,b)=1$ ، برهن أن m هو أحد الأعداد الموصوفة في (a) أو (b).

(٢٧,٦) لأي عدد صحيح موجب m ، ليكن $S(m)=$ (عدد طرق كتابة $m=a^2+b^2$ حيث $a\ge b\ge 0$).

على سبيل المثال :

$S(5)=1$ ، لأن $5=2^2+1^2$

$S(65)=2$ ، لأن $65=8^2+1^2=7^2+4^2$

بينما $S(15)=0$.

(a) احسب القيم التالية :

$(i)\ S(10)$ $(ii)\ S(70)$ $(iii)\ S(130)$ $(iv)\ S(1105)$

(b) إذا كان p عدداً أوليًّا و $p\equiv 1 \pmod 4$ ، ما قيمة $S(p)$ ؟ برهن أن إجابتك صحيحة.

(c) ليكن p , q عددين أوليين مختلفين، كليهما يطابق 1 قياس 4 . ما قيمة $S(pq)$ ؟ برهن أن إجابتك صحيحة.

(d) بشكل أعم ، إذا كان $p_1,\dots,p_r$ أعداداً أولية مختلفة ، جميعها تطابق 1 قياس 4 ، ما قيمة $S(p_1p_2\dots p_r)$ ؟ برهن أن إجابتك صحيحة.

(٢٧,٧) اكتب برنامجاً يحل المعادلة $x^2 + y^2 = n$ من خلال تحليل n إلى حاصل ضرب عوامله الأولية، أولاً قم بحل كل $u^2 + v^2 = p$ باستخدام الانحدار (تمرين 26.7) ومن ثم جَمعْ الحلول لإيجاد (x, y) .