الفصل السادس والعشرون

أي الأعداد الأولية تساوي مجموع مربعين؟
Which Primes are Sums of Two Squares?

على الرغم من أن بحثنا في التطابقات كان مثيراً للاهتمام ومسليًّا، فلا شك أن الأسئلة الأساسية في نظرية الأعداد هي أسئلة متعلقة بالأعداد الطبيعية. التطابق

$$A \equiv B \pmod{M}$$

يخبرك أن الفرق $A - B$ من مضاعفات M، لكنه لا تستطيع مقارنة طبيعة المساواة $A = B$.

إحدى طرق التفكير في التطابقات هي إنها تقريبات لمتساويات صحيحة. مثل هذه التقريبات ليست عديمة الأهمية. بل إن لها أهمية حقيقية، وأكثر من ذلك، فإنه غالباً ما يمكن استخدامها كأداة لإنشاء متساويات صحيحة. هذا هو المسار الذي سنسلكه في هذا الفصل، حيث إننا سنستخدم قانون التعاكس التربيعي، والذي هو نظرية تتعلق بالتطابقات، كأداة لإنشاء متساويات بين كل الأعداد.

إن سؤالنا الذي نريد الإجابة عنه هو:

أي الأعداد يمكن كتابتها كمجموع مربعين؟

فعلى سبيل المثال، 5 , 10 , 65 هي مجموع مربعين؛ لأن:

$$5=2^2+1^2 \quad , \quad 10=3^2+1^2 \quad , \quad 65=7^2+4^2$$

من جهة أخرى، الأعداد 3 , 19 , 154 لا يمكن كتابتها كمجموع مربعين. ولنبين ذلك بالنسبة للعدد 19 على سبيل المثال، فإننا نحتاج فقط لأن نعرف أن أي من الفروقات:

$$19-1^2=18 \quad , \quad 19-2^2=15 \quad , \quad 19-3^2=10 \quad , \quad 19-4^2=3$$

ليست مربعات، بشكل عام، لاختبار إذا كان عدد معطى m يساوي مجموع مربعين، فقم بكتابة قائمة الأعداد:

$$m-0^2 \ , \ m-1^2 \ , \ m-2^2 \ , \ m-3^2 \ , \ m-4^2$$

حتى تحصل على مربع أو أن تصبح الأعداد سالبة[1].

كالمعتاد، سنبدأ بجدول صغير ونبحث عن النمط.

$1=1^2+0^2$	11 *NO*	21 *NO*	31 *NO*	$41=4^2+5^2$
$2=1^2+1^2$	12 *NO*	22 *NO*	$32=4^2+4^2$	42 *NO*
3 *NO*	$13=2^2+3^2$	23 *NO*	33 *NO*	43 *NO*
$4=0^2+2^2$	14 *NO*	24 *NO*	$34=3^2+5^2$	44 *NO*
$5=1^2+2^2$	15 *NO*	$25=3^2+4^2$	35 *NO*	$45=3^2+6^2$
6 *NO*	$16=0^2+4^2$	$26=1^2+5^2$	$36=0^2+6^2$	46 *NO*
7 *NO*	$17=1^2+4^2$	27 *NO*	$37=1^2+6^2$	47 *NO*
$8=2^2+2^2$	$18=3^2+3^2$	28 *NO*	38 *NO*	48 *NO*
$9=0^2+3^2$	19 *NO*	$29=2^2+5^2$	39 *NO*	$49=0^2+7^2$
$10=1^2+3^2$	$20=2^2+4^2$	30 *NO*	$40=2^2+6^2$	$50=5^2+5^2$

---

(١) في الحقيقة، من الضروري فقط اختبار فيما إذا كان m^2-a^2 مربعاً لكل قيم a المحصورة بين 0 و $\sqrt{m/2}$. هل ترى لماذا يكفي هذا ؟

أعداد تساوي مجموع مربعين

من الجدول، سنعمل قائمة بالأعداد التي تساوي مجموع مربعين وبالأعداد التي لا تساوي مجموع مربعين.

الأعداد التي تساوي مجموع مربعين	1,2,4,5,8,9,10,13,16,17,18,20,25 26,29,32,34,36,37,40,41,45,49,50
الأعداد التي لا تساوي مجموع مربعين	3,6,7,11,12,14,15,19,21,22,23,24,27,28 30,31,33,35,38,39,42,43,44,46,47,48

هل توصلت لأي نمط؟

الملاحظة المباشرة هي أن العدد الذي يطابق 3 قياس 4 لا يمكن كتابته كمجموع مربعين. بالنظر مرة أخرى لأول عمودين من الجدول، قد نخمن أيضاً أنه إذا كان $m \equiv 1 \pmod 4$ فإن m يساوي مجموع مربعين. ولكن هذا التخمين غير صحيح؛ لأن 21 لا يساوي مجموع مربعين. أيضاً 33 هو استثناء آخر. على كل حال، كل من 21 , 33 أعداد غير أولية، $21 = 3 \cdot 7$, $33 = 3 \cdot 11$. إذا بحثنا فقط في الأعداد الأولية، سنرى أن كل عدد أولي في جدولنا يحقق:

$$p \equiv 1 \pmod 4$$

هو في الحقيقة يساوي مجموع مربعين. هذه الملاحظة تذكرنا بـ "التوجه الأولي" عند عمل البحوث النظرية على الأعداد: ابدأ دائماً البحث في الأعداد الأولية. هناك سببان لعمل ذلك. أولهما، سهولة اكتشاف الأنماط للأعداد الأولية غالباً ما يمكن استخدامها لاستنتاج أنماط لكل الأعداد، لأن النظرية الأساسية للحساب (الفصل السابع) تقول إن الأعداد الأولية هي اللبنات الأساسية لكل الأعداد.

الآن، بما أننا قررنا التركيز على الأعداد الأولية، دعنا نقوم بتوسيع قائمتنا للأعداد الأولية ونرى أي منها يمكن كتابته كمجموع مربعين.

$2=1^2+1^2$	31 NO	$73=3^2+8^2$	127 NO	179 NO
3 NO	$37=1^2+6^2$	79 NO	131 NO	$181=9^2+10^2$
$5=1^2+2^2$	$41=4^2+5^2$	83 NO	$137=4^2+9^2$	191 NO
7 NO	43 NO	$89=5^2+8^2$	139 NO	$193=7^2+12^2$
11 NO	47 NO	$97=4^2+9^2$	$149=7^2+10^2$	$197=1^2+14^2$
$13=2^2+4^2$	$53=2^2+7^2$	$101=1^2+10^2$	151 NO	199 NO
$17=1^2+4^2$	59 NO	103 NO	$157=6^2+11^2$	211 NO
19 NO	$61=5^2+6^2$	107 NO	163 NO	223 NO
23 NO	67 NO	$109=3^2+10^2$	167 NO	227 NO
$29=2^2+5^2$	71 NO	$113=7^2+8^2$	$173=2^2+13^2$	$229=2^2+15^2$

أعداد أولية تساوي مجموع مربعين

هذا يعطي القائمتين التاليتين

أعداد أولية تساوي مجموع مربعين	2,5,13,17,29,37,41,53,61,73,89,97,101, 109,113,137,149,157,173,181,193,197,229
أعداد أولية لا تساوي مجموع مربعين	3,7,11,19,23,31,43,47,59,67,71,79,83,103,107, 127,131,139,151,163,167,179,191,199,211,223,227

التخمين الصحيح واضح. الأعداد الأولية التي تطابق 1 قياس 4 تبدو أنها تساوي مجموع مربعين، والأعداد الأولية التي تطابق 3 قياس 4 تبدو أنها ليست كذلك.

(أهملنا العدد 2 ، والذي يساوي مجموع مربعين، ولكنه نوعاً ما يشكل وضعاً شاذاً). سنركز فيما بقي من هذا الفصل على مناقشة وبرهان هذا التخمين.

نظرية (١, ٢٦) (نظرية مجموع مربعين للأعداد الأولية)

ليكن p عدداً أوليًا. عندئذ فإن p يساوي مجموع مربعين إذا وفقط إذا $p \equiv 1 \pmod 4$ *أو* $(p = 2)$.

تتضمن هذه النظرية عبارتين.

العبارة 1: إذا كان p يساوي مجموع مربعين، فإن $p \equiv 1 \pmod 4$

العبارة 2: إذا كان $p \equiv 1 \pmod 4$ فإن p يساوي مجموع مربعين.

إحدى هاتين العبارتين إثباتها سهل جداً، بينما الأخرى فبرهانها صعب بما فيه الكفاية.

هل تستطيع أن تعرف أي منهما هذا وأيهما ذاك دون أن تحاول برهان أي منهما؟ هذا ليس سؤالاً للعب أو لتضييع الوقت، قبل محاولة برهان عبارة رياضية، من المفيد أن تكون لديك فكرة عن مدى صعوبة برهانها، أو كما يحب الرياضيون أن يقولوا، أن تعرف عمق العبارة. إن برهان النظرية العميقة يتطلب أدوات قوية وكثير من الجهد مقارنة مع نظرية "ضحلة"، تماماً كما يتطلب بناء ناطحة سحاب إلى آلات خاصة وكثير من الجهد، بينما بناء بيت للطيور يحتاج فقط إلى مطرقة وبعض المسامير.

إذاً سؤالي لك هو " أي العبارتين 1 و 2 أعمق ؟" . حدسياً، تكون العبارة عميقة إذا بدأت بمعطى سهل يستخدم لبرهان نتيجة صعبة. العبارتان 1 و 2 تتعاملان مع الجملتين التاليتين:

الجملة A : p يساوي مجموع مربعين.

الجملة B : $p \equiv 1 \pmod 4$

من الواضح أن B جملة سهلة ؛ لأن لأي عدد أولي معطى p ، من السهل فحص فيما إذا كانت B صحيحة أم لا. من ناحية أخرى، الجملة A أصعب ؛ لأنها قد تتطلب الكثير من العمل لمعرفة فيما إذا كان عدد أولي ما مساوياً لمجموع مربعين. لذلك، العبارة 1 تنص على أنه إذا كانت الجملة العميقة A صحيحة، فإن الجملة السهلة B تكون صحيحة. هذا يعني أن برهان العبارة 1 لن يكون صعباً. العبارة 2 تنص على أنه إذا كانت الجملة السهلة B صحيحة، فإن الجملة العميقة A تكون صحيحة. هذا يعني أن برهان العبارة 2 يبدو صعباً إلى حد ما.

الآن، بما أننا نعلم أن برهان العبارة 1 سيكون سهلاً، فدعنا نبرهنه أولاً. ليكن p مجموع مربعين :

$$p = a^2 + b^2$$

نعلم أيضاً أن p فردي، إذن a , b أحدهما فردي والآخر سيكون زوجيًّا. ولنفرض أن a فردي و b زوجي ، أي :

$$b = 2m \qquad , \qquad a = 2n + 1$$

إذاً :

$$\begin{aligned} p = a^2 + b^2 &= (2n+1)^2 + (2m)^2 \\ &= 4n^2 + 4n + 1 + 4m^2 \\ &\equiv 1 \pmod 4 \end{aligned}$$

وهذا تماماً ما نحاول برهانه.

بعد أن عرضت عليك هذا البرهان البسيط جداً للعبارة 1 ، أريد الآن أن أريك برهاناً معقداً أكثر. لماذا نرغب كثيراً في استخدام برهان معقد بدلاً من استخدام برهان

سهل؟ أحد الأجوبة الشائعة هي أن البرهان المعقد يمكن تطبيقه في أوضاع لا تعمل فيها الأفكار السهلة.

برهاننا السهل أخذ الصيغة $p = a^2 + b^2$ كمعطى، واختزلها قياس 4، واستنتج أشياء عن p قياس 4. إن هذا إجراء طبيعي جداً. بالنسبة لبرهاننا الجديد، سوف نختزل الصيغة قياس p. هذا يعطي:

$$0 = a^2 + b^2 \pmod p \text{ إذاً } -a^2 \equiv b^2 \pmod p$$

بعد ذلك سنأخذ رمز لجندر للطرفين:

$$\left(\frac{-a^2}{p}\right) = \left(\frac{b^2}{p}\right)$$

$$\left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)^2 = \left(\frac{b}{p}\right)^2$$

$$\left(\frac{-1}{p}\right) = 1$$

إذاً -1 راسب تربيعي قياس p؛ وعليه فإن قانون التعاكس التربيعي (الفصل 25) يخبرنا أن $p \equiv 1 \pmod 4$. البرهان الثاني هذا مضحك؛ لأننا اختزلنا قياس p لنحصل على معلومة قياس 4.

برهان العبارة 2، أن أي عدد أولي p يحقق $p \equiv 1 \pmod 4$ يمكن كتابته كمجموع مربعين أصعب بكثير. البرهان الذي سنعطيه الآن يعتمد على "طريقة الانحدار" (*Method of Descent*) المشهورة لفيرما. سنبدأ بوصف الفكرة الأساسية لطريقة الانحدار لفيرما، وإذا قمت باستيعاب المفهوم؛ فإن التفاصيل ستصبح أقل رهبة.

سنعتبر أن $p \equiv 1 (\mathrm{mod}\, 4)$ ونريد أن نكتب p كمجموع مربعين. بدلاً من أن نحاول مباشرة كتابة $p = a^2 + b^2$ ، دعنا نعالج مسألة كتابة أحد مضاعفات p كمجموع مربعين. على سبيل المثال، التعاكس التربيعي يخبرنا أن $x^2 \equiv -1 (\mathrm{mod}\, p)$ لها حل، وليكن $x = A$ إذاً $A^2 + 1$ من مضاعفات p. لذلك سنبدأ من معلومية أن:

$$A^2 + B^2 = Mp$$

حيث A , B , M أعداد صحيحة. إذا كان $M = 1$ ؛ يتحقق المطلوب؛ لذلك سنفرض أن $M \geq 2$.

فكرة فيرما الرائعة هي استخدام الأعداد A , B , M لإيجاد أعداد صحيحة جديدة a , b , m بحيث:

$$a^2 + b^2 = mp \quad , \quad m \leq M - 1$$

بالتأكيد، إذا كان $m = 1$ ، يتحقق المطلوب. وإذا كان $m \geq 2$ ، فإننا نستطيع تطبيق إجراء انحدار فيرما مرة أخرى مبتدئين بالأعداد a , b , m لإيجاد مضاعف أصغر للعدد p يساوي مجموع مربعين. بالاستمرار بنفس الأسلوب سنحصل حتماً على العدد p نفسه مكتوباً كمجموع مربعين.

لقد حذفنا بعض التفاصيل: كيف نستخدم بعض الأعداد المعروفة A , B , M لنحصل على أعداد جديدة a , b , m. قبل وصف هذا الجزء الحاسم من البرهان ندعوك لإلقاء نظرة على متطابقة جميلة ومفيدة.

تقول هذه المتطابقة إنه إذا ضربنا عددين كل منهما يساوي مجموع مربعين فإن الناتج أيضاً يساوي مجموع مربعين.

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

ولا يوجد صعوبة في برهان أن هذه المتطابقة صحيحة، وبرهانها وارد فيما يلي:

(اكتشافها في الموضوع الأول مسألة أخرى سنناقشها في نهاية هذا الفصل). بفك أقواس الطرف الأيمن، نحصل على ما يلي:

$$\begin{aligned}&\left(uA+vB\right)^2+\left(vA-uB\right)^2\\&=\left(u^2A^2+2uAvB+v^2B^2\right)+\left(v^2A^2-2vAuB+u^2B^2\right)\\&=u^2A^2+v^2B^2+v^2A^2+u^2B^2\\&=\left(u^2+v^2\right)\left(A^2+B^2\right)\end{aligned}$$

نحن الآن مستعدون لوصف إجراء انحدار فيرما لكتابة أي عدد أولي

$$p\equiv 1\left(\mathrm{mod}\,4\right)$$

كمجموع مربعين. كما شرحنا سابقاً، الفكرة هي أن نبدأ بأحد المضاعفات Mp التي تساوي مجموع مربعين وبقليل من الحركات الذكية، نجد مضاعفاً أصغر أيضاً يساوي مجموع مربعين. ولمساعدتك على فهم الخطوات المختلفة سنعطي هذا المثال:

$$a^2+b^2=881$$

ونوضحه جنباً إلى جنب مع الإجراء العام. إجراء الانحدار، بكل عظمته، موضح في الجدول صفحة 192. تأكد من فهمك للإجراء خطوة خطوة قبل أن تبدأ في قراءة ما بعده.

إجراء الانحدار الموصوف في صفحة سابقة اختزل المعادلة الابتدائية:

$$387^2+1^2=170\cdot 881$$

إلى المضاعف الأصغر

$$107^2 + 2^2 = 13 \cdot 881$$

للعدد 881. ولنكمل ذلك بكتابة 881 كمجموع مربعين، سنعيد

إجراء الانحدار

$p = 881$	p any prime $\equiv 1 \pmod 4$
اكتب $387^2 + 1^2 = 170 \cdot 881$ و $170 < 881$	**اكتب** $A^2 + B^2 = Mp$ و $M < p$
اختر أعداد بحيث $47 \equiv 387 \pmod{170}$ $1 \equiv 1 \pmod{170}$ $-\frac{170}{2} \le 47,1 \le \frac{170}{2}$	**اختر عددين u و v بحيث** $u \equiv A \pmod M$ $v \equiv B \pmod M$ $-\frac{1}{2}M \le u,v \le \frac{1}{2}M$
لاحظ أن $47^2 + 1^2 \equiv 387^2 + 1^2$ $\equiv 0 \pmod{170}$	**لاحظ أن** $u^2 + v^2 \equiv A^2 + B^2$ $\equiv 0 \pmod M$
لذلك يمكننا أن نكتب $47^2 + 1^2 = 170 \cdot 13$ $387^2 + 1^2 = 170 \cdot 881$	**لذلك يمكننا أن نكتب** $u^2 + v^2 = Mr$ $A^2 + B^2 = Mp$ $1 \le r < M$

اضرب لتحصل على $\left(u^2+v^2\right)\left(A^2+B^2\right)=M^2\cdot p$	اضرب لتحصل على $\left(47^2+1^2\right)\left(387^2+1^2\right)$ $=170^2\cdot 13\cdot 881$
استخدم المتطابقة $\left(u^2+v^2\right)\left(A^2+B^2\right)=\left(uA+vB\right)^2+\left(vA-uB\right)^2$	
$\underbrace{\left(uA+vB\right)^2}+\underbrace{\left(vA-uB\right)^2}=M^2\cdot p$ كلاهما يقبل القسمة على M	$\left(47\cdot 387+1\cdot 1\right)^2+\left(1\cdot 387-47\cdot 1\right)^2$ $=170^2\cdot 13\cdot 881$ $\underbrace{18190^2}+\underbrace{340^2}=170^2\cdot 13\cdot 881$ كلاهما يقبل القسمة على 170
اقسم على m^2 $\left(\frac{uA+vB}{M}\right)^2+\left(\frac{vA-uB}{M}\right)^2=p$ هذا يعطي مضاعفاً أصغر لـ p مكتوباً على شكل مجموع مربعين	اقسم على 170^2 $\left(\frac{18190}{170}\right)^2+\left(\frac{340}{170}\right)^2=13\cdot 881$ $107^2+2^2=13\cdot 881$ هذا يعطي مضاعفاً أصغر للعدد 881 مكتوباً على شكل مجموع مربعين.

أعد الإجراء حتى تكتب p نفسها كمجموع مربعين

باجراء الانحدار مبتدئين بالمعادلة $107^2+2^2=13\cdot 881$. هذا يعطي

$p=881$	p any prime $\equiv 1 \pmod 4$
$107^2+2^2=13\cdot 881$ $3\equiv 107 \pmod{13}$ $2\equiv 2 \pmod{13}$	$A^2+B^2=Mp$ $u\equiv A \pmod M$ $v\equiv B \pmod M$
$3^2+2^2=13\cdot 1$	$u^2+v^2=Mr$
$\left(3^2+2^2\right)\left(107^2+2^2\right)=13^2\cdot 1\cdot 881$	$\left(u^2+v^2\right)+\left(A^2+B^2\right)=M^2rp$
استخدم المتطابقة $\left(u^2+v^2\right)\left(A^2+B^2\right)=(uA+vB)^2+(vA-uB)^2$	
$(3\cdot 107+2\cdot 2)^2+(2\cdot 107-3\cdot 2)^2$ $=13^2\cdot 881$ $325^2+208^2=13^2\cdot 881$	$(uA+vB)^2+(vA-uB)^2=M^2rp$
اقسم على 13^2 $25^2+16^2=881$	اقسم على M^2 $\left(\frac{uA+vB}{M}\right)^2+\left(\frac{vA-uB}{M}\right)^2=rp$

هذا التطبيق الثاني لإجراء الانحدار أعطانا الحل لمسألتنا الأصلية :

$$881=25^2+16^2$$

بالطبع ، لعدد صغير مثل 881 قد يكون من السهل حل $881=a^2+b^2$ بالمحاولة والخطأ ، لكن عندما يكون p عدداً كبيراً ، فإن إجراء الانحدار يكون فعّالاً لدرجة كبيرة. في الحقيقة ، كلما يطبق إجراء الانحدار ، مضاعف العدد p يقسم إلى النصف على الأقل.

لنبين أن إجراء الانحدار فعلاً يعمل، فإننا نحتاج لبرهان خمس جمل. في الخطوة الأولى نحتاج لإيجاد عددين A , B ، بحيث:

$$A^2 + B^2 = Mp \quad , \quad M < p \qquad \text{(i)}$$

ولعمل ذلك، سنأخذ حلاً للتطابق:

$$x^2 \equiv -1 \pmod{p}$$

حيث $1 \le x < p$. التعاكس التربيعي يخبرنا عن وجود حل[1] ؛ لأننا افترضنا أن $p \equiv 1 \pmod{4}$ ؛ وعليه $A = x$ و $B = 1$ لهما الخاصية $A^2 + B^2$ تقبل القسمة على p. كذلك:

$$M = \frac{A^2 + B^2}{p} \le \frac{(p-1)^2 + 1^2}{p} = p - \frac{2p-2}{p} < p$$

في الخطوة الثانية لإجراء الانحدار قمنا باختيار عددين u , v يحققان:

$$u \equiv A \pmod{M} \quad , \quad v \equiv B \pmod{M}$$

و

$$-\frac{1}{2}M \le u \, , \, v \le \frac{1}{2}M$$

ولاحظنا أن:

---

(١) من الطرق السهلة لحل $x^2 \equiv -1 \pmod{p}$ هي حساب $b \equiv a^{(p-1)/4} \pmod{p}$ لبعض القيم المختارة بشكل عشوائي للعدد a. صيغة أويلر (الفصل الرابع والعشرون) تقول إن $b^2 \equiv \left(\frac{a}{b}\right) \pmod{p}$ ، لذلك أي اختيار لقيمة a يعطينا احتمالية 50% للنجاح.

$$u^2+v^2 \equiv A^2+B^2 \equiv 0 \pmod{M}$$

لـذلك u^2+v^2 تقبـل القسـمة علـى M ، ولـيكن $u^2+v^2=Mr$.

العبارات الأربع المتبقية التي نحتاج لفحصها هي :

(ii) $r \geq 1$

(iii) $r < M$

(iv) $uA+vB$ تقبل القسمة على M .

(v) $vA-uB$ تقبل القسمة على M .

سنبدأ بفحصها بترتيب مقلوب. لنتحقق من (v) نحسب :

$$vA-uB \equiv B \cdot A - A \cdot B \equiv 0 \pmod{M}$$

نفس الشيء ، بالنسبة للعبارة (iv) فإن :

$$uA+vB \equiv A \cdot A + B \cdot B \equiv Mp \equiv 0 \pmod{M}$$

بالنسبة للعبارة (iii) نستخدم حقيقة أن u , v هما بين $M/2$ و $-M/2$ لنقدر أن :

$$r = \frac{u^2+v^2}{M} \leq \frac{(M/2)^2+(M/2)^2}{M} = \frac{M}{2} < M$$

لاحظ أن هذا يبين بالفعل أن $r \leq M/2$ ؛ لذلك في كل مرة نطبق فيها إجراء الانحدار فإن مضاعف p يقسم من النصف على الأقل.

أخيراً، لنبين أن العبارة (ii) صحيحة، نحتاج أن نختبر فيما إذا كان $r \neq 0$. لذلك لنفرض أن $r=0$ ونرى ماذا يحدث. حسناً، إذا كان $r=0$ فإن $u^2+v^2=0$ ؛ إذاً $u=v=0$. لكن $u \equiv A \pmod{M}$

و $v \equiv B \pmod{M}$ ؛ لذلك فإن A و B يقبلان القسمة على M. لكن $A^2 + B^2 = Mp$ ؛ إذاً العدد الأولي p يقبل القسمة على M. كذلك فإننا نعلم أن $M < p$ ؛ إذاً $M = 1$. هذا يعني أن $A^2 + B^2 = p$ ونحن تلقائياً كتبنا p كمجموع مربعين! لذلك إما (ii) صحيحة وإما أن لدينا $A^2 + B^2 = p$ ولا يوجد سبب لاستخدام إجراء الإنحدار في المكان الأول.

إن هذا يكمل برهان أن إجراء الانحدار دائماً قابل للتطبيق، بذلك نكون الآن قد أنهينا برهان كلا الجزأين لنظرية مجموع مربعين للأعداد الأولية.

استطراد في مجموع المربعات والأعداد المركبة

رأينا مدى فائدة المتطابقة:

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

والتي تعطي ناتج ضرب عددين كل منهما يساوي مجموع مربعين كمجموع مربعين، وسنرى استخدامات أخرى لها في الفصل اللاحق. وربما تسأل عن مصدر هذه المتطابقة.

الجواب يكمن في عالم الأعداد المركبة، وهي الأعداد التي على الشكل $z = x + iy$ ، حيث i هو الجذر التربيعي للعدد -1. يمكن ضرب عددين مركبين بالطريقة العادية طالما أنك تتذكر أن تستبدل i^2 بالعدد -1. لذلك

$$\begin{aligned}\left(x_1 + iy_1\right)\left(x_2 + iy_2\right) &= x_1x_2 + ix_1y_2 + iy_1x_2 + i^2y_1y_2 \\ &= \left(x_1x_2 - y_1y_2\right) + i\left(x_1y_2 + y_1x_2\right)\end{aligned}$$

الأعداد المركبة أيضاً لها قيمة مطلقة،

$$|z| = |x + iy| = \sqrt{x^2 + y^2}$$

هذه الفكرة توحي بتصور العدد $z = x + iy$ كنقطة (x, y) في المستوى، ومن ثم تكون القيمة $|z|$ ما هي إلا المسافة من z إلى نقطة الأصل $(0,0)$. الآن تكون متطابقتنا قد أتت من الحقيقة التالية:

"القيمة المطلقة للضرب تساوي ضرب القيم المطلقة".

بمعنى، $|z_1 z_2| = |z_1| \cdot |z_2|$. وبكتابة هذه المعادلة بدلالة x , y ينتج:

$$\left|(x_1 + iy_1)(x_2 + iy_2)\right| = |x_1 + iy_1| \cdot |x_2 + iy_2|$$

$$\left|(x_1 x_2 - y_1 y_2) + i(x_1 y_2 - y_1 x_2)\right| = |x_1 + iy_1| \cdot |x_2 + iy_2|$$

$$\sqrt{(x_1 x_2 - y_1 y_2)^2 + (x_1 y_2 + y_1 x_2)^2} = \sqrt{x_1^2 + y_1^2}\sqrt{x_2^2 + y_2^2}$$

وبتربيع طرفي هذه المعادلة الأخيرة، سنحصل بالضبط على متطابقتنا

(حيث $x_1 = u$, $y_1 = v$, $x_2 = A$, $y_2 = -B$).

هناك متطابقة مماثلة تتضمن مجموع أربعة مربعات، وضعها أويلر:

$$\begin{aligned}&(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2)\\ &= (aA + bB + cC + dD)^2 + (aB - bA - cD + dC)^2\\ &\quad + (aC + bD - cA - dB)^2 + (aD - bC + cB - dA)^2\end{aligned}$$

هذه المتطابقة المعقدة ترتبط بنظرية الرباعيات[1] بنفس الطريقة التي ترتبط فيها متطابقتنا بالأعداد المركبة. ومن سوء الحظ عدم وجود متطابقة مناظرة لمجموع ثلاثة

---

(١) الرباعيات هي أعداد على الشكل $a + ib + jc + kd$ ، حيث i , j و k ثلاثة جذور تربيعية، مختلفة للعدد -1 تحقق قوانين ضرب غريبة مثل $j = k = -ji$.

مربعات، وفي الحقيقة فإن مسألة كتابة أعداد كمجموع ثلاثة مربعات أصعب بكثير من مسألة كتابتها كمجموع مربعين أو أربعة مربعات.

تمارين

(٢٦,١) (a) اعمل قائمة بكل الأعداد الأولية $p<50$ التي يمكن كتابتها على الشكل $p=a^2+ab+b^2$. مثلاً، $p=7$ لها هذا الشكل عندما $a=2$ و $b=1$، بينما $p=11$ لا يمكن كتابته بهذا الشكل. حاول أن تجد نمطاً وتعمل تخميناً عن ماهية الأعداد الأولية التي يمكن كتابتها على هذا الشكل. (هل يمكنك إثبات أن جزءاً واحداً على الأقل من تخمينك يكون صحيحاً؟).

(b) نفس السؤال بالنسبة للأعداد الأولية التي يمكن كتابتها على الشكل[1] $p=a^2+2b^2$.

(٢٦,٢) إذا أمكن كتابة العدد الأولي p على الشكل $p=a^2+5b^2$، بيّن أن $p\equiv 1 \text{ or } 9 \pmod{20}$ (طبعاً تجاهلنا $5=0^2+5\cdot 1^2$).

(٢٦,٣) استخدم إجراء الانحدار مرتين، مبتدءاً من المعادلة:

$$557^2+55^2=26\cdot 12049$$

لكتابة العدد الأولي 12049 كمجموع مربعين.

(٢٦,٤) (a) ابدأ من المعادلة $259^2+1^2=34\cdot 1973$، واستخدم إجراء الانحدار لكتابة العدد الأولي 1973 كمجموع مربعين.

---

(١) السؤال عن أي الأعداد الأولية يمكن كتابتها على الشكل $p=a^2+nb^2$ تدرس على نطاق واسع في كثير من فروع الرياضيات. حتى أنه يوجد أحد الموضوعات في كتاب ديفيد كوكس تحت عنوان أعداد أولية على الشكل x^2+ny^2.

(b) إبدأ من المعادلة :

$$261^2 + 947^2 = 10 \cdot 96493$$

واستخدم إجراء الانحدار لكتابة العدد الأولي 96493 كمجموع مربعين.

(٢٦.٥) (a) أي الأعداد الأولية $p < 100$ يمكن كتابتها كمجموع ثلاثة مربعات، $p = a^2 + b^2 + c^2$ ، (نسمح لواحد من المجاهيل a,b,c أن يساوي 0 ، لذلك، على سبيل المثال، $5 = 2^2 + 1^2 + 0^2$ يساوي مجموع ثلاثة مربعات).

(b) معتمداً على البيانات التي جمعتها من (a)، حاول عمل تخمين يصف أي الأعداد الأولية يمكن كتابتها كمجموع ثلاثة مربعات. يجب أن يحتوي تخمينك على العبارتين التاليتين، واملأ الفراغ :

(i) إذا حقق p الخاصية .....، فإن p يساوي مجموع ثلاثة مربعات.

(ii) إذا حقق p الخاصية..... ، فإن p لا يساوي مجموع ثلاثة مربعات.

(c) برهن تخمينك في الجزء (ii) من فقرة (b) [قد تحاول أيضاً برهان الجزء (i) ، ولكن كنّ حذراً، فهو صعب بما فيه الكفاية].

(٢٦.٦) اكتب برنامجاً يحل المعادلة $x^2 + y^2 = n$ من خلال المحاولة بالقيم $x = 0,1,2,3,\ldots$ واختبر فيما إذا كان $n - x^2$ مربعاً كاملاً. برنامجك يجب أن يعطي كل الحلول بحيث $x \le y$ إذا وجدت، ويجب أن يعطي رسالة مناسبة إذا لم توجد حلول.

(٢٦.٧) (a) اكتب برنامجاً يحل المعادلة $x^2 + y^2 = p$ للأعداد الأولية $p \equiv 1 \pmod 4$ باستخدام إجراء الانحدار لفيرما. المدخل يجب أن يحوي

الأعداد الأولية p وزوج الأعداد (A,B) الذي يحقق:

$$A^2 + B^2 = 0 \pmod{p}$$

(b) في الحالة $p \equiv 5 \pmod{8}$ ، عَدّلْ برنامجك بحيث لا يحتاج المستخدم إلى إدخال (A,B).

أولاً، استخدم التربيع المتعاقب لحساب العدد $A \equiv -2 \cdot (-4)^{(p-5)/8} \cdot \pmod{p}$. ثم $A^2 + 1 \equiv 0 \pmod{p}$ (انظر تمرين 25.7)، لذلك يمكن أن تستخدم $(A,1)$ كقيمة ابتدائية لإنجاز الانحدار.