المنحنيات التكعيبية والمنحنيات الناقصية

Cubic Curves and Elliptic Curves

لقد درسنا حتى الآن حلولاً لأنواع مختلفة من معادلات كثيرات الحدود، منها:

$X^2 + Y^2 = Z^2$ معادلة الثلاثيات الفيثاغورية (الفصلان الثاني والثالث).

$x^4 + y^4 = z^4$ معادلة فيرما من الدرجة الرابعة (الفصل الثامن والعشرون).

$x^2 - Dy^2 = 1$ معادلة بِلْ (الفصول: الثلاثون واثنين وثلاثون والأربعون).

إن هذه جميعها أمثلة على ما يعرف بـ "المعادلات الديوفانتينيه" (Diophantine Equations). المعادلة الديوفانتينيه هي معادلة كثيرة حدود في متغير واحد أو عدة متغيرات، والتي نبحث في إيجاد حلول لها في الأعداد الصحيحة أو الأعداد النسبية. فعلى سبيل المثال، في الفصل الثاني بَيَّنا أن كل حل (أولي نسبيًّا) في الأعداد الصحيحة لمعادلة الثلاثيات الفيثاغورية تعطى بالصيغة

$$X = st, \qquad Y = \frac{s^2 - t^2}{2}, \qquad Z = \frac{s^2 + t^2}{2}$$

ولقد توصلنا إلى نتيجة مختلفة جدًّا في الفصل الثامن والعشرون عن معادلة فيرما من الدرجة 4. حيث بَيَّنا أنه لا يوجد لها حلول في الأعداد الصحيحة عندما $xyz \neq 0$. من جهة أخرى، رأينا أن معادلة بِلْ لها عدد لا نهائي من الحلول في الأعداد الصحيحة، وبَيَّنا في الفصل الثاني والثلاثون أن كل حل يمكن الحصول عليه بأخذ حل أساسي واحد ورفعه إلى قوى.

في الفصول القليلة القادمة سنناقش نوعاً جديداً من المعادلات الديوفانتينيه، إحداها يُعطى بكثير حدود من الدرجة رقم (3). وسنهتم بشكل خاص في الحلول العددية النسبية، لكننا سنناقش أيضاً الحلول في مجموعة الأعداد الصحيحة والحلول "قياس p " (modulo p). المعادلات الديوفانتينيه من الدرجة 2 مفهومة بشكل ممتاز من الرياضيين المعاصرين، لكن معادلات الدرجة 3 صعبة بما فيه الكفاية لتكون موضع بحث في هذا الكتاب. مما يثير الدهشة أيضاً أن "أندرو ويلز" (Andrew Wiles) استخدم معادلات من الدرجة 3 لإثبات أن معادلة فيرما $x^n + y^n = z^n$ ليس لها حلول صحيحة عندما $xyz \neq 0$ لكل $n \geq 3$.

معادلات الدرجة 3 التي سوف ندرسها تسمى " منحنيات ناقصية "[١] (*elliptic curves*). المنحنيات الناقصية هي معادلات على الشكل :

$$y^2 = x^3 + ax^2 + bx + c$$

الأعداد a , b , c هي أعداد ثابتة ونبحث عن زوج من الأعداد (x, y) لحل المعادلة.

---

(١) على خلاف التصور العام، فالمنحنى الناقصي ليس قطع ناقص. فربما تتذكر أن شكل القطع الناقص يشبه دائرة منبعجة. وهذا ليس شكل المنحنيات الناقصية إطلاقاً كما يتضح ذلك في الشكل رقم 43.1. أول ظهور للمنحنيات الناقصية كان عندما حاول الرياضيون حساب محيط قطع ناقص.

هنا ثلاثة منحنيات ناقصية بسيطة :

$$E_1 : y^2 = x^3 + 17$$
$$E_2 : y^2 = x^3 + x$$
$$E_3 : y^2 = x^3 - 4x^2 + 16$$

التمثيل البياني للمنحنيات E_3 , E_2 , E_1 موضح في الشكل رقم 43.1. سوف نعود إلى هذه الأمثلة الثلاثة في كثير من الأحيان في الفصول القادمة لتوضيح النظرية العامة.

كما أشرنا سابقاً، سوف ندرس الحلول في الأعداد النسبية، وفي الأعداد الصحيحة ، وكذلك قياس p . كل معادلة في أمثلتنا الثلاثة لها حلول صحيحة ، فمثلاً

E_1 لها الحلول $(-2,3)$, $(-1,4)$, $(2,5)$.

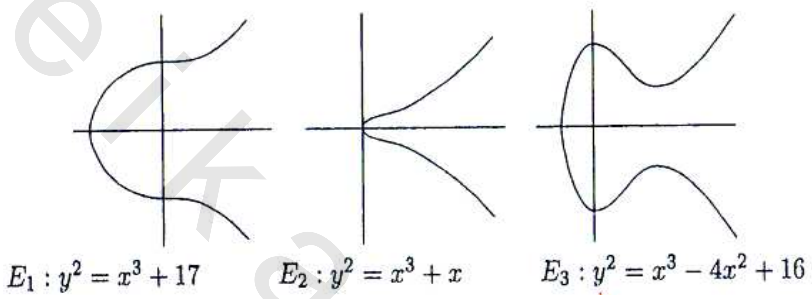
E_2 لها الحل $(0,0)$.

E_3 لها الحلان $(0,4)$, $(4,4)$.

لقد أوجدنا هذه الحلول بالمحاولة والخطأ. بكلمات أخرى نختار قيم صغيرة لـ x ونرى فيما إذا كان المقدار $x^3 + ax^2 + bx + c$ مربعاً كاملاً. بنفس هذه الطريقة ، اخترنا قيم نسبية صغيرة للمتغير x ، واكتشفنا الحل النسبي $(1/4 , 33/8)$ للمعادلة E_1 . كيف يمكن أن نجد حلولاً أكثر؟

إن الموضوع الرئيسي لهذا الفصل هو التفاعل بين الهندسة و نظرية الأعداد. ولقد رأينا هذه الفكرة خلال عملنا في الفصل الثالث ، حيث قمنا باستخدام هندسة الخطوط والدوائر لإيجاد الثلاثيات الفيثاغورية. باختصار ، قمنا في الفصل الثالث بأخذ خط يمر بالنقطة $(-1,0)$ الواقعة على دائرة الوحدة وبحثنا عن النقطة الأخرى التي يتقاطع فيها الخط مع الدائرة. فبأخذ خطوط ميلها عدد نسبي وجدنا أن إحداثيات نقطة

التقاطع الثانية هي أعداد نسبية. بهذه الطريقة نكون قد استخدمنا خطوط تمر بنقطة واحدة $(-1,0)$ لإيجاد العديد من النقاط الجديدة التي إحداثياتها أعداد نسبية. إننا نريد استخدام نفس الطريقة لإيجاد العديد من النقاط الواقعة على منحنيات ناقصية وإحداثياتها أعداد نسبية.



الشكل رقم (١,٤٣). التمثيل البياني لثلاثة منحنيات ناقصية.

دعنا نحاول استخدام نفس الفكرة على المنحنى الناقصي

$$E_1 :\ y^2 = x^3 + 17$$

نرسم خطوطاً تمر بالنقطة $P = (-2,3)$ ولنرى ما هي النقاط الأخرى التي نحصل عليها. على سبيل المثال، لنفرض أننا نحاول بالخط الذي ميله 1 ،

$$y - 3 = x + 2$$

لإيجاد نقاط تقاطع هذا الخط مع E_1 ، نعوض $y = x + 5$ في معادلة E_1 ونحل المعادلة في x . لذلك :

$$(x+5)^2 = x^3 + 17$$
$$x^3 - x^2 - 10x - 8 = 0$$

ربما لا تعرف كيف توجد جذور كثير حدود تكعيبي[١] ، لكننا نعلم أحد هذه الحلول. المنحنى الناقصي E_1 والخط كلاهما يمر بالنقطة $P = \left(-2,3\right)$ ، إذن $x = -2$ جذر. إن هذا يمكننا من تحليل كثير الحدود التكعيبي على الشكل

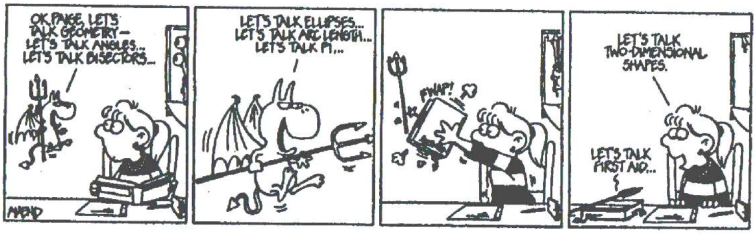
$$x^3 - x^2 - 10x - 8 = \left(x+2\right)\left(x^2 - 3x - 4\right)$$

الآن نستطيع إيجاد الصيغة التربيعية لإيجاد الجذرين $x = -1$, $x = 4$ للمقدار $x^2 - 3x - 4$. بتعويض هذه القيم في المعادلة $y = x + 5$ نحصل على ألإحداثي y لنقاطنا الجديدة $\left(-1,4\right), \left(4,9\right)$. يجب أن نتأكد من أن هذه النقاط تحقق المعادلة $y^2 = x^3 + 17$.

(١) في الواقع هناك صيغة تكعيبية ، على الرغم من أنها تعتبر أكثر تعقيداً من ابنة عمها الصيغة التربيعية. الخطوة الأولى في إيجاد جذور المعادلة $x^3 + Ax^2 + Bx + C = 0$ هي عمل التعويض $x = t - A/3$. بعد بعض العمل نحصل على معادلة في t على الشكل $t^3 + pt + q = 0$. جذر هذه المعادلة يُعطى من خلال صيغة "كاردانو" (Cardano) :

$$t = \sqrt[3]{-q/2 + \sqrt{q^2/4 + p^3/27}} + \sqrt[3]{-q/2 - \sqrt{q^2/4 + p^3/27}}$$

إن هناك صيغة تربيعية أكثر تعقيداً لإيجاد جذور كثير الحدود من الدرجة الرابعة ، ولكن هناك تنتهي القصة. في بدايات العام 1800 برهن Niels Abel و Evarisbe Galois أنه لا يوجد صيغ شبيهة تُعطي جذور كثيرات الحدود من الدرجة 5 فأكثر. إن هذه النتيجة تُعد إحدى أعظم انتصارات الرياضيات الحديثة ، والأدوات التي طُوِّرت لإثباتها ما يزال لها أهمية استثنائية في الجبر و نظرية الأعداد.



إن هذا يبدو جيداً، ولكن قبل أن نفرط في الثقة، يجب أن نحاول مع مثال آخر (على الأقل). افرض أننا أخذنا الخط المار بالنقطة $P = \left(-2, 3\right)$ وميله يساوي 3. إن معادلة هذا الخط هي :

$$y - 3 = 3(x + 2)$$

والتي تصبح بعد إعادة ترتيبها على الشكل :

$$y = 3x + 9$$

نعوض $y = 3x + 9$ في معادلة E_1 :

$$\begin{aligned}
&\left(3x + 9\right)^2 = x^3 + 17 \\
&x^3 - 9x^2 - 54x - 64 = 0 \\
&\left(x + 2\right)\left(x^2 - 11x - 32\right) = 0
\end{aligned}$$

كما فعلنا سابقاً يمكننا استخدام الصيغة التربيعية لإيجاد جذور $x^2 - 11x - 32$ ، لكن لسوء الحظ سنحصل على القيمتين :

$$x = \frac{11 \pm \sqrt{249}}{2}$$

وهذه ليست الإجابة التي نأملها، لأننا نبحث عن النقاط الواقعة على E_1 التي إحداثياتها أعداد نسبية.

ما الذي سبب المشكلة؟ افرض أننا رسمنا الخط L الذي ميله m المار بالنقطة $P = \left(-2,3\right)$ ونريد إيجاد نقاط تقاطعه مع E_1. إن معادلة الخط L هي

$$L : y - 3 = m\left(x + 2\right)$$

لإيجاد نقاط تقاطع L مع E_1، نعوض $y = m\left(x + 2\right) + 3$ في معادلة E_1 ونحل في x. عند عمل ذلك نحصل على:

$$\begin{aligned} &\left(m\left(x+2\right)+3\right)^2 = x^3 + 17 \\ &x^3 - m^2x^2 - \left(4m^2 + 6m\right)x - \left(4m^2 + 12m - 8\right) = 0 \end{aligned}$$

طبعاً نعلم أن أحد الجذور هو $x = -2$، إذن:

$$\left(x+2\right)\left(x^2 - \left(m^2 + 2\right)x - \left(2m^2 + 6m - 4\right)\right) = 0$$

لسوء الحظ، الجذران الآخران لا يبدو أنهما عددان نسبيان.

إن فكرة استخدام خطوط تمر بنقاط معلومة لإيجاد نقاط جديدة يبدو أنها وصلت إلى طريق مسدود. كما هي الحال غالباً في الرياضيات (وفي الحياة؟)، فإن التراجع وأخذ نظرة أوسع قد يكشف عن وسيلة للحل. في الحالة هذه، مسألتنا هي أن لدينا كثير حدود تكعيبي، ونعلم أن أحد جذوره عدد نسبي، لكن الجذرين الآخرين هما حلان لكثير حدود تربيعي، وقد لا يكونان عددين نسبيين. كيف نُجْبر كثير الحدود التربيعي ليكون جذراه عددين نسبيين؟ بالعودة إلى عملنا في الفصل الثالث، نرى أنه إذا كان أحد جذري كثير الحدود التربيعي عدداً نسبيًّا فإن الجذر الآخر هو عدد نسبي أيضاً. بكلمات أخرى، نحن نريد إجبار كثير الحدود التكعيبي الأصلي على أن يكون له

جذران نسبيان ، ومن ثم فإن الثالث سيكون نسبيًّا أيضاً. إن هذا يُدخلنا في صُلْب المسألة. كثير الحدود التكعيبي الأصلي له جذر نسبي لأننا اخترنا خطاً يمر بالنقطة $(-2,3)$ ، أي أن $x=-2$ جذر. ولكي نُجبر كثير الحدود التكعيبي ليكون له جذران نسبيان ، فيجب علينا أن نختار خطاً يمر بنقطتين نسبيتين (أي الإحداثيات أعداد نسبية) تقعان على المنحنى الناقصي E_1 .

لنطرح مثالاً لتوضيح هذه الفكرة ، سنبدأ مع النقطتين $P=(-2,3)$, $Q=(2,5)$ الواقعتين على المنحنى الناقصي :

$$E_1 : y^2 = x^3 + 17$$

ميل الخط الواصل بين النقطتين Q,P يساوي $(5-3)/(2-(-2)) = 1/2$ ، إذن معادلته هي :

$$y = \frac{1}{2}x + 4$$

بتعويض هذه المعادلة في معادلة E_1 نحصل على :

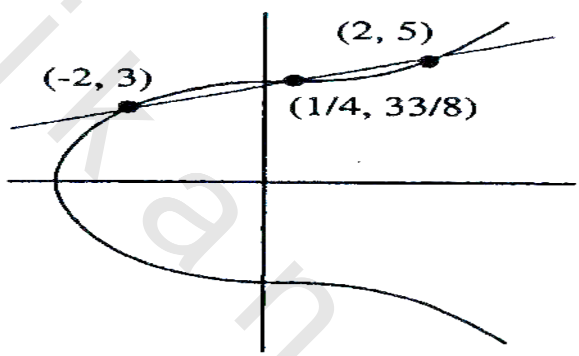
$$\left(\frac{1}{2}x+4\right)^2 = x^3+17$$

$$x^3 - \frac{1}{4}x^2 - 4x + 1 = 0$$

وهذا يقتضي أن $x=-2$, $x=2$ جذران ، إذن :

$$(x-2)(x+2)\left(x-\frac{1}{4}\right) = 0$$

لاحظ أن الجذر الثالث $x = \dfrac{1}{4}$ هو عدد نسبي، وبتعويض هذه القيمة في معادلة الخط نحصل على إحداثي y المناظر $y = 33/8$. باختصار، بأخذ الخط المار بالحلين المعلومين $(-2,3)$, $(2,5)$، أوجدنا الحل النسبي $(1/4, 33/8)$ لمنحنانا الناقصي. هذا الإجراء موضح بالشكل رقم 43.2.



الشكل رقم (٤٣,٢). استخدام نقطتين معلومتين لإيجاد نقطة جديدة.

افرض أننا نحاول إعادة هذا الإجراء مع الحل الجديد $(1/4, 33/8)$. إذا رسمنا الخط المار بالنقطتين $(-2,3)$, $(1/4, 33/8)$، ولنقل أننا نعلم أن نقطة التقاطع الثالثة مع E_1 هي النقطة $(2,5)$. إذن انتهينا بالعودة إلى حيث بدأنا. مرة أخرى، يبدو أننا وصلنا إلى طريق مسدود، لكن ملاحظة بسيطة تحركنا مرة أخرى. هذه الملاحظة البسيطة هي أنه إذا كان (x, y) نقطة على المنحنى الناقصي E_1 فإن النقطة $(x, -y)$ أيضاً نقطة على المنحنى E_1. وهذا واضح لأن منحنى E_1 متناظر حول المحور x (انظر الشكل 43.2). إذن ما علينا فِعله هو استبدال النقطة الجديدة $(1/4, 33/8)$ بالنقطة $(1/4, -33/8)$، ومن ثم نعيد الإجراء السابق باستخدام الخط المار بالنقطتين

$\left(1/4,-33/8\right)$, $\left(-2,3\right)$ ، إن هـذا الخـط ميلـه يسـاوي $-19/6$ ومعادلتـه هـي $y=-19x/6-10/3$. بالتعويض في معادلة E_1 ، سننتهي بإيجاد جذور المقدار :

$$x^3-\frac{361}{36}x^2-\frac{190}{9}x+\frac{53}{9}$$

جذران من الجذور الثلاثة لهذا المقـدار همـا $1/4$, -2 ، إذن يمكننـا قسمة كثير الحدود التكعيبي هذا على $\left(x-1/4\right)\left(x+2\right)$ لإيجاد الجذر الثالث :

$$x^3-\frac{361}{36}x^2-\frac{190}{9}x+\frac{53}{9}=\left(x-\frac{1}{4}\right)\left(x+2\right)\left(x-\frac{106}{9}\right)$$

إذن الجذر الثالث هـو $x=106/9$ ، وبتعـويض قيمـة x هـذه في معادلـة الخط نحصـل علـى $y=-1097/27$. بـذلك نكـون قـد أوجـدنا نقطـة جديـدة $\left(106/9,-1097/27\right)$ تحقق المعادلة :

$$E_1:\ y^2=x^3+17$$

بالاستمرار بهذا الأسلوب ، نجد الكثير والكثير من النقـاط. في الواقـع ، كمـا حدث مع معادلة بِلْ ، فسوف نحصل على عدد لا نهائي مـن النقـاط إحـداثياتها نسـبية. بالنسبة لمعادلة بِـلْ ، فقـد بَيَّنـا أن جميـع الحلـول يمكـن اسـتخدامها بأخـذ قـوى لأصـغر حل. هذا يُبيِّن أن كل نقطـة علـى E_1 إحـداثياتها نسـبية يمكـن إيجادهـا مـن خـلال البـدء بالنقطتين Q,P ، نصل هاتين النقطتين بخط لإيجاد نقطة جديـدة ، نعمـل انعكاسـاً في المحور x ، نرسم خطوطاً أكثر تمر بنقاط معلومـة لإيجـاد نقـاط جديـدة ، نعمـل انعكاسـاً مرة أخرى ، ونعيد الإجراء مرة بعد مـرة. الجـدير بالملاحظـة هنـا هـو أن كـل نقطـة علـى E_1 إحداثياتها نسبية يمكن الحصول عليها من خلال البدء بنقطتين فقط وبتكـرار إجـراء

هندسي بسيط ، تماماً كما أن كل حل لمعادلة پِلْ حصلنا عليه من خلال البدء بحل أساسي واحد ومن ثم نكرر تطبيق قاعدة بسيطة. إن حقيقة أن الحلول النسبية اللانهائية للمعادلة E_1 يُمكن إيجادها من مجموعة مُولِدَة منتهية هي حالة خاصة من نظرية مشهورة.

نظرية رقم (٤٣,١) (نظرية موردل (Mordell)) (L. J. Mordell, 1922)

ليكن E منحنى ناقصًّا مُعطى بالمعادلة :

$$E : y^2 = x^3 + ax^2 + bx + c$$

حيث a, b, c أعداد صحيحة بحيث أن المميّز :

$$\Delta\left(E\right) = -4a^3c + a^2b^2 - 4b^3 - 27c^2 + 18abc$$

لا يساوي صفراً[1]. عندئذ يوجد قائمة منتهية من الحلول ،

$$P_1 = \left(x_1, y_1\right),\ P_2 = \left(x_2, y_2\right), \ldots, P_r = \left(x_r, y_r\right)$$

إحداثياتها نسبية بحيث أن كل حل نسبي للمعادلة E يمكن إيجاده بدايةً من هذه النقاط وتكرار أخذ خطوط تمر بزوج من هذه النقاط ، تتقاطع مع E ، وعمل انعكاس لنقاط التقاطع لإيجاد نقاط جديدة.

---

(١) إذا كان $\Delta\left(E\right) = 0$ ، عندئذ فإن كثير الحدود التكعيبي $x^3 + ax^2 + bx + c$ له جذر مكرر مرتين أو ثلاث مرات ، والمنحنى E إما أن يتقاطع مع نفسه وإما أن له رأساً مدبباً (انظر التمرين رقم ٤٣,٧). المميّز $\Delta\left(E\right)$ سيظهر في عدة أشكال عندما نستمر في دراستنا للمنحنيات الناقصية.

لقد برهن "موردل" (Mordell) نظريته في عام ١٩٢٢م. لسوء الحظ، فإن البرهان صعب جدًّا علينا لنعرضه بالتفصيل، لكن الخطوط العريضة التالية لبرهان "موردل" (Mordell) تبين أنه ليس أكثر من كونه طريقة الانحدار لفيرما:

(1) الخطوة الأولى هي عمل قائمة من نقاط "صغيرة" $P_1, P_2, \ldots, P_r$ واقعة على E وإحداثياتها نسبية.

(2) الخطوة التالية، هي أن نبين أنه إذا كانت Q أي نقطة إحداثياتها نسبية ليست من ضمن القائمة، فإنه من الممكن اختيار واحدة من النقاط P_i's بحيث أن الخط المار بالنقطتين Q, P_i يقطع E في نقطة ثالثة Q' تكون "أصغر" من Q.

(3) بتكرار هذا الإجراء، نحصل على قائمة من النقاط $Q, Q', Q'', Q''', \ldots$ تتناقص في الحجم، ونبين في النهاية أن الحجم يصبح صغيراً جدًّا لنحصل في نهاية المطاف على إحدى نقاط قائمتنا الأصلية P_i's.

لاحظ التشابه مع عملنا في معادلة بِلْ، حيث بيَّنا أن أي حل كبير هو دائماً حاصل ضرب حل أصغر بالحل الأصغر. طبعاً، ليس من الواضح ماذا نعني بقولنا "أكبر" و "أصغر" بالنسبة للنقاط التي إحداثياتها نسبية والواقعة على منحنى ناقصي E. إن هذه إحدى أفكار عديدة عمل عليها "موردل" (Mordell) قبل أن يكمل برهانه.

دعنا نلقي نظرة على بعض الحلول النسبية للمعادلة E_1. لنبدأ بالنقطتين $P_1 = (-2, 3)$, $P_2 = (-1, 4)$. إن الخط المار بالنقطتين P_2, P_1 يقطع E_1 في نقطة ثالثة، والتي نعمل لها انعكاساً حول محور x لنحصل على النقطة P_3. بعد ذلك نأخذ الخط المار بالنقطتين P_1 , P_3، ونعمل انعكاساً لنقطة تقاطعه مع E_1 حول المحور x لنحصل على النقطة P_4. باستخدام الخط المار بالنقطتين P_1 , P_4، سنحصل على

النقطة P_5 ، وهكذا. وفيما يلي النقاط القليلة الأولى P_n's . وكما ترى ، الأعداد تصبح أكبر وأكبر بشكل سريع.

$$P_1=(-2,3),\quad P_2=(-1,4),\quad P_3=(4,-9),\quad P_4=(2,5),$$
$$P_5=\left(\frac{1}{4},\frac{-33}{8}\right),\quad P_6=\left(\frac{106}{9},\frac{1097}{27}\right),\quad P_7=\left(\frac{-2228}{961},\frac{-63465}{29791}\right),$$
$$P_8=\left(\frac{76271}{289},\frac{-21063928}{4913}\right),\quad P_9=\left(\frac{-9776276}{6145441},\frac{54874234809}{15234548239}\right),$$
$$P_{10}=\left(\frac{3497742218}{607770409},\frac{-215890250625095}{14983363893077}\right)$$

إننا نتطلع إلى إيجاد طريقة كمية لقياس "حجم" هذه النقاط ، إحدى الطرق لعمل ذلك هي النظر إلى بسط ومقام الإحداثي x . بكلمات أخرى ، إذا كتبنا إحداثيات P_n على الشكل

$$P_n=\left(\frac{A_n}{B_n},\frac{C_n}{D_n}\right)$$

فإننا يمكن أن نعرف "حجم" (size) P_n على أنه[١] :

حجم $(P_n)=$ أعلى قيمة لـ $|A_n|$, $|B_n|$

$$\text{Size}(P_n)=\text{maximum of}\,|A_n|\,\text{and}\,|B_n|$$

على سبيل المثال ،

$$size(P_1)=\max\{|-2|,|1|\}=2$$

(١) المصطلح الرياضي لما أسميناه الحجم (size) هو الارتفاع (height).

و : $$size\left(P_7\right)=\max\left\{\left|-2228\right|,\left|961\right|\right\}=2228$$

أول 20 P_n's وحجومها مبينة في جدول 43.1.

هل لاحظت أي نمط في جدول 43.1؟ لا يبدو أن الأعداد تتبع أي نمط ، لكن حاول التحديق في الجدول مرة أخرى. تخيل أن الأعداد صناديق سوداء مُصْمَتَة وانظر في المنحنى الذي يفصل بين المساحة السوداء والمساحة البيضاء. هل هذا شيء مألوف لديك؟ إذا كان جوابك لا ، فانظر إلى جدول 43.2 ، وهو امتداد للجدول 43.1 حتى $n \geq 50$ واستبدلنا فيه الأرقام بصناديق سوداء.

المنحنى الذي يفصل المنطقة السوداء عن المنطقة البيضاء يشبه كثيراً القطع المكافئ. إن ما يعنيه هذا هو أن عدد الخانات (Digits) في $size\left(P_n\right)$ هو عدد على الشكل cn^2 حيث c عدد ثابت. باستخدام أساليب متقدمة، يمكن أن نبين أن c عدد يساوي تقريباً 0.1974 [1]. بمعنى آخر، لقيم n الكبيرة، حجم P_n يبدو على الشكل

$$\#\,of\ digits\ in\ size\left(P_n\right)\approx 0.1974n^2$$

$$size\left(P_n\right)\approx 10^{0.1974n^2}\approx\left(1.574\right)^{n^2}$$

من المفيد مقارنة هذا مع حلول معادلة بِلْ التي أوجدناها في الفصل 30. لقد بيَّنا هناك أن حجم الحل النوني $\left(x_n,y_n\right)$ لمعادلة بِلْ $x^2-2y^2=1$ يساوي تقريباً :

$$x_n\approx\frac{1}{2}\left(5.82843\right)^n$$

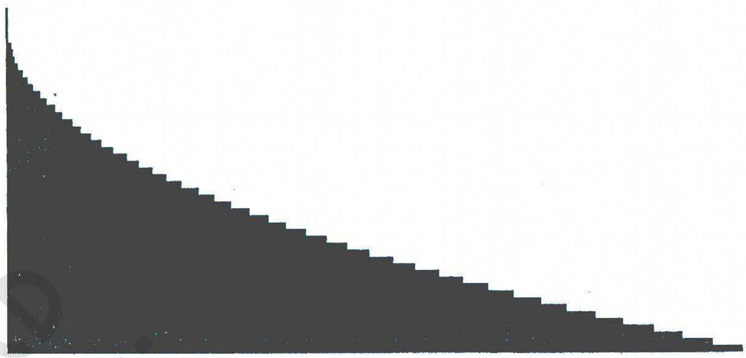
إن معدل النمو الأسي لمعادلة بِلْ سريع جدًّا، ولكنه يتضاءل إذا ما قارنَّاه مع سرعة نمو نقاط المنحنى الناقصي.

---

(١) حُسِبَت قيمة c عن طريق نظرية الارتفاعات القانونية وذلك على يد كل من "Andre Neron" و "John Tate" في العام 1960. باستخدام هذه النظرية يمكننا أن نبين أن النسبة $ln\left(size\left(P_n\right)\right)/n^2$ تقترب أكثر فأكثر من العدد ...0.4546168651 كلما كبرت n أكثر فأكثر.

الجدول رقم (٤٣,١). حجم النقاط P_n الواقعة على E_1 .

n	$size(P_n)$
1	2
2	1
3	4
4	2
5	4
6	106
7	2228
8	76271
9	9776276
10	3497742218
11	1160536538401
12	1610419388060961
13	43923749623043363812
14	102656671584861356692801
15	185318468583598078787345152 84
16	370183335711420357564604634095918
17	1250679403436209575468050166346178817 61
18	148038963965462958804632421208197172532484 09
19	4149533762127407460342548867530280775668019699737 2
20	83094719816361303226380666143399722139698613105279866991



جدول رقم (٤٣). حجم النقاط P_n الواقعة على E_1 .

تمارين

(٤٣,١) لكل زوج من النقاط التالية الواقعة على المنحنى الناقصي $E_1 : y^2 = x^3 + 17$ ، استخدم الخط المار بالنقطتين لإيجاد نقطة جديدة إحداثياتها نسبية واقعة على E_1.

(a) النقطتان $(-1,4)$, $(2,5)$.

(b) النقطتان $(43,282)$, $(52,-375)$.

(c) النقطتان $(-2,3)$, $(19/125, 522/1125)$

(٤٣,٢) المنحنى الناقصي :

$$E : y^2 = x^3 + x - 1$$

تقع عليه النقطتان $P = (1,1)$, $Q = (2,-3)$ ذواتا الإحداثيات النسبية.

(a) استخدم الخط المار بالنقطتين Q, P لإيجاد نقطة جديدة R واقعة على E إحداثياتها نسبية.

(b) لتكن R' النقطة الناتجة من انعكاس R في المحور x. [أي، إذا كانت $R=\left(x,y\right)$ فإن $R'=\left(x,-y\right)$]. استخدم الخط المار بالنقطتين R',P لإيجاد نقطة جديدة S واقعة على E إحداثياتها نسبية.

(c) تماماً مثل (b) ، لكن استخدم الخط المار بالنقطتين Q,R' لإيجاد نقطة جديدة T .

(d) لتكن S النقطة التي أوجدتها في (b)، ولتكن S' النقطة الناتجة من انعكاس S في المحور x. ما هي النقطة التي ستحصل عليها إذا استخدمت الخط المار بالنقطتين $\left(S',R\right)$ لإيجاد نقطة جديدة على E.

(٤٣,٣) افرض أن $Q_1,Q_2,Q_3,\ldots$ قائمة من نقاط إحداثياتها نسبية واقعة على المنحنى الناقصي E ، وافرض أن حجومها متناقصة :

$$size\left(Q_1\right) > size\left(Q_2\right) > size\left(Q_3\right) > \ldots$$

اشرح لماذا يجب أن تتوقف القائمة بعد عدد منتهٍ من النقاط. بمعنى آخر، اشرح لماذا يجب أن تكون قائمة نقاط أحجامها متناقصة فعلاً قائمة منتهية. هل رأيت لماذا ذلك يجعل الحجم أداة جيدة للبراهين التي تستخدم الانحدار؟

(٤٣,٤) اكتب باختصار عن "كاردانو" (Girolamo Cardano)، خصوصاً عن بحثه المنشور في حل المعادلة التكعيبية والخلاف والجدل الذي عَقِب ذلك.

(٤٣,٥) (هذا التمرين للذين درسوا التفاضل والتكامل). هناك طريقة أخرى لإيجاد نقاط إحداثياتها نسبية تقع على منحنى ناقصي، هذه الطريقة تستخدم المماسات. هذا التمرين يشرح هذه الطريقة على المنحنى :

$$E: y^2 = x^3 - 3x + 7$$

(a) النقطة $P=\left(2,3\right)$ نقطة على E. أوجد معادلة المماس L للمنحنى الناقصي E عند النقطة P.

(مساعدة: استخدم الاشتقاق الضمني لإيجاد الميل dy/dx عند P).

(b) أوجد أين يقطع المماس المنحنى الناقصي E، وذلك بتعويض معادلة L في E ومن ثم الحل. عليك اكتشاف نقطة جديدة Q إحداثياتها نسبية تقع على E. (لاحظ أن $x=2$ هو جذر مكرر للمعادلة التكعيبية التي تريد حلها. هذا يبين حقيقة أن L هو مماس للمنحنى E عند النقطة التي إحداثيها السيني $x=2$).

(c) لتكن R النقطة التي حصلت عليها بعمل انعكاس للنقطة Q في المحور x. [بكلمات أخرى، إذا كانت $Q=\left(x_1,y_1\right)$، فإن $R=\left(x_1,-y_1\right)$]. خذ الخط المار بالنقطتين R,P وقاطعه مع E لإيجاد نقطة ثالثة إحداثياتها نسبية تقع على E.

(٤٣,٦) ليكن L الخط $y=m\left(x+2\right)+3$ الذي ميله m ويمر بالنقطة $\left(-2,3\right)$. هذا الخط يقطع المنحنى الناقصي $y^2=x^3+17$ في النقطة $\left(-2,3\right)$ وفي نقطتين أخرتين.

إذا كانت جميع هذه النقاط الثلاث إحداثياتها نسبية، فبين أن المقدار:

$$m^4+12m^2+24m-12$$

يجب أن يكون مربع عدد نسبي. عوض عن m بقيم بين 10 , -10 لمعرفة أي هذه القيم تجعل هذا المقدار مربعاً. واستخدم القيم التي أوجدتها لاستنتاج حلول للمعادلة $y^2=x^3+17$.

(٤٣,٧) مميز كل من المنحنيين :

$$C_1 :\ y^2 = x^3 \quad , \quad C_2 :\ y^2 = x^3 + x^2$$

يساوي صفراً. ارسم هذين المنحنيين، ووضح وجه الاختلاف بين الرسمين، ووجه الاختلاف بينهما وبين رسم المنحنيات الناقصة الموضحة في الشكل رقم 43.1.

(٤٣,٨) ليكن E المنحنى الناقصي :

$$E : y^2 = x^3 + ax^2 + bx + c$$

وليكن $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ نقطتان على E.

(a) ليكن L الخط المار بالنقطتين P_1, P_2. اكتب برنامجاً لحساب النقطة الثالثة $P_3 = (x_3, y_3)$ التي تمثل نقطة تقاطع L مع E.
(إذا كان L خطاً رأسيًّا، إذن لن تكون هناك نقطة تقاطع ثالثة حقيقية، إذن يجب على برنامجك أن يكتب رسالة تحذير). يجب عليك أن تتأكد من أن الإحداثيات هي أعداد نسبية. إذا كانت لغة برنامجك لا تتيح لك التعامل مع الأعداد النسبية مباشرة، فيجب عليك أن تخزن العدد النسبي A/B كزوج مرتب (A, B)، وفي هذه الحالة يجب عليك دائماً أن تلغي $\gcd(A, B)$.

(b) عدّل برنامجك ليُعطي النقطة المنعكسة $(x_3, -y_3)$. سنرمز لهذه النقطة بالرمز $P_1 \oplus P_2$، على أنه قانون "جمع" لنقاط E.

(c) ليكن E المنحنى الناقصي :

$$E : y^2 = x^3 + 3x^2 - 7x + 3$$

ولنعتبر النقاط $P = \left(2,-3\right)$, $Q = \left(37/36, 53/216\right)$, $R = \left(3,6\right)$.

استخدم برنامجك لحساب $P \oplus Q$, $Q \oplus R$, $P \oplus R$ بعد ذلك احسب :

$$P \oplus \left(Q \oplus R\right) \quad , \quad \left(P \oplus Q\right) \oplus R$$

هل حصلت على نفس الإجابة بغض النظر عن ترتيب جمع النقاط؟ هل تجد ذلك غريباً؟

(إذا لم تجد ذلك غريباً، حاول إثبات أن هذه الحقيقة صحيحة لكل منحنى ناقصي).