# منحنيات ناقصية بقليل من النقاط النسبية

# Elliptic Curves with Few Rational Points

المنحنى الناقصي $E_1$ الذي معادلته $y^2 = x^3 + 17$ تقع عليه الكثير من النقاط التي إحداثياتها أعداد نسبية. من جهة أخرى، يبدو أن النقاط النسبية الواقعة على المنحنى الناقصي $E_2$ الذي معادلته $y^2 = x^3 + x$ قليلة جدًّا. في الحقيقة، النقطة الوحيدة التي نستنتج مباشرة أنها واقعة على $E_2$ هي $(0,0)$. سوف نبين أن هذه النقطة هي النقطة النسبية الوحيدة الواقعة على $E_2$.

***نظرية رقم (٤٤,١)***

*النقطة الوحيدة بإحداثيات نسبية الواقعة على $E_2 : y^2 = x^3 + x$ هي النقطة $(x,y) = (0,0)$.*

**البرهان**

افرض أن $(A/B, C/D)$ هي النقطة الواقعة على $E_2$ والتي إحداثياتها نسبية، حيث إننا كتبنا الكسرين $A/B$ ، $C/D$ بأبسط صورة. وبشكل خاص، أخذنا

المقامين $D, B$ عددين موجبين. إن هدفنا هو أن نبين أن $A = 0$ , $C = 0$. بتعويض $x = A/B$ و $y = C/D$ في معادلة $E_2$ وبالتخلص من المقامات ، نحصل على المعادلة :

$$C^2B^3 = A^3D^2 + AB^2D^2 \quad ........................(*)$$

أي حل لهذه المعادلة في مجموعة الأعداد الصحيحة (حيث $D, B$ لا يساويان الصفر) يعطي نقطة نسبية على $E_2$.

إن المعادلة $(*)$ تحوي العديد من المعلومات عن قابلية القسمة ، يمكننا من خلالها عمل العديد من الاستنتاجات. فمثلاً ، بتحليل الطرف الأيمن للمعادلة $(*)$ نحصل على

$$C^2B^3 = D^2A\left(A^2 + B^2\right)$$

إذن $D^2A$ تقسم $C^2B^3$. على كل حال، نحن نعلم أن $\gcd\left(C, D\right) = 1$ ، إذن $D^2$ يقسم $B^3$. كذلك إذا أعدنا ترتيب $(*)$ وحللنا نحصل على :

$$A^3D^2 = C^2B^3 - AB^2D^2 = B^2\left(C^2B - AD^2\right)$$

إذن $B^2$ يقسم $A^3D^2$. بما أن $\gcd\left(A, B\right) = 1$ ، فإن $B^2$ يقسم $D^2$ ، وهذا يعني بالطبع أن $B$ يقسم $D$. لقد بينا حتى الآن أن :

$$B/D \quad , \quad D^2/B^3$$

ليكن $v = D/B$ ، إذن نعلم أن $v$ عدد صحيح. تعويض $D = Bv$ في العلاقة $D^2/B^3$ يخبرنا أن $B^2v^2/B^3$ ، إذن $v^2/B$. بكلمات أخرى ، يمكننا أن نكتب

$B$ على الشكل $B = v^2 z$ حيث $z$ عدد صحيح. لاحظ أن $D = Bv = v^3 z$.
بتعويض $B = v^2 z$ و $D = v^3 z$ في المعادلة $(*)$ ينتج:

$$\begin{aligned} C^2 B^3 &= A^3 D^2 + AB^2 D^2 \\ C^2 \left(v^2 z\right)^3 &= A^2 \left(v^3 z\right)^2 + A\left(v^2 z\right)^2 \left(v^3 z\right)^2 \\ C^2 z &= A^3 + Av^4 z^2 \end{aligned}$$

إذن :

$$A^3 = C^2 z - Av^4 z^2 = z\left(C^2 - Av^4 z\right)$$

لذلك فإن $z$ يقسم $A^3$. على كل حال، $z$ يقسم $B$ أيضاً وحيث إن $\gcd\left(A, B\right) = 1$ فإن $z = \pm 1$. من جهة أخرى، $B = v^2 z$ ونعلم أن $B$ عدد موجب ، إذن $z = 1$. نحن نعلم الآن أن :

$$B = v^2 \qquad , \qquad D = v^3$$

إذن نقطتنا الأصلية $\left(A/B, C/D\right)$ الواقعة على $E_2$ هي على الشكل $\left(A/v^2, C/v^3\right)$، والمعادلة $(*)$ تصبح :

$$C^2 = A^3 + Av^4$$

بتحليل الطرف الأيمن:

$$C^2 = A\left(A^2 + v^4\right)$$

إن هذه معادلة مثيرة الاهتمام؛ لأنها تُعبّر عن مربع كامل $C^2$ كحاصل ضرب عددين $A$ , $A^2 + v^4$. إنني أدعي أن هذين العددين ليس بينهما عوامل مشتركة. هل تعرف لماذا؟

حسناً، إذا كان للعددين $A$ , $A^2+v^4$ عامل مشترك، ولنقل أن كليهما يقبل القسمة على عدد أولي $p$، فإن $v$ أيضاً يقبل القسمة على $p$. على كل حال، لا يمكن أن يقبل كلا العددين $A$ , $v$ القسمة على $p$؛ لأن الكسر $A/B=A/v^2$ مكتوب بأبسط صورة.

إذن، نعلم الآن أن $A$ , $A^2+v^4$ ليس بينهما عوامل مشتركة، وأن حاصل ضربهما مربع كامل. الاحتمال الوحيد لحدوث هذا هو إذا كان كل منهما مربعاً. (هل هذا السبب يبدو مألوفاً لديك؟ لقد استخدمناه في الفصل 2 عندما استنتجنا صيغة الثلاثيات الفيثاغورية). بكلمات أخرى، لقد استطعنا إيجاد عددين صحيحين $w,u$ بحيث:

$$A=u^2 \quad , \quad A^2+v^4=w^2$$

بتعويض القيمة $A=u^2$ في المعادلة الثانية نحصل على:

$$u^4+v^4=w^2$$

لنلخص ما عملناه، لقد بدأنا بحل للمنحنى الناقصي $E_2$، والذي كتبناه على الشكل $\left(A/B, C/D\right)$ بأبسط صورة. بالبدأ من هذا الحل، بينَّا أنه يجب أن تكون هناك أعداد صحيحة $w,u,v$ تحقق المعادلة:

$$u^4+v^2=w^2$$

علاوة على ذلك، بمعلومية هذه الأعداد الصحية $u,v,w$، يمكننا إيجاد حل المعادلة $E_2$ من الصيغتين $A/B=u^2/v^2$ و $C/D=uw/v^3$. هل ميَّزت هذه المعادلة المكتوبة بدلالة $u,v,w$؟ يجب أن تكون مألوفة لديك، لأنها نفس المعادلة التي درسناها في الفصل الثامن والعشرون، حيث برهنا وقتها أن الحلول الوحيدة هي تلك

التي فيها $u=0$ أو $v=0$. فإذا كانت $u=0$ فذلك يؤدي إلى أن $\left(A/B, C/D\right)=\left(0,0\right)$ وإذا كان $v=0$ فذلك يؤدي إلى أن المقام يساوي صفراً، وعليه؛ فإن النقطة الوحيدة التي إحداثياتها نسبية وتقع على $E_2$ هي $\left(0,0\right)$. وبذلك يكتمل البرهان.

لنرى الآن المنحنى الناقصي الثالث :

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

بحث قصير يكشف عن أربع نقاط تقع على $E_3$ ،

$$P_1=\left(0,4\right), \quad P_2=\left(4,4\right), \quad P_3=\left(0,-4\right), \quad P_4=\left(4,-4\right),$$

ماذا سوف يحدث إذا استخدمنا هذه النقاط الأربع ولعبنا نفس اللعبة التي لعبناها مع $E_1$ ؟ معادلة الخط المار بالنقطتين $P_2, P_1$ هي $y=4$. لإيجاد أين يقطع هذا الخط المنحنى $E_3$ ، نعوض $y=4$ في معادلة $E_3$ ونحل في $x$ :

$$\begin{aligned} 4^2 &= x^3 - 4x^2 + 16 \\ 0 &= x^3 - 4x^2 = x^2\left(x-4\right) \end{aligned}$$

لاحظ أن $x=0$ هو جذر مكرر؛ لذلك فإن الخط المار بالنقطتين $P_2, P_1$ يقطع $E_3$ فقط في النقطتين $P_2, P_1$. فقدنا اللعبة ، لقد فشلنا في إيجاد أي نقاط جديدة. نفس الشيء سيحدث لو أننا اخترنا أي نقطتين من بين النقاط $P_1, P_2, P_3, P_4$. في الحقيقة ، يظهر أن النقاط النسبية الواقعة على $E_3$ هي فقط $P_1, P_2, P_3, P_4$. (لسوء الخط ، البرهان طويل جدًّا لعرضه هنا).

بشكل عام ، المجموعة المنتهية من النقاط :

$$P_1, P_2, \ldots, P_t$$

(حيث $t \geq 3$) الواقعة على منحنى ناقصي :

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

تسمى "تجمعاً ملتوياً" (*torsion collection*) إذا كانت ، لأي خط ترسمه يمر بنقطتين من النقاط $P_i$'s ، فإن جميع نقاط تقاطع $E, L$ موجودة أصلاً في هذا التجمع. طريقة أخرى لقول ذلك هي أن التجمع الملتوي لا يمكن توسيعه باستخدام الطريقة الهندسية من أخذ خطوط ونقاط تقاطع. فمثلاً ، $E_3$ له التجمع الملتوي الذي يضم النقاط الأربع $(4, \pm 4), (0, \pm 4)$. النظرية المهمة التالية تصف التجمعات الملتوية.

***نظرية (٢, ٤٤) (نظرية الالتواء)***

*ليكن $E: y^2 = x^3 + ax^2 + bx + c$ منحنى ناقصًا معاملاته $a, b, c$ أعداد صحيحة ، وليكن $P_1, P_2, \ldots, P_t$ تجمعاً ملتوياً على $E$ نقاطه إحداثياتها أعداد نسبية. كذلك ليكن :*

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

*هو مميز $E$ ، ولنفرض أن $\Delta(E) \neq 0$.*

*(a) (نظرية Nagell - Lutz , 1935/37) إذا كتبنا إحداثيات كل نقطة $P_i$ على الشكل $P_i = (x_i, y_i)$ ، فإن كل الـ $x_i$'s و $y_i$'s هي أعداد صحيحة. علاوة على ذلك ، إذا كان $y_i \neq 0$ ، فإن $y_i^2 / 16\Delta(E)$.*

*(b) (نظرية Mazur , 1977) التجمع الملتوي يضم على الأكثر 15 نقطة.*

إن جزء Nagell – Lutz من نظرية الالتواء ينص على أن إحداثيات نقاط تجمع ملتوٍ هي أعداد صحيحة. رأينا أيضاً أمثلة على نقاط إحداثياتها أعداد صحيحة لا تقع في تجمع ملتوٍ، مثل النقطة $\left(-2,3\right)$ الواقعة على المنحنى $E_1 : y^2 = x^3 + 17$. لقد اكتشفت أبحاثنا نقاط قليلة على $E_1$ إحداثياتها صحيحة، تضم

$$\begin{array}{llll} \left(-2,\pm 3\right), & \left(-1,\pm 4\right), & \left(2,\pm 5\right), & \left(4,\pm 9\right), \\ \left(8,\pm 23\right), & \left(43,\pm 282\right), & \left(52,\pm 375\right), & \end{array}$$

نعلم أن هناك عدداً لا نهائيًّا من النقاط إحداثياتها نسبية تقع على المنحنى $E_1$، لذلك ليس هناك سبب لعدم إمكانية توسيع القائمة لتصبح لا نهائية. باستمرار البحث، سنجد بسرعة نقطة أخرى على $E_1$ بإحداثيات صحيحة،

$$\left(5234,\pm 378661\right)$$

ولكن بعد ذلك لن نجد نقطة أخرى، حتى لو استمرينا في البحث حتى $x < 10^{100}$. أخيراً، بدأنا نشك أنه لا توجد نقطة أخرى صحيحة (أي إحداثياتها صحيحة) على $E_1$. إن هذا يبدو صحيحاً، وأنها حالة خاصة من النتيجة الأساسية التالية.

***نظرية (٣,٤٤) (نظرية سيجل Siegel , 1926)***

*ليكن $E$ منحنى ناقصيًّا:*

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

*مُعطى بمعادلة معاملاتها $a,b,c$ أعداد صحيحة وبمميز $\Delta\left(E\right) \neq 0$. عندئذ يوجد فقط عدد منتهٍ من الحلول الصحيحة في $x$ و $y$.*

لقد أعطى Siegel برهانين مختلفين تماماً لهذه النظرية. الأول ، نُشِر عام 1926 في (Journal of the London Mathematical Society[١]) وتعامل فيه بشكل مباشر مع المعادلة $E$ واستخدم طرقاً في التحليل إلى عوامل. البرهان الثاني ، نُشِر عام 1929 ، وبدأ فيه بنظرية Mordell واستخدم الطريقة الهندسية لتوليد نقاط جديدة من نقاط قديمة. في النهاية ، وعلى كل حال ، كلا البرهانين اعتمد على نظرية تقريب ديوفانتين (الفصل الواحد والثلاثون)، خصوصاً على النتائج التي تنص على أن بعض الأعداد لا يمكن أن تُقرَّب كثيراً بأعداد نسبية.

## تمارين

(٤٤،١) الثلاثي الفيثاغوري $(a,b,c)$ يصف مثلثاً قائماً أطوال أضلاعه أعداد صحيحة. نسمي مثل هذا المثلث مثلث فيثاغوري. أوجد جميع المثلثات الفيثاغورية التي مساحتها تساوي ضعف مربع كامل.

(٤٤،٢) (a) ليكن $E$ المنحنى الناقصي $E : y^2 = x^3 + 1$. بيِّن أن النقاط :

$$(-1,0),\ (0,1),\ (0,-1),\ (2,3),\ (2,-3)$$

تشكل تجمعاً ملتويًّا على $E$.

(b) ليكن $E$ المنحنى الناقصي $E : y^2 = x^3 - 43x + 166$. النقاط الأربع :

$$(3,8),\ (3,-8),\ (-5,16),\ (-5,-16)$$

(١) في عشرينات القرن العشرين (1920s) كان ما يزال هناك مرارة عالقة بين كل من إنجلترا وألمانيا جراء الحرب العالمية الأولى، لذلك نشر Siegel بحثه تحت الاسم المستعار "$X$".

تشكل جزءاً من تجمع ملتوٍ على $E$. ارسم خطوطاً تمر بزوج من هذه النقاط وقاطع هذه الخطوط مع $E$ لإيجاد كامل التجمع الملتوي.

(c) ليكن $E$ منحنى ناقصيًّا مُعطى بالمعادلة $y^2=(x-\alpha)(x-\beta)(x-\gamma)$ تحقق من أن مجموعة النقاط $(\alpha,0),(\beta,0),(\gamma,0)$ تشكل تجمعاً ملتوياً.

(٤٤،٣) كم عدد الحلول الصحيحة (أي أن كل من قيمة $y, x$ أعداد صحيحة) التي يمكنك إيجادها على المنحنى الناقصي $y^2=x^3-16x+16$ ؟

(٤٤،٤) هذا التمرين يقودك لإثبات أن المنحنى الناقصي $E: y^2=x^3+7$ ليس له حلول صحيحة في $y, x$. (هذه حالة خاصة من نظرية Siegel والتي أثبتت أصلاً على يد V. A. Lebesgue في عام 1869).

(a) افرض أن $(x,y)$ حل صحيح. بين أن $x$ يجب أن يكون فرديًّا.

(b) بين أن $y^2+1=(x+2)(x^2-2x+4)$.

(c) بين أن $x^2-2x+4$ يجب أن يطابق 3 قياس 4. اشرح لماذا $x^2-2x+4$ يجب أن يقبل القسمة على عدد ما أولي $q$ بحيث $q\equiv 3 \pmod 4$.

(d) اختزل المعادلة الأصلية $y^2=x^3+7$ قياس $q$، واستخدم التطابق الناتج لإثبات أن $-1$ هو راسب تربيعي قياس $q$. اشرح لماذا من غير الممكن أن يكون للمعادلة $y^2=x^3+7$ حلول صحيحة.

(٤٤،٥) المنحنى الناقصي $E: y^2=x^3-2x+5$ تقع عليه النقاط الصحيحة الأربع $P(-2,\pm 1)$ , $Q(1,\pm 2)$.

(a) أوجد أربع نقاط صحيحة أخرى، وذلك بالتعويض بالقيم $x=2,3,4,\ldots$ ورؤية فيما إذا كان $x^3-2x+5$ مربعاً.

(b) استخدم الخط المار بالنقطتين $Q, P$ لإيجاد نقطة جديدة $R$ إحداثياتها نسبية. اعمل انعكاساً للنقطة $R$ في المحور $x$ لتحصل على نقطة $R'$. الآن خذ الخط المار بالنقطتين $R', Q$ وقاطعه مع $E$ لإيجاد نقطة إحداثياتها أعداد صحيحة كبيرة إلى حد ما.

(٤٤,٦) (a) بين أن للمعادلة $y^2 = x^3 + x^2$ عدداً لا نهائيًّا من الحلول الصحيحة في $y, x$.

(مساعدة: حاول بالتعويض $y = tx$).

(b) هل إجابتك في (a) تعني أن نظرية Siegel غير صحيحة ؟

(c) بين أن للمعادلة $y^2 = x^3 - x^2 - x + 1$ عدداً لا نهائيًّا من الحلول الصحيحة في $x$.

(٤٤,٧) ليكن $E : y^2 = x^3 + ax^2 + bx + c$ منحنى ناقصيًّا، حيث $a, b, c$ أعداد صحيحة. افرض أن $P = \left(\frac{A}{B}, \frac{C}{D}\right)$ نقطة على $E$ إحداثياتها أعداد نسبية، مكتوبة بأبسط صورة و $D, B$ عددان موجبان. برهن أن هناك عدداً صحيحاً $v$ بحيث $B = v^2$ , $D = v^3$.

(٤٤,٨) اكتب برنامجاً يبحث عن جميع النقاط الواقعة على المنحنى الناقصي :

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

حيث $x$ عدد صحيح و $|x| < H$ واعمل ذلك بأن تحاول مع جميع القيم الممكنة لـ $x$، وافحص فيما إذا كان $x^3 + ax^2 + bx + c$ مربعاً كاملاً؟

(٤٤,٩) (a) اكتب برنامجاً يبحث عن نقاط على المنحنى الناقصي :

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

بحيث أن $y\,,x$ عددين نسبيين. تمرين 44.7 يقول إن أي نقطة مثل هذه يجب أن تكون على الشكل $(x,y)=\left(A\big/D^2\,,B\big/D^3\right)$ ، لذلك يجب أن يُدخل المستخدم حدًّا أعلى $H$ ، ويجب أن يقوم برنامجك بفحص جميع الأعداد الصحيحة $|A|\le H$ و $1\le D\le\sqrt{H}$ ويفحص فيما إذا كان:

$$A^3+aA^2D^2+bAD^4+cD^6$$

مربعاً كاملاً. إذا كان يساوي $B^2$ ، فإنك تكون قد أوجدت النقطة $.\left(A\big/D^2\,,B\big/D^3\right)$

(b) استخدم برنامجك لإيجاد جميع النقاط الواقعة على المنحنى الناقصي :

$$y^2=x^3-2x^2+3x-2$$

التي يكون إحداثيها السيني على الشكل $x=A\big/D^2$ حيث $\left|A\right|\le 1500$ و $.1\le D\le 38$