الفصل السادس والأربعون

مجموعات الالتواء قياس p والأعداد الأولية الرديئة

Torsion Collections Modulo p And Bad Primes

قمنا في الفصل السابق بإيجاد أنماط بسيطة لـ انحرافات p – للمنحنيين E_1, E_2 ، ولكن لم يظهر أي نمط مشابه للمنحنى E_3. على كل حال N_p's للمنحنى E_3 تُظهر نمطاً ربما لاحظته بشكل تلقائي. إذا لم تلاحظه بعد، فألقِ نظرة على جدول 45.6 وحاول اكتشاف النمط بنفسك قبل متابعة القراءة.

يُظهر الجدول أن N_p's للمنحنى E_3 له الخاصية التالية:

$N_p \equiv 4 \pmod 5$ لجميع الأعداد الأولية ما عدا $p = 2$, $p = 11$.

على الرغم من أننا لن نعطي برهاناً كاملاً لهذه الخاصية، فإننا نستطيع على الأقل إعطاء فكرة تبين أن هذه الخاصية صحيحة. نتذكر من الفصل الرابع والأربعون أن E_3 له مجموعة التواء تضم النقاط الأربع:

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

هذا يعني أن الخطوط المارة بأي نقطتين من هذه النقاط لا تقطع E_3 في أي نقاط

إضافية. إن طريقة أخذ زوج من النقاط على المنحنى الناقصي ، وربط كل منهما بخط ، ومن ثم إيجاد نقاط تقاطعه مع المنحنى ، يمكن إنجازها باستخدام المعادلات بدون أي رجوع للهندسة. هذا يعني أننا نستطيع استخدام نفس الطريقة لإيجاد نقاط قياس p !

دعنا ننظر إلى المثال التالي ، النقطة $Q=\left(1,8\right)$ هي حل للتطابق

$$y^2 \equiv x^3 - 4x^2 + 16 \pmod{17}$$

الخط المار بالنقطتين Q , $P=\left(0,4\right)$ هو $y=4x+4$. تعويض معادلة الخط في معادلة المنحنى الناقصي يُعطي :

$$\begin{aligned} \left(4x+4\right)^2 &\equiv x^3 - 4x^2 + 16 \pmod{17} \\ x^3 - 3x^2 + 2x &\equiv 0 \pmod{17} \\ x\left(x-1\right)\left(x-2\right) &\equiv 0 \pmod{17} \end{aligned}$$

إذن حصلنا على النقطتين المعلومتين P_1, Q بإحداثيات سينية $x=1, x=0$ ، وكذلك حصلنا على نقطة جديدة إحداثيها السيني $x=2$. تعويض $x=2$ في معادلة الخط يُعطي $y=12$ ، وبذلك نكون قد أوجدنا الحل الجديد $\left(2,12\right)$ للمنحنى E_3 قياس 17.

إذا استخدمنا نفس الفكرة مع النقطتين $Q=\left(1,8\right)$, $P_3=\left(4,4\right)$ ، سنحصل على الخط $y=-\left(4/3\right)x+28/3$. ما المعنى الذي يمكن استنتاجه لهذا الخط قياس 17 ؟ حسناً، الكسر $-4/3$ ما هو إلا حل المعادلة $3u=-4$. إذن العدد " $-4/3$ قياس 17" هو حل للتطابق $-3u \equiv 4 \pmod{17}$. نحن نعلم كيف نحل مثل هذه التطابقات ، في هذه الحالة ، الجواب هو $u=10$. نفس الشيء "$28/3$ قياس 17" هو 15 ، إذن الخط المار بالنقطتين $Q=\left(1,8\right)$, $P_3=\left(4,4\right)$ قياس 17

هو $y = 10x + 15$. الآن نعوض في معادلة E_3 ونحل كما فعلنا سابقاً لإيجاد الحل الجديد $(14,2)$ على E_3 قياس 17.

نستطيع كذلك عمل نفس الشيء مع النقطتين Q , P_2 ، وهذا يُعطي الحل $(11,9)$ ، ومع النقطتين Q , P_4 والذي يُعطي الحل $(15,3)$. لذلك ، فنحن بدأنا بنقطة وحيدة Q ، واستخدمنا نقاط مجموعة الإلتواء الأربع لإيجاد أربعة حلول أخرى.

لنعتبر الآن المنحنى E_3 قياس p لأي عدد أولي p . نعلم مسبقاً أن المنحنى E_3 له النقاط الأربع P_1, P_2, P_3, P_4. في كل مرة نجد فيها نقطة أخرى Q على E_3 قياس p يمكننا أخذ الخط L_i المار بالنقطة Q وكل نقطة من النقاط $P_i's$. كل خط L_i يقطع E_3 في نقطة جديدة Q_i. بهذه الطريقة نحصل على أربع نقاط إضافية Q_1, Q_2, Q_3, Q_4 بالإضافة إلى النقطة الأصلية Q. إذن، النقاط على E_3 قياس p تأتي في حزم من خمس نقاط، ما عدا وجود أربع نقاط $P_i's$ فقط. لذلك.

$$\left\{\begin{array}{c}\text{الحلول لـ } E_3 \\ \text{قياس } p\end{array}\right\} = \left\{\begin{array}{c}\text{الحلول الأربعة} \\ P_1, P_2, P_3, P_4\end{array}\right\} + \left\{\begin{array}{c}\text{حُزَم تحوي 5 حلول لكل} \\ \text{حزمة}\end{array}\right\}$$

إذن ، عدد الحلول الكلي لـ E_3 قياس p يساوي 4 زائد مضاعف للعدد 5 ، أي $N_p \equiv 4 \pmod 5$. إن هذا صحيح لجميع الأعداد الأولية ما عدا $p = 2$, $p = 11$. (للعددين الأوليين $p = 2$, $p = 11$ ، بعض حُزم النقاط الخمس تحوي تكرارات).

التطابق $N_p \equiv 4 \pmod 5$ يشرح أيضاً ملاحظتنا السابقة عن الأعداد الأولية التي لها $a_p = 0$. لنرى لماذا هذا، افرض أن $a_p = 0$. عندئذ :

$$p = N_p \equiv 4 \pmod 5$$

علاوة على ذلك، p فردي ، إذن $p \equiv 9 \pmod{10}$. هذا يثبت أنه إذا كان $a_p = 0$ فإن p يكون 9 قياس 10 ، لكن هذا لا يعني أن كل عدد أولي 9 قياس 10 يكون له $a_p = 0$. وهذا اختلاف مهم يُشكل تناقضاً حاداً مع نتائجنا عن E_1, E_2.

الحوار السابق جيد، لكن ماذا عن العددين الأوليين $p = 2, p = 11$ اللذين لا يتبعان أي نمط؟ لقد تبين أن 2 و 11 حالتان خاصتان إلى حد ما للمنحنى الناقصي $E_3 : y^2 = x^3 - 4x^2 + 16$. السبب وراء ذلك هو أنهما العددان الأوليان الوحيدان اللذان يجعلان لكثير الحدود $x^3 - 4x^2 + 16$ جذراً ثنائيًّا أو ثلاثيًّا قياس p. لذلك

$x^3 - 4x^2 + 16 \equiv x^3 \pmod 2$ له جذر ثلاثي $x = 0$ ، و

$x^3 - 4x^2 + 16 \equiv (x+1)^2 (x+5) \pmod{11}$ له جذر ثنائي $x = -1$.

بشكل عام، نقول إن p عدد أولي "رديء" (*bad prime*) للمنحنى الناقصي

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

إذا كان لكثير الحدود $x^3 + ax^2 + bx + c$ جذر ثنائي أو ثلاثي قياس p. ليس من الصعب إيجاد الأعداد الأولية الرديئة للمنحنى E ، حيث يمكننا أن نبين أنها

تماماً الأعداد الأولية التي تقسم المميز (*discriminan*) للمنحنى E[1].

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

على سبيل المثال،

$$\Delta\left(E_1\right) = -7803 = -3^3 \cdot 17^2$$
$$\Delta\left(E_2\right) = -4 = -2^2$$
$$\Delta\left(E_3\right) = -2816 = -2^8 \cdot 11$$

تمارين

(٤٦,١) افرض أن للمنحنى الناقصي E مجموعة التواء تضم النقاط $P_1, P_2, \ldots, P_t$.

إشرح لماذا عدد الحلول للمنحنى E قياس p يجب أن يحقق:

$$N_p \equiv t \left(\mathrm{mod}\, t+1\right)$$

(٤٦,٢) تمرين (c) 44.2 يقول إن للمنحنى الناقصي $E: y^2 = x^3 - x$ مجموعة الالتواء $\left\{\left(0,0\right),\left(1,0\right),\left(-1,0\right)\right\}$ والتي تضم ثلاث نقاط.

(a) أوجد عدد النقاط على E قياس p للأعداد $p = 2,3,5,7,11$. أيها تحقق $N_p \equiv 3\left(\mathrm{mod}\, 4\right)$؟

(b) أوجد الحلول للمنحنى E قياس 11، غير حلول مجموعة الالتواء، وقسمها في حزم، بحيث كل حزمة تضم أربعة حلول، وذلك برسم خطوط

---

(١) إن وصفنا للأعداد الأولية الرديئة لا يخلو من الخدعة، حيث إنه لأسباب تقنية متعددة يكون العدد الأولي 2 دائماً رديئاً لمنحنياتنا الناقصية. على كل حال، من الممكن أحياناً تحويل عدد أولي رديء إلى عدد أولي جيد باستخدام معادلة للمنحنى E تحوي الحد xy أو الحد y.

تمر بنقاط مجموعة الالتواء.

(٤٦.٣) هذا التمرين يبحث في قيم a_p للأعداد الأولية الرديئة.

(a) أوجد الأعداد الأولية الرديئة لكل منحنى من المنحنيات التالية :

$$(i)\ \ E:\ y^2 = x^3 + x^2 - x + 2$$
$$(ii)\ \ E:\ y^2 = x^3 + 3x + 4$$
$$(iii)\ \ E:\ y^2 = x^3 + 2x^2 + x + 3$$

(b) لكل منحنى في (a)، احسب الانحرافات $p - a_p$ لأعدادها الأولية الرديئة.

(c) هنا عينة قليلة إضافية لمنحنيات ناقصية مع قائمة للانحرافات $p -$ لأعدادها الأولية الرديئة.

E	$\Delta(E)$	a_p للأعداد الأولية الرديئة
$y^2 = x^3 + 2x + 3$	$-5^2 \cdot 11$	$a_5 = -1\ ,\ a_{11} = -1$
$y^2 = x^3 + x^2 + 2x + 3$	$-5^2 \cdot 7$	$a_5 = 0\ ,\ a_7 = 1$
$y^2 = x^3 + 5$	$-3^3 \cdot 5^2$	$a_3 = 0\ ,\ a_5 = 0$
$y^2 = x^3 + 2x^2 - 7x + 3$	$11 \cdot 43$	$a_{11} = -1\ ,\ a_{43} = 1$
$y^2 = x^3 + 21x^2 + 37x + 42$	$-31 \cdot 83 \cdot 239$	$a_{31} = -1\ ,\ a_{83} = 1,$ $a_{239} = -1$

الانحرافات $p -$ للأعداد الأولية الرديئة تبين أنماطاً متعددة وعلى درجات مختلفة من الدقة. صف هذه الأنماط بقدر ما تستطيع.

(٤٦,٤) في هذا التمرين، اعتبر أن p عدد أولي أكبر من 3.

(a) تأكد من أن p عدد أولي رديء للمنحنى الناقصي $y^2 = x^3 + p$. اكتشف قيمة a_p. برهن أن تخمينك صحيح.

(b) تأكد من أن p عدد أولي رديء للمنحنى الناقصي $y^2 = x^3 + x^2 + p$. اكتشف قيمة a_p. برهن أن تخمينك صحيح.

(c) تأكد من أن p عدد أولي رديء للمنحنى الناقصي $y^2 = x^3 - x^2 + p$. اكتشف قيمة a_p. برهن أن تخمينك صحيح.

[مساعدة: في الفقرة (c)، قيمة a_p سوف تعتمد على p].