نقاط على منحنيات ناقصية قياس p

Points on Elliptic Curves Modulo p

قد يكون من الصعب جدًّا حل معادلة ديوفانتينية. لذلك وبدلاً من محاولة إيجاد الحل في الأعداد الصحيحة أو الأعداد النسبية، سنتعامل مع المعادلة الديوفانتينية كتطابق ونحاول إيجاد الحلول قياس p. إن هذه مهمة سهلة جدًّا. ولنرى لماذا ، فلنعتبر المثال التالي.

كيف يمكننا إيجاد جميع الحلول "قياس 7" للمعادلة :

$$x^2 + y^2 = 1 \text{ ؟}$$

بمعنى آخر، ما هي حلول التطابق :

$$x^2 + y^2 \equiv 1 \pmod 7 \text{ ؟}$$

هذا سؤال سهل، فما علينا إلا أن نحاول مع كل زوج (x, y) بحيث $0 \le x, y \le 6$ ونرى أيها يجعل التطابق صحيحاً. لذلك ، $(1,0)$, $(2,2)$ حلان، بينما $(1,2)$, $(3,2)$ ليست حلول. مجموعة الحلول الكاملة هي

$$(0,1),\ (0,6),\ (1,0),\ (2,2),\ (2,5),\ (5,2),\ (5,5),\ (6,0)$$

نستنتج أن المعادلة $x^2 + y^2 = 1$ لها ثمانية حلول قياس 7. نفس الشيء ، هناك 12 حلاً قياس 11 :

$$(0,1),\ (0,10),\ (1,0),\ (3,5),\ (3,6),\ (5,3),\ (5,8),$$
$$(6,3),\ (6,8),\ (8,5),\ (8,6),\ (10,0)$$

الجدول رقم (٤٥,١). نقاط قياس p تقع على E_2 .

p	نقاط قياس p تقع على $E_2: y^2 = x^3 + x$	N_p
2	$(0,0),(1,0)$	2
3	$(0,0),(2,1),(2,2)$	3
5	$(0,0),(2,0),(3,0)$	3
7	$(0,0),(1,3),(1,4),(3,3),(3,4),(5,2),(5,5)$	7
11	$(0,0),(5,3),(5,8),(7,3),(7,8),(8,5),(8,6),$ $(9,1),(9,10),(10,3),(10,8)$	11
13	$(0,0),(2,6),(2,7),(3,2),(3,11),(4,4),(4,9),$ $(5,0),(6,1),(6,12),(7,5),(7,8),(8,0),(9,6),$ $(9,7),(10,3),(10,10),(11,4),(11,9)$	19
17	$(0,0),(1,6),(1,11),(3,8),(3,9),$ $(4,0),(6,1),(6,16),(11,4),(11,13),$ $(13,0),(14,2),(14,15),(16,7),(16,10)$	15
19	$(0,0),(3,7),(3,12),(4,7),(4,12),(5,4)(5,15),$ $(8,8),(8,11),(9,4),(9,15),(12,7),(12,12),$ $(13,5),(13,14),(17,3),(17,16),(18,6)(18,13)$	19

الآن لننظر إلى بعض المنحنيات الناقصية ونَعِد كم نقطة قياس p تقع عليها وذلك لأعداد أولية p مختلفة وسنبدأ بالمنحنى :

$$E_2 : \ y^2 = x^3 + x$$

الذي النقطة النسبية الوحيدة له هي $(0,0)$. على كل حال، كما يشير جدول 45.1 ، فإن هناك العديد من النقاط قياس p تقع على E_2. في العمود الأخير من الجدول 45.1 سردنا N_p وهي عدد النقاط قياس p.

إن عدد النقاط قياس p الواقعة على منحنى ناقصي تعرض العديد من الأنماط المدهشة والدقيقة. دقق النظر في الجدول 45.1. هل تلاحظ أي نمط؟ إذا لم تلاحظ، فربما تساعدك بيانات أكثر. جدول 45.2 يُعطي عدد الحلول قياس p دون عناء سرد الحلول الفعلية.

إن أحد الأنماط الجزئية التي تلاحظها مباشرة هو أن العديد من الأعداد الأولية يكون لها N_p يساوي p. هذا يظهر للأعداد الأولية.

$$p = 2, 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71$$

والتي غالباً ما تكون أعداداً عشوائية. في الحقيقة، فيما عدا العدد 2 ، فإن هذه القائمة هي بدقة مجموعة الأعداد الأولية (الأقل من 71) التي تطابق 3 قياس 4. لذلك من الطبيعي أن نعمل الحدس التالي:

حدس. إذا كان $p \equiv 3 \pmod 4$ ، فإن المنحنى الناقصي $E_2 : \ y^2 = x^3 + x$ يقع عليه بالضبط $N_p = p$ نقطة قياس p.

الجدول رقم (٤٥,٢). عدد النقاط N_p قياس p الواقعة على E_2

p	2	3	5	7	11	13	17	19	23	29
N_p	2	3	3	7	11	19	15	19	23	19

تابع الجدول رقم (٢,٤٥).

p	31	37	41	43	47	53	59	61	67	71
N_p	31	35	31	43	47	67	59	51	67	71

ماذا عن الأعداد الأولية الأخرى، أي التي تطابق 1 قياس 4 ؟ N_p's في هذه الحالة تبدو عشوائية تماماً. أحياناً يكون N_p أقل من p ، مثل $p=5$, $p=17$ ، وفي أحيان أخرى يكون N_p أكبر من p ، مثل $p=13$, $p=53$. على كل حال ، فإنه يبدو صحيحاً أيضاً أنه كلما أصبح p أكبر فإن N_p يصبح أكبر أيضاً. في الحقيقة ، غالباً ما نجد N_p في جوار p . بقليل من التفكير سنجد أن هذا منطقي جدًّا.

بشكل عام، إذا كنا نحاول إيجاد الحلول قياس p لمنحنى ناقصي :

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

فإننا نعوض بالقيم $x = 0,1,2,\ldots, p-1$ ونختبر عند كل قيمة لـ x فيما إذا كان :

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

مربعاً إنه من المنطقي افتراض أن القيم التي نحصل عليها للمقدار $x^3 + ax^2 + bx + c$ تكون موزعه بشكل عشوائي ؛ لذلك فنحن نتوقع أن نصف القيم تكون مربعة والنصف الآخر لا. هذا الاستنتاج من حقيقة أن، المبرهنة في الفصل 23، نصف الأعداد من 1 إلى $P-1$ تكون راسباً تربيعيًّا والنصف الآخر يكون راسباً غير تربيعي. نلاحظ أيضاً أنه إذا حدث وكان $x^3 + ax^2 + bx + c$ مربعاً، ولنقل إنه يطابق $t^2 \pmod p$ ، فإن هناك قيمتين محتملتين لـ y : $y=t$, $y=-t$. باختصار ، تقريباً نصف قيم x تعطي حلين قياس p ، وحوالي النصف لا يعطي أي حل قياس

p ؛ لذلك نتوقع أن نجد $2\times\frac{1}{2}p=p$ حلاً تقريباً. بالطبع، فإن هذا الحوار لا يثبت أن هناك دائماً p من الحلول، إنه يعطي مجرد تبرير لماذا يكون عدد الحلول أكثر أو أقل في جوار p.

إن كل هذا يشير إلى أنه قد يكون من المهم أن نبحث في الفرق بين p ، N_p . لنكتب هذا الفرق على الشكل:

$$a_p = p - N_p$$

الجدول رقم (٤٥,٣). الانحراف $-p$ ($p-Defect$) $a_p = p - N_p$ **للمنحنى** E_2

p	5	13	17	29	37	41	53	61	73	89
N_p	3	19	15	19	35	31	67	51	79	79
a_p	2	−6	2	10	2	10	−14	10	−6	10

p	97	101	109	113	137	149	157	173	181	193
N_p	79	99	115	127	159	163	179	147	163	207
a_p	18	2	−6	−14	−22	−14	−22	26	18	−14

ونسميه " الانحراف $-p$ ($p-Defect$) للمنحنى E_2 ". الجدول 45.3 يسرد الإنحرافات $-p$ للمنحنى الناقصي E_2 .

إن هذا الجدول يعرض نمطاً دقيقاً قريباً جدًّا من موضوع درسناه سابقاً. خذ بضع دقائق لترى إذا كان باستطاعتك اكتشاف النمط بنفسك قبل أن تكمل القراءة.

خلال بحوثنا في نظرية الأعداد، وجدنا أن الأعداد الأولية التي تطابق 1 قياس 4 تعرض الكثير من الخصائص الهامة. واحد من أكثر الاكتشافات أهمية كان في

الفصل السادس والعشرون وهو أن هذه الأعداد الأولية يمكن كتابتها كمجموع مربعين. فعلى سبيل المثال :

$$5 = 1^2 + 2^2 \quad , \quad 13 = 3^2 + 2^2 \quad , \quad 17 = 4^2 + 1^2 \quad , \quad 29 = 5^2 + 2^2$$

علاوة على ذلك، نظرية لجندر الواردة في الفصل 34 تخبرنا أنه إذا أردنا أن يكون A فردي و B, A كلاهما موجباً، فإن هناك خياراً واحداً فقط لـ A و B [بالإشارة إلى نظرية 34.5 $R(p) = 8(D_1 - D_3) = 8$ ، حيث حُسِبَ العدد 8 بتبديل A و B و/أو تغيير إشارتيهما]. قارن هذه الصيغ بالقيم :

$$a_5 = 2 \;,\; a_{13} = -6 \;,\; a_{17} = 2 \;,\; a_{29} = 10$$

هل ترى الآن نمطاً؟ يبدو وكأن a_p إما تساوي $2A$ وإما تساوي $-2A$ ، وذلك عندما نكتب $p = A^2 + B^2$ حيث A موجب وفردي. طريقة أخرى لقول ذلك هي أنه يبدو أن المقدار $p - (a_p/2)^2$ يساوي دائماً مربعاً كاملاً. سنختبر هذا على قيم قليلة أخرى لـ p : $53 - (a_{53}/2)^2 = 2^2, \quad 73 - (a_{73}/2)^2 = 8^2, \quad 193 - (a_{193}/2)^2 = 12^2$ مدهش، النمط ما يزال متحققاً.

الجدول رقم (٤٥,٤). قيمة $a_p/2$ للمنحنى E_2 .

p	5	13	17	29	37	41	53	61	73	89
$a_p/2$	1	–3	1	5	1	5	–7	5	–3	5

p	97	101	109	113	137	149	157	173	181	193
$a_p/2$	9	1	–3	–7	–11	–7	–11	13	9	–7

بقي سؤال واحد. متى $a_p = 2A$ ومتى $a_p = -2A$ ؟
بالنظر إلى الجدول نجد أن :

$$a_p = 2A \quad \text{عند} \quad p = 5,17,29,37,41,61,89,97,101,173,181$$

$$a_p = -2A \quad \text{عند} \quad p = 13,53,73,109,113,137,149,157,193$$

يبدو أن هاتين القائمتين لا تتبعان أي نمط منتظم. على كل حال، إذا نظرنا إلى قيم $a_p/2$ الواردة في الجدول 45.4 فسيظهر نمط.كل قيمة $a_p/2$ تطابق 1 قياس 4. لذلك إذا كتبنا $p = A^2 + B^2$ حيث A موجب فردي ، فإن $a_p = 2A$ إذا كان $A \equiv 1 \pmod 4$ و $a_p = -2A$ إذا كان $A \equiv 3 \pmod 4$. العبارة التالية تلخص جميع استنتاجاتنا.

نظرية (٤٥,١). (عدد النقاط قياس p الواقعة على $E_2 : y^2 = x^3 + x$).

ليكن p عدداً أوليًا فرديًا ، وليكن N_p عدد النقاط على المنحنى الناقصي $E_2 : y^2 = x^3 + x$ قياس p.

(a) إذا كان $p \equiv 3 \pmod 4$ ، فإن $N_p \equiv p$.

(b) إذا كان $p \equiv 1 \pmod 4$ وكتبنا $p = A^2 + B^2$ حيث A عدد موجب وفردي. (نحن نعلم من الفصل 26 أن هذا ممكن دائماً.) فإن $N_p = p \pm 2A$ ، حيث نختار الإشارة السالبة إذا كان $A \equiv 1 \pmod 4$ ونختار الإشارة الموجبة إذا كان $A \equiv 3 \pmod 4$.

برهان الجزء الأول من النظرية سهل نسبيًّا ، لكننا سنحذف البرهان لأننا سنبرهن نتيجة مماثلة لاحقاً. الجزء الثاني يعتبر أصعب ، لذلك نحن نحبذ توضيحه بمثال إضافي آخر. العدد الأولي $p = 130657$ يطابق 1 قياس 4. بالمحاولة والخطأ ، أو

باستخدام الكمبيوتر، أو بالطريقة المشروحة في الفصل السادس والعشرون، نكتب $130657 = 111^2 + 344^2$ كمجموع مربعين. الآن $111 \equiv 3 \pmod 4$ إذن نستنتج أن E_2 تقع عليه $130657 + 2 \cdot 111 = 130879$ نقطة قياس 130657.

لنرى الآن صديقنا القديم، المنحنى الناقصي

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

الجدول رقم (٤٥,٥). عدد النقاط قياس p والانحراف a_p للمنحنى E_1.

p	2	3	5	7	11	13	17	19	23	29
N_p	2	3	5	12	11	20	17	26	23	29
a_p	0	0	0	−5	0	−7	0	−7	0	0

p	31	37	41	43	47	53	59	61	67	71
N_p	42	48	41	56	47	53	59	48	62	71
a_p	−11	−11	0	−13	0	0	0	13	5	0

p	73	79	83	89	97	101	103	107	109	113
N_p	63	75	83	89	102	101	110	107	111	113
a_p	10	4	0	0	−5	0	−7	0	−2	0

تماماً كما فعلنا مع E_2، سننشئ جدولاً يُعطي عدد النقاط N_p قياس p والانحراف $a_p = p - N_p$. القيم معطاة في الجدول 45.5.

مرة أخرى، هناك العديد من الأعداد الأولية يكون لها الانحراف a_p يساوي صفراً:

$$p = 2, 3, 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101, 107, 113$$

هذه الأعداد الأولية لا تتبع أي نمط قياس 4، لكنها تتبع نمطاً قياس 3. فيما عدا العدد 3 نفسه، فإن هذه الأعداد جميعها تطابق 2 قياس 3. لذلك قد نخمن أنه إذا كان $p \equiv 2 \pmod 3$، فإن $N_p = p$. يمكننا استخدام الجذور الأولية للتحقق من أن هذا التخمين صحيح.

نظرية (٢, ٤٥).

إذا كان $p \equiv 2 \pmod 3$، فإن عدد النقاط N_p على المنحنى الناقصي $E_1 : y^2 = x^3 + 17$ قياس p تحقق $N_p = p$.

البرهان

قبل محاولة إعطاء برهان، دعنا نلقي نظرة على مثال. لنأخذ العدد الأولي $p = 11$. لإيجاد النقاط على E_1 قياس 11، نعوض $x = 0, 1, \ldots, 10$ في $x^3 + 17$ ونرى فيما إذا كانت القيمة مربعاً قياس 11. الجدول التالي يوضح ماذا يحدث عند التعويض:

$x \pmod{11}$	0	1	2	3	4	5	6	7	8	9	10
$x^3 \pmod{11}$	0	1	8	5	9	4	7	2	6	3	10
$x^3 + 17 \pmod{11}$	6	7	3	0	4	10	2	8	1	9	5

لاحظ أن الأعداد $x^3 \pmod{11}$ ما هي إلا الأعداد $0, 1, \ldots, 10$ بعد إعادة

ترتيبها، ونفس الشيء بالنسبة للأعداد $x^3+17 \pmod{11}$. لذلك عندما نبحث عن حلول :

$$y^2 \equiv 0^3+17 \pmod{11},\quad y^2 \equiv 1^3+17 \pmod{11},\quad y^2 \equiv 2^3+17 \pmod{11},$$
$$y^2 \equiv 3^3+17 \pmod{11},\quad \ldots \quad y^2 \equiv 10^3+17 \pmod{11},$$

فإن ما علينا إلا البحث عن حلول :

$$y^2 \equiv 0 \pmod{11},\quad y^2 \equiv 1 \pmod{11},\quad y^2 \equiv 2 \pmod{11},$$
$$y^2 \equiv 3 \pmod{11},\quad \ldots \quad y^2 \equiv 10 \pmod{11},$$

التطابق الأول $y^2 \equiv 0 \pmod{11}$ له حل واحد $y \equiv 0 \pmod{11}$. أما بالنسبة للتطابقات العشرة الأخرى، فكما نعلم من الفصل 23 أن نصف الأعداد من 1 إلى 10 تكون راسباً تربيعيًّا قياس 11 والنصف الآخر يكون راسباً غير تربيعي. لذلك فإن نصف التطابقات $y^2 \equiv a \pmod{11}$ لها حلان (تذكر أنه إذا كان b حلاً فإن $p-b$ حلاً أيضاً)، والنصف الآخر ليس له حل. لذلك، بشكل عام، يوجد $1+2\cdot 5=11$ حلاً.

إذا حاولت مع أمثلة أخرى، ستجد أن نفس الظاهرة تحدث. طبعاً، يجب أن تتمسك بالأعداد الأولية $p \equiv 2 \pmod 3$ ؛ لأن الوضع يختلف تماماً مع الأعداد الأولية $p \equiv 1 \pmod 3$، كما يمكنك التحقق من ذلك بنفسك من خلال حساب $x^3+17 \pmod 7$ عند $x=0,1,2,\ldots,6$.

لذلك سنحاول إثبات أنه إذا كان $p \equiv 2 \pmod 3$ فإن الأعداد :

$$0^3+17,\quad 1^3+17,\quad 2^3+17,\quad \ldots\ ,(p-1)^3+17 \pmod p$$

هي نفس الأعداد :

$$0,1,2,\ldots,p-1\pmod p$$

مع اختلاف الترتيب. لاحظ أن كل قائمة تضم بالضبط p من الأعداد. لذلك كل ما تحتاج عمله هو أن نبين أن الأعداد في القائمة الأولى متمايزة ؛ لأن هذا يعني أنها تشمل جميع أعداد القائمة الثانية.

لنفرض أننا أخذنا عددين من القائمة الأولى، ولنقل b_1^3+17 و b_2^3+17 ، ولنفرض أنهما متساويان قياس p. بكلمات أخرى، $b_1^3+17\equiv b_2^3+17\pmod p$ إذن $b_1^3\equiv b_2^3\pmod p$. إننا نريد أن نثبت أن $b_1=b_2$. إذا كان $b_1\equiv 0\pmod p$ ، فإن $b_2\equiv 0\pmod p$ ، والعكس بالعكس، لذلك يجوز لنا أيضاً أن نفترض أن $b_1\not\equiv 0\pmod p$, $b_2\equiv 0\pmod p$.

نريد الآن أن نأخذ الجذر التكعيبي لطرفي التطابق

$b_1^3\equiv b_2^3\pmod p$ ،

ولكن كيف؟ الجواب هو تطبيق نظرية فيرما الصغرى $b^{p-1}\equiv 1\pmod p$. أيضاً سنستخدم الفرض $p\equiv 2\pmod 3$ ، والذي يخبرنا أن 3 لا يقسم $p-1$. لذلك 3 , $p-1$ أوليان نسبياً، إذن من نظرية المعادلة الخطية (الفصل السادس) يمكننا إيجاد حل للمعادلة :

$$3u-(p-1)v=1$$

في الحقيقة، من السهل إيجاد الحل $u=(2p-1)/3$ و $v=2$. بالطبع، $(2p-1)/3$ عدد صحيح لأن $p\equiv 2\pmod 3$.

لاحظ أن $3u \equiv 1 \pmod{p-1}$ ، إذن يفهم من ذلك أن الرفع إلى القوة u^{th} هو نفسه الرفع للقوة $1/3$. (بمعنى ، أخذ جذر تكعيبي ، ربما لاحظت أننا طورنا هذه الفكرة في حالات أكثر تعميماً في الفصل السابع عشر). لذلك سنرفع طرفي التطابق $b_1^3 \equiv b_2^3 \pmod p$ للقوة u^{th} ونستخدم نظرية فيرما الصغرى لحساب

$$\begin{gathered}
\left(b_1^3\right)^u \equiv \left(b_2^3\right)^u \pmod p \\
b_1^{3u} \equiv b_2^{3u} \pmod p \\
b_1^{1+(p-1)v} \equiv b_2^{1+(p-1)v} \pmod p \\
b_1 \cdot \left(b_1^{p-1}\right)^v \equiv b_2 \cdot \left(b_2^{p-1}\right)^v \pmod p \\
b_1 \equiv b_2 \pmod p
\end{gathered}$$

هذا يثبت أن الأعداد $0^3+17, 1^3+17, \ldots, (p-1)^3+17$ جميعها مختلفة قياس p ، إذن يجب أن تساوي $0, 1, \ldots, p-1$ بترتيب ما.

لتلخيص ما سبق ، بينا أنه إذا عوضنا :

$$x = 0, 1, 2, \ldots, p-1$$

في $x^3 + 17 \pmod p$ ، سنحصل مرة أخرى على الأعداد :

$$0, 1, 2, \ldots, p-1 \pmod p$$

التطابق $y^2 \equiv 0 \pmod p$ له حل واحد : $y \equiv 0 \pmod p$. من جهة أخرى ، نصف التطابقات :

$$\begin{gathered}
y^2 \equiv 1 \pmod p, \quad y^2 \equiv 2 \pmod p, \quad y^2 \equiv 3 \pmod p, \ \ldots, \\
y^2 \equiv p-2 \pmod p, \quad y^2 \equiv p-1 \pmod p
\end{gathered}$$

لها حلان، والنصف الآخر ليس له حل؛ لذلك نصف الأعداد هي راسب تربيعي والنصف الآخر راسب غير تربيعي (انظر الفصل رقم 23). لذلك فإن المعادلة الديوفانتينية $y^2 = x^3 + 17$ لها بالضبط:

$$N_p = 1 + 2 \cdot \left(\frac{p-1}{2} \right) = p$$

حل قياس p.

الجدول رقم (٤٥,٦). عدد النقاط قياس p والانحراف a_p للمنحنى E_3.

p	2	3	5	7	11	13	17	19	23	29
N_p	2	4	4	9	10	9	19	19	24	29
a_p	0	−1	1	−2	1	4	−2	0	−1	0

p	31	37	41	43	47	53	59	61	67	71
N_p	24	34	49	49	39	59	54	49	74	74
a_p	7	3	−8	−6	8	−6	5	12	−7	−3

p	73	79	83	89	97	101	103	107	109	113
N_p	69	89	89	74	104	99	119	89	99	104
a_p	4	−10	−6	15	−7	2	−16	18	10	9

فهمنا الآن ماذا يحدث للنقاط على E_1 قياس p للأعداد الأولية $p \equiv 2 \pmod 3$. التمرين 45.3 يطلب منك اكتشاف نمط أكثر مكراً يكمن في a_p's عندما $p \equiv 1 \pmod 3$.

دعنا نتوقف لمراجعة الأنماط التي اكتشفناها. بالنسبة للمنحنيين الناقصيين E_2, E_1، وجدنا أن الانحراف $p - a_p$ يساوي 0 لحوالي نصف الأعداد الأولية، واستطعنا بدقة شديدة وصف هذه الأعداد الأولية التي لها انحراف $0 -$. للأعداد الأولية الأخرى رأينا أن a_p's تحقق نمطاً أكثر مكراً يحوي مربعات، وهو، $p - \left(a_p/2\right)^2$ وهو مربع كامل بالنسبة للمنحنى E_2، ويشبهه بعرض الشيء بالنسبة للمنحنى E_1 (انظر تمرين رقم 45.3). طبعاً، E_2, E_1 هما فقط منحنيان ناقصيان من بين منحنيات ناقصية لا تعد ولا تحصى، لذلك فإن اكتشافنا لأنماط مشتركة بين E_2, E_1 يدفعنا للبحث في مثال أو مثالين آخرين على الأقل. جدول رقم 45.6 يعطي عدد النقاط قياس p والانحرافات $p -$ للمنحنى الناقصي

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

يبدو أن هناك عدداً قليلاً جدًّا من الأعداد الأولية يكون لها الانحراف $p -$ يساوي صفر. حتى لو وسَّعنا جدول رقم 45.6 ، سنجد أن الأعداد الأولية $p < 5000$ التي لها $a_p = 0$ هي فقط.

$$p = 2, 19, 29, 199, 569, 809, 1289, 1439, 2539, 3319, 3559, 3919$$

جميع هذه الأعداد الأولية تطابق 9 قياس 10 ، لكن لسوء الحظ هناك الكثير من الأعداد الأولية تطابق 9 قياس 10 ، مثل $59, 79, 89, 109$ لم ترد في القائمة.

لا يظهر أن هناك نمطاً بسيطاً يتحكم بوجود هذه الأعداد الأولية في القائمة، وفي الحقيقة لم يستطيع أحد إيجاد نمط. بقي الوضع كذلك حتى عام 1937 عندما استطاع Noam Elkies أن يبرهن أن هناك دائماً عدداً لا نهائيًا من الأعداد الأولية يكون لها $a_p = 0$.

إن ندرة الأعداد الأولية التي لها $a_p = 0$ تجعلنا نحاول البحث عن أنماط تحوي مربعات، ولكن مرة أخرى نحن نبحث بدون جدوى، ولن يظهر نمط. في الواقع، إن ما سنجده إذا ما بحثنا في منحنيات ناقصية أخرى، هو أن معظمهم مثل E_3، لها قيم قليلة جدًّا a_p's تساوي صفراً ولا توجد أنماط تحوي مربعات. المنحنيان الناقصيان E_2, E_1 هما من نوع خاص جدًّا، إنهما منحنيان ناقصيان "بمضاعف مركب"[١] (complex multiplication). لن نعطي التعريف الدقيق، ولكن سنكتفي بالقول إن المنحنيات الناقصية بمضاعف مركب يكون نصف الـ a_p's لها يساوي صفراً، بينما المنحنيات الناقصية بدون مضاعف مركب يكون لها a_p's المساوية للصفر قليلة جدًّا.

تماريـــــن

(٤٥,١) (a) لكل عدد أولي p، ليكن M_p هو عدد الحلول قياس p للمعادلة $x^2 + y^2 = 1$. أوجد القيم M_3, M_5, M_{13}, M_{17}.

(مساعدة: هنا طريقة فعَّالة لحساب ذلك. أولاً، اعمل قائمة بجميع المربعات قياس p. ثانياً، عوض بكل القيم $0 \le y < p$ واختبر فيما إذا كان $1 - y^2$ مربعاً قياس p).

---

(١) يكون للمنحنى الناقصي مضاعف مركب إذا حققت معادلته نوعاً معيّنًا خاصًّا من خاصية التحويل. فمثلاً إذا كان (x, y) حلاً للمعادلة $y^2 = x^3 + x$، فإن الزوج $(x, -iy)$ يكون أيضاً حلاً. وجود أعداد مثل $i = \sqrt{-1}$ في هذه الصيغ قاد إلى التسمية " مضاعف مركب ".

(b) استخدم بياناتك من (a) والقيم $M_7 = 8$, $M_{11} = 12$ التي حسبتها سابقاً لعمل تخمين عن قيمة M_p. اختبر تخمينك بحساب M_{19}. وفقاً لتخمينك ، ما قيمة M_{1373} و M_{1987} ؟

(c) برهن أن تخمينك في (b) صحيح. (مساعدة : قد تساعدك الصيغ الواردة في الفصل الثالث).

(٤٥,٢) (a) أوجد جميع حلول المعادلة الديوفانتينية $y^2 = x^5 + 1$ قياس 7. كم عدد الحلول؟

(b) أوجد جميع حلول المعادلة الديوفانتينية $y^2 = x^5 + 1$ قياس 11. كم عدد الحلول؟

(c) ليكن p عدداً أوليًّا له الخاصية $p \not\equiv 1 \pmod 5$. برهن أن المعادلة الديوفانتينية $y^2 = x^5 + 1$ لها بالضبط p من الحلول قياس p.

(٤٥,٣) لكل عدد أولي $p \equiv 1 \pmod 3$ في الجدول للمنحنى E_1 ، أحسب المقدار $4p - a_p^2$. هل الأعداد التي تحسبها لها شكل خاص؟

(٤٥,٤) اكتب برنامجاً لحساب عدد حلول التطابق $E : y^2 \equiv x^3 + ax^2 + bx + c \pmod p$ باستخدام إحدى الطرق التالية :

(i) أولاً اعمل قائمة للمربعات قياس p ، ثم عوض $x = 0,1,\ldots,p-1$ في $x^3 + ax^2 + bx + c$ وانظر إلى الباقي قياس p. إذا كان مربعاً غير صفري ، أضف 2 إلى قائمتك ، إذا كان صفراً ، أضف 1 إلى قائمتك ، إذا لم يكن مربعاً ، تجاهله.

(ii) لكل $x = 0,1,\ldots,p-1$ احسب رمز لجندر $\left(\dfrac{x^3 + ax^2 + bx + c}{p}\right)$.

إذا كان $+1$ أضف 2 إلى قائمتك ، إذا كان -1 ، تجاهله. [وإذا كان

$x^3 + ax^2 + bx + c \equiv 0 \,(\bmod p)$ فأضف 1 لقائمتك].

استخدم برنامجك لحساب عدد النقاط N_p والانحراف $p-$ $a_p = p - N_p$ لكل منحنى من المنحنيات التالية ولكل عدد أولي $2 \le p \le 100$. أي منحنى (منحنيات) تعتقد أن له مضاعفاً مركباً؟

$(a)\ \ y^2 = x^3 + x^2 - 3x + 11$ $\qquad (c)\ \ y^2 = x^3 + 4x^2 + 2x$

$(b)\ \ y^2 = x^3 - 595x + 5586$ $\qquad (d)\ \ y^2 = x^3 + 2x - 7$

(٤٥,٥) في هذا التمرين سوف تكتشف نمط الانحرافات $p-$ للمنحنى الناقصي $E: y^2 = x^3 + 1$. سأعرض القائمة التالية لمساعدتك.

p	2	3	5	7	11	13	17	19	23	29
a_p	0	0	0	-4	0	2	0	8	0	0

p	31	37	41	43	47	53	59	61	67	71
a_p	-4	-10	0	8	0	0	0	14	-16	0

p	73	79	83	89	97	101	103	107	109	113
a_p	-10	-4	0	0	14	0	20	0	2	0

الانحراف a_p للمنحنى الناقصي $E: y^2 = x^3 + 1$

(a) اعمل تخميناً عن أي الأعداد الأولية يكون لها الانحراف $a_p = 0$، وبرهن أن تخمينك صحيح.

(b) للأعداد الأولية التي لها $a_p \neq 0$، احسب القيمة $4p - a_p^2$ واكتشف خصوصية هذه الأعداد.

(c) لكل عدد أولي $p < 113$ حيث $p \equiv 1 \pmod 3$ ، أوجد كل أزواج الأعداد الصحيحة

(A,B) التي تحقق $4p = A^2 + 3B^2$.(لاحظ أنه قد تكون هناك عدة حلول. فمثلاً $28 = 4 \cdot 7$ تساوي $4^2 + 3 \cdot 2^2$ و $5^2 + 3 \cdot 1^2$. من الطرق الفعَّالة لإيجاد الحلول هي حساب قيمة $4p - 3B^2$ لكل $B < \sqrt{4p/3}$ واختيار القيم التي تجعل $4p - 3B^2$ مربعاً كاملاً).

(d) قارن قيم B, A مع قيم a_p المعطاة في الجدول. اعمل تخميناً عن ماهية العلاقة بينهما.

(e) لكل عدد من الأعداد الأولية p التالية ، قُمْت بإعطائك زوجاً (A,B) يحقق $4p = A^2 + 3B^2$. استخدم تخمينك في (d) لتحزر قيمة a_p .

$(i)\ p = 541 \qquad (A,B) = (46,4),(29,21),(17,25)$

$(ii)\ p = 2029 \qquad (A,B) = (79,25),(77,27),(2,52)$

$(iii)\ p = 8623 \qquad (A,B) = (173,39),(145,67),(28,106)$