الفصل الرابع والعشرون

هل -1 مربع قياس p ؟ هل 2 ؟
Is -1 a Square Modulo p? Is 2 ?

في الفصل السابق أخذنا أعداداً أولية متنوعة p ، ورأينا قيم a التي كانت راسباً تربيعيًّا وقيم a التي كانت راسباً غير تربيعي ، على سبيل المثال ، عملنا جدولاً للمربعات قياس 13 ، واستخدمنا الجدول لنرى أن 3 و 12 هما QR قياس 13 ، بينما 2 و 5 هما NR قياس 13.

بالحفاظ على التقاليد الرياضية ، سنقلب الآن هذه المسألة رأساً على عقب. فبدلاً من أخذ عدد أولي محدد p ونكون قائمة لقيم a التي تكون QR و NR ، سنثبت قيمة a ونبحث عن أي الأعداد الأولية p يكون a بالنسبة له QR. لتوضيح ذلك ، سنبدأ مع القيمة الخاصة $a=-1$. إن السؤال الذي نريد الإجابة عنه هو :

لأي الأعداد الأولية p يكون -1 QR؟

يمكننا إعادة صياغة هذا السؤال بطرق أخرى ، مثل "لأي الأعداد الأولية p يكون للتطابق $x^2 \equiv -1 \pmod p$ حل؟ " و "لأي الأعداد الأولية p يكون $\left(\frac{-1}{p}\right)=1$ ؟".

كالعادة ، فإننا بحاجة لبعض البيانات قبل أن نتمكن من وضع أي فرضيات.

نستطيع الإجابة عن سؤالنا عند الأعداد الأولية الصغيرة بالطريقة التي تفتقر إلى الذكاء، وذلك بعمل جدول للقيم $1^2,2^2,3^2,\ldots,(\text{mod } p)$ ؛ ومن ثم نرى إذا كان أي من هذه الأعداد يطابق -1 قياس p . لذلك، وعلى سبيل المثال، -1 ليس مربعاً قياس 3 ؛ لأن $1^2 \not\equiv -1(\text{mod}\,3)$, ، $2^2 \not\equiv -1(\text{mod}\,3)$ ، بينما -1 مربع قياس 5 ؛ لأن $2^2 \equiv -1(\text{mod}\,5)$. وهنا قائمة لبعض قيم p .

p	3	5	7	11	13	17	19	23	29	31
حلول $x^2 \equiv -1(\text{mod}\,p)$	NR	2,3	NR	NR	5,8	4,13	NR	NR	12,17	NR

من هذا الجدول نستنتج أن:

١- راسباً تربيعيًّا للأعداد الأولية $p = 5,13,17,29$.

٢- راسباً غير تربيعي للأعداد الأولية $p = 3,7,11,19,23,31$.

ليس صعباً أن ندرك النمط. إذا كان p يطابق 1 قياس 4 ، فإن -1 يبدو راسباً تربيعيًّا قياس p ، إذا كان p يطابق 3 قياس 4 ، فإن -1 يبدو راسباً غير تربيعي. يمكن أن نعبر عن هذا الحدس باستخدام رموز لجندر:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & ,\mathit{if}\ \ p \equiv 1(\text{mod}\,4) \\ \\ -1 & ,\mathit{if}\ \ p \equiv 3(\text{mod}\,4) \end{cases}$$

دعنا نفحص تخميننا في حالات قليلة أخرى. العددان الأوليان اللاحقان 37 , 41 كلاهما يطابق 1 قياس 4 ومن المؤكد أن:

$x^2 \equiv -1 \pmod{37}$ لها الحلان :

$$x \equiv 6 \pmod{41} \quad , \quad x \equiv 31 \pmod{41}$$

و $x^2 \equiv -1 \pmod{41}$ لها الحلان :

$$x \equiv 9 \pmod{41} \quad , \quad x \equiv 32 \pmod{41}$$

نفس الشيء ، العددان الأوليان اللاحقان 43 , 47 كلاهما يطابق 3 قياس 4 وسنرى فيما إذا كان -1 راسباً غير تربيعي للعددين 43 , 47 . يبدو أن حدسنا جيد!

إن الأداة التي استخدمناها للتحقق من تخميننا يمكن تسميتها "الجذر التربيعي لنظرية فيرما الصغرى". قد تسأل، كيف يمكن أخذ الجذر التربيعي لنظرية؟ تذكر أن نظرية فيرما الصغرى (الفصل 9) تقول :

$$a^{p-1} \equiv 1 \pmod{p}$$

طبعاً، لن نأخذ الجذر التربيعي لهذه النظرية. ولكن، نأخذ الجذر التربيعي للمقدار a^{p-1} ونبحث عن قيمته. لذلك فإننا نريد الإجابة عن السؤال التالي :

ليكن $A = a^{(p-1)/2}$. ما قيمة A قياس p ؟

هناك شيء واضح . إذا ربعنا A ، فإن نظرية فيرما الصغرى تخبرنا أن :

$$A^2 = a^{p-1} \equiv 1 \pmod{p}$$

إذاً، p يقسم $A^2-1=(A-1)(A+1)$ ، لذلك، إما p يقسم $A-1$ وإما p يقسم $A+1$. (لاحظ خاصية الأعداد ألولية المثبتة في صفحة سابقة). إذاً A يجب أن يطابق $+1$ أو -1 .

هنا بعض القيم العشوائية للأعداد p , a , A . سنضمن في الجدول أيضاً قيمة رمز لجندر $\left(\frac{a}{p}\right)$ بهدف المقارنة. هل تلاحظ نمط؟

p	11	31	47	97	173	409	499	601	941	1223
a	3	7	10	15	33	78	33	57	222	129
$A(\bmod p)$	1	1	-1	-1	1	-1	1	-1	1	1
$\left(\frac{a}{p}\right)$	1	1	-1	-1	1	-1	1	-1	1	1

من الواضح أن $A\equiv 1(\bmod p)$ عندما تكون a راسباً تربيعيًّا و $A\equiv -1(\bmod p)$ عندما تكون a راسباً غير تربيعي . بكلمات أخرى، يبدو أن $A(\bmod p)$ له نفس قيمة رمز لجندر $\left(\frac{a}{p}\right)$. يمكننا استخدام الجذور الأولية لتأكيد هذه العبارة والتي سميت فيما بعد معيار أويلر.

نظرية (٢٤,١) (معيار أويلر)

ليكن p عدداً فرديًّا أوليًّا. فإن:

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

البرهان

ليكن g جذراً أوليًّا قياس p . كل عدد a يطابق قوة ما للعدد g ، ونعلم أيضاً أن a راسب تربيعي يطابق قوة زوجية للعدد g . دعنا نرى ماذا يحدث أولاً عندما يكون a راسباً تربيعيًّا ثم عندما يكون a راسباً غير تربيعي.

لذلك لنفرض أن a هو QR ، وهذا يعني أن $\left(\frac{a}{p}\right)=1$. حقيقة أن a هو QR يعني أن a قوة زوجية للعدد g ، أي $a \equiv g^{2k} \pmod p$. يمكن الآن استخدام نظرية فيرما الصغرى (الفصل 9) لحساب:

$$a^{(p-1)/2} \equiv \left(g^{2k}\right)^{(p-1)/2} \equiv \left(g^{p-1}\right)^{k} \equiv 1^{k} \equiv 1 \pmod p$$

لذلك، إذا كان a QR ؛ فإن $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p$.

بعد ذلك سنفرض أن a NR ؛ لذلك $\left(\frac{a}{p}\right)=-1$. بما أن a NR ؛ إذاً a قوة فردية للعدد g ، أي $a \equiv g^{2k+1} \pmod p$. مرة أخرى نستخدم نظرية فيرما الصغرى لحساب:

$$a^{(p-1)/2} \equiv \left(g^{2k+1}\right)^{(p-1)/2} \equiv \left(g^{p-1}\right)^{k} \cdot g^{(p-1)/2} \equiv g^{(p-1)/2} \pmod p$$

طبعاً $g^{(p-1)/2}$ سيطابق إما $+1$ وإما -1 قياس p . لكن g جذر أولي ، لذلك، فإن أصغر قوة للعدد g تطابق $+1$ هي القوة $(p-1)^{st}$. هذا يعني أن $g^{(p-1)/2}$ يجب أن يطابق -1 قياس p ، وهذا يبين أن:

$$a^{(p-1)/2} \equiv -1 \pmod p$$

وهذا يكمل برهان أن $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p$ عندما تكون a NR.

باستخدام معيار أويلر، يكون من السهل جداً تحديد فيما إذا كان -1 راسباً تربيعيًّا قياس p. فمثلاً، إذا أردنا أن نعرف فيما إذا كان -1 مربع قياس العدد الأولي $p = 6911$، فإننا نحتاج فقط لحساب:

$$(-1)^{(6911-1)/2} = (-1)^{3455} = -1$$

معيار أويلر يخبرنا أن:

$$\left(\frac{-1}{6911}\right) \equiv -1 \pmod{6911}$$

لكن $\left(\frac{a}{p}\right)$ دائماً إما $+1$ وإما -1 لذلك في هذه الحالة فإن $\left(\frac{-1}{6911}\right) = -1$.

لذلك، -1 راسب غير تربيعي قياس 6911.

نفس الشيء إذا كان $p = 7817$ ؛ نجد أن:

$$(-1)^{(7817-1)/2} = (-1)^{3908} = 1$$

لذلك، $\left(\frac{-1}{7817}\right) = 1$ ، لذلك -1 راسب تربيعي قياس 7817. لاحظ أنه على الرغم من أننا نعلم الآن أن التطابق:

$$x^2 \equiv -1 \pmod{7817}$$

له حل، فإننا ما زلنا لا نمتلك أي أسلوب فعَّال لإيجاد هذا الحل. الحلول هي:

هل -1 مربع قياس p ؟ هل 2 ؟

$$x \equiv 2564 \pmod{7817}$$

$$x \equiv 5253 \pmod{7817}$$

إن هذين المثالين يوضحان أن معيار أويلر يمكن استخدامه لنحدد بالضبط أي الأعداد الأولية يكون لها -1 راسباً تربيعيًّا. إن النتيجة الأنيقة التي تجيب عن السؤال الاستهلالي لعنوان هذا الفصل ، هي الجزء الأول من قانون التعاكس التربيعي.

نظرية (٢٤,٢) (التعاكس التربيعي)

(الجزء I) ليكن p عدداً فرديًّا أوليًّا. فإن:

١- -1 راسباً تربيعيًّا قياس p إذا كان $p \equiv 1 \pmod 4$ و

٢- -1 راسباً غير تربيعي قياس p إذا كان $p \equiv 3 \pmod 4$

بكلمات أخرى، باستخدام رمز لجندر،

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

البرهان

معيار أويلر يقول إن :

$$(-1)^{(p-1)/2} \equiv \left(\frac{-1}{p}\right) \pmod p$$

افرض أولاً أن $p \equiv 1 \pmod p$ ، قل إن $p = 4k + 1$ ؛ فإن :

$1 = {(-1)}^{2k} = {(-1)}^{(p-1)/2}$ إذاً $\left(\frac{-1}{p}\right) \equiv 1 \pmod p$.

لكن $\left(\frac{-1}{p}\right)$ إما $+1$ وإما -1 ، إذاً يجب أن يساوي 1.

هـذا يثبـت أنـه إذا كـان $p \equiv 3 \pmod 4$ ؛ فـإن $\left(\frac{-1}{p}\right) = 1$. بعـد ذلـك سنفرض أن $p \equiv 3 \pmod 4$. قل إن $p = 4k + 3$ فإن:

$${(-1)}^{(p-1)/2} = {(-1)}^{2k+1} = -1$$

إذاً $\left(\frac{-1}{p}\right) \equiv -1 \pmod p$.

إن هـذا يـبين أن $\left(\frac{-1}{p}\right)$ يجب أن تساوي -1 ، وبـذلك يكتمـل برهـان نظريـة التعاكس التربيعي (الجزء I).

يمكننا استخدام الجزء الأول من نظرية التعاكس التربيعي للإجابة عن سؤال ورد في الفصل 12 تركناه دون إجابة. كما تذكر، لقد بينا أن هناك عدداً لا نهائيًّا من الأعـداد الأولية تطابق 3 قياس 4 ، لكننـا تركنـا الإجابـة عـن السـؤال المنـاظر المتعلـق بالأعـداد الأولية المطابقة للعدد 1 قياس 4.

نظرية (٢٤,٣) (الأعداد الأولية قياس $1 \pmod 4$)

يوجد عدد لا نهائي من الأعداد الأولية التي تطابق 1 قياس 4.

البرهان

لنفرض أننا أُعطينا قائمة من الأعداد الأولية $p_1, p_2, \ldots, p_r$ ، جميعها تطابق 1 قياس 4 . سنذهب الآن لإيجاد عدد أولي جديد، ليس من ضمن قائمتنا، يطابق 1 قياس 4 . إعادة هذا الإجراء يعطي قائمة لأي طول مطلوب.

لنعتبر العدد:

$$A = (2p_1p_2\ldots p_r)^2 + 1$$

نعلم أن العدد A يمكن تحليله إلى حاصل ضرب أعداد أولية، ليكن:

$$A = q_1q_2\ldots q_s$$

من الواضح أن $q_1, q_2, \ldots, q_s$ ليست من ضمن قائمتنا الأصلية؛ لأن أي من p_i’s لا يقسم A . لذلك كل ما نحتاج عمله هو أن نبين أن واحداً على الأقل من q_i’s يطابق 1 قياس 4 . في الواقع ، سنرى أن جميعهم يحققون هذه الخاصية.

نلاحظ أولاً أن A عدد فردي، لذلك كل q_i’s فردي. ثم، كل q_i تقسم A ، لذلك:

$$(2p_1p_2\ldots p_r)^2 + 1 = A \equiv 0 \pmod{q_i}$$

هذا يعني أن $x = 2p_1p_2\ldots p_r$ حل للتطابق:

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

إذاً -1 راسب تربيعي قياس q_i . الآن، التعاكس التربيعي يخبرنا أن $q_i \equiv 1 \pmod 4$.

يمكننا استخدام الإجراء الوارد في هذا البرهان لنحصل على قائمة من الأعداد الأولية التي تطابق 1 قياس 4 . لذلك، إذا بدأنا بالعدد $p_1 = 5$ ؛ فإن $A = (2p_1)^2 + 1 = 101$ ، إذاً عددنا الأولي الثاني هو $p_2 = 101$. إذاً :

$$A = (2p_1p_2)^2 + 1 = 1020101$$

وهذا مرة أخرى عدد أولي ؛ لذلك عددنا الأولي الثالث هو $p_3 = 1020101$. سنعمل خطوة واحدة أخرى،

$$\begin{aligned} A &= (2p_1p_2p_3)^2 + 1 \\ &= 1061522231810040101 \\ &= 53.1613.12417062216309 \end{aligned}$$

لاحظ أن جميع الأعداد الأولية 53 , 1613 , 12417062216309 ، تطابق 1 قياس 4 .تماماً كما تنص النظرية.

وبعد أن أجبنا بنجاح على السؤال الأول الوارد في عنوان هذا الفصل، سنتجه الآن إلى السؤال الثاني ونعتبر $a = 2$ ، وهو العدد "الأغرب" كل الأعداد الأولية. كما فعلنا سابقاً مع $a = -1$ ، سنبحث الآن عن وصف بسيط للأعداد الأولية بحيث يكون 2 راسباً تربيعيًّا قياس p . هل يمكنك إيجاد نمط من البيانات التالية، حيث السطر $x^2 \equiv 2$ يعطي حلول $x^2 \equiv 2 (\bmod p)$ إذا كان 2 راسباً تربيعيًّا قياس p و NR إذا كان 2 راسباً غير تربيعي؟

p	3	5	7	11	13	17	19	23	29	31
$x^2 \equiv 2$	NR	NR	$3,4$	NR	NR	$6,11$	NR	$5,18$	NR	$8,23$

p	37	41	43	47	53	59	61	67	71	73
$x^2 \equiv 2$	NR	$17,24$	NR	$7,40$	NR	NR	NR	NR	$12,59$	$32,41$

p	79	83	89	97	101	103	107	109	113	127
$x^2 \equiv 2$	$9,70$	NR	$25,64$	$14,83$	NR	$38,65$	NR	NR	$51,62$	$16,111$

القائمة التالية تعطي الأعداد الأولية عندما يكون 2 راسباً تربيعيًّا والأعداد الأولية عندما يكون 2 راسباً غير تربيعي.

2 راسب تربيعي للقيم :

$$p = 7,17,23,31,41,47,71,73,79,89,97,103,113,127$$

2 راسب غير تربيعي للقيم :

$$p = 3,5,11,13,19,29,37,43,53,59,61,67,83,101,107,109$$

عندما $a = -1$ فصلنا صف التطابق للعدد p قياس 4 . هل هناك نمط مشابه إذا اختزلنا هاتين القائمتين للأعداد الأولية قياس 4 ؟ سنرى هنا ما سيحدث إذا عملنا ذلك.

$$7,17,23,41,47,71,73,79,89,97,103,113,127$$
$$\equiv 3,1,3,3,1,3,3,1,3,1,1,3,1,3 \pmod 4$$
$$3,5,11,13,19,29,37,43,53,59,61,67,83,101,107,109$$
$$\equiv 3,1,3,1,3,1,1,3,1,3,1,3,3,1,3,1 \pmod 4$$

وهذا لا يعد بالكثير. ربما يجب أن نحاول الاختزال قياس 3 .

$$7,17,23,41,47,71,73,79,89,97,103,113,127$$
$$\equiv 1,2,2,1,2,2,2,1,1,2,1,1,2,1 \pmod 3$$
$$3,5,11,13,19,29,37,43,53,59,61,67,83,101,107,109$$
$$\equiv 0,2,2,1,1,2,1,1,2,2,1,1,2,2,2,1 \pmod 3$$

وهذا لا يبدو أفضل. دعنا نحاول مرة واحدة أخرى قبل أن نتوقف عن المحاولة . ماذا سيحدث إذا اختزلنا قياس 8 ؟

$$7,17,23,41,47,71,73,79,89,97,103,113,127$$
$$\equiv 7,1,7,7,1,7,7,1,7,1,1,7,1,7 \pmod 8$$
$$3,5,11,13,19,29,37,43,53,59,61,67,83,101,107,109$$
$$\equiv 3,5,3,5,3,5,5,3,5,3,5,3,3,5,3,5 \pmod 8$$

يوريكا (كلمة إغريقية تعني وجدتها)! من المؤكد أن هذا لا يمكن أن يكون مصادفة ، وذلك أن يكون السطر الأول كله 1 و 7. والسطر الثاني كله 3 و 5 إن هذا يقترح القانون العام الذي مفاده أن 2 راسب تربيعي قياس p إذا كان p يطابق 1 أو 7 قياس 8 و 2 راسب غير تربيعي إذا كان p يطابق 3 أو 5 قياس 8. وباستخدام رموز لجندر :

$$\left(\frac{2}{p}\right)=\begin{cases}1 & \text{if} \quad p\equiv 1 \text{ or } 7 \pmod 8\\ \\ -1 & \text{if} \quad p\equiv 3 \text{ or } 5 \pmod 8\end{cases}$$

هل يمكننا استخدام معيار أويلر للتحقق من صحة تخميننا؟ لسوء الحظ، الجواب لا، أو على الأقل ليس بطريقة واضحة، حيث لا يبدو وجود طريقة واضحة لحساب $2^{(p-1)/2} \pmod p$. على كل حال، إذا رجعت للوراء وقمت بفحص برهاننا لنظرية فيرما الصغرى في الفصل التاسع، سترى أننا أخذنا الأعداد $1,2,\ldots,p-1$، كل منها مضروب بالعدد a، ومن ثم ضربناهم جميعهم في بعضهم البعض. وهذا أعطانا عامل للعدد a^{p-1}. لكي نستخدم معيار أويلر، نريد فقط $\frac{1}{2}(p-1)$ عاملاً للعدد a، لذلك بدلاً من أن نبدأ بكل الأعداد من 1 إلى p، فإننا نأخذ فقط الأعداد من 1 إلى $\frac{1}{2}(p-1)$. سنوضح هذه الفكرة، والتي ستساعدنا في التخمين، لتحديد فيما إذا كان 2 راسباً تربيعيًّا قياس 13.

نبدأ بنصف الأعداد من 1 إلى 12 : $1,2,3,4,5,6$. إذا ضربنا كل عدد بالعدد 2 ومن ثم ضربناهم مع بعضهم البعض؛ سنحصل على:

$$\begin{aligned} 2.4.6.8.10.12 &= (2.1)(2.2)(2.3)(2.4)(2.5)(2.6) \\ &= 2^6 \cdot 1.2.3.4.5 \cdot 6 \\ &= 2^6.6! \end{aligned}$$

لاحظ العامل للعدد $2^{(13-1)/2} = 2^6$، وهو بالفعل العدد الذي نبحث عنه.

إن فكرة "جاوس" هي أخذ الأعداد $2,4,6,8,10,12$ واختزال كل منها قياس 13 لنحصل على رقم يقع بين 6 و -6. أول ثلاثة تبقى نفسها، ولكننا نحتاج لطرح 13 من آخر ثلاثة لنحصل عليهم في هذا المدى. لذلك

$$\begin{array}{lll} 2 \equiv 2 \pmod{13} & 4 \equiv 4 \pmod{13} & 6 \equiv 6 \pmod{13} \\ 8 \equiv -5 \pmod{13} & 10 \equiv -3 \pmod{13} & 12 \equiv -1 \pmod{13} \end{array}$$

بضرب هذه الأعداد مع بعضها : نجد أن :

$$
\begin{aligned}
2.4.6.8.10.12 &\equiv 2.4.6.(-5)\cdot(-3).(-1) \\
&\equiv (-1)^3 \cdot 2.4.6.5.3.1 \\
&\equiv -6!\,(\bmod 13)
\end{aligned}
$$

بمساواة هاتين القيمتين للعدد $2.4.6.8.10.12\,(\bmod 13)$ ، نحصل على $2^6 \cdot 6! \equiv -6!\,(\bmod 13)$.

هذا يقتضي أن $2^6 \equiv -1\,(\bmod 13)$ ؛ لذلك معيار أويلر يخبرنا أن 2 راسباً غير تربيعي قياس 13.

دعنا نستخدم نفس الأفكار لنختبر فيما إذا كان 2 راسباً تربيعيًّا قياس 17. نأخذ الأعداد من 1 إلى 8 ، نضرب كل منها بالعدد 2 ، نضربهم ببعضهم البعض، ونحسب الناتج بطريقتين مختلفتين. الطريقة الأولى تعطي :

$$2.4.6.8.10.12.14.16 = 2^8 \cdot 8!$$

بالنسبة للطريقة الثانية، نختزل قياس 17 لنحصل على المدى من 8 إلى -8 . لذلك :

$$
\begin{array}{lll}
2 \equiv 2\,(\bmod 17) & 4 \equiv 4\,(\bmod 17) & 6 \equiv 6\,(\bmod 17) \\
8 \equiv 8\,(\bmod 17) & 10 \equiv -7\,(\bmod 17) & 12 \equiv -5\,(\bmod 17) \\
14 \equiv -3\,(\bmod 17) & 16 \equiv -1\,(\bmod 17) &
\end{array}
$$

بضرب هذه مع بعضها البعض نحصل على :

$$
\begin{aligned}
2.4.6.8.10.12.14.16 &\equiv 2.4.6.8(-7).(-5)\cdot(-3).(-1) \\
&\equiv (-1)^4 \cdot 8!\,(\bmod 17)
\end{aligned}
$$

لـــــــــذلك $(\bmod 17)\ 8! \cdot 4(-1) \equiv 8! \cdot 8^2$ ، إذاً $2^8 \equiv 1(\bmod 17)$
ولذلك 2 راسب تربيعي قياس 17.

لنفكر الآن في قليل من التعميم لطريقة جاوس. ليكن p أي عدد فردي أولي. لنجعل صيغتنا أكثر بساطة،

سنفرض أن:

$$P = \frac{p-1}{2}$$

سنبدأ بالأعداد الزوجية $2,4,6,\ldots,p-1$. بضربهم مع بعضهم البعض وأخذ 2 عاملاً مشتركاً من كل عدد نحصل على:

$$2\cdot 4\cdot 6\cdots(p-1) = 2^{(p-1)/2}\cdot 1\cdot 2\cdot 3\cdots\frac{p-1}{2} = 2^P\cdot P!$$

الخطوة التالية هي أخذ القائمة $2,4,6,\ldots,p-1$ واختزال كل عدد قياس p لــذلك؛ فإنــه ســيقع في المــدى مــن $-p$ إلى p ، أي، بــين $-(p-1)/2$ و $(p-1)/2$. الأعداد القليلة الأولى لن تتغير، ولكن عند نقطة معينة في القائمة سنبدأ بمواجهة أعداد أكبر من $(p-1)/2$ ، وكل عدد من هذه الأعداد الكبيرة يحتاج أن يكون العدد p مطروحاً منه. لاحظ أن عدد الإشارات السالبة يساوي بالضبط عدد المرات التي نحتاجها لطرح p . بكلمات أخرى،

عدد الإشارات السالبة $=$ $\left(\begin{array}{c}\text{عدد الأعداد الصحيحة في القائمة}\\ 2,4,6,\ldots,(p-1)\\ \text{الأكبر من } \frac{1}{2}(p-1)\end{array}\right)$

المثال التوضيحي التالي قد يساعد في شرح هذا الإجراء.

$$\underbrace{2.4.6.8.10.12\ldots}_{\text{أعداد } \le (p-1)/2} \; \underbrace{\ldots(p-5)\cdot(p-3)\cdot(p-1)}_{\text{أعداد } > (p-1)/2}$$

تترك بدون تغيير ــــ تحتاج لطرح p من كل منها

بمقارنة حاصلي الضرب، نحصل على :

$$2^{P}\cdot P! = 2\cdot 4\cdot 6\cdots(p-1) \equiv (-1)^{\text{Number of minus}}\cdot P!\pmod p$$

حذف $P!$ من الطرفين يعطي الصيغة الأساسية :

$$2^{(p-1)/2} \equiv (-1)^{\text{Number of minus}} \pmod p$$

(ملاحظة. القوة في التطابقين السابقين تعني : عدد الإشارات السالبة).

باستخدام هذه الصيغة، يمكن بسهولة التحقق من تخميننا السابق، وبذلك نكون قد أجبنا على السؤال الثاني المطروح في عنوان هذا الفصل.

نظرية رقم (٤,٢٤) (التعاكس التربيعي). (الجزء II)

ليكن p عدداً فرديًّا أوليًّا. فإن 2 راسب تربيعي قياس p ، إذا كان p يطابق 1 أو 7 قياس 8 ، و 2 راسب غير تربيعي قياس p إذا كان p يطابق 3 أو 5 قياس 8. وباستخدام رمز لجندر،

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } \; p \equiv 1 \;\; or \;\; 7 \pmod 8 \\ -1 & \text{if } \; p \equiv 3 \;\; or \;\; 5 \pmod 8 \end{cases}$$

البرهان

هناك أربع حالات تؤخذ بعين الاعتبار ، تعتمد على قيمة $p(\bmod 8)$. سنقوم بعمل اثنتين منهم ونترك الاثنتين الأخريين لك.

سنبدأ بالحالة $p \equiv 3(\bmod 8)$ ، ليكن $p = 8k + 3$. نحتاج لعمل قائمة بالأعداد $2,4,\ldots,p-1$ ومن ثم نحدد كم عدد منهم أكبر من $\frac{1}{2}(p-1)$.

في هذه الحالة $p-1 = 8k+2$ و $\frac{1}{2}(p-1) = 4k+1$ ، لذلك سيكون مكان القطع كما يشير الشكل التالي :

$$2.4.6\ldots4k \,\Big|\, (4k+2)\cdot(4k+4)\cdots(8k+2)$$

نحتاج الآن لمعرفة كم عدد موجود على يمين الشريط الرأسي. بمعنى آخر ، كم عدداً زوجيًّا يوجد بين $4k+2$ و $8k+2$ ؟ الجواب هو $2k+1$. (إذا لم يكن هذا واضحاً بالنسبة لك ، حاول مع بعض قيم k وسترى لماذا هذا صحيح). إن هذا يبين وجود $2k+1$ إشارة سالبة ، إذاً الصيغة الأساسية المعطاة سابقاً تخبرنا أن :

$$2^{(p-1)/2} \equiv (-1)^{2k+1} \equiv -1(\bmod p)$$

الآن ، معيار أويلر يقول إن 2 راسب غير تربيعي ، وبذلك نكون قد برهنا أن 2 راسب غير تربيعي لأي عدد أولي p يطابق 3 قياس 8.

بعد ذلك دعنا نرى الأعداد الأولية p التي تطابق 7 قياس 8 وليكن $p = 8k + 7$.

الآن ، الأعداد الزوجية $2,4,\ldots,p-1$ هي الأعداد من 2 إلى $8k+6$ ، والعدد الأوسط هو $\frac{1}{2}(p-1) = 4k+3$. مكان القطع في هذه الحالة هو :

$$2\cdot 4\cdot 6\cdots(4k+2)\,\Big|\,(4k+4)\cdot(4k+6)\cdots(8k+6)$$

هناك بالضبط $2k+2$ عدد على يمين الشريط الرأسي ، وبذلك نحصل على $2k+2$ إشارة سالبة. إذاً :

$$2^{(p-1)/2}\equiv(-1)^{2k+2}\equiv 1\pmod p$$

إذاً ، يخبرنا معيار أويلر أن 2 راسب تربيعي . وهذا يثبت أن 2 راسب تربيعي لأي عدد أولي p يطابق 7 قياس 8.

تمارين

(٢٤,١) حدد أي من هذه التطابقات لها حل. (جميع المقاييس أعداد أولية).

(a) $x^2\equiv -1\pmod{5987}$

(b) $x^2\equiv 6780\pmod{6781}$

(c) $x^2+14x-35\equiv 0\pmod{337}$

(d) $x^2-64x+943\equiv 0\pmod{3011}$

[مساعدة : بالنسبة للفقرة (c) ، استخدم الصيغة التربيعية لإيجاد ما هو العدد الذي تحتاجه لأخذ الجذر التربيعي بالنسبة للعدد 337 ، نفس الشيء بالنسبة للفقرة (d)].

(٢٤,٢) استخدم الإجراء المتبع في نظرية الأعداد الأولية $1\pmod 4$ لتوليد قائمة بالأعداد الأولية التي تطابق 1 قياس 4 ، ابدأ بالعدد $p_1=17$.

(٢٤,٣) هنا قائمة بالأعداد الأولية الأولى التي يكون لها العدد 3 راسباً تربيعيًّا وراسباً غير تربيعي.

راسب تربيعي :

$$p = 11,13,23,37,47,59,61,71,73,83,97,107,109$$

راسب غير تربيعي :

$$p = 5,7,17,19,29,31,41,43,53,67,79,89,101,103,113,127$$

حاول اختزال هذه القائمة قياس m لقيم متعددة للعدد m حتى تجد نمطاً ، وإعمل تخميناً يشرح أي الأعداد الأولية يكون لها العدد 3 راسباً تربيعيًّا.

(٢٤,٤) أكمل برهان نظرية التعاكس التربيعي (الجزء II) للحالتين الأخيرتين : الأعداد الأولية التي تطابق 1 قياس 8 والأعداد الأولية التي تطابق 5 قياس 8.

(٢٤,٥) استخدم نفس الأفكار التي استخدمناها لبرهان نظرية التعاكس التربيعي (الجزء II) لإثبات العبارتين التاليتين :

(a) إذا كان p يطابق 1 قياس 5 ، فإن 5 ؛ راسب تربيعي قياس p .

(b) إذا كان p يطابق 2 قياس 5 ، فإن 5 ؛ راسب غير تربيعي قياس p .

[مساعدة : اختزل الأعداد $5,10,15,\ldots,\frac{5}{2}(p-1)$ بحيث تقع في المدى من $-\frac{1}{2}(p-1)$ إلى $\frac{1}{2}(p-1)$ وافحص كم عدد منهم عدد سالب].

(٢٤,٦) افرض أن q عدد أولي يطابق 1 قياس 4 ، وافرض أن العدد $p = 2q + 1$ عدد أولي أيضاً. (مثال ، $q = 5$, $p = 11$). بيّن أن 2 جذر أولي قياس p .