الأعداد المربعة قياس p

Squares Modulo p

تعلمنا سابقاً كيف نحل التطابقات الخطية $ax \equiv c \pmod{m}$ ، (انظر الفصل الثامن)، وحان الوقت الآن لنتعامل مع المعادلات التربيعية. سوف نخصص الفصول الثلاثة القادمة للإجابة عن الأنواع التالية من الأسئلة:

هل العدد 3 يطابق مربع عدد ما قياس 7؟

هل التطابق $x^2 \equiv -1 \pmod{13}$ له حل؟

لأي الأعداد الأولية يكون للتطابق $x^2 \equiv 2 \pmod{p}$ حل؟

حتى الآن نستطيع الإجابة عن أول سؤالين. لنرى فيما إذا كان العدد 3 يطابق مربع عدد ما قياس 7 ، فيكفي أن نربع كل الأعداد من 0 إلى 6 ، مختزلة قياس 7 ، ونرى فيما إذا كان أي منهم يساوي 3. لذلك:

$$0^2 \equiv 0 \pmod{7}$$
$$1^2 \equiv 1 \pmod{7}$$
$$2^2 \equiv 4 \pmod{7}$$
$$3^2 \equiv 2 \pmod{7}$$
$$4^2 \equiv 2 \pmod{7}$$
$$5^2 \equiv 4 \pmod{7}$$
$$6^2 \equiv 1 \pmod{7}$$

obeikandi.com

نرى أن العدد 3 لا يطابق العدد المربع قياس 7. بنفس الأسلوب، إذا ربعنا كل عدد من 0 إلى 12 واختزلنا قياس 13 ، سنجد أن :

التطابق $x^2 \equiv -1 \pmod{13}$ له حلان،

$x \equiv 5 \pmod{13}$, $x \equiv 8 \pmod{13}$ (١)

b	b^2
0	0
1	1
2	4
3	4
4	1

Modulo 5

b	b^2
0	0
1	1
2	4
3	2
4	2
5	4
6	1

Modulo 7

b	b^2
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

Modulo 11

b	b^2
0	0
1	1
2	4
3	9
4	3
5	12
6	10
7	10
8	12
9	3
10	9
11	4
12	1

Modulo 13

(١) لسنوات عديدة خلال القرن التاسع عشر، كان الرياضيون غير مرتاحين لفكرة العدد $\sqrt{-1}$. كانت التسمية الجارية وقتها "عدد تخيلي" تعكس حالة القلق هذه عندهم. لكن إذا قمت بالعمل قياس العدد 13 ، على سبيل المثال، فإنك لن تجد أي لبس حول $\sqrt{-1}$. في الحقيقة، فإن 5 , 8 كليهما جذران تربيعيان للعدد -1 قياس 13.

كالمعتاد، نحتاج للنظر في بعض البيانات قبل أن نتمكن من ملاحظة أنماط ثم عمل تخمينات. هنا بعض الجداول التي تعطي كل التربيعات قياس p للقيم $p = 5,7,11,13$.

بعض الأنماط الهامة تظهر مباشرة من هذه القوائم. مثلاً، كل عدد (غير الصفر) يظهر مربعه مرتين بالضبط. فالعدد 5 هو كلا العددين 4^2 , 7^2 قياس 11، والعدد 3 هو كلا العددين 4^2 , 9^2 قياس 13. في الحقيقة، سنجد أن عمود التربيعات متناظر حول منتصفه.

كيف نستطيع وصف هذا النمط بصيغة ما؟

نقول إن مربع العدد b ومربع العدد $p-b$ قياس p هو نفس العدد. لكن الآن يمكننا وصف هذا النمط بصيغة يسهل إثباتها. لذلك:

$$(p-b)^2 = p^2 - 2pb + b^2 \equiv b^2 \pmod p$$

لذلك إذا أردنا وضع قائمة بكل الأعداد (غير الصفرية) بحيث تكون تربيعاتها قياس p، فإننا نحتاج فقط لحساب نصف هذه الأعداد:

$$1^2 \pmod p\ ,\ 2^2 \pmod p\ ,\ 3^2 \pmod p\ ,\ \ldots,\left(\frac{p-1}{2}\right)^2 \pmod p$$

إن هدفنا هو إيجاد أنماط يمكن استخدامها لتمييز المربعات من غير المربعات قياس P، أخيراً، نحن نتجه إلى واحدة من أجمل النظريات في نظرية الأعداد، قانون التعاكس التربيعي (the Law of quadratic reciprocity)، ولكن قبل ذلك يجب أن نطلق بعض الأسماء على الأعداد التي نريد دراستها.

العدد غير الصفري الذي يطابق مربع عدد قياس p يسمى الراسب التربيعي قياس p.

$\left(\text{a uadratic residue modulo p}\right)$. العدد الذي لا يطابق مربع عدد قياس p يسمى الراسب غير التربيعي قياس p (p (a quadratic) nonresideue modulo).

سنختصر هذه التسميات الطويلة بقولنا QR عن الراسب التربيعي و NR عن الراسب غير التربيعي. العدد الذي يطابق 0 قياس p لا يعتبر هذا ولا ذاك.

لتوضيح هذا المصطلح باستخدام البيانات من جداولنا، فإن 3 , 12 كليهما QR قياس 13 ، بينما 2 , 5 فكل منهما NR قياس 13.

لاحظ أن 2 , 5 كليهما NR ؛ لأنهما لا يظهران في قائمة التربيعات قياس 13. المجموعة الكاملة للأعداد QR قياس 13 هي $\{1,3,4,9,10,12\}$ ، والمجموعة الكاملة للأعداد NR قياس 13 هي $\{2,5,6,7,8,11\}$. نفس الشيء ، مجموعة الأعداد QR قياس 7 هي $\{1,2,4\}$ ، ومجموعة الأعداد NR قياس 7 هي $\{3,5,6\}$.

لاحظ أن هناك 6 أعداد راسب تربيعي و 6 أعداد راسب غير تربيعي قياس 13 ، كذلك فإن هناك 3 أعداد راسب تربيعي و 3 أعداد راسب غير تربيعي قياس 7. بالاعتماد على ملاحظتنا السابقة أن $(p-b)^2 \equiv b^2 \pmod{p}$ ، يمكننا أن نتحقق بسهولة من أن عدد الأعداد الراسب التربيعي يساوي عدد الأعداد الراسب غير التربيعي قياس أي عدد أولي (فردي).

نظرية (٢٣,١)

ليكن p عدداً أوليًّا فرديًّا. عندئذ هناك بالضبط $(p-1)/2$ راسباً تربيعيًّا قياس p ، وبالضبط $(p-1)/2$ راسباً غير تربيعي قياس p.

البرهان

الرواسب التربيعية هي الأعداد غير الصفرية التي تربيعاتها قياس p ؛ لذلك هي :

$$1^2, 2^2, \ldots, (p-1)^2 \pmod p$$

ولكن ، كما لاحظنا سابقاً ، فإننا نحتاج للذهاب إلى نصف الطريق فقط ،

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \pmod p$$

وحيث إن نفس الأعداد تعاود الظهور بترتيب مقلوب إذا ربعنا الأعداد الباقية :

$$\left(\frac{p+1}{2}\right)^2, \ldots, (p-2)^2, (p-1)^2 \pmod p$$

لذلك ؛ إذا أردنا أن نبين أن هناك بالضبط $(p-1)/2$ راسباً تربيعيًّا ، فإننا نحتاج لفحص فيما إذا كانت الأعداد $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ جميعها مختلفة قياس p .

لنفرض أن b_1, b_2 عددان بين 1 و $(p-1)/2$ ، ولنفرض أن $b_1^2 \equiv b_2^2 \pmod p$. نريد الآن أن نبين أن $b_1 = b_2$. بما أن $b_1^2 \equiv b_2^2 \pmod p$ ، فإن :

p يقسم $b_1^2 - b_2^2 = (b_1 - b_2)(b_1 + b_2)$.

على كل حال ، $b_1 + b_2$ يقع بين 2 و $p-1$ ، لذلك فإنه لا يقبل القسمة على p . إذاً p يقسم $b_1 - b_2$. لكن $|b_1 - b_2| < (p-1)/2$ ؛ لذلك فإن الاحتمال الوحيد ليكون $b_1 - b_2$ قابلاً للقسمة على p هو أن يكون $b_1 = b_2$. هذا

obeikandl.com

يبين أن الأعداد $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ جميعها مختلفة قياس p ، لذلك هناك بالضبط $(p-1)/2$ راسباً تربيعيًّا قياس p . الآن نحتاج فقط لملاحظة أن هناك $p-1$ عدد بين 1 و $p-1$ ، لذلك إذا كان نصفهم راسباً تربيعيًّا ، فإن النصف الآخر راسب غير تربيعي.

لنفرض أننا أخذنا راسبين تربيعيين وضربناهما ببعضهما. هل سنحصل على QR أو NR ، أو إننا نحصل أحياناً على أحدهما وفي أحيان أخرى على الآخر؟ على سبيل المثال، 3 , 10 هما QR قياس 13 ، وحاصل ضربهما $3 \cdot 10 = 30 \equiv 4$ هو مرة أخرى QR قياس 13. في الحقيقة، فإن هذا يجب أن يكون واضحاً بدون أي حسابات ؛ لأننا إذا ضربنا مربعين فإننا حتماً سنحصل على مربع.

يمكننا التحقق من ذلك كما يلي :

لنفرض أن a_1 , a_2 كليهما QR قياس p . إن هذا يعني أن هناك عددين b_1 , b_2 بحيث :

$$a_1 \equiv b_1^2 \pmod{p} \quad , \quad a_2 \equiv b_2^2 \pmod{p}.$$

بضرب هذين التطابقين مع بعضهما نحصل على $a_1 a_2 \equiv (b_1 b_2)^2 \pmod{p}$ ، ما يبين أن $a_1 a_2$ هو QR.

تكون الحالة أقل وضوحاً إذا قمنا بضرب عدد QR مع عدد NR أو إذا ضربنا عددين NR مع بعضهما. وفيما يلي بعض الأمثلة من جداولنا :

obeikandi.com

$QR \times NR \equiv ??\ (\mathrm{mod}\ p)$	
$2 \times 5 \equiv 3\ (\mathrm{mod}\ 7)$	NR
$5 \times 6 \equiv 8\ (\mathrm{mod}\ 11)$	NR
$4 \times 5 \equiv 7\ (\mathrm{mod}\ 13)$	NR
$10 \times 7 \equiv 5\ (\mathrm{mod}\ 13)$	NR

$NR \times NR \equiv ??\ (\mathrm{mod}\ p)$	
$3 \times 5 \equiv 1\ (\mathrm{mod}\ 7)$	QR
$6 \times 7 \equiv 9\ (\mathrm{mod}\ 11)$	QR
$5 \times 11 \equiv 3\ (\mathrm{mod}\ 13)$	QR
$7 \times 11 \equiv 12\ (\mathrm{mod}\ 13)$	QR

يبدو من هذه الأمثلة أن ضرب راسب تربيعي وراسب غير تربيعي يعطي راسباً غير تربيعي ، بينما ضرب راسبين غير تربيعيين دائماً يعطي راسباً تربيعيًّا. وبالرموز يمكننا أن نكتب :

$$QR \times QR = QR \quad , \quad QR \times NR = NR \quad , \quad NR \times NR = QR$$

لقد رأينا سابقاً أن العلاقة الأولى صحيحة. قبل أن نفحص العلاقتين الأخريين ، سنجري مناقشة مختصرة عن العلاقة بين الجذور الأولية والرواسب التربيعية.

ليكن g جذراً أوليًّا للعدد p . نظرية الجذر الأولي (الفصل الحادي والعشرون) تؤكد لنا وجود جذر أولي واحد على الأقل. عندئذ قوى g ،

$$g, g^2, g^3, \ldots, g^{p-3}, g^{p-2}, g^{p-1}$$

جميعها تعطي أعداداً غير صفرية قياس p . نحن نعلم أن نصفها رواسب تربيعية ونصفها الآخر لا. كيف يمكن أن نعرف أي النصفين هذا وأي النصفين ذاك؟

بلا شك أن g^2 هو QR ؛ لأنه مربع. نفس الشيء g^4 هو QR لأنه يساوي $(g^2)^2$ ، و g^6 هو QR لأنه يساوي $(g^3)^2$. إذاً، أي قوة زوجية للعدد g ، ولنقل g^{2k} هو QR ؛ لأنه يساوي $(g^k)^2$. إذاً، من المؤكد أن القوى الزوجية للعدد g هي QR.

في القائمة $g, g^2, \ldots, g^{p-1}$ ، نصف الأسس زوجية ونصفها فردية. رأينا أن هناك بالضبط $(p-1)/2$ راسباً تربيعيًّا قياس p ؛ لذلك فإن القوى الزوجية للعدد g يجب أن تعطي جميع الرواسب التربيعية. الأعداد المتبقية، القوى الفردية للعدد g ، لابد أنها الرواسب غير التربيعية.

هنا طريقة أخرى لقول نفس الشيء. نذكر أن دليل a قياس p (للجذر الأولي p) هو القوة $\mathrm{I}(a)$ والذي له الخاصية $a \equiv g^{\mathrm{I}(a)} \pmod{p}$. لذلك؛ فإن دليل a زوجي إذا كان a يطابق قوة زوجية للعدد g ، ودليل a فردي إذا كان a يطابق قوة فردية للعدد g .

الرواسب التربيعية هي تلك الأعداد a التي دليلها $\mathrm{I}(a)$ زوجي.

الرواسب غير التربيعية هي تلك الأعداد a التي دليلها $\mathrm{I}(a)$ فردي.

باستخدام هذا الوصف للرواسب التربيعية والرواسب غير التربيعية ، يمكننا الآن بسهولة أن نبرهن قوانين الضرب للرواسب التربيعية.

obeikandl.com

نظرية (٢٣,٢) (قانون ضرب الراسب التربيعي)

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

(i) حاصل ضرب راسبين تربيعيين قياس p يكون راسباً تربيعيًّا.

(ii) حاصل ضرب راسب تربيعي مع راسباً غير تربيعي يكون راسباً غير تربيعيًّا.

(iii) حاصل ضرب راسبين غير تربيعيين يكون راسباً تربيعيًّا.

هذه القوانين الثلاثة يمكن تلخيصها بالرموز من خلال الصيغ التالية:

$$QR\times QR=QR \quad , \quad QR\times NR=NR \quad , \quad NR\times NR=QR$$

البرهان

لأي عددين a , b أوليين نسبياً مع p ، فإن قانون ضرب الأدلة (فصل الثاني والعشرون) يقول:

$$\mathrm{I}(ab)\equiv \mathrm{I}(a)+\mathrm{I}(b)\pmod{p-1}$$

نلاحظ أن $p-1$ زوجي ؛ لأننا فرضنا أن p فردي أولي. وعليه يكون من الصحيح كحالة خاصة أن:

$$\mathrm{I}(ab)\equiv \mathrm{I}(a)+\mathrm{I}(b)\pmod{2}$$

[بكلمات أخرى، نعلم أن $p-1$ يقسم $\mathrm{I}(ab)-\mathrm{I}(a)-\mathrm{I}(b)$ و $p-1$ زوجي ؛ لذلك من المؤكد أن 2 يقسم $\mathrm{I}(ab)-\mathrm{I}(a)-\mathrm{I}(b)$].

يمكننا الآن اعتبار الحالات الثلاث للعددين a , b :

(i) إذا كـان a , b كلاهمـا راسـباً تربيعيًّـا، فـإن $\mathrm{I}(a)$, $\mathrm{I}(b)$ كليهمـا زوجي ، إذاً :

$$\mathrm{I}(ab) \equiv \mathrm{I}(a) + \mathrm{I}(b) \equiv 0 + 0 \equiv 0 \pmod{2}$$

لذلك $\mathrm{I}(ab)$ زوجي، إذاً ab راسب تربيعي.

(ii) إذا كـان a راسـباً تربيعيًّـا و b راسـباً غـير تربيعـي ؛ فـإن $\mathrm{I}(a)$ زوجـي و $\mathrm{I}(b)$ فردي، إذاً

$$\mathrm{I}(ab) \equiv \mathrm{I}(a) + \mathrm{I}(b) \equiv 0 + 1 \equiv 1 \pmod{2}$$

لذلك $\mathrm{I}(ab)$ فردي، إذاً ab راسب غير تربيعي.

(iii) أخيراً، إذا كان a , b كلاهما راسباً غير تربيعي ؛ فإن $\mathrm{I}(a)$, $\mathrm{I}(b)$ كليهما فردي، إذاً

$$\mathrm{I}(ab) \equiv \mathrm{I}(a) + \mathrm{I}(b) \equiv 1 + 1 \equiv 0 \pmod{2}$$

لذلك، $\mathrm{I}(ab)$ زوجي، إذاً ab راسب تربيعي.

هذا يكمل برهان قوانين ضرب الراسب التربيعي. الآن خذ دقيقة لتتأمل هذه القوانين:

$$QR \times QR = QR \quad , \quad QR \times NR = NR \quad , \quad NR \times NR = QR$$

هل هذه القوانين تذكرك بأي شيء؟ إذا كـان الجـواب لا ، فخـذ هـذه المسـاعدة . افرض أننا حاولنا استبدال الرمزين QR و NR بأعداد؟ أي الأعداد تصلح لذلك؟ هـذا صحيح، الرمز QR يبدو وكأنه $+1$ والرمز NR يبدو وكأنه -1 . لاحظ أن القانون الثالث غامض بعض الشيء، إن القانون الذي ينص على أن حاصل ضرب راسبين

غير تربيعين يكون راسباً تربيعيًّا، يعكس غموضاً مساوياً لغموض القانون $+1=(-1)\times(-1)$ [١].

بملاحظة أن سلوك الأعداد QR يشبه $+1$ وسلوك الأعداد NR يشبه سلوك -1، قام "أدرين- ماري ليجندر Adrien-Marie Legendre" بوضع القاعدة المفيدة التالية:

رمز لجندر للعدد a قياس p (The legendre symbol of a modulo p) هو:

$$\left(\frac{a}{b}\right)=\begin{cases}1, & \text{إذا كان } a \text{ راسباً تربيعيًّا قياس } p\\ -1, & \text{إذا كان } a \text{ راسباً غير تربيعي قياس } p\end{cases}$$

على سبيل المثال، إذا استخدمنا بعض البيانات من جداولنا السابقة، فإن:

$$\left(\frac{3}{13}\right)=1,\quad \left(\frac{11}{13}\right)=-1,\quad \left(\frac{2}{7}\right)=1,\quad \left(\frac{3}{7}\right)=-1$$

باستخدام رمز لجندر، فإن قوانين ضرب الراسب التربيعي يمكن استخدامها مباشرة من خلال صيغة مفردة.

---

(١) قد لا تعتبر أن الصيغة $+1=(-1)\times(-1)$ يكتنفها بعض الغموض؛ وذلك لأنها مألوفة بالنسبة لك. لكن من المؤكد أنك وجدتها كذلك عندما رأيتها للمرة الأولى. وإذا توقفت عن التفكير فيها، فإن هذا لا يبرر لماذا حاصل ضرب عددين سالبين يساوي بالضرورة عدداً موجباً. هل يمكن أن تعطي سبباً مقنعاً لماذا $(-1)\times(-1)$ يجب أن يساوي $+1$؟

نظرية (٢٣,٢) (قانون ضرب الراسب التربيعي)

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

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$$

إن رمز لجندر مفيد جداً في إنجاز الحسابات. مثلاً، إفرض أننا نريد معرفة فيما إذا كان 75 مربع قياس 97 أم لا. يمكننا أن نحسب:

$$\left(\frac{75}{97}\right)=\left(\frac{3\cdot5\cdot5}{97}\right)=\left(\frac{3}{97}\right)\left(\frac{5}{97}\right)\left(\frac{5}{97}\right)=\left(\frac{3}{97}\right)$$

لاحظ أنه من غير المهم فيما إذا كان $\left(\frac{5}{97}\right)$ هو $+1$ أو -1؛ لأنه يظهر مرتين، $(+1)^2=(-1)^2=1$ الآن نلاحظ أن $10^2\equiv3\pmod{97}$، إذاً 3 يكون QR لذلك:

$$\left(\frac{75}{97}\right)=\left(\frac{3}{97}\right)=1$$

طبعاً كنا محظوظين بقدرتنا على تمييز العدد 3 على أنه QR قياس 97. هل هناك طريقة لحساب رمز لجندر مثل $\left(\frac{3}{97}\right)$ دون الاعتماد على الحظ أو المحاولة والخطأ؟ الجواب نعم، ولكن ذلك الموضوع يناقش في فصل آخر.

تمارين

(٢٣,١) اعمل قائمة بكل الرواسب التربيعية وكل الرواسب غير التربيعية قياس 19.

(٢٣,٢) اكتب برنامجاً يأخذ عدداً أوليًّا p كَمُدُخَل، ويُعطي كمخرج العددين:

$A =$ مجموع كل الأعداد $1 \le a < p$ ، حيث a راسب تربيعي قياس p .

$B =$ مجموع كل الأعداد $1 \le a < p$ ، حيث a الراسب غير التربيعي قياس p .

على سبيل المثال، إذا كان $p = 11$ ، فإن الرواسب التربيعية هي :

$$1^2 \equiv 1 \pmod{11} \quad , \quad 2^2 \equiv 4 \pmod{11} \quad , \quad 3^2 \equiv 9 \pmod{11}$$
$$4^2 \equiv 5 \pmod{11} \quad , \quad 5^2 \equiv 3 \pmod{11}$$

إذاً :

$$A = 1 + 4 + 9 + 5 + 3 = 22 \quad , \quad B = 2 + 6 + 7 + 8 + 10 = 33$$

(a) اعمل قائمة للعددين A , B لكل الأعداد الأولية $p < 100$.

(b) ما قيمة $A + B$ ؟ برهن أن تخمينك صحيح.

(c) احسب $A \bmod p$ و $B \bmod p$. أوجد نمطاً وبرهن أنه صحيح.

(d) لأي أعداد أولية يكون $A = B$ ؟ بعد قراءة الفصل الرابع والعشرون، برهن أن تخمينك صحيح.

(e) إذا كان $A \ne B$ ، أيهما يميل لأن يكون أكبر A أم B ؟ حاول أن تبرهن أن تخمينك صحيح، لكن كن حذراً من أن هذا البرهان صعب جداً.

(٢٣,٣) يسمى عدد a راسباً تكعيبيًّا قياس p (a cubic residue modulo p) إذا كان مطابقاً لتكعيب قياس p [أي إذا وجد عدد ما بحيث $a \equiv b^3 \pmod{p}$].

(a) اعمل قائمة بكل الرواسب التكعيبية قياس 5 ، قياس 7 ، قياس 11 ، وقياس 13.

(b) أوجد عددين a_1 , b_1 ، بحيث لا يكون a_1 ولا b_1 راسباً تكعيبيًّا قياس 13 ، لكن $a_1 b_1$ راسب تكعيبي قياس 19. نفس الشيء، أوجد عددين a_2 , b_2

بحيث لا يكون أي من الأعداد الثلاثة a_2 , b_2 أو a_2b_2 راسباً تكعيبيًّا قياس 19 .

(c) إذا كان $p \equiv 2 \pmod 3$ ، اعمل تخميناً تعرف من خلاله أي قيم a تكون راسباً تكعيبيًّا. برهن أن تخمينك صحيح.

(d) إذا كان $p \equiv 1 \pmod 3$ ، بيّن أن a راسب تكعيبي قياس p فقط عندما يكون دليله $\mathrm{I}(a)$ يقبل القسمة على 3 .

obeikandl.com