التطابقـات
Congruences

تعتبر قابلية القسمة من الأدوات المهمة في نظرية الأعداد. وقد رأينا أهمية هذه الأداة عندما تحدثنا عن الثلاثيات الفيثاغورية ، القاسم المشترك الأعظم ، والتحليل إلى العوامل الأولية. في هذا الفصل سوف ندرس نظرية التطابقات. إن التطابقات تزودنا بطريقة فاعلة لوصف خصائص قابلية القسمة. في الحقيقة، إن التطابقات مقنعة وطبيعية بحيث تجعل نظرية قابلية القسمة شبيهة جداً بنظرية المعادلات.

نقول إن "a يطابق b قياس m" a is congruent to b modulo m

ويُعبر عن ذلك بالرمز

$$a \equiv b \pmod{m}$$

إذا كان m يقسم $a-b$. على سبل المثال،

$7 \equiv 2 \pmod{5}$ و $5 \mid (7-2)$ لأن $47 \equiv 35 \pmod{6}$ و $6 \mid (47-35)$

على وجه الخصوص، إذا كان حاصل قسمة a على m يعطينا باقي قسمة r فإن a مطابق لـ r قياس m. لاحظ أن الباقي يحقق $0 \le r < m$ ؛ وعليه فإن أي عدد صحيح مطابق (قياس m) لعدد صحيح بين 0 و $m-1$.

العدد m يسمى "مقياس" (*modulus*) التطابق. التطابقات التي لها نفس المقياس تتصرف في كثير من الأحيان كالمعادلات العادية. لذلك إذا كان $a_1 \equiv b_1 \pmod{m}$ و $a_2 \equiv b_2 \pmod{m}$ ؛ فإن:

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m} \quad \text{و} \quad a_1 a_2 \equiv b_1 b_2 \pmod{m}$$

تحذير:

ليس بالإمكان دائماً قسمة التطابقات. بمعنى آخر، إذا كان $ac \equiv bc \pmod{m}$، فليس صحيحاً بالضرورة أن تكون $a \equiv b \pmod{m}$. فمثلاً، $15 \cdot 2 \equiv 20 \cdot 2 \pmod{10}$، ولكن $15 \not\equiv 20 \pmod{10}$. والأكثر إثارة من ذلك أنه من الممكن أن يكون $uv \equiv 0 \pmod{m}$، ولكن $u \not\equiv 0 \pmod{m}$ و $v \not\equiv 0 \pmod{m}$.

فمثلاً، $6 \cdot 4 \equiv 0 \pmod{12}$. ولكن $6 \not\equiv 0 \pmod{12}$ و $4 \not\equiv 0 \pmod{12}$. على أي حال، إذا كان $\gcd(c,m) = 1$، فإنه من الممكن اختصار c من التطابق $ac \equiv bc \pmod{m}$. سيُطلب منك برهنة هذه الحقيقة في التمارين.

التطابقات التي تحتوي على مجاهيل يمكن حلها بنفس الطريقة التي تحل بها المعادلات. فمثلاً، لحل التطابق:

$$x + 12 \equiv 5 \pmod{8}$$

نطرح 12 من الطرفين لنحصل على:

$$x \equiv 5 - 12 \equiv -7 \pmod{8}$$

هـذا يعتـبر حـلاً جيـداً للتطـابق ، ومـن الممكـن اسـتبداله بالحـل المكـافئ $x \equiv 1 \pmod 8$. لاحـظ أن $7\ ,\ -1$ تعطـي نفـس العـدد قيـاس 8 ؛ لأن حاصـل طرحهم يقبل القسمة على 8 .

فيما يلي نقدم مثالاً آخر. لحل :

$$4x \equiv 3 \pmod{19}$$

نضرب الطرفين بـ 5 . هذا يعطينا :

$$20x \equiv 15 \pmod{19}$$

ولكـن $20 \equiv 1 \pmod{19}$ ؛ وعليـه فـإن $20x \equiv x \pmod{19}$. وبالتـالي ؛ فإن الحل هو $x \equiv 15 \pmod{19}$.

يمكننـا التحقـق مـن صـحة حلنـا بتعـويض 15 في التطـابق الأصـلي. هـل $4 \cdot 15 \equiv 3 \pmod{19}$ ؟ نعـم ؛ لأن $4 \cdot 15 - 3 = 57 = 3 \cdot 19$ يقبـل القسـمة على 19.

لاحظ أننا حللنا التطابق السابق باستخدام خدعة بسيطة ، لكن إذا لم تستطع حل التطابق ، فهناك دائماً ما يعرف بأسلوب "تسلق كل جبل". لحل أي تطابق قياس m ، جرب كل قيمة من القيم $0,1,\ldots,m-1$ لكل متغير. مثلاً ، لحل التطابق :

$$x^2 + 2x - 1 \equiv 0 \pmod{7}$$

فما علينا إلى أن نحاول مع القيم $x = 0\ ,\ x = 1,\ldots,x = 6$. هذا يقودنا إلى الحلين $x \equiv 2 \pmod{7}$ و $x \equiv 3 \pmod{7}$. بالطبع ، يوجد هناك حل آخر مثل $x \equiv 9 \pmod{7}$ ولكن $9\ ,\ 2$ ليسا حلين مختلفين في الحقيقة ؛ لأنهما نفس العدد قياس 7 . لذلك عندما نتكلم عن "إيجاد جميع الحلول لتطابق ما" ، فإننا نعني إيجاد

جميع الحلول غير المتطابقة، أي جميع الحلول التي لا تطابق بعضها بعضاً.

نلاحظ أيضاً أن هناك العديد من التطابقات التي ليس لها حل مثل $x^2 \equiv 3 \pmod{10}$. وهذا لا يجب أن يكون مفاجئاً، فقبل كل شيء هناك معادلات عادية مثل $x^2 = -1$ ليس لها حلول (حقيقية).

مهمتنا الأخيرة في هذا الفصل هي حل التطابق الذي على الصورة :

$$ax \equiv c \pmod{m}.$$

بعض التطابقات من هذا النوع ليس لها حل. مثلاً، إذا كان التطابق :

$$6x \equiv 15 \pmod{514}$$

له حل، فإن 514 يجب أن يقسم $6x - 15$. لكن $6x - 15$ دائماً عدد فردي؛ وعليه فإنه لا يقبل القسمة على العدد الزوجي 514. لذلك فإن التطابق $6x \equiv 15 \pmod{514}$ ليس له حل.

قبل الحديث عن الجانب النظري، لنجرب المثال التالي. سنقوم بحل التطابق :

$$18x \equiv 8 \pmod{22}$$

هذا يعني أننا بحاجة إلى إيجاد قيمة لـ x بحيث أن 22 يقسم $18x - 8$، بمعنى، أن علينا إيجاد قيمة لـ x، بحيث $18x - 8 = 22y$ و y عدد صحيح. بكلمات أخرى، نحن بحاجة لحل المعادلة الخطية :

$$18x - 22y = 8$$

ونعرف من دراستنا للفصل السادس أنه بإمكاننا حل المعادلة :

$$18u - 22v = \gcd(18, 22) = 2$$

وبسهولة نجد أن الحل هـو $u = 5$, $v = 4$. ولكننـا نريـد أن يكـون الطـرف الأيمن للمعادلة 8 وليس 2. وعليه نضرب في 4 لنحصل على:

$$18 \cdot (5 \cdot 4) - 22 \cdot (4 \cdot 4) = 8$$

لـذا $18 \cdot 20 \equiv 8 \pmod{22}$ ، وعليـه فـإن $x \equiv 20 \pmod{22}$ هـو الحـل للتطابق الأصلي. قريباً سنرى أن هذا التطابق له حلان مختلفـان قيـاس 22 ; أحـدها هـو الحل $x \equiv 9 \pmod{22}$.

افرض الآن أنه طلب منا حل تطابق ما على الصورة:

$$ax \equiv c \pmod{m}$$

نحـن نحتـاج إلى إيجـاد عـدد صـحيح x بحيـث m يقسـم $ax - c$. العـدد m سيقسـم $ax - c$ إذا اسـتطعنا إيجـاد عـدد صـحيح y بحيـث $ax - c = my$. بإعـادة ترتيب المعادلة الأخيرة نستطيع أن نستنتج أن $ax \equiv c \pmod{m}$ لها حل إذا وفقط إذا كان للمعادلة الخطية $ax - my = c$ حل. يبـدو أن هـذا مـألوف لنـا; إنهـا تمامـاً نفـس المسألة التي قمنا بحلها في الفصل السادس.

لجعـل الصـيغ أكثـر إتقانـاً، سـوف نفـرض أن $g = \gcd(a, m)$. ملاحظتنـا الأولى هـي أن أي عـدد علـى الشـكل $ax - my$ هـو أحـد مضـاعفات g ، وعليـه إذا كـان g لا يقسـم c ، فـإن $ax - my = c$ لـيس لهـا حـل وبالتـالي فـإن $ax \equiv c \pmod{m}$ ليس لها حل أيضاً.

بعد ذلك نفرض أن g يقسم c. نعرف من نظرية المعادلة الخطية في الفصل السادس أنه يوجد دائماً حل للمعادلة :

$$au + mv = g$$

افرض أن حل هذه المعادلة هو $u = u_0 \ , \ v = v_0$ ، إما بالمحاولة والخطأ وإما باستخدام طريقة الخوارزمية الإقليدية المشروحة في الفصل السادس. بما أننا فرضنا أن g يقسم c فبإمكاننا ضرب هذه المعادلة بالعدد الصحيح c/g لنحصل على المعادلة:

$$a\frac{cu_0}{g} + m\frac{cv_0}{g} = c$$

وهذا يعني أن:

$$x_0 \equiv \frac{cu_0}{g} (\mathrm{mod}\, m)$$

هو حل التطابق $ax \equiv c \left(\mathrm{mod}\, m\right)$.

هل هناك حل آخر؟ افرض أن x_1 هو حل آخر للتطابق $ax \equiv c \left(\mathrm{mod}\, m\right)$. إذن $ax_1 \equiv ax_0 \left(\mathrm{mod}\, m\right)$، وعليه فإن m يقسم $ax_1 - ax_0$. هذا يقتضي أن:

$\frac{a\left(x_1 - x_0\right)}{g}$ يقسم $\frac{m}{g}$،

بما أننا نعرف أن m/g و a/g ليس لهما عوامل مشتركة، فإن m/g يجب أن يقسم $x_1 - x_0$. بعبارة أخرى، يوجد عدد k بحيث:

$$x_1 = x_0 + k \cdot \frac{m}{g}$$

لكن أي حلين الفرق بينهما أحد مضاعفات m يعتبران نفس الحل، وعليه سيكون هناك بالضبط g من الحلول المختلفة، والتي يمكن الحصول عليها بأخذ $k = 0,1,\ldots,g-1$.

بهذا يكتمل تحليلنا للتطابق $ax \equiv c \pmod{m}$. سنلخص ما توصلنا إليه بالنظرية التالية.

نظرية (٨,١) (نظرية التطابق الخطي).

ليكن a , c ، و m أعداداً صحيحة، حيث $m \geq 1$ ، وليكن $g = \gcd(a, m)$.

a. *إذا كان $g \nmid c$ ؛ فإن التطابق $ax \equiv c \pmod{m}$ ليس له حل.*

b. *إذا كان $g \mid c$ ؛ فإن التطابق $ax \equiv c \pmod{m}$ له بالضبط g من الحلول غير المتطابقة. لإيجاد الحلول، أولاً أوجد حل (u_0, v_0) للمعادلة الخطية:*

$$au + mv = g$$

(طريقة حل هذه المعادلة مشروحة في الفصل السادس).

عندئذ يكون $x_0 = cu_0 / g$ حلاً للتطابق $ax \equiv c \pmod{m}$ ، وأما بقية الحلول غير المتطابقة تعطى بالعلاقة :

$$x \equiv x_0 + k \cdot \frac{m}{g} \pmod{m} \quad , \quad k = 0, 1, 2, \ldots, g-1$$

على سبيل المثال، التطابق $943x \equiv 381 \pmod{2576}$ ليس له حلول ؛ لأن $\gcd(943, 2576) = 23$ لا يقسم 381. من جهة أخرى، فإن التطابق :

$$893x \equiv 266 \pmod{2432}$$

له 19 حلاً ، لأن $\gcd\left(893,2432\right)=19$ يقسم 266. لاحظ أننا استطعنا معرفة عدد الحلول دون أن نضطر لحساب أي منها. لإيجاد الحلول نقوم أولاً بحل :

$$893u-2432v=19$$

مستخدمين الطريقة التي تعلمناها في الفصل السادس ، نجد الحل $\left(u,v\right)=\left(79,29\right)$. والضرب بـ $266/19=14$ يعطينا الحل $\left(x,y\right)=\left(1106,406\right)$ للمعادلة $893x-2432y=266$

أخيراً، مجموعة الحل الكاملة للتطابق :

$$893x\equiv 266\left(\mathrm{mod}\,2432\right)$$

تستنبط بداية بالتطابق $x\equiv 1106\left(\mathrm{mod}\,2432\right)$ وإضافة مضاعفات المقدار $2432/19=128$. (لا تنسى أنه إذا كانت الأعداد أكثر من 2432 فبإمكاننا طرح 2432). التسعة عشر حلاً غير المتطابقة هي :

$$1106,1234,1362,1490,1618,1746,1874,2002,2130,2258,$$
$$2386,82,210,338,466,594,722,850,978$$

ملاحظة مهمة:

أهم حالة من حالات نظرية التطابق الخطي هي عندما يكون $\gcd\left(a,m\right)=1$. في هذه الحالة تنص النظرية على أن التطابق :

$$ax\equiv c(\mathrm{mod}\,m) \qquad (*)$$

له حل واحد فقط. بإمكاننا أيضاً كتابة الحل على شكل كسر :

$$x \equiv \frac{c}{a} \pmod{m}$$

لكـن إن فعلنـا ذلـك، فيجـب أن نتـذكر أن الرمـز "$\frac{c}{a} \pmod{m}$" هـو فقـط اختزال مناسب لحل التطابق (*).

تماريـــــن

(٨,١) افرض أن $a_1 \equiv b_1 \pmod{m}$ و $a_2 \equiv b_2 \pmod{m}$.

(a) تحقـــــــــق مـــــــــن أن $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$ وأن

$$a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$$

(b) تحقق من أن $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

(٨,٢) افرض أن $ac \equiv bc \pmod{m}$ وافرض أيضاً أن $\gcd(c,m) = 1$. برهن أن $a \equiv b \pmod{m}$.

(٨,٣) أوجد جميع الحلول غير المتطابقة لكل من التطابقات التالية:

$(a)\ 7x \equiv 3 \pmod{15}$ $(b)\ 6x \equiv 5 \pmod{15}$

$(c)\ x^2 \equiv 1 \pmod{8}$ $(d)\ x^2 \equiv 2 \pmod{7}$

$(e)\ x^2 \equiv 3 \pmod{7}$

(٨,٤) برهن أن اختبارات قابلية القسمة التالية تعمل:

(a) العدد a يقبل القسـمة علـى 4 إذاً وفقـط، إذا كـان العـدد المكـون مـن آخـر خانتين فيه يقبل القسمة على 4.

(b) العدد a يقبل القسـمة علـى 8 إذاً وفقـط، إذا كـان العـدد المكـون مـن آخـر خانتين فيه يقبل القسمة على 8.

(c) العـدد a يقبـل القسـمة علـى 3 إذاً وفقـط، إذا كـان مجمـوع خاناتـه يقبـل القسمة على 3.

(d) العدد a يقبل القسمة على 9 إذاً وفقط، إذا كان مجموع خاناته يقبل القسمة على 9.

(e) العدد a يقبل القسمة على 11 إذاً وفقط، إذا كان مجموع خاناته التبادلي يقبل القسمة على 11. (إذا كانت خانات a هي $a_1a_2a_3\ldots a_{d-1}a_d$ ، فإن المجموع التبادلي يعني أخذ $a_1 - a_2 + a_3 - \cdots$ أي بالتبادل بين إشارة الزائد وإشارة الناقص.

[مساعدة: بالنسبة للفقرة (a) ، اختزل قياس 100 ، وكذلك نفس الشيء بالنسبة للفقرة (b) . بالنسبة للفقرات (c) ، (d)، و (e) ، اكتب a كمجموع مضاعفات قوى العدد 10 واختزل قياس $11,9,3$].

(٨,٥) أوجد جميع الحلول غير المتطابقة لكل من التطابقات الخطية التالية.

$$(a) \quad 8x \equiv 6 \pmod{14}$$
$$(b) \quad 66x \equiv 100 \pmod{121}$$
$$(c) \quad 21x \equiv 14 \pmod{91}$$

(٨,٦) حدد عدد الحلول غير المتطابقة لكل من التطابقات التالية. لست مضطراً لكتابة هذه الحلول.

$$(a) \quad 72x \equiv 47 \pmod{200}$$
$$(b) \quad 4183x \equiv 5781 \pmod{15087}$$
$$(c) \quad 1537x \equiv 2863 \pmod{6731}$$

(٨,٧) اكتب برنامجاً يحل التطابق :

$$ax \equiv c \pmod{m}$$

[إذا كان $\gcd(a,m)$ لا يقسم c ، اجعل البرنامج يُعطي رسالة خطأ ويُعطي قيمة $\gcd(a,m)$].