الفصل الخامس

قابلية القسمة والقاسم المشترك الأكبر
Divisibility and the Greatest Common Divisor

رأينا خلال دراستنا للثلاثيات الفيثاغورية أن مفاهيم قابلية القسمة والتحليل تعتبر من الأدوات المهمة لدراسة نظرية الأعداد. في هذا الفصل سوف نتعرف على هذه الأفكار بشكل أكثر عمقاً.

افرض أن m و n عددان صحيحان و $m \neq 0$. نقول إن m يقسم n إذا كان n من مضاعفات m، بمعنى أنه يوجد عدد صحيح k بحيث $m = nk$. إذا كان m يقسم n فإننا نعبر عن ذلك بالرمز $n \mid m$. بينما إذا كان m لا يقسم n فإننا نعبر عن ذلك بالرمز $m \nmid n$. على سبيل المثال $6 \mid 3$ و $132 \mid 12$ لأن $3 \cdot 2 = 6$ و $12 \cdot 11 = 132$. من جهة أخرى، فإن $7 \nmid 5$ لأنه لا يوجد عدد صحيح من مضاعفات 5 يساوي 7. إن العدد الذي يقسم n يسمى قاسماً(divisor) لـ n.

إذا كان لدينا عددان فإنه من الممكن البحث عن قواسم مشتركة لهذين العددين بمعنى إيجاد الأعداد التي تقسم كليهما. على سبيل المثال العدد 4 قاسم مشترك لكل من 12 و 20 ؛ لأن $12 \mid 4$ و $20 \mid 4$. لاحظ أن 4 هو أكبر قاسم مشترك لكل من 12 و 20. وكمثال آخر، فإن 3 قاسم مشترك لكل من 18 و 30 ، لكنه ليس أكبر

قاسم مشترك ؛ لأن 6 أيضا قاسم مشترك. إن القاسم المشترك الأكبر لعددين هو مفهوم مهم جدا ، وسيمر معنا مرارا وتكرارا أثناء دراستنا لنظرية الأعداد ، ولهذا سنفرد له التعريف التالي :

القاسم المشترك الأكبر لعددين (a و b (The greatest common divisor for a and b) (ليس كلاهما صفرا) هو أكبر عدد يقسم كلا العددين ، ويرمز له بالرمز $\gcd(a,b)$.

إذا كان $\gcd(a,b) = 1$ نقول إن a و b عددان أوليان نسبياً (relatively prime).

المثالان المذكوران أعلاه يمكن التعبير عنهما كما يلي :

$$\gcd(12,20) = 4 \quad \text{و} \quad \gcd(18,30) = 6.$$

مثال آخر هو :

$$\gcd(225,120) = 15$$

يمكننا التأكد من أن هذه الإجابة صحيحة بتحليل $225 = 3^2 \cdot 5^2$ و $120 = 2^3 \cdot 3 \cdot 5$ ، لكن بشكل عام ، تحليل a و b ليست طريقة فعّالة لحساب القاسم المشترك الأكبر لهما.[١]

أكثر طريقة فعّالة معروفة لإيجاد القاسم المشترك الأكبر لعددين تسمى "خوارزمية إقليدس" (Euclidean algorithm). وتتم بعمل متتالية قواسم مع البواقي حتى يصبح الباقي صفراً. سوف نوضح هذه الطريقة بمثالين قبل وصفها بشكل عام.

سنحسب $\gcd(36,132)$. الخطوة الأولى هي قسمة 132 على 36 ، ويكون الناتج 3 والباقي 24. نكتب ذلك على الشكل :

$$132 = 3 \times 36 + 24.$$

---

(١) من الطرق الأقل فاعلية لحساب القاسم المشترك الأكبر لعددين a و b هي الطريقة التي تُدرسها المعلمة لابنتي في الصف الرابع ، حيث تطلب من الطالبات عمل قائمتين كاملتين بجميع قواسم العددين a و b ثم يؤخذ أكبر عدد يظهر في كلتا القائمتين!

الخطوة التالية هي أخذ 36 وقسمته على الباقي 24 الذي حصلنا عليه من الخطوة السابقة. هذا يعطي $36 = 1\times 24 + 12$.

بعد ذلك نقسم 24 على 12 ، لنجد الباقي 0 $24 = 2\times 12 + 0$.

خوارزمية إقليدس تقول أنه عندما تحصل على الباقي 0 ؛ فإن الباقي الذي حصلت عليه من الخطوة السابقة هو القاسم المشترك الأكبر للعددين الأصليين. لذلك نجد في هذه الحالة أن $\gcd(36,132) = 12$.

دعنا نأخذ مثالاً كبيراً. سوف نحسب :

$$\gcd(1160718174, 316258250)$$

هدفنا من حل مثال كبير مثل هذا هو إقناعك أن خوارزمية إقليدس هي طريقة فعّالة أكثر لحساب القاسم المشترك الأكبر من طريقة التحليل. نبدأ بقسمة 1160718174 على 316258250 فيكون ناتج القسمة 3 وباقي القسمة 211943424 . الخطوة التالية هي قسمة 316258250 على 211943424 . نستمر في هذه العملية حتى نحصل على الباقي 0 كما هو موضح في الجدول التالي :

$$\begin{aligned}
1160718174 &= 3\times 316258250 + 211943424\\
316258250 &= 1\times 211943424 + 104314826\\
211943424 &= 2\times 104314826 + 3313772\\
104314826 &= 31\times 3313772 + 1587894\\
3313772 &= 2\times 1587894 + 137984\\
1587894 &= 11\times 137984 + 70070\\
137984 &= 1\times 70070 + 67914\\
70070 &= 1\times 67914 + 2156\\
67914 &= 31\times 2156 + 1078 \leftarrow \gcd\\
2156 &= 2\times 1078 + 0
\end{aligned}$$

لاحظ أننا في كل خطوة قمنا بقسمة العدد A على العدد B لنحصل على ناتج القسمة Q وباقي القسمة R. بعبارة أخرى:

$$A = Q \times B + R.$$

في الخطوة التالية قمنا بتبديل A و B القديمتين بالعددين B و R، ونستمر في هذه العملية حتى نحصل على باقي 0. عند ذلك يكون الباقي R الذي حصلنا عليه من الخطوة السابقة هو القاسم المشترك الأكبر للعددين الأصليين. أي أن

$$\gcd(1160718174, 316258250) = 1078.$$

بإمكاننا التأكد من صحة الحل (وهذه خطوة جيده دائما) بإثبات أن 1078 هو فعلا قاسم مشترك على النحو التالي:

$$1160718174 = 1078 \times 1076733$$

و

$$316258250 = 1078 \times 293375.$$

بقي هناك شيء واحد مهم تجب الإشارة إليه قبل البدء بالتحليل النظري لخوارزمية إقليدس. إذا كان لدينا العددان A و B فكيف نحصل على ناتج القسمة Q وباقي القسمة R؟ بالطبع بإمكانك دائما استخدام القسمة الطويلة، ولكن عيب هذه الطريقة أنها تأخذ وقتاً طويلاً واحتمال الوقوع بالخطأ وارد إذا كان العددان A و B كبيرين.

الطريقة الأفضل هي استخدام الآلة الحاسبة أو برنامج كمبيوتر يقوم بشكل آلي بحساب كل من Q و R. حتى لو كنت تملك آله حاسبة بدائية فإنه يوجد ثلاث خطوات سهلة لحساب Q و R.

إستراتيجية لحساب Q و R باستخدام الآلة الحاسبة بحيث

$$A = Q \times B + R.$$

١- استخدم الآلة الحاسبة لقسمة A على B. سينتج لدينا عدد بفاصلة عشرية.

٢- خذ جميع الخانات على يمين الفاصلة العشرية. هذا يعطيك Q.

٣- لإيجاد R استخدم القانون $R = A - B \times Q$.

على سبيل المثال، إذا كانت $A = 12345$ و $B = 417$ ؛ فإن:

$A/B = 29.6043.......$. إذاً:

$Q = 29$ و $R = 12345 - 417 \cdot 29 = 252.$.

الآن أصبحنا جاهزين للبدء في التحليل النظري لخوارزمية إقليدس. الطريقة العامة تبدو كما يلي:

$$\begin{aligned}
a &= q_1 b + r_1\\
b &= q_2 r_1 + r_2\\
r_1 &= q_3 r_2 + r_3\\
r_2 &= q_4 r_3 + r_4\\
&\vdots\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}\\
r_{n-2} &= q_n r_{n-1} + r_n \leftarrow \text{gcd}\\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

إذا فرضنا أن $r_0 = b$ و $r_{-1} = a$ ؛ فإن كل خطوة من الخطوات السابقة ستبدو على الشكل:

$$r_{i-1} = q_{i+1}r_i \quad + \quad r_{i+1}.$$

السؤال الآن: لماذا يكون آخر باقي غير صفري هو قاسم مشترك لـ a و b ؟ للإجابة عن هذا السؤال سنبدأ بالعكس، أي بدءا من الخطوة الأخيرة وصعودا لأعلى. إن الخطوة الأخيرة :

$$r_{n-1} = q_{n+1}r_n$$

تبين أن r_n يقسم r_{n-1}. وعليه؛ فإن الخطوة قبل الأخيرة

$$r_{n-2} = q_n r_{n-1} \quad + \quad r_n$$

توضح أن r_n يقسم r_{n-2}، لأنه يقسم كلا من r_{n-1} و r_n. انظر الآن إلى المعادلة التي قبلها، نحن نعلم أن r_n يقسم كلا من r_{n-1} و r_{n-2}؛ لذلك فإن r_n يقسم r_{n-3} أيضا. وهكذا بالتدرج بالخطوات صعودا فإنه وعند وصولنا إلى الخطوة الثانية سنستنتج أن r_n يقسم كلا من r_2 و r_1. عندئذ فإن الخطوة الثانية :

$$b = q_2 r_1 \quad + \quad r_2$$

تخبرنا بأن r_n يقسم b. وأخيراً، وبالصعود إلى الخطوة الأولى ومن حقيقة أن r_n يقسم كلا من r_1 و b ، نستنتج أن r_n يقسم أيضا a. هذا يثبت برهاننا أن آخر باقي غير صفري r_n هو قاسم مشترك لكل من a و b. ولكن لماذا r_n هو القاسم المشترك الأكبر للعددين a و b؟ افرض أن d أي قاسم مشترك للعددين a و b . للإجابة عن هذا السؤال سنتتبع خوارزمية إقليدس نزولا، بدءا من الخطوة الأولى. من المعادلة الأولى $a = q_1 b \quad + \quad r_1$ ومن حقيقة أن d يقسم كلا من a و b، نستنتج أن d يقسم أيضا r_1. عندئذ فإن المعادلة الثانية $b = q_2 r_1 \quad + \quad r_2$ توضح لنا أن d

يجب أن يقسم r_2. وهكذا بالتدرج بالخطوات نزولا ، سنستنتج في كل خطوة أن d يقسم الباقيين السابقين r_{i-1} و r_i ، وعليه فإن الخطوة الحالية

$$r_{i-1} = q_{i+1}r_i \quad + \quad r_{i+1}.$$

تخبرنا أن d يقسم أيضاً الباقي اللاحق r_{i+1}. وهكذا نزولا إلى الخطوة قبل الأخيرة :

$$r_{n-2} = q_n r_{n-1} \quad + \quad r_n$$

والتي نستنتج منها أن d يقسم r_n. وبذلك نكون قد بينا أنه إذا كان d أي قاسم مشترك للعددين a و b فإن d سوف يقسم r_n. لذلك فإن r_n يجب أن يكون القاسم المشترك الأكبر للعددين a و b .

وهكذا نكون قد وضحنا أن خوارزمية إقليدس تحسب في الحقيقية القاسم المشترك الأكبر. هذه الحقيقة المهمة سنسجلها على شكل نظرية.

نظرية (١ ,٥) (خوارزمية إقليدس). *لحساب القاسم المشترك الأكبر لعددين a و b ، افرض أن $r_{-1} = a$ و $r_0 = b$ واحسب نواتج القسمة والبواقي المتتالية :*

$$r_{i-1} = q_{i+1}r_i \quad + \quad r_{i+1}.$$

للقيم $i = 0,1,2,....$ حتى الحصول على باقي r_{n+1} يساوي 0. عندئذ فإن آخر باقي غير صفري r_n هو القاسم المشترك الأكبر للعددين a و b.

بقي سؤال أخير وهو ، لماذا خوارزمية إقليدس دائما منتهية؟ بمعنى أننا نعلم أن آخر باقي غير صفري هو القاسم المشترك الأكبر المطلوب ، ولكن كيف نعرف أننا سنحصل دائما على باقي يساوي صفراً؟

السؤال السابق ليس سؤالا سخيفا، فمن السهل إعطاء خوارزمية لا تنتهي، ويوجد حتى خوارزميات بسيطة جدا لا نعرف إذا كانت تنتهي أم لا. لحسن الحظ، من السهل التأكد من أن خوارزمية إقليدس دائما منتهية، والسبب بسيط. ففي كل مرة نحسب فيها ناتج القسمة والباقي

$$A = Q \times B + R,$$

فإن الباقي سيكون بين 0 و $B-1$، وهذا واضح لأنه إذا كانت $R \geq B$ فإننا نستطيع إضافة واحد إلى Q ونطرح B من R. وبالتالي فإن البواقي المتتالية التي نحصل عليها من خوارزمية إقليدس تتناقص باستمرار:

$$b = r_0 > r_1 > r_2 > r_3 > \ldots\ldots$$

لكن جميع البواقي أكبر من أو تساوي 0، وعليه تكون لدينا متتالية متناقصة من أعداد صحيحة غير سالبة، وهذا يعني أننا سنصل إلى باقي يساوي 0 في b خطوة على الأكثر.

في الحقيقة، إن خوارزمية إقليدس أكثر فاعلية من ذلك. سيطلب منك في التمارين أن تثبت أن عدد الخطوات في خوارزمية إقليدس يساوي على الأكثر سبعة أضعاف عدد خانات b. وعليه وباستخدام الحاسوب سيكون من السهل حساب $\gcd(a,b)$ حتى عندما يكون للعددين a و b مئات أو حتى آلاف الخانات.

تمارين

(٥,١) استخدم خوارزمية إقليدس لحساب القاسم المشترك الأكبر.

$$(a)\ \gcd(12345, 67890) \qquad (b)\ \gcd(54321, 9876)$$

(٥,٢) اكتب برنامجاً لحساب القاسم المشترك الأكبر $\gcd(a,b)$ لعددين a , b. يجب أن يكون برنامجاً صالحاً للعمل حتى لو كان أحد العددين a أو b مساوياً للصفر. تأكد من أن برنامجك لا يعمل حلقة (Loop) لا نهائية إذا كان كلٌّ من a , b مساوياً للصفر!

(٥,٣) ليكن $b = r_0, r_1, r_2, \ldots$ البواقي المتتالية عند تطبيق خوارزمية إقليدس على العددين a, b. بين أن كل خطوتين تختزل الباقي إلى النصف على الأقل. بعبارة أخرى، تحقق من أن $r_{i+2} < \frac{1}{2} r_i$ لكل $i = 0, 1, 2, \ldots$

واستنتج أن خوارزمية إقليدس تنتهي بعد $2\log_2(b)$ خطوة على الأكثر. بشكل خاص، بين أن عدد الخطوات يساوي على الأكثر سبعة أضعاف عدد خانات b. [مساعدة: ما قيمة $\log_2(10)$ ؟]

(٥,٤) يسمى العدد L مضاعفاً مشتركاً للعددين n, m إذا كان كل من n, m يقسم L. أصغر قيمة للعدد L تسمى المضاعف المشترك الأصغر للعددين n, m

The least common multiple for m and n

ويرمز له بالرمز $LCM(m,n)$. على سبيل المثال،

$$LCM(12, 66) = 132 \quad , \quad LCM(3, 7) = 21$$

(a) أوجد

$(i)\ LCM(8,12)$ $(ii)\ LCM(20,30)$

$(iii)\ LCM(51,68)$ $(iv)\ LCM(23,18)$

(b) لكل LCM قمت بحسابه في (a) ، قارن قيمة $LCM\left(m,n\right)$ مع قيم $m\,,n$ و $\gcd\left(m,n\right)$ حاول إيجاد علاقة.

(c) أعطِ برهاناً على أن العلاقة التي أوجدتها صحيحة لأي قيم للعددين $n\,,m$.

(d) استخدم نتيجتك في (b) لحساب $LCM\left(301337,307829\right)$.

(e) افرض أن $\gcd\left(m,n\right)=18$ و $LCM\,(m,n)=720$. أوجد $n\,,m$.
هل هناك أكثر من احتمال واحد؟ إذا كان الجواب نعم، أوجد جميع هذه الاحتمالات.

(٥,٥) " خوارزمية $3n+1$ " تعمل كما يلي: إبدأ بأي عدد n. إذا كان n عدداً زوجيًّا، فاقسمه على 2. إذا كان n عدداً فرديًّا، فاستبدله بالعدد $3n+1$. كرر ذلك. لذلك، وعلى سبيل المثال، إذا بدأنا بالعدد 5 فسنحصل على قائمة الأعداد

$$5,16,8,4,2,1,4,2,1,4,2,1,\ldots$$

وإذا بدأنا بالعدد 7 فسنحصل على

$$7,22,11,34,17,52,26,13,40,20,10,5,16,8,4,2,1,4,2,1,\ldots$$

لاحظ أننا إذا حصلنا على العدد 1 فإن القائمة ستستمر بتكرار $4,2,1$. بشكل عام، أحد هذين الاحتمالين سوف يظهر:

(i) قد ننتهي بتكرار عدد a يظهر مبكراً في القائمة، في هذه الحالة سوف تتكرر الأعداد بين العددين a بشكل لا نهائي.

في هذه الحالة نقول إن الخوارزمية تنتهي عند آخر قيمة غير مكررة ، ويسمى عدد هذه الأعداد " طول الخوارزمية " (*length of the algorithm*). على سبيل المثال ، كل من خوارزمية العدد 5 والعدد 7 تنتهي بالعدد 1. طول خوارزمية العدد 5 يساوي 6 ، وطول خوارزمية العدد 7 يساوي 17.

(ii) قد لا يُكرر عدد بعينه ، في هذه الحالة نقول إن الخوارزمية غير منتهية.

(a) أوجد الطول والقيمة التي تنتهي عندها خوارزمية $3n+1$ لكل قيمة ابتدائية n فيما يلي :

$$(i)\ n = 21 \qquad (ii)\ n = 13 \qquad (iii)\ n = 31$$

(b) قم بعمل مزيد من التجارب وحاول أن تقرر فيما إذا كانت خوارزمية $3n+1$ تنتهي دائماً، وإذا كانت كذلك ، فما هي القيمة (القيم) التي تنتهي عندها.

(c) ليكن $L(n)$ طول الخوارزمية التي تبدأ بالقيمة N (طبعاً ، افترض أنها منتهية) . مثلاً $L(5) = 6$, $L(7) = 17$. بيّن أنه إذا كان $n = 8k+4$ فإن $L(n) = L(n+1)$.

(مساعدة: ما هي طبيعة عمل الخوارزمية عند القيمتين الابتدائيتين $8k+4$, $8k+5$).

(b) بين أنه إذا كان $n = 128k + 28$ ؛ فإن :

$$L(n) = L(n+1) + L(n+2)$$

(e) أوجد بعض الشروط الأخرى ، كتلك الواردة في (c) و (d) ، ليكون لقيمتين لـ n نفس الطول. (قد يكون من المفيد أن تبدأ باستخدام التمرين التالي لجمع بعض البيانات).

(٥,٦) اكتب برنامجاً لتنفيذ خوارزمية $3n+1$ المشروحة في التمرين السابق. المُستخدِم سيُدخل قيمة n ويجب على برنامجك أن يُعطي الطول $L(n)$ وآخر قيمة $\mathrm{T}(n)$ للخوارزمية $3n+1$. استخدم برنامجك لإنشاء جدول يُعطي الطول والقيمة الأخيرة لجميع القيم الابتدائية $1 \le n \le 100$.