GCD و LCM

القاسم المشترك الأكبر مفهوم مهم جدًا.

ليكن a,b عددين صحيحين غير صفريين. يقال للعدد الصحيح الذي يقسم كلًا من a,b (مثلًا ± 1) قاسم مشترك للعدين a,b. ولمحدودية عدد قواسم العددين a,b (لأن أي قاسم للعدد a لن تزيد قيمته عن $|a|$)، فإن القاسم الأكبر بين القواسم المشتركة للعددين a,b يقال له القاسم المشترك الأكبر ونرمز له $\gcd(a,b)$، ومن الواضح أنه سيكون عددًا صحيحًا موجبًا.

إذا كان $\gcd(a,b)=1$، يقال أن العددين a,b أوليان نسبيًا، وهي حالة لها أهمية خاصة كما سنرى.

لأكثر من عددين صحيحين (كل منها بخلاف الصفر) $a,b,\dots,c$، يمكن أن نعرف بطريقة مشابهة القاسم المشترك الأكبر لهم $\gcd(a,b,\dots,c)$. وأيضًا إذا كان $\gcd(a,b,\dots,c)=1$ فيقال الأعداد أولية نسبيًا.

تنبيه: في هذه الحالة لا يمكنك استنتاج أن الأعداد $a,b,\dots,c$ أولية مثنى مثنى (بمعنى أي اثنين منهم أوليان نسبيًا).

على الجانب الآخر إذا كانت الأعداد $a,b,\dots,c$ أولية مثنى مثنى فإن $\gcd(a,b,\dots,c)=1$.

تنتج الخواص البسيطة التالية من تعريف القاسم المشترك الأكبر.

إذا غيرنا إشارة a أو b، فإن قيمة $\gcd(a,b)$ لا تتغير. بمعنى $\gcd(\pm a,\pm b)=\gcd(a,b)$.

التعبير $\gcd(a,b)$ متماثل بالنسبة للعددين a,b. بمعنى $\gcd(a,b)=\gcd(b,a)$.

$\gcd(a,b)$ كدالة في المتغير b ستكون دورية، طول دورتها a بمعنى $\gcd(a,b+ax)=\gcd(a,b)$ لأي عدد صحيح x.

النظرية التالية في الفقرة (1) التالية هي إحدى النتائج الكبرى والتي ستمكننا لنذهب أبعد مع القاسم المشترك الأكبر.

(1) نظرية: ليكن a,b عددين صحيحين غير صفريين. ومن ثم يوجد عددان صحيحان x,y بحيث

$$ax+by=\gcd(a,b) \qquad (*)$$

البرهان: يقال للمقدار $ax+by$ تركيب خطي في a,b. لتكن S مجموعة كل التراكيب الخطية لذلك المقدار، ومعاملاته $(x_1,y_1),(x_2,y_2),\dots$ أعداد صحيحة. وبملاحظة أن بوضع $x_1=a, y_1=b$، فإن a^2+b^2 عدد موجب سيكون أحد عناصر S. لذا يوجد أصغر عنصر موجب d في S. سنثبت أن $d=\gcd(a,b)$. لأن d عنصر في S فهو تركيب خطي في a,b ، وبالتالي فهو مضاعف ل $\gcd(a,b)$، لذا يكفي أن نثبت أن d يقسم كلًا من a,b، سنبدأ بإثبات أن d يقسم كل عنصر s في المجموعة S.

بفرض d لا يقسم عنصر s من المجموعة S. وبالتالي يمكننا أن نفرض $s=qd+r$ حيث q,r عددان صحيحان موجبان و $0<r<d$. الآن s,d تركيبان خطيان في a,b، وبالتالي $r=s-qd$ تركيب خطي في a,b كذلك.

وبالتالي r عنصر موجب في S وهو أصغر من d. وهذا يناقض أصغرية d في المجموعة S.

أخيرًا، بما أن $a(1)+b(0)=a$ و $a(0)+b(1)=b$ عنصران في S. إذن d يقسم كلًا من a,b. انتهى البرهان.

سنبين سريعًا أن هناك عدد لا نهائي من الحلول لقيم (x,y). ليكن $x=x_0, y=y_0$ زوج من الأعداد الصحيحة يحقق المعادلة $(*)$. فإن المعادلة

$$a(x_0+bu)+b(y_0-au)=\gcd(a,b)$$

صحيحة لجميع قيم u الصحيحة، وبالتالي المعادلة $(*)$ لها عدد لا نهائي من الحلول.

الفقرة (2) التالية نتيجة واضحة للفقرة (1).

(2) الشرط اللازم والكافي ليكون العددان الصحيحان a,b أوليين نسبيًا هو

$$ax+by=1$$

يطلق عليها عادة "متطابقة بيزو Bezout 's identity ".

البرهان: حالة a,b أوليان نسبيًا، ومن ثم يوجد عددان صحيحان x,y يحققان $ax+by=1$ تنتج مباشرة من النظرية السابقة والمتطابقة $(*)$.

حالة $ax+by=1$، سنثبت أن a,b أوليان نسبيًا. بفرض $\gcd(a,b)=d$، فيصبح d يقسم الطرف الأيسر، وبالتالي d يقسم الطرف الأيمن ومنها $d\,|1$، ومنها $d=1$. إذن a,b أوليان نسبيًا.

من الفقرتين (1) و (2) يمكننا استنتاج النتائج الأساسية في الفقرات التالية بسهولة.

(3) إذا كان $m\,|a$ و $m\,|b$ فإن $m\,|\gcd(a,b)$. بمعنى كل قاسم مشترك للعددين a,b سيكون قاسمًا لقاسمهما المشترك الأكبر.

(4) إذا كان $m>0$، فإن $\gcd(ma,mb)=m\gcd(a,b)$.

(5) إذا كان $\gcd(a,b)=d$، فإن $\gcd(\frac{a}{d},\frac{b}{d})=1$.

(6) إذا كان $\gcd(a,m)=1$ و $\gcd(b,m)=1$ فإن $\gcd(ab,m)=1$. هذا يعني أن خاصية الضرب لمجموعة الأعداد الصحيحة الأولية نسبية مع عدد معين تتمتع بخاصية الانغلاق. من هذه الحقيقة ينتج أن، إذا كان $\gcd(a,b)=1$، فإن $\gcd(a^k,b^l)=1$ لأي عددين صحيحين موجبين k,l.

(7) بفرض $b\,|ac$. إذا كان $\gcd(b,c)=1$، فإن $b\,|a$.

(8) بفرض حاصل ضرب عددين صحيحين a,b قوة k لعدد صحيح ($k\geq 2$). إذا كان $\gcd(a,b)=1$، فإن كل من a,b قوة k لعدد صحيح. والخاصية قابلة للتعميم لأكثر من عددين.

الخواص (6) و (7) و (8) تبين أهمية أن تكون الأعداد أولية نسبيًا، ولها كثير من التطبيقات كما سنرى.

سنناقش الآن بإيجاز المضاعف المشترك الأصغر.

ليكن a,b عددين صحيحين غير صفريين. يقال للعدد الصحيح المضاعف لكل من a,b مضاعف مشترك للعدين a,b. من الواضح أن هناك عدد غير محدود من المضاعفات المشتركة للعددين a,b، فإن المضاعف الأصغر بين المضاعفات المشتركة للعددين a,b يقال له المضاعف المشترك الأصغر ونرمز له $[a,b]$، ومن الممكن تعريفه بالمثل لأكثر من عددين. نذهب الآن لبعض الخواص الرئيسية للمضاعف المشترك الأصغر.

(9) أي مضاعف مشترك للعددين a,b يكون مضاعفًا للعدد $[a,b]$.

(10) لأي عددين a,b لدينا الخاصية التالية

$$\gcd(a,b)[a,b]=|ab|$$

على أي حال الحالة غير قابلة للتعميم لعدة أعداد (أعط أمثلة عددية بنفسك). غير ذلك لدينا الخاصية التالية.

(11) إذا كانت الأعداد $a,b,\ldots,c$ أولية نسبيًا مثنى مثنى، فإن

$$[a,b,\ldots,c]=|ab\cdots c|$$

مفهوم الأعداد الأولية نسبيًا مهم جدًا في نظرية الأعداد، وهو المفتاح أو الأساس للكثير من المسائل.

مثال 1(IMO): لأي عدد صحيح n، أثبت أن الكسر $\dfrac{21n+4}{14n+3}$ غير قابل للتبسيط.

مثال 2: ليكن n عددًا صحيحًا موجبًا. أثبت أن

$$\gcd(n!+1,(n+1)!+1)=1$$

مثال 3: ليكن $F_k=2^{2^k}+1$ حيث $k\geq 0$. برهن أن إذا كان $m\neq n$، فإن $\gcd(F_m,F_n)=1$.

ملاحظة: F_k المعرف في مثال 3 يسمى عدد فيرما. ويعطينا المثال نتيجة أساسية جميلة، أن أعداد فيرما أولية نسبيًا.

مثال 4: بفرض $a>1, m,n>0$. أثبت أن:

$$\gcd(a^m-1,a^n-1)=a^{\gcd(m,n)}-1.$$

ملاحظة: نتيجة مثال 4 قوية جدًا، ولها استخدامات كثيرة، من المهم أن تتذكرها جيدًا.

مثال 5: بفرض $m,n>0$، أثبت أن إذا كان $mn\mid(m^2+n^2)$، فإن $m=n$.

مثال 6: ليكن $\gcd(a,b,c)=1$ حيث a,b,c أعداد صحيحة موجبة، $\dfrac{ab}{a-b}=c$. أثبت أن $a-b$ مربع كامل.

مثال 7: ليكن k عدد صحيح موجب فردي. أثبت أن:

$$(1+2+....+n) \mid (1^k+2^k+....+n^k).$$

ملاحظة: عندما يتعذر إثبات أن $a \mid b$، من الحيل المفيدة اعتبار أن $b=b_1b_2\cdots b_n$، بحيث $b_1,b_2,...,b_n$ أولية نسبيًا مثنى مثنى، ثم إثبات أن كل منها يقسم a على حدة.

تمارين

1) ليكن n عدد صحيح. أثبت أن $\gcd(12n+5,9n+4)=1$.

2) تحدي: ليكن m,n عددين صحيحين موجبين، m فردي. أثبت أن $\gcd(2^m-1,2^n+1)=1$.

3) ليكن $\gcd(a,b)=1$. أثبت $\gcd(a^2+b^2,ab)=1$.

4) بين أن الجذور النسبية لكثيرة حدود ذات معاملات صحيحة ومعامل رئيس ±1 تكون أعداد صحيحة.

5) تحدي: لتكن m,n,k أعداد صحيحة موجبة تحقق أن $[m+k,m]=[n+k,n]$. أثبت أن $m=n$.

6) تحدي: يقف البيدق على أحد مربعات رقعة شطرنج لانهائية في كلا الاتجاهين. يمكن نقل البيدق m مربعًا إلى اليمين أو n مربعًا إلى اليسار. أي قيم m,n تحقق الخاصية أن البيدق يمكن تحريكه إلى المربع الأيمن المجاور لمربع الوضع الابتدائي (في عدة حركات)؟ ما هو الحد الأدنى لعدد الحركات اللازمة للقيام بذلك؟

7) تحدي: بفرض $m\geq n\geq 1$. أثبت أن $\dfrac{\gcd(m,n)}{m}\dbinom{m}{n}$ عدد صحيح.

8) بفرض أن $\gcd(m,n)=1$. اثبت أن $m \mid \dbinom{m+n-1}{n}$.