كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : الاولى/نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

* مفهوم قابلية القسمة في مجموعة الأعداد الصحيحة:

- تعريف:

يُقال عن العدد الصحيح $m \neq 0$ إنّه يقسم العدد الصحيح n إذا وجد عدد صحيح q بحيث $n = qm$

ونقول إنّ m قاسم لـ n (n مضاعف لـ m)

ونكتب $m \mid n$

- خواص قابلية القسمة في مجموعة الأعداد الصحيحة:

1. $n \mid 1 \Rightarrow n = 1$ or $n = -1$
2. $a \mid b$ & $c \mid d$
$\Rightarrow ac \mid bd$
3. $a \mid b$ & $b \mid c \Rightarrow a \mid c$
(علاقة $\mid$ هي علاقة متعدية)
4. $\left.\begin{array}{l} a \mid b \\ a \neq 0 \\ b \neq 0 \end{array}\right\} \Rightarrow |b| \geq |a|$
5. إذا كان $a, b \in \mathbb{Z}$
$a \neq 0 \Rightarrow a \mid b$ و $a \mid c$
عندئذٍ:
$a \mid (mb + nc)$
$\forall m, n \in \mathbb{Z}$

6. إذا كان $a \mid (b+c)$ و $a \mid b$

$\Rightarrow a \mid c$

الإثبات:

$a \mid (b+c) \Rightarrow \exists q \in \mathbb{Z}:$

$b+c = qa$ ⊛

$a \mid b \Rightarrow \exists q \in \mathbb{Z}:$

$b = q_1 a$

نعوض في ⊛ نجد:

$c = qa - q_1 a$

$c = (q - q_1) a$

$c = ta \quad ; \quad t = q - q_1$

$\Rightarrow a \mid c$

- مبرهنة القسمة الإقليدية (مبرهنة إقليدس):

إذا كان $a, b \in \mathbb{Z}$ ، $b \neq 0$ فإنه يوجد عددان صحيحان r, q ووحيدان بحيث:

$a = qb + r$

حيث $0 \leq r < |b|$

مثال:

$a = 112$

$b = 5$

$a = 22 \times 5 + 2$

* مفهوم القاسم المشترك الأعظم:

ليكن a, b عددين صحيحين (أحدهما على الأقل لا يساوي الصفر).

يُقال عن العدد الصحيح d بأنّه قاسم مشترك أعظم للعددين a و b إذا تحقّقت الشروط التالية:

1. $d > 0$
2. $d \mid a$ و $d \mid b$
3. إذا كان $c \in \mathbb{Z}^+$ قاسماً مشتركاً لـ a و b فإنّ $c \mid d$ ، ونكتب عندئذٍ:

$$d = gcd(a,b)$$

ملاحظة:

القاسم المشترك الأعظم لعددين a و b غير معدومين معاً دوماً موجود وهو وحيد.

ملاحظة:

* $gcd(a,b) = gcd(-a,b)$
$= gcd(a,-b)$
$= gcd(-a,-b)$
* $gcd(a,1) = 1$
$gcd(0,a) = |a|$

مبرهنة:

إذا كان a و b عددين صحيحين غير معدومين فإنّ القاسم المشترك الأعظم لهما $(gcd(a,b))$ هو تركيب خطي للعددين a و b أي يوجد عددان صحيحان m,n بحيث:

$$d = gcd(a,b) = ma + nb$$

ملاحظة: إنّ تمثيل القاسم المشترك الأعظم لعددين كتركيب خطي ليس وحيداً فمثلاً على سبيل المثال:

$$d = gcd(15, 24) = 3$$

$$d = (-3) \times 15 + 2 \times (24)$$

$$= (-27) \times 15 + 17 \times (24)$$

ملاحظة:

إذا كان $d = gcd(a, b)$

وكان $x = ma + nb$

عندئذٍ: $d \mid x$

أي x مضاعف لـ d.

تعريف:

إذا كان a, b عددين صحيحين يُقال أنّ a, b أوليان فيما بينهما إذا كان $gcd(a, b) = 1$

مثال:

~~gcd(a,b)~~

$$gcd(32, 15) = 1$$

بالتالي 32 و 15 أوليان فيما بينهما.

مبرهنة:

ليكن a, b عددين صحيحين ليسا معدومين معاً عندئذٍ:

a و b أوليان فيما بينهما إذا وفقط إذا وجد عددان صحيحان x, y يحققان:

$$ax + by = 1$$

الإثبات: $\Leftarrow$ a و b أوليان فيما بينهما عندئذٍ:

$$gcd(a,b)=1$$

عندئذٍ حسب مبرهنة سابقة يوجد $x,y\in\mathbb{Z}$

بحيث: $1=ax+by$

$\Rightarrow$ لدينا فرضاً $\boxed{ax+by=1}$ (*)

ولكن $d=gcd(a,b)$ ولنبرهن أنّ $d=1$

$$d=gcd(a,b)\Rightarrow\begin{cases} d\mid a \Rightarrow a=q_1 d \;;\; q_1\in\mathbb{Z} \\ d\mid b \Rightarrow b=q_2 d \;;\; q_2\in\mathbb{Z}\end{cases}$$

نعوّض $a=q_1 d$ و $b=q_2 d$ في (*) نجد:

$$d(q_1x+q_2y)=1$$

$$\Rightarrow d\mid 1 \;\&\; d>0$$

$$\Rightarrow d=1$$

$\Leftarrow$ a و b أوليان فيما بينهما

مبرهنة: إذا كان $d=gcd(a,b)$

فإنّه يوجد عددان صحيحان a_0, b_0 بحيث أنّ:

$$\begin{cases} gcd(a_0,b_0)=1 \\ a=a_0 d \\ b=b_0 d\end{cases}$$

الإثبات:

لدينا فرضاً $d=gcd(a,b)$

$$\exists x,y\in\mathbb{Z} \;;\; d=xa+yb$$

$$1=x\left(\frac{a}{d}\right)+y\left(\frac{b}{d}\right)$$

$1 = x a_0 + y b_0$;

$a_0 = \frac{a}{d}$

$b_0 = \frac{b}{d}$

نستنتج بأنّ $\gcd(a_0, b_0) = 1$

$\Leftarrow$

$a = a_0 d$

$b = b_0 d$

مبرهنة: ليكن a, b, m أعداد صحيحة عندئذٍ يكون

لدينا التالي:

1) إذا كان

$\gcd(a, m) = 1$

و $\gcd(b, m) = 1$

فإنّ:

$\gcd(ab, m) = 1$

2) إذا كان

$m \mid ab$

و $\gcd(m, a) = 1$ عندئذٍ:

$m \mid b$

3) إذا كان $a \mid m$ و $b \mid m$ و $\gcd(a, b) = 1$

عندئذٍ $ab \mid m$

الإثبات:

① لدينا فرضاً:

*) $1 = gcd(a, m)$

$\exists x, y \in \mathbb{Z} \; ; \; 1 = ax + my$

$\Rightarrow \boxed{b = abx + mby}$ ⊛

*) ليكن $d = gcd(ab, m)$

$d \mid ab \Rightarrow ab = q_1 d$

و

$d \mid m \Rightarrow m = q_2 d$

نعوض من ⊛ نجد:

$b = q_1 dx + q_2 dby$

$b = d(q_1 x + q_2 by)$

$\Rightarrow d \mid b$

و $\Rightarrow d \mid gcd(b, m)$

$d \mid m$ $\Rightarrow d \mid 1$ و $d > 0$

$\Rightarrow d = 1$

③ $a \mid m \Rightarrow m = q_0 a \; ; \; q_0 \in \mathbb{Z}$

ولدينا:

$b \mid m \Rightarrow b \mid q_0 a$

بما أنّ: $gcd(a, b) = 1$

عندئذٍ حسب ② نجد:

$b \mid q_0 \Rightarrow q_0 = q b$

$\Rightarrow m = q(ab) \Rightarrow ab \mid m$

مبرهنة:

إذا كان $d = gcd(a,b)$ و $m > 0$

فإن: $gcd(ma, mb) = md$

مبرهنة:

إذا كان $d = gcd(a,b)$ فإن:

1. $d = gcd(a + qb, b)$ حيث $q \in \mathbb{Z}$
2. $d = gcd(a - qb, b)$ حيث $q \in \mathbb{Z}$
3. $d = gcd(a, b + ka)$ حيث $k \in \mathbb{Z}$

$d = gcd(a, b - ka)$ حيث $k \in \mathbb{Z}$

خوارزمية:

ليكن $a, b \in \mathbb{Z}$ و $b \neq 0$

$a = qb + r$; $0 \leq r < |b|$

$d = gcd(a,b) = gcd(b,r)$

الإثبات:

$$\begin{aligned} d &= gcd(a,b) \\ &= gcd(qb + r, b) \\ &= gcd(qb + r - qb, b) \\ &= gcd(r, b) \\ &= gcd(b, r) \end{aligned}$$

مثال:

$51 = 8 \times 6 + 3$

$\gcd(51, 6) = \gcd(6, 3) = 3$

$\gcd(51, 8) = \gcd(8, 3) = 1$

انتهت