كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

المادة : نظرية الاعداد

المحاضرة : الاولى /نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

1 مبدأ الترتيب الجيّد: كل مجموعة جزئية غير خالية A من مجموعة الأعداد الصحيحة الموجبة تملك عنصر أصغر a_0 وهي يحقّق التالي

$\forall a \in A \quad a \geq a_0$

2 مبدأ الاستقراء الرياضي: لتكن $p(n)$ عبارة تتعلّق بالمتغير n حيث $n \in \mathbb{N}$ ولتكن n_0 عدداً طبيعياً بحيث يتحقّق الشرطان

1 العبارة $p(n_0)$ صحيحة

2 لأجل أي عدد طبيعي k فإنّ صحّة العبارات التالية

$p(n_0), p(n_0+1), \ldots, p(k)$

تقتضي صحّة العبارة $p(k+1)$

عندئذٍ تكون العبارة $p(n)$ صحيحة لأجل جميع قيم n

مثال: أثبت بطريقة الاستقراء الرياضي أنّه إذا كان x عدداً صحيحاً موجباً مغايراً للعدد 1 فإنّ

$$\sum_{i=0}^{n-1} x^i = 1 + x + x^2 + \ldots + x^{n-1} = \frac{x^n - 1}{x - 1}$$

وذلك من أجل أي عدد صحيح موجب n ؟

الإثبات:

نثبت صحّة الملاحظة من أجل $n=1$:

$$\left.\begin{aligned} P_1 &= \sum_{i=0}^{0} x_i = 1 \\ P_2 &= \frac{x-1}{x-1} = 1 \end{aligned}\right\} \Rightarrow P_1 = P_2$$

بالتالي القضية صحيحة من أجل

$n=1$

• نفرض صحّة العلاقة من أجل $n=k$

$$1+x+x^2+\dots+x^{k-1}=\frac{x^k-1}{x-1}$$

• نثبت صحّة العلاقة من أجل $n=k+1$:

أي يجب أن نثبت أنّ: $1+x+\dots+x^k \overset{?}{=} \frac{x^{k+1}-1}{x-1}$

لدينا $P_1 = 1+x+\dots+x^{k-1}+x^k = \frac{x^k-1}{x-1}+x^k =$

$$\frac{x^k-1+x^{k+1}-x^k}{x-1} = \frac{x^{k+1}-1}{x-1} = P_2$$

بالتالي القضية صحيحة من أجل $n=k+1$

بالتالي مما سبق نجد بأنّ العلاقة صحيحة من أجل أي عدد صحيح موجب n.

مثال 2: أثبت بطريقة الاستقراء الرياضي صحة العلاقة:

$$1^2+2^2+3^2+\dots+n^2=\frac{n(n+1)(2n+1)}{6}$$

وذلك $\forall n \in \mathbb{N}^*$ ؟

الاثبات:

• نثبت صحة العلاقة من أجل $n=1$:

$$\left.\begin{array}{l} P_1 = 1^2 = 1 \\ P_2 = \frac{1(2)(3)}{6} = \frac{6}{6} = 1 \end{array}\right\} \Rightarrow P_1 = P_2$$

والعلاقة صحيحة من أجل $n=1$

• نفرض صحّة العلاقة من أجل $n=k$:

$$1^2+2^2+3^2+\dots+k^2=\frac{k(k+1)(2k+1)}{6}$$

• نثبت صحة العلاقة من أجل $n=k+1$

$$1^2+2^2+\dots+(k+1)^2 \overset{?}{=} \frac{(k+1)(k+2)(2k+3)}{6}$$

لدينا $P_1 = 1^2+2^2+\dots+k^2+(k+1)^2 = \frac{k(k+1)(2k+1)}{6}+(k+1)^2$

$$= \frac{k(k+1)(2k+1)+6(k+1)^2}{6}$$

$$= \frac{(k+1)\left((k(2k+1)) + 6(k+1)\right)}{6} = \frac{(k+1)(2k^2+k+6k+1)}{6}$$

$$= \frac{(k+1)(2k^2+7k+1)}{6} = \frac{(k+1)(k+2)(2k+3)}{6} = P_2$$

العلاقة صحيحة من أجل $n=k+1$

ممّا سبق نجد أنّ العلاقة صحيحة من أجل كل قيم n حيث $n \in \mathbb{N}^*$

• مفهوم قابلية القسمة في مجموعة الأعداد الصحيحة :

تعريف : يُقال عن العدد الصّحيح $m \neq 0$ أنّهُ يقسم العدد الصّحيح n إذا وفقط إذا وُجِدَ عدد صحيح q بحيث $n = q.m$ ونقول إنّ m قاسم لـ n ($m \mid n$) أو بمعنى آخر n مضاعف لـ m

• خواص قابلية القسمة في $\mathbb{Z}$:

1. $n \mid 1 \Rightarrow n = +1 \text{ or } n = -1$ (يقسم)
2. $a \mid b \;\&\; c \mid d \Rightarrow a.c \mid b.d$
3. $a \mid b \;\&\; b \mid c \Rightarrow a \mid c$

أي أنّ علاقة يقسم هي علاقة متعدية.

4. $a \mid b \;\&\; a \neq 0 \;\&\; b \neq 0 \Rightarrow |b| \geq |a|$
5. إذا كانت $a,b,c \in \mathbb{Z}$ و $a \neq 0$ و $a \mid b$ و $a \mid c$

عندئذٍ $\forall n,m \in \mathbb{Z}$ $a \mid (mb+nc)$

أي : إذا كان $a \neq 0$ قاسم لعددين منهما قاسم لأي تركيب خطي لهما

الإثبات :

$$a \mid b \Rightarrow \exists q_1 \in \mathbb{Z} \;;\; b = q_1 . a$$

$$a \mid c \Rightarrow \exists q_2 \in \mathbb{Z} \;;\; c = q_2 . a$$

$$mb+nc = m(q_1.a) + n(q_2.a) = a(q_1 m) + a(q_2 n)$$

$$= a\left[q_1 m + q_2 n\right] = a.q \;;\; q = (q_1 m + q_2 n) \in \mathbb{Z}$$

$$\Rightarrow a \mid (mb+nc)$$

مبرهنة القسمة الاقليدية :

إذا كانت $a,b \in \mathbb{Z}$ و $b \neq 0$ عندئذٍ فإنّهُ يوجد عددان صحيحان q و r ووحيدان بحيث $0 \leq r < |b|$; $a = q.b + r$

باقي القسمة + (المقسوم عليه x ناتج القسمة) = المقسوم

مثال 1 : $a = 50$, $b = 6$

$\Rightarrow a = qb + r \Rightarrow 50 = (8 \times 6) + 2$

مثال 2 : $a = 1000$, $b = 57$

$1000 = (17 \times 57) + 31$

مثال 3 : $a = -51$ $b = -6$

$-51 = 9(-6) + 3$

مفهوم القاسم المشترك الأعظم :

ليكن a و b عددين صحيحين (إحداهما على الأقل لا يساوي الصفر)

يُقال عن العدد الصحيح d بأنّهُ قاسم مشترك أعظم للعددين a و b

إذا تحققت الشروط التالية :

1. $d > 0$.
2. $d|a$ & $d|b$.
3. إذا كان $c \in \mathbb{Z}^+$ قاسماً مشتركاً لـ a و b فإنّ $c|d$.

ونكتب عندئذٍ $d = gcd(a,b)$.

ملاحظة (1) : القاسم المشترك الأعظم لعددين a و b غير معدومين معاً دوماً موجود وهو وحيد .

ملاحظة (2) : $d = gcd(a,b) = gcd(-a,b) = gcd(a,-b) =$

$gcd(-a,-b) = gcd(|a|,|b|)$

$d = gcd(a,0) = |a|$. $d = gcd(a,1) = 1$.

مبرهنة: إذا كان a و b عددين صحيحين غير معدومين فإنّ القاسم المشترك الأعظم لهما $(d=gcd(a,b))$ هو تركيب خطّي للعددين a و b

أي: يوجد دوماً عددان صحيحان m و n بحيث $d=m.a+n.b$

ملاحظة: إنّ تمثيل القاسم المشترك الأعظم لعددين كتركيب خطّي لهما ليس وحيداً

مثال: $d=gcd(15,24)=3 \Rightarrow 3=15(-3)+24(2)$

أو $3=15(-27)+24(17)$

ملاحظة: إذا كانت $d=gcd(a,b)$ وكانت $x=ma+nb$; $m,n\in\mathbb{Z}$ عندئذٍ $d|x$

تعريف: إذا كان a و b عددين صحيحين يُقال بأنّ a و b أوليان فيما بينهما إذا كان $gcd(a,b)=1$.

مثال: $gcd(32,15)=1 \Leftarrow$ 32 و 15 أوليان فيما بينهما

مبرهنة: ليكن a و b عددين صحيحين غير معدومين معاً عندئذٍ a و b أوليان فيما بينهما إذا وفقط إذا وُجِدَ عددان صحيحان x و y يحقّقان $a.x+b.y=1$.

الإثبات:

$\Leftarrow$ a و b أوليان فيما بينهما بالتّالي $gcd(a,b)=1$

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

$\Rightarrow$ لدينا $1=ax+by$ ⊛ حيث $x,y\in\mathbb{Z}$ ولكن $d=gcd(a,b)$ بالتّالي

$d|a \Rightarrow a=q_1.d$; $q_1\in\mathbb{Z}$

$d|b \Rightarrow b=q_2.d$; $q_2\in\mathbb{Z}$

نعوّض في ⊗ فنجد أنّ $1 = d(q_1 x + q_2 y)$

$\Rightarrow d \mid 1 \;\&\; d > 0 \Rightarrow d = 1 \Rightarrow \gcd(a,b) = 1$

بالتّالي a و b أوليان فيما بينهما

نتيجة: إذا كان $d = \gcd(a,b)$ فإنّهُ يوجد عددان صحيحان b_0 و a_0 بحيث أنّ $\gcd(a_0, b_0) = 1$ و $a = a_0 d$ و $b = b_0 d$

الإثبات:

$d = \gcd(a,b)$ فإنّهُ يوجد عددان صحيحان x و y بحيث أنّ $d = ax + by$ وبما أنّ $\frac{a}{d}$ و $\frac{b}{d}$ عددان صحيحان بالتّالي $1 = \left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y$.

نضع $a_0 = \frac{a}{d}$ و $b_0 = \frac{b}{d}$ بالتّالي

$1 = a_0 x + b_0 y$

$\Rightarrow \gcd(a_0, b_0) = 1 \;\&\; a = a_0 d \;\&\; b = b_0 d$

مبرهنة: ليكن m و a و b أعداد صحيحة عندئذٍ يكون لدينا التّالي:

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

الإثبات:

إثبات ①: ليكن $d = \gcd(a.b, m)$ عندئذٍ $d \mid a.b$ و $d \mid m$

$d \mid a.b \Rightarrow a.b = q_1 . d \;;\; q_1 \in \mathbb{Z}$

$d \mid m \Rightarrow m = q_2 d \;;\; q_2 \in \mathbb{Z}$

لدينا: $1 = \gcd(a,m) \Rightarrow \exists a_0, m_0 \in \mathbb{Z}$ و

$1 = a_0 . a + m_0 . m$ ⊛

نضرب طرفي العلاقة ⊛ بـ b فنجد أنّ:

$b = a_0 (a.b) + m_0 (m.b)$

$b = a_0 . q_1 . d + m_0 . q_2 . d . b$

$b = d (a_0 . q_1 + m_0 . q_2 . b) \Rightarrow d | b \ \& \ d | m$

$\Rightarrow d | gcd(b, m)$

$\Rightarrow d | 1 \ \& \ d > 0$

$\Rightarrow d = 1$

بالتّالي $gcd(ab, m) = 1$.

اثبات ②: لدينا:

- $m | a.b \Rightarrow \exists q \in \mathbb{Z} \ ; \ a.b = q.m$
- $1 = gcd(m, a) \Rightarrow \exists q_0, m_0 \in \mathbb{Z} \ ; \ 1 = m_0 . m + q_0 . a$

نضرب الطرفين بـ b فنجد:

$b = m_0 . m b + q_0 . a . b$

$b = m_0 . m . b + a_0 (q . m)$

$b = m (m_0 b + a_0 . q) \Rightarrow m | b$

اثبات ③: لدينا:

- $a | m \Rightarrow \exists q_0 \in \mathbb{Z} \ ; \ \boxed{m = q_0 . a}$ ⊛
- $b | m \Rightarrow b | q_0 . a \ \& \ gcd(a, b) = 1 \Rightarrow b | q_0$

$\Rightarrow q_0 . q . b \ ; \ q \in \mathbb{Z}$

نعوّض في ⊛

$m = q (a.b) \Rightarrow (a.b) | m$

ملاحظة: إذا كانت $d = gcd(a, b)$ فإنّ:

① $d = gcd(a + q.b, b) \ ; \ q \in \mathbb{Z}$

② $d = gcd(a - q.b \; ; b)$; $q \in \mathbb{Z}$

③ $d = gcd(a, b + k.a)$; $k \in \mathbb{Z}$

④ $d = gcd(a, b - k.a)$; $k \in \mathbb{Z}$

اثبات ①:

ليكن $d_1 = gcd(a+q.b, b)$ ولنثبت أنّ $d = d_1$ يكفي أن نثبت أنّ $d_1 | d$ و $d | d_1$.

لدينا $d_1 = gcd(a+q.b, b)$ بالتّالي

$d_1 | (a+q.b)$

$d_1 | b \Rightarrow d_1 | qb$

$\left.\begin{matrix} d_1 | (a+q.b) \\ d_1 | q.b \end{matrix}\right\} \Rightarrow d_1 | (a+q.b-q.b) \Rightarrow d_1 | a$ ①

بما أنّ $d_1 | a$ & $d_1 | b \Leftarrow d_1 | gcd(a,b) \Leftarrow d_1 | d$

ولدينا $d = gcd(a,b)$ بالتالي:

$\left.\begin{matrix} d | a \\ d | b \Rightarrow d | q.b \end{matrix}\right\} \Rightarrow \left.\begin{matrix} d | (a+qb) \\ \& \; d | b \end{matrix}\right\} \Rightarrow d | gcd(a+qb, b)$

$\Rightarrow d | d_1$ ②

من ① و ② نجد أنّ $d = d_1$.

• **ملاحظة:** إذا كانت $d = gcd(a,b)$ و $m \neq 0$ عندئذٍ:

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

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

$0 \leq r < |b|$; $a = q.b + r$ عندئذٍ فإنّ:

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

الاثبات:

$d=gcd(a,b) = gcd(qb+r, b) = gcd(qb+r-qb, b)$
$= gcd(r, b)$

• خوارزميّة اقليدس في إيجاد القاسم المشترك الأعظم للعددين a, b :

نعلم أنّ $gcd(a,b) = gcd(|a|, |b|)$

لذا نفرض $b \neq 0, a \neq 0$ ونشرح الخوارزمية كما يلي :

$b = q_1 a + r_1$; $0 \leq r_1 < a$

فإذا كانت $r_1 = 0$ فإنّ $gcd(a,b) = gcd(a,0) = a$

أما إذا كانت $r_1 \neq 0$ نتابع القسمة $a = q_2 r_1 + r_2$; $0 \leq r_2 < r_1$

فإذا كانت $r_2 = 0$ فإنّ

$gcd(a,b) = gcd(a, r_1) = gcd(r_1, 0) = r_1$

وإذا كانت $r_2 \neq 0$ نكتب $r_1 = q_3 r_2 + r_3$

ونتابع حتّى نصل على باقي صفري ونكتب $r_{t-1} = q_{t+1} \cdot r_t + 0$

عندئذٍ يكون $gcd(a,b) = gcd(a, r_1) = gcd(r_1, r_2) = \cdots$

$= gcd(r_t, r_{t+1}) =$

$gcd(r_t, 0) = r_t$ حيث $a > r_1 > r_2 > \cdots > r_t > 0$

أي للبحث عن القاسم المشترك الأعظم لعددين موجبين نطبق خوارزمية القسمة بشكل متتالٍ حتّى نصل إلى باقي صفري ويكون الباقي الأخير قبل الباقي الصفري هو القاسم المشترك الأعظم الذي نبحث عنه.

مثال: أوجد القاسم المشترك الأعظم للعددين $b = 3054$ و $a = 12378$ ثمّ اكتب القاسم المشترك الأعظم لهما كتركيب خطي بهما؟

الحل:

$12378 = 4 \times 3054 + 162$

$3054 = 18 \times 162 + 138$

$162 = 1 \times 138 + 24$

$138 = 5 \times 24 + 18$

$24 = 1 \times 18 + \boxed{6}$

$18 = 3 \times 6 + 0 \Rightarrow \gcd(a,b) = 6$

• لكتابة 6 كتركيب خطي لـ a و b:

$d = 6 = 24 - 18$

$= 24 - (138 - 5 \times 24)$

$= 6 \times 24 - 138$

$= 6(162 - 138) - 138 = 6 \times 162 - 7 \times 138$

$= 6 \times 162 - 7(3054 - 18 \times 162)$

$= 132 \times 162 - 7 \times 3054$

$= -7 \times 3054 + 132(12378 - 4 \times 3054)$

$= -7 \times 3054 + 132 \times 12378 - 528 \times 3054$

$= 132 \times 12378 - 535 \times 3054$

$\Rightarrow \boxed{d = 132a - 535b}$

• القاسم المشترك الأعظم لمجموعة أعداد صحيحة:

تعريف: a_i ; $i = 1, 2, 3, \ldots$ أعداد صحيحة ليست جميعها أصفار يُقال إنّ d هو القاسم المشترك الأعظم لها ونكتب $d = \gcd(a_1, \ldots, a_n)$ إذا وفقط إذا كان:

1- $d > 0$

2- $d \mid a_i \quad \forall\, 1 \le i \le n$

3- إذا كان $c \mid a_i$ حيث $1 \le i \le n$ و $c > 0$ فإنّ $c \le d$ أي $c \mid d$

• ملاحظة: $d = \gcd(a_1, a_2, \ldots, a_{n-1}, a_n)$

$= \gcd(a_1, a_2, \ldots, a_{n-2}, \gcd(a_{n-1}, a_n))$

مثال: لإيجاد $\gcd(256, 112, 72)$ لدينا

$\gcd(256, 112, 72) = \gcd(256, \gcd(112, 72)) =$

$\gcd(256, 8) = 8$

تعريف: إذا كان القاسم المشترك الأعظم للأعداد غير صفرية معاً $(a_1, \ldots, a_n)$ يساوي الواحد عندئذٍ نقول أن الأعداد a_i أولية فيما بينها.

مثال: $\gcd(4, 14, 21) = 1$

⇐ الأعداد 4 و 14 و 21 أولية فيما بينها.

انتهت المحاضرة