نظريّة الأعداد

مدرّس المقرّر

الدكتور نادر ضبّيط

الفصل الثاني: الأعداد الصحيحة (Integer)

(1-1)مبرهنة (خوارزمية القسمة):

من أجل أي عددين صحيحين a , b بحيث أحدهما ، وليكن a ،موجباً، فإنه يوجد عددان صحيحان وحيدان r , q بحيث يتحقق

$$b = qa + r \quad ; \quad 0 \le r < a$$

(نسمي q ناتج قسمة b علىa ، r باقي هذه القسمة، و من الواضح تحقق التكافؤات الآتية: $r = 0 \quad \Leftrightarrow \quad b = qa \quad \Leftrightarrow \quad a|b$)

البرهان: لنبرهن أولاً على وجود العددين q , r ، ثم نبرهن على وحدانيتهما ، إنّ المجموعة $S = \{x \in \mathbb{Z} \ | x = b - ta \ge 0 \quad ; \quad t \in \mathbb{Z}\}$ الجزئية من مجموعة الأعداد الصحيحة غير السالبة ليست خالية لأن العدد $(b - ta)$ يكون غير سالب إذا وفقط إذا كانت $t \le b \,/\, a$ ، وهذه القيم لـ t موجودة دائماً. وبالتالي، حسب مبدأ الترتيب الحسن ، يوجد عنصر أصغر في المجموعة S وليكن r توافقه قيمة للعدد الصحيح t ولتكن q وبالتالي نحصل على أن $r = b - qa$ ومنه $b = qa + r$ ، ومن تعريف عناصر المجموعة S فإن $r \le 0$، لنبين أن $r < a$.لذلك نفرض جدلاً أن $r \ge a$ ومنه : $0 \le r - a = b - qa - a = b - (q + 1)a$ وهذا يجعل من العدد $(r - a)$ عنصراً من S ، ويحقق $r - a < r$ حيث $(a > 0)$ وهذا يناقض كون r عنصراً أصغر في المجموعة S ، إذاً الفرض الجدلي بأن $r \ge a$ ليس صحيحاً ، إذاً $r < a$.

ثانياً ، لنبرهن على وحدانية العددين q , r المحققان لـ $0 \le r < a$ و $b = qa + r$ (1) . لذلك نفرض وجود عددين صحيحين $\grave{r}$، $\grave{q}$ بحيث $0 \le r \grave{<} a$ و$b = q\grave{a} + \grave{r}$ (2) . بطرح (2) من (1) نحصل على $r - \grave{r} = (q - \grave{q})a$ (3) ومنه $\frac{r'-r}{\mathrm{a}} = \mathrm{q} - \mathrm{q}'$ ، وبجمع المتباينتين:

$0 \le r' < a \quad ; \quad -a < -r \le 0$. نجد أن $-a < r' - r < a$ ، وبالتالي نحصل على أن $-1 < \frac{r'-r}{\mathrm{a}} < 1$ ، وبما أن $\frac{r'-r}{\mathrm{a}} = \mathrm{q} - q'$

عدد صحيح فان $q - q \grave{=} 0$ ومنه $q = \grave{q}$ وبالتعويض في العلاقة (3) نجد $r = \grave{r}$ ، وهذا يبين أن العددين q , r وحيدان .

نتيجة (1): (تعميم خوارزمية القسمة)

إذا كان a,b عددين صحيحين ، وكان a مختلفاً عن الصفر ، فإنه يوجد عددان صحيحان وحيدان q , r بحيث: $b = qa - r \quad ; \quad 0 \le r < |a|$

البرهان: عندما $0 < a$ فان $\mathrm{a} = |a|$ والنتيجة السابقة صحيحة لأنها تمثل خوارزمية القسمة . إذا لنبرهن النتيجة عندما $a < 0$. في هذه الحالة $|a| = -a$ ، وبما أن $|a|$ عدد صحيح موجب فإننا نستطيع تطبيق مبرهنة خوارزمية القسمة على العددين $|a|, b$ التي تؤكد وجود عددين صحيحين ووحيدين $\dot{q}$,r بحيث $0 \le r < |a| \quad ; \quad b = \dot{q}\,|a| + r = q'(-a) + r = qa + r$ ، وحيث $\mathrm{q} = -\dot{q}$. وهكذا نجد أن :

$0 \le r < |a| \quad ; \quad b = qa + r$ ، ويتم المطلوب .

مثال : إذا كان $b = -7$ فإنه بالقسمة العادية على العدد $0 < a = 3$ نجد أن ناتج القسمة هو $q = -3$ وباقي القسمة هو $r = 2$ وبالتالي فإنّ $-7 = -3(3) + 2$. أما إذا كان $a=-3$ فإننا نجد أن 2+3(-3)=-7 . وكما ذكرنا ، فإنّq يسمّى ناتج قسمة bعلىa، أما العدد غير السالب r فإنه يسمى باقي هذه القسمة . في الحالة الخاصة ، عندما $r = 0$ فان ذلك يكافئ قولنا إن a يقسم b .

(1-2) قابلية القسمة(divisibifily)

تعريف (1-1): نقول عن عدد صحيح مختلف عن الصفر a إنه قاسم (divisor) للعدد الصحيح b ونكتب $\mathrm{a} \mid \mathrm{b}$ إذا (وفقط إذا) وجد عدد صحيح c يحقق $\mathrm{b} = \mathrm{c} \,.\, \mathrm{a}$ ، أما إذا لم يتحقق ذلك قلنا إن a لا يقسم b ونكتب $\mathrm{b} \nmid \mathrm{a}$.

ونستطيع بالحقيقة قراءة الرمز $\mathrm{a} \mid \mathrm{b}$ بعدة أشكال،بالإضافة إلى قراءتنا a يقسم b ، نقول b مضاعفاً لـ a ، أو b يقبل القسمة على a ، وأيضاً a عامل في b

مثال: العدد 4 يقسم العدد 12 (لأن $4 \times 3 = 12$) فنكتب $4 \mid 12$ ، ونفس الرمز يصلح لقولنا العدد 4 عامل في 12 وأن العدد 12 مضاعفاً للعدد 4 . ونلاحظ أن العدد 4 لا يقسم العدد 15 ، فنكتب $4 \nmid 15$ والتي يمكن أن نعبر عنها بقولنا إن العدد15 ليس مضاعفاً للعدد 4 .

نتائج مباشرة :

1- مهما كان العدد الصحيح a فإنه يكتب بالشكل a=1.a وبالتالي فإن $1 \mid a$ وإذا كان $a \ne 0$ فإن $a \mid a$.
2- $0 = 0 \,.\, a$ لكل a من $\mathbb{Z}$ ، مجموعة الأعداد الصحيحة، وبالتالي فإن $a \mid 0$.
3- إن كل قاسم موجب x لعدد صحيح a يوافقه قاسم سالب x– وبالعكس لأن $x|a \ \Leftrightarrow \ -x|a$.

مبرهنة(1-1)(خواص اساسية لمفهوم القسمة):

مهما كانت الأعداد الصحية a , b , c فانه يتحقق:

1- إذا كان العدد الصحيح $a \ne 0$ فإن كلاً من العدد a وقيمته المطلقة $|a|$ يقسم الآخر .
2- إذا كان العدد a يقسم كلاً من العددين b , c فإنه يقسم أي تركيب خطي لهما $bx + cy$ وحيث x , y عددين صحيحين . ونعبر عن هذه الخاصة رمزياً بالشكل : $\forall\, x, y \in z \qquad a|(bx + cy) \qquad \Rightarrow \qquad a|c \ \wedge \ a|b$.
3- إذا كان العدد a يقسم العدد b ، فإن a يقسم حاصل ضرب b بأي عدد صحيح c أي أنّ : $\forall\, c \in \mathbb{Z} \qquad a|bc \qquad \Rightarrow \qquad a|b$

(لاحظ أن العكس ليس صحيحاً . قدم مثالاً على ذلك)

4- إذا كان العدد a يقسم العدد b وكان b بدوره يقسم العدد c فإن a يقسم c أيّ : $a|b \quad \wedge b|c \quad \Rightarrow \quad a|c$

(نعبر عن هذه الخاصة بقولنا إن علاقة القسمة على الأعداد متعدية)

5- إذا كان كل من العددين a , b عدداً صحيحاً موجباً وكان $a|b$ فان $a \leq b$. أي أنّ : $a|b \quad \wedge \ a > 0 \quad \wedge \ b > 0 \quad \Rightarrow \quad a \leq b$

6- إذا كان العدد a يقسم العدد b فإن القيمة المطلقة لـ a تقسم القيمة المطلقة لـ b . أي أن: $a|b \implies |a||b|$

7- إذا كان كل من العددين a , b يقسم الآخر فإن $|a| = |b|$. (أي أن $a = \mp b$) . وبشكل رمزي: $a|b \ \wedge \ b|a \implies |a| = |b|$

البرهان :

1- نعلم أن $|a| = \pm a \ = \ (\pm 1)a$ وبالتالي فإن $a = \mp|a| = (\pm 1)|a|$ ، أي أن كل من $|a|$ و a يقسم الآخر .

2- $a|b \quad \wedge \quad a|c \quad \Rightarrow \quad \exists\, d,e \in \mathbb{Z} \ ; \ b = da \ \wedge \ c = ea$ ،

وبالتالي من أجل أي عددين صحيحين x, y يتحقق :

$a|(bx + cy)$. وبما أن $bx + cy = dax + eay = \ a(dx + ey)$عدد صحيح فإن المساواة الأخيرة تبين لنا أن

3- بما أن $a|b$ فإنه يوجد عدد صحيح d بحيث $b = ad$ ، وبضرب الطرفين بـ c نجد أن $bc = a(cd)$ وهذا يبين لنا أن $a|bc$.

4- $\left.\begin{matrix} a|b \implies \exists\, d \in \mathbb{Z} \ ; b = ad \\ b|c \implies \exists\, e \in \mathbb{Z} \ ; \ c = be \end{matrix}\right\} \Rightarrow c = a(e.d) \Rightarrow \mathrm{a}|c$

5- $a|b \quad \wedge \quad a > 0 \quad \wedge \quad b > 0 \quad \Rightarrow \quad \exists \ c \in \mathbb{Z}^+ \ ; \ \ b = ac$

إن $c \geq 1$ ، وبضرب الطرفين بـ $a > 0$ نجد أن $a \leq ac$ أي أن $a \leq b$.

6- $|a||b| \implies |b| = |a|.|c| \implies \exists\ c \in \mathbb{Z} \ ; \ b = ac \implies a|b$.

طريقة ثانية : $|a|\big||b| \implies |a|\big|b \ \wedge \ b\big||b| \implies |a|\big|a \ \wedge a\big|b$.

7- $\boldsymbol{a\big|b \quad \wedge \quad b\big|a \quad \Rightarrow \quad |a|\big||b| \ \wedge \quad |b|\big||a| \Rightarrow}$

$\boldsymbol{|a| \leq |b| \quad \wedge \quad |b| \leq |a| \quad \Rightarrow \quad |a| = |b|}$

تطبيقات خوارزمية القسمة

A) تصنيف الأعداد الصحيحة وفق صفات محددة :

1- كل عدد صحيح b يكتب بالشكل $2k$ أو $2k + 1$ وحيث k عدد صحيح يتعلق بالعدد b .

لبرهان ذلك نأخذ العدد $a = 2$ وb أي عدد صحيح ، وبالتالي حسب خوارزمية القسمة يوجد عددان صحيحان وحيدان k, r بحيث $0 \leq r < 2$ ؛ $b = 2k + r$، وبالتالي العددr يأخذ القيم $r = 0,1$ ومنه نجد أن $b = 2k + 1 \quad \vee \quad b = 2k$

وبذلك نكون قد برهنا على أن كل عدد صحيح b يكتب بالشكل $2k$ أو بالشكل $2k+1$ وحيث k عدد صحيح ما ، وهذا يكافئ قولنا إن كل عدد صحيح إما أن يكون زوجياً أو أن يكون فردياً .

2- إن كل عدد صحيح **فردي** b يكتب بالشكل $4k + 1$ او $4k + 3$ وحيث k أي عدد صحيح .

وكذلك كل عدد صحيح **زوجي** يكتب بالشكل $4k$ او $4k + 2$ وحيث k أي عدد صحيح .

يتم برهان ذلك بأخذ $a = 4$ وb أي عدد صحيح ، فإنه حسب خوارزمية القسمة يوجد عددان صحيحان وحيدان k, r بحيث

$$b = 4k + r \quad ; \quad 0 \leq r < 4$$

إن القيم التي يأخذها العدد الصحيح r هي $r = 0,1,2,3$ ومنه نجد أن للعدد b أحد الأشكال التالية: $b = \begin{cases} 4k \\ 4k + 1 \\ 4k + 2 \\ 4k + 3 \end{cases}$

فإذا كان b فردياً يكتب بأحد الشكلين $4k + 3$ ، $4k + 1$، وإذا كان b زوجياً يكتب بأحد الشكلين $4k + 2$ ،$4k$ ويتم المطلوب .

3- إن كل عدد صحيح **فردي** b يكتب بأحد الأشكال : $6K + 5$, $6K + 3$, $6K + 1$

وإن كل عدد صحيح **زوجي** b يكتب بأحد الأشكال : $6k + 4$, $6k + 2$, $6k$. البرهان يتم بطريقة البندين السابقين نفسها

بشكل عام : إذا كان n عدداً صحيحاً موجباً فإن كل عدد صحيح x يكون من أحد الأشكال:$nk\ ,\ nk+1\ ,\ \ldots\ldots,\ nk+(n-1)$
من الواضح أن باقي قسمة أي عدد صحيح x على $0<n$ يكون أحد عناصر المجموعة$z_n=\{0,1,2,\ldots,n-1\}$ والتي تسمى مجموعة بواقي القسمة على العدد الصحيح الموجب n .

4- إن مربع أي عدد صحيح b يكتب بأحد الشكلين : $4k\ ,\ 4k+1$ حيث k عدد صحيح .

البرهان : يتم البرهان بالاعتماد على (1) . بما أن كل عدد صحيح b يكتب بأحد الشكلين $2q$ أو $2q+1$، فإن مربعه b^2 يكتب بأحد الشكلين $(2q+1)^2=4(q+q^2)+1$ أو $4q^2$ ، أي بأحد الشكلين $4k$ أو $4k+1$ وحيث k عدد صحيح .

B) تمثيل الأعداد الصحيحة (Representation of integers)

في النظام العشري المعروف، نستخدم الأرقام من صفر إلى تسعة، لتكوين أي عدد في هذا النظام، لذلك نسمي هذه الأرقام العشرة (من الصفر إلى تسعة) بأرقام النظام (digits)، بينما عدد هذه الأرقام (وهو عشرة في نظامنا) فإنه يسمى أساس النظام.
هناك الكثير من الأنظمة العددية بالإضافة إلى النظام العشري، مثل النظام الذي أساسه 20، والنظام الذي أساسه 60، وأهمها النظام الذي أساسه 2، الذي يسمى بالنظام الثنائي (binary system). المبرهنة التالية تبين أن:
كل عدد صحيح أكبر من الواحد يمكن أن يكون أساساً لنظام عددي، وهذه الحقيقة يمكن برهانها بالاعتماد على نظرية خوارزمية القسمة أيضاً.

مبرهنة (1,3):
إذا كان k عدداً صحيحاً أكبر من الواحد فإننا نستطيع كتابة أي عدد صحيح موجب N بطريقة وحيدة بالشكل:

$N=a_mk^m+a_{m-1}k^{m-1}+\ldots\ldots\ldots+a_2k^2+a_1k+a_0$ ، وحيث المعاملات a_i تأخذ قيماً صحيحة تحقق $a_m\neq 0\ ,\ 0\le a_i<k$.

البرهان:

برهان الوجود: بتطبيق خوارزمية القسمة على العددين K,N ، فإنه يوجد عددان صحيحان وحيدان q_1,a_0 بحيث: $N=q_1K+a_0\ ;\ 0\le a_0<k$
إذا كان ناتج القسمة $k\le q_1$ فإننا نطبق خوارزمية القسمة مرة **ثانية** على العددين q_1,K ونحصل على عددين صحيحين ووحيدين q_2,a_1 بحيث:

$$q_1=q_2K+a_1\ ;\ 0\le a_1<K$$

وبالتعويض عن قيمة q_1 في المعادلة الأولى نحصل على المساواة: $N=(q_2K+a_1)k+a_0=q_2k^2+a_1K+a_0$
(قارن مع الصيغة الواردة في نص المبرهنة، حيث العوامل a_i يجب أن تكون أصغر من K)
وهكذا نستطيع تكرار ما تقدم وتطبيق خوارزمية القسمة علي العددين K و q_{m-1} (وحيث $K\le q_{m-1}$) إلى أن نحصل على العددين الوحيدين q_m,a_{m-1}، بحيث:

$$q_{m-1}=q_mK+a_{m-1}\ ;\ 0\le a_{m-1}<K\ ;$$

(إن $q_1>q_2>\ldots>q_m>0$ متتالية متناقصة وبالتالي لابد من الحصول في خطوة m على أن $0<q_m<K$ عند ذلك نتوقف، ونضع$0<a_m=q_m$
وبتعويض كل قيمة لـ q_i بعبارة q_{i-1} التي تسبقها (وهكذا حتى عبارة N) فإننا نحصل على:

$$N=a_mk^m+a_{m-1}k^{m-1}+\ldots.+a_2k^2+a_1k+a_0 \qquad (1)$$

وحيث المعاملات a_i تحقق $0\le a_i<k$ من أجل كل $0\le I<m$
(إن الشرط $k\le q_{m-1}$ يضمن أن ناتج قسمة q_{m-1} على k (وهو q_m) أكبر من الصفر)
برهان **الوحدانية**: نفرض أن العدد N يكتب بطريقتين كما يلي :

$$N=a_mk^m+a_{m-1}k^{m-1}+\ldots\ldots\ldots\ldots+a_1k+a_0 \qquad ;0\le a_i<k$$
$$=b_nk^n+b_{n-1}k^{n-1}+\ldots\ldots\ldots\ldots+b_1k+b_0 \qquad ,0\le b_j<k$$

ولنفرض أن $m\ge n$ ، عند ذلك بإضافة حدود معاملاتها أصفاراً في التمثيل الثاني فإنه يمكننا الفرض بأن $m=n$ ، وبالطرح نحصل على أن:

$$(a_m-b_m)k^m+(a_{m-1}-b_{m-1})k^{m-1}+\ldots\ldots\ldots\ldots+(a_1-b_1)k+(a_0-b_0)=0 \qquad (2)$$

لنبرهن على أن جميع المعاملات في (2) مساوية للصفر وذلك بنقض الفرض، نفرض جدلاً وجود معامل (على الأقل) لايساوي صفراً، وليكن (a_i-b_i) أول معامل يختلف عن الصفر في العلاقة (2) (اعتباراً من الحد الثابت) بحذف الحدود التي معاملاتها أصفاراً، وبنقل الحد $(a_i-b_i)k^i$ إلى الطرف الأيمن من العلاقة (2) نحصل على المساواة:

$$(a_m-b_m)k^m+(a_{m-1}-b_{m-1})k^{m-1}+\ldots\ldots\ldots\ldots(a_{i+1}-b_{i+1})k^{i+1}=-(a_i-b_i)k^i$$

بتقسيم الطرفين على k^i وإخراج k عاملاً مشتركاً فإن المساواة الأخيرة تكتب بالشكل:

$$\left[(a_m-b_m)k^{m-i-1}+(a_{m-1}-b_{m-1})k^{m-i-2}+\cdots+(a_{i+1}-b_{i+1})\right]k=-(a_i-b_i) \quad \ldots\ldots \qquad (3)$$

من العلاقة الأخيرة (3) نجد أن : $k\ |-(a_i-b_i)|$ وبالتالي $|a_i-b_i|\ |k$ ومنه نجد حسب خواص القسمة أن:$k\le|a_i-b_i|$
ولكن $0\le b_i<k$ و $0\le a_i<k$ و $a_i-b_i\neq 0$ وبالتالي فإن $0<|a_i-b_i|<k$ ، وهذا يتناقض مع $k\le|a_i-b_i|$ ، إذاً:
الفرض الجدلي بوجود معاملات مختلفة عن الصفر غير صحيح. إذاً: $a_i-b_i=0$ لكل $i=0,1,2,\ldots\ldots\ldots m$ وبالتالي N يمثل بشكل وحيد.
ملاحظة: عادة يرمز لتمثيل عدد بالأساس k كما يلي :$a_mk^m+a_{m-1}k^{m-1}+\ldots\ldots\ldots+a_1k+a_0=(a_m\ a_m\ldots\ldots\ldots\ldots a_1\ a_0)_k$

مثال (1) لنكتب العدد 35 بالأساس 2.

لدينا N=35 و K=2 . بتطبيق خوارزمية القسمة عليهما نجد أن: $q_1 = 17 > 2 = K$; $N=35=(17)2 + 1$

$q_1=17=(8)2 +1$; $q_2 = 8 > 2$

$q_2=8=(4)2+0$; $q_3 = 4 > 2$

$q_3=4=(2)2+0$; $q_4 = 2 \geq 2$

$q_4=2=(1)2+0$; $q_5 = 1 < 2 \Rightarrow q_5=a_5$

وبالتالي نحصل على التمثيل الثنائي للعدد (35): $35=(1\ 0\ 0\ 0\ 1\ 1)= 1\times2^5+0\times2^4+0\times2^3+0\times2^2+1\times2+1\times2^0$

مثال(2) اكتب العدد N=61469 بالأساس k=16 .

بتطبيق خوارزمية القسمة على العدد k=16 والعدد N نجد:

$16,61469 \xrightarrow{\text{خ.ق}} N=61469 =(3841)\times16+13$; $q_1=3841>16=k$

$3841=(240)\times16+ 1$; $q_2=240>16$

$240=(15)\times16+0$; $q_3=15<16$

الآن لنضع $q_3=a_3$ فنحصل على التمثيل الستة عشري(hexadecimal system) للعدد المعطى كما يلي :

$61469=(a_3\ a_2\ a_1\ a_0\ )_{16}=(\ 15\ 0\ 1\ 13\ )_{16}$

وعادة في النظام الستة عشري نعبر عن الأعداد 10,11,12,13,14,15 ،على الترتيب ، بالأحرف A,B,C,D,E,F على الترتيب.

وبالتالي فإن العدد المعطى يكتب على هذا الأساس بالشكل:$(F\ 0\ 1\ D\ )_{16}$ = 61469 .

القاسم المشترك الأكبر: (g.c.d= Greatest common divisor)

من المعروف أن القواسم الصحيحة للعدد 10 مثلاً هي ،بالإضافة إلى 10-,10+,1-,1+ ، الأعداد 5-,5+,2-,2+ لأن : $10=2\times5=(-2)(-5)$

وذلك حسب مفهوم القاسم في مجموعة الأعداد الصحيحة.

ونلاحظ أن كل قاسم موجب x للعدد 10 يقابله القاسم السالب x– وبالتالي يكفي دراسة القواسم الموجبة لعدد، دون الإنقاص من عمومية هذه الدراسة.

فإذا كان a عدداً صحيحاً فإننا سنرمز لمجموعة القواسم الموجبة لهذا العدد بالرمز D(a) أي أن: $D(a) = \{x \in \mathbb{Z}^+; x|a\}$. فمثلاً عندما a=10 فإن: D(10)={1,2,5,10} . ومن المفيد هنا لعدم نسيان أي قاسم كتابة جدول من الشكل: $10=1\times10$

$=2\times5$

$=3\times$--

$=4\times$--

$2\times5=$ (مكرر)

والذي يبين وبالترتيب (من الأعلى في الطرف الأيمن نزولاً بالأرقام ..1,2,3, ثم العودة من الأسفل إلى الأعلى) القواسم الموجبة للعدد 10. لنوجد كتطبيق على ذلك مجموعة القواسم الموجبة للعدد 32 فنكتب: $32=1\times32$

$=2\times16$

$=3\times$--

$=4\times8$

$=5\times$--

$=6\times$--

$=7\times$--

$8\times4=$(مكرر) ومنه $D(30) = \{1,2,4,8,16,32\}$

- إذا كانت D(b) و D(a) مجموعتي القواسم الموجبة للعددين الصحيحين a , b ، بحيث أن أحد العددين a , b مختلفاً عن الصفر ، فإنه من الواضح أن تقاطعهما D(a)∩D(b) يمثل مجموعة القواسم الموجبة المشتركة للعددين a , b والتي نرمز لها بـ D(a,b) .أي أن:

$$D(a , b) = D(a) \cap D(b) = \{x \in \mathbb{Z}^+;\ x\ |a\ \wedge\ x\ |b\}$$

ومن الواضح أن هذه المجموعة منتهية وغير خالية، وبالتالي تحوي دوماً عنصراً أكبر، الذي نرمز له بالرمز g.c.d (a ,b) أو اختصاراً (a,b) ونسميه القاسم المشترك الأكبر للعددين الصحيحين a , b .

فمثلاً لإيجاد القاسم المشترك الأكبر للعددين 10,32 نوجد العنصر الأكبر للمجموعة: $D(10,32)=D(10)\cap D(32)=\{1,2\}$
والذي من الواضح أنه العدد 2، لذلك نكتب $(10,32)=2$ أو $g.c.d\ (10,32)=2$ ، نقرأ ذلك :القاسم المشترك الأكبر للعددين 10,32 هو2 .
-من السهل تعميم مفهوم القاسم المشترك الأكبر لعددين على ثلاثة أعداد أو أكثر، بحيث أحدها على الأقل مختلف عن الصفر، كما يلي:
إذا كانت $a_1, a_2, \dots, a_n$ أعداداً صحيحة ليست جميعها أصفاراً ، وكانت $D(a_1), D(a_2), \dots, D(a_n)$ مجموعات القواسم الموجبة لكلّ منها ، التي تقاطعها يمثّل مجموعة القواسم المشتركة الموجبة للأعداد $a_1, a_2, \dots, a_n$ ، والتي نرمز لها بالرّمز :
$D(a_1, a_2, \dots, a_n) = D(a_1) \cap D(a_2) \cap \dots \cap D(a_n)$ ، والتي من الواضح أنّها مجموعة منتهية (لأنّ أحد الاعداد مختلف عن الصّفر وليكن a_i الذي تكون مجموعة قواسمه $D(a_i)$ منتهية) وغير خالية (لأنّ العدد 1 ينتمي إلى كل منها)، وبالتالي تحوي عنصر أكبر وحيد نرمز له بالرّمز $\gcd(a_1, a_2, \dots, a_n)$ أو $(a_1, a_2, \dots, a_n)$ اختصاراً ، نسمّيه القاسم المشترك الأكبر للأعداد $a_1, a_2, \dots, a_n$.

مثال: لإيجاد القاسم المشترك الأكبر للأعداد الثلاثة 10,32,18 ، نوجد العنصر الأكبر للمجموعة :
$D(10,32,18) = D(10) \cap D(32) \cap D(18) = \{1,2\} \cap \{1,2,3,6,9,18\} = \{1,2\}$ والذي من الواضح أنّه العدد2 أيّ أنّ $(10,32,18) = 2$
مما تقدّم نلاحظ أنّه إذا كانت الأعداد المراد إيجاد القاسم المشترك الأكبر لها كبيرة فإنّ العمليّة السّابقة طويلة ، لذلك لا بدّ من إيجاد خوارزميّة تقدّم طريقة لحساب القاسم المشترك الأكبر ، من أجل ذلك سوف نبدأ أوّلاً بتقديم مفهوم القاسم المشترك الأكبر لعددين أو أكثر ليست جميعها أصفاراً ،بشكل مجرد وبدون استخدام المجموعات والعمليات عليها، للاستفادة من ذلك في تقديم مبرهنات توصلنا إلى خوارزميّة مفيدة في هذا المجال (والتي ستعرف بخوارزميّة إقليدس) وتسهيل عملية تعميم هذا المفهوم على بنى جبرية أخرى لاسيما الحلقات .

تعريف: (القاسم المشترك الأكبر لعددين)
ليكن a,b عددين صحيحين ليس كلاهما صفراً ، نقول عن العدد الصّحيح الموجب d إنّه القاسم المشترك الأكبر للعددين a,b إذا وفقط إذا تحقّق الشّرطان:

1. $d \mid a \wedge d \mid b$ (أيّ أنّ d قاسماً مشتركاً للعددين a , b) .
2. إذا كان العدد الصّحيح الموجب c قاسماً مشتركاً آخر للعددين a , b (أي إذا كان $c>0 , c \mid a , c \mid b$) فإنّ $c \le d$.

ونرمز عادةً للقاسم المشترك الأكبر للعددين a , b بالرّمز gcd (a , b) أو اختصاراً (a , b) .

تعريف (القاسم المشترك الأكبر لأكثر من عددين)
ليكن $a_1, a_2, \dots, a_n$ أعداداً صحيحة ليست جميعها أصفاراً ، نقول عن العدد الصّحيح الموجب d إنّه القاسم المشترك الأكبرللأعداد $a_1, a_2, \dots, a_n$ ونرمز له بالرّمز $\gcd(a_1, a_2, \dots, a_n)$ ، أو اختصارا $(a_1, a_2, \dots, a_n)$ ، إذا وفقط إذا تحقّق الشرطان :

1. $d \mid a_i$ لكل $1 \le i \le n$ (أيّ أنّ d قاسم مشترك للأعداد $a_1, a_2, \dots, a_n$).
2. إذا كان c عدداً صحيحا موجبا بحيث $c \mid a_i$ لكلّ $1 \le I \le n$ فإنّ $c \le d$.

ملاحظة:في التعريف السّابق ورد مايلي (d القاسم المشترك الأكبر للعددين a , b)، التي تعني وجود هذا القاسم ووحدانيّته ، هذه الوحدانيّة (التي كانت واضحة في التمهيد لمفهوم القاسم المشترك الأكبر باستخدام المجموعات) تبرهن بسهولة كمايلي :
نفرض وجود عددين صحيحين موجبين d, d' يحقّقان تعريف القاسم المشترك الأكبر ، وبالتالي حسب الشّرط الثاني من التّعريف نجد أنّ $d \mid d'$ ، وأنّ $d' \mid d$ ، وبالتّالي من خواصّ القسمة نجد أنّ $d = \mp d'$ ، لكن بما أنّ كلّاً من d, d' موجبين فإنّه ينتج أنّ $d = d'$.
وأمّا الوجود فإنه سيقدّم في المبرهنة الهامّة الآتية ، بعد أن نورد المثال الآتي :
مثال: لاحظ ما يأتي:

$$(0,-2) = 2 \text{ ، } (0,2) = 2 \implies (0,a) = |a| \ \ \forall a \in \mathbb{Z} - \{0\} .$$

$$(-3,6) = 3 \text{ , } (3,6) = 3 \implies$$

$$a \mid b \implies (a,b) = |a|$$

$$(1,-6) = 1 \implies (\mp 1, a) = 1 \ \ \forall\, a \in \mathbb{Z} \qquad (1,6) = 1 \text{ , }$$

إنّ للقاسم المشترك الأكبر لعددين صحيحين صيغة هامّة نقدّمها في المبرهنة الآتية:
مبرهنة: (القاسم المشترك الأكبر لعددين هو تركيب خطّي لهما)
إذا كان a , b عددين صحيحين ليس كلاهما صفراً ، فإنّه يوجد عددان صحيحان x_0, y_0 بحيث $(a,b) = ax_0 + by_0$ ،(نسمّي العبارة $ax + by$ تركيباً خطيّاً للعددين a,b) .
البرهان: [الفكرة: هي برهان أنّ مجموعة كلّ التراكيب الخطيّة الموجبة للعددين a,b هي مجموعة غير خالية وأنّ العنصر الأصغر فيها يمثّل (a,b)]
بما أنّ a,b ليس كلاهما صفراً فإنّ المجموعة $S = \{ax + by > 0 \mid x, y \in \mathbb{Z}\}$ غير خالية ، لأنّه إذا كان $a \neq 0$ فإنّ $|a| > 0$ يكون عنصرا من S لأنّه يكتب بالشّكل $|a| = \frac{|a|}{a}.a + 0.b$ وحيث $\frac{|a|}{a} = \pm 1$ عنصرا من $\mathbb{Z}$. وبالتالي فإنّ المجموعةS غير خالية ، وهي جزئيّة من مجموعة الأعداد الصّحيحة الموجبة ، وبالتالي فهي تملك عنصراً أصغر (حسب مبدأ الترتيب الحسن) وليكن d ، الذي من أجله يوجد عددان صحيحان x_0, y_0 بحيث

$d = ax_0 + by_0$. لنبرهن على أنّ هذا العدد الموجب هو القاسم المشترك الأكبر للعددين a , b ، لذلك نبرهن أولاً على أنّ $d|a \wedge d|b$ ، وذلك بنقض الفرض . نفرض جدلاً أنّ $d \nmid a$، وبتطبيق خوارزميّة القسمة على العددين a,d حيث (d>0) فإنّه يوجد عددان صحيحان وحيدان q,r بحيث : a=dq+r ; 0<r<d . ومنه نستطيع كتابة : $r = a - dq = a - (ax_0 + by_0)q = a(1 - x_0q) + b(-y_0q)$ ، وهذا يبيّن أنّ r عنصراً من S ، ولكن r<d يتناقض مع كون d هو العنصر الأصغر في S ، إذاً يجب أن يكون d|a. بالطّريقة نفسها نبرهن على أنّ d|b .

لنبرهن ثانياً على أنّه إذا كان c عدداً صحيحاً موجباً يقسم كلّاً من a , b فإنّ c ≤ d ، من خواصّ القسمة نستطيع كتابة :

$$c|a \wedge c|b \Rightarrow c|ax_0 + by_0 \Rightarrow c|d \xrightarrow{c>0\ ,d>0} c \leq d$$

من أوّلاً و ثانية نجد أنّ $d = ax_0 + by_0$ هو القاسم المشترك الأكبر للعددين a,b أيّ أنّ ، $(a, b) = ax_0 + by_0$.

مثال وملاحظة (1): من الواضح أنّ القاسم المشترك الأكبر للعددين 15,24 هو 3 ، أيّ أنّ 3=(15,24) ، وإذا لاحظنا أنّ : 3=15(-3)+24(2)
=15(-27)+24(17)

فإنّنا نتفهّم لماذا لم يرد في نصّ المبرهنة السّابقة وحدانيّة العددين x_0, y_0 .

مثال وملاحظة(2): بما أنّ D(18)={1,2,3,6,9,18}= و D(24)={1,2,3,4,6,8,12,24}= ، فإنّ مجموعة القواسم المشتركة الموجبة للعددين 18,24 هي:
D(18,24)={1,2,3,6}⇒gcd(18,24)=6

ونلاحظ أنّ كلّ عدد من مجموعة القواسم المشتركة يقسم العدد 6 . فهل تصحّ هذه النتيجة بشكلٍ عامّ ؟ أي هل يصحّ أنّ كلّ قاسم مشترك للعددين a,b يقسم القاسم المشترك الأكبر لهما (a,b) ؟ الإجابة في المبرهنة الهامّة الآتية:

مبرهنة: (العلاقة بين كلّ قاسم مشترك لعددين والقاسم المشترك الأكبر لهما)

ليكن a,b عددين صحيحين ليس كلاهما صفراً ، عند ذلك يتحقّق :

العدد الصّحيح c يكون قاسما مشتركاً للعددين a,b إذا وفقط إذا كان c يقسم (a,b) . أو بشكل رمزيّ : $c|a \wedge c|b \Leftrightarrow c|(a, b)$.

البرهان: (⇒) بما أنّ $(a, b) = ax_0 + by_0$ ،حسب المبرهنة السّابقة ، وبما أنّ العدد c يقسم كلّاً من a,b فإنّه يقسم أي تركيب خطّي لهما ،حسب مبرهنة الخواصّ الأساسيّة للقسمة ،أي أنّ c يقسم $ax_0 + by_0$ وبالتالي c يقسم (a,b) .

العكس (⇐) بما أنّ c يقسم (a,b) فرضاً و (a,b) يقسم a فإنّه حسب خاصّة التّعدّي للقسمة ينتج أنّ c يقسم a ، بالطّريقة ذاتها ، بما أنّ (a,b) يقسم b ينتج أنّ c يقسم b ، أيّ أنّه إذا كان c يقسم (a,b) فإنّ c يقسم a ويقسم b معاً .

نتيجة : من أجل كلّ عددين صحيحين ليس كلاهما صفراً يتحقّق $D\big((a, b)\big) = D(a, b) = D(a) \cap D(b)$ وهذا ينتج مباشرة من التكافؤ الوارد في المبرهنة السّابقة .

للوصول إلى كيفيّة حساب القاسم المشترك الأكبر لعددين . نبدأ بالتمهيديّة الآتية:

تمهيديّة : إذا كان a,b عددين صحيحين ليس كلاهما صفراً ، فإنّه يتحقّق : $\forall m \in Z$ (a,b)=(a,b+ma) (لاحظ أن ma مضاعف لـ a)

البرهان: نفرض أنّ d=(a,b) ولنبرهن على أنّ d=(a,b+ma)، لذلك لنبرهن أوّلاً على أنّ d يقسم a ويقسم (b+ma).

بما أنّ d=(a,b) فإنّ d يقسم a ويقسم b وبالتّالي فإنّ d يقسم أي تركيب خطّي لهما مثل b+ma، حسب مبرهنة خواصّ القسمة.

لنبرهن ثانياً على أنّه إذا كان العدد الصّحيح الموجب c يقسم a ويقسم (b+ma) فإنّ c≤d .

بما أنّ c يقسم a ويقسم b+ma فإنّه يقسم أي تركيب خطّي لهما مثل b=(-ma)+(b+ma) ، أيّ أنّ c يقسم b ، وبالتالي فإنّ c قاسم مشترك موجب للعددين a,b وبالتالي فهو أصغر أو يساوي القاسم المشترك الأكبر d أي أن c ≤ d.

نتيجة: إذا كان $a \neq 0$ عدداً صحيحاً وكان باقي قسمة العدد الصحيح b على a هو $\bar{b}$ ، فإنّ $(a, b) = (a, \bar{b})$.

البرهان: بتطبيق تعميم خوارزميّة القسمة على العددين $a, b \neq 0$ ، فإنّه يوجد عددان صحيحان وحيدان $q, r = \bar{b}$ بحيث $b = qa + \bar{b}\ ; 0 \leq \bar{b} < |a|$.

وباستخدام التمهيديّة السابقة نجد أن : $(a, b) = \big(a, qa + \bar{b}\big) = (a, \bar{b})$.

أمثلة وملاحظات :(تمهيد لخوارزميّة حساب (a,b))

1) نعلم أنّه إذا كان a|b فإنّ (a,b)=|a| .

2) أمّا إذا كان a∤b (مثل 30∤8) فإنّه لحساب (a,b) نستخدم النّتيجة السّابقة عدّة مرّات (مع وجوب الانتباه للرموز بشكل دقيق) إلى أن نحصل على زوج من الأعداد أحدهما يقسم الآخر . مثلاً لحساب (8,30) نكتب : $(8,30) = (8,\overline{30}) = (8,6) = (\overline{8},6) = (2,6) = 2$.

هذه الخطوات في حساب (8,30) هي توضيح لمضمون خوارزميّة إقليدس لحساب (a,b) ، عندما يكون كلّ من a,b عدداً صحيحاً موجباً ، وبالرّغم من ذلك سوف تكون كافية لحساب القاسم المشترك الأكبر لأيّ عددين صحيحين ، ليس كلاهما صفراً ، اعتماداً على التمهيديّة الآتية :

تمهيدية (2): إذا كان a , b عددين صحيحين ليس كلاهما صفرا فإنه يتحقق : (a , b) = (|a| , |b|)
البرهان: نفرض أنّ (a,b)=d ولنبرهن على أنّ d=(|a|,|b|) . أولا : بما أنّ d يقسم كلّا من a , b فإنه يقسم كلاً من |a|، |b|(وذلك من كون كلّ من a و |a| يقسم الآخر وباستخدام خاصّة التعدّي للقسمة)
ثانيا:إذا كان c عددا صحيحا موجبا يقسم كلّا من |a|و|b| فإنّه يقسم كلّاً من a , b . إذا c قاسم مشترك موجب للعددين a , b وبالتالي فإنّه أصغر أو يساوي القاسم المشترك الأكبر لهما ، أي أن $c \leq d$. من أولاً وثانياً نجد أن d=(|a|,|b|) .

مبرهنة: (وجود gcd(a,b) وكتابته كتركيب خطي لـa,b ،خوارزمية إقليدس في حساب (a,b))
إذا كان a , b عددين صحيحين بحيث $0 < a \leq b$ ، فإنّه بتطبيق خوارزمية القسمة عليهما ، نحصل على عددين صحيحين وحيدين ، $r_1 = \bar{b}$, q_1 بحيث :
$b = q_1a + r_1 \; ; \; 0 \leq r_1 < a$ (وحسب النتيجة الأخيرة يكون(a,b)=(a,r1)=(a,b̄)).
فإذا كان باقي القسمة $r_1 \neq 0$ (أي أنّ $0<r_1<a$) فإنّنا نستخدم خوارزمية القسمة (مرة ثانية) من أجل العددين $r_1<a$ ،فنحصل على عددين صحيحين وحيدين $q_2, r_2 = \bar{a}$ بحيث $a = q_2r_1 + r_2 \; ; \; 0 \leq r_2 < r_1$ [وحسب النتيجة الأخيرة يكون(a,r1)=(r2,r1)=(ā,r1)]
فإذا كان مجددا $r_2 \neq 0$ (أي أنّ $0<r_2 <r_1$) فإننا نستخدم خوارزمية القسمة (مرة ثالثة) من أجل العددين r_2,r_1 فنحصل على عددين صحيحين وحيدين $q_3, r_3 = \bar{r_1}$ بحيث $r_1 = q_3r_2 + r_3 \; ; \; 0 \leq r_3 < r_2$.
بملاحظة أنّ $r_3<r_2<r_1$...فإنّه لا بدّ من الحصول في المرّة m+1 على أنّ $r_{m+1}= 0$ ، أمّا في المرّة m السابقة لذلك يكون $0 < r_{m+1} < r_{m-1}$ ونكون قد طبقنا خوارزمية القسمة على العددين r_{m-2},r_{m-1} وحصلنا على عددين صحيحين وحيدين r_m , q_m بحيث :

$r_{m-2}=q_{m-1}+r_m \; ; \; 0 < r_m < r_{m-1}$ [$(r_{m-2},r_{m-1}) = (r_{m-2}\bar{}, r_{m-1}) = (r_m , r_{m-1})$]
طبعا في المرّة (m+1) وحيث $r_{m+1}=0$ (يكون $r_m|r_{m-1}$) نحصل على :

$r_{m-1}=q_{m+1} + r_m \; ; \; r_{m+1}=0$ [$(r_m,r_{m-1})=r_m \; ; \; r_m \mid r_{m-1}$]
وباستخدام نتيجة التمهيدية الأولى عدّة مرّات نجد أنّ: $(b,a) = (r_1,a) = (r_1,r_2) = (r_3,r_2) =\ldots\ldots= (r_{m-1},r_m) = r_m$.

(لاحظ أن $r_m \mid r_{m-1} \; \wedge \; 0 < r_m$) حيث r_mهو آخر باقي قسمة مختلفة عن الصفر في الخوارزمية السابقة (التي **تسمّى** خوارزمية إقليدس في حساب القاسم المشترك الأكبر لعددين صحيحين موجبين) . بالإضافة إلى ذلك فإن خوارزمية إقليدس تقدّم طريقة لإيجاد عددين صحيحين x_0 , y_0 [ليسا وحيدين كما وجدنا سابقا على الرّغم من وحدانيّة العددين الصحيحين في كل مرّة تستخدم خوارزمية القسمة] بحيث $(a ,b) = ax_0 + by_0$ ويتمّ ذلك انطلاقا من المساواة قبل الأخيرة في خوارزمية اقليدس وبخطوات عكسية لحساب (a,b).ونوضّح ذلك في المثال الآتي :

مثال :لنوجد أوّلا ,(1904,510) وذلك بتطبيق خوارزمية القسمة كما يلي:

$$1904 , 510 \overset{\text{خ.ق}}{\rightarrow} 1904 = 3(510) + 374$$

$$374 , 510 \overset{\text{خ.ق}}{\rightarrow} 510 = 1(374) + 136$$

$$374 , 136 \overset{\text{خ.ق}}{\rightarrow} 374 = 2(136) + 102$$

$$102 , 136 \overset{\text{خ.ق}}{\rightarrow} 136 = 1(102) + 34$$

$$102 , 34 \overset{\text{خ.ق}}{\rightarrow} 102 = 3(34) + 0 \implies (1904,510) = 34$$

أما لإيجاد عددين صحيحين x,y بحيث $34=1904x+510y$ فإننا ننطلق من المساواة قبل الأخيرة في الخوارزمية اقليدس السابقة وبخطوات تراجعية نجد:

$$34 = 136 - 1(102) = 136 - [374 - 2(136)] = 3(136) - 374 = 3[510 - 374] - 374 = 3(510) - 4(374) = 3(510) - 4[1904 - 3(510)\,] = 15(510) - 4(1904) \Longrightarrow\Longrightarrow x = -4, y = 15$$

تمرين: باستخدام خوارزمية إقليدس أوجد مايلي: (123456789,987654321),(3799,7337),(3827,74329),(360,2250)
ثمّ أوجد x_0,y_0 بحيث $(a,b)=ax_0 +by_0$.
تعريف : إذا كان a , b عددين صحيحين ليس كلاهما صفراً ، وكان (a , b)=1 فإنّنا نقول عن العددين إنهما أوّليّان نسبيّاً (relatively prime).
مثال: إنّ (-3,8)=1 وبالتالي العددان 3,8- أوّليان نسبيّاً.
مبرهنة: إذا كان a,b عددان صحيحان ليس كلاهما صفرا فإنّه يتحقق :
(a , b) أوّليّان نسبيّاً ⇔ يوجد عددان صحيحان x_0,y_0بحيث $ax_0+by_0=1$.(أيّ انّ $ax_0+by_0=1$⇔(a,b)=1 وحيثx_0وy_0 عددان صحيحان)

البرهان : (⇐) بما أنّ (a , b) يكتب بشكل تركيب خطّي للعددين a , b ،حسب مبرهنة الوجود للقاسم المشترك الأكبر وبما أنّ (a,b)=1 فإنّه يوجد عددان صحيحان x_0,y_0 بحيث $ax_0+by_0=1$.

(⇒) بما أنّ (a,b) الموجب دوما يقسم كلّا من a , b فإنّه يقسم أي تركيب خطّي لهما ،وبالتالي فإنّه يقسم $ax_0+by_0=1$ ،ومنه ينتج أنّ:

$1 \leq (a,b)$ ، وبما أن $(a,b) \geq 1$ ، فإنّه تنتج المساواة (a,b)=1 ، أيّ أنّ a,b أوّليّان نسبيّاً.

نتائج: إذا كان a,b عددين صحيحين ليس كلاهما صفراً فإنّه يتحقق:

(1) $1 = \left(\frac{a}{(a,b)} , \frac{b}{(a,b)}\right)$ (وبالتّالي يمكن كتابة أي عدد كسري موجب $m=\frac{a}{b}$ بشكل وحيد بالشّكل $m = \frac{a/(a,b)}{b/(a,b)}$)

(2) إذا كان $1 = (a , b)$ ، وكان كلّ من a و b يقسم العدد الصحيح c فإنّ العدد (a,b) يقسم c وبشكل رمزي $\{(a,b)=1 \ \& \ a|c \ \& \ b|c \Rightarrow a.b|c\}$

ويمكن قراءة ذلك بلغة المضاعفات كما يلي : إذا كان c مضاعفا مشتركاً لعددين أوّليّين نسبيّاً a,b فإنّه يكون مضاعفا لجداءهما .

(3) (تمهيديّة إقليدس) : إذا كان العدد الصحيح a يقسم الجداء (b.c) للعددين الصحيحين b , c ، وكان a أوّلي نسبيّاً مع أحدهما وليكن b، فإنّه يقسم الآخر c وبشكل رمزي : $a|b.c \ \wedge \ (a,b) = 1 \Rightarrow a|c$

البرهان:

(1) لإثبات $1 = \left(\frac{a}{(a,b)} , \frac{b}{(a,b)}\right)$ يكفي حسب المبرهنة الأخيرة إيجاد تركيب خطّي للعددين الصّحيحين $\frac{b}{(a,b)}$, $\frac{a}{(a,b)}$ مساوٍ للواحد.

بما أنّ (a,b) يكتب بشكل تركيب خطّي للعددين a , b حسب مبرهنة الوجود ، فإنّه يوجد عددان صحيحان x_0,y_0 بحيث $(a,b)= ax_0+by_0$ ، وبقسمة الطرفين على $(a , b) \geq 1$ ينتج أنّ $\frac{a}{(a,b)} x_0 + \frac{b}{(a,b)} y_0 = 1$ ، وبالتالي ينتج المطلوب.

(2) بما أنّ كلاً من a , b يقسم c ، فإنّه يوجد عددان صحيحان s,t بحيث $c = t.a = sb$ ، وبما أنّ a , b أوّليان نسبيّاً ، فإنّه يوجد عددان صحيحان x_0,y_0 بحيث $1=ax_0+by_0$. بضرب طرفي المساواة الأخيرة بالعدد c واستخدام العبارات السابقة للعدد c نجد :

$c = c.a.x_0 + c.b.y_0 = s.b.a.x_0 + t.a.b.y_0 = a.b(s.x_0 + t.y_0)$ ، وهذا يبيّن أنّ (a , b) يقسم c.

(أو بطريقة أخرى: $\frac{c}{a.b} \in \mathbb{Z} \Leftrightarrow a.b|c$ لدينا : $\left(1=ax_0+by_0 \Rightarrow \frac{c}{a.b} = \frac{c}{b}x_0 + \frac{c}{a}y_0 \Rightarrow c = c.a.x_0+c.b.y_0\right)$

(3) بما انّ (a,b)=1 فإنّه يوجد عددان صحيحان x_0,y_0 بحيث $ax_0 + by_0 = 1$ ، وبضرب طرفي المساواة الأخيرة بالعدد c ، نحصل على المساواة:

$c = c.a.x_0 +c.b.y_0$.....(1) ، وبما أنّ a يقسم b.c ، فإنّه يوجد عدد صحيح t بحيث $b.c = a.t$ وبالتعويض في المساواة (1) نجد:

$c = c.a.x_0 +a.t.y_0 = a(c.x_0 +t.y_0)$ وهذا يبيّن أنّ a يقسم c .

ملاحظات:

(1) إنّ الشرط (a,b)=1 أساسي في النتيجة (2) ، لأنّه مثلا : العدد 32 مضاعفاً لكلّ من العددين 4 و16 ، ولكنّه ليس مضاعفاً لجداءهما $64 = 16 \times 4$.

(2) كذلك الشرط (a,b)=1 أساسي في النتيجة (3) ، لأنّه مثلاً : العدد 6 يقسم $12 = 4 \times 3$ ولكن 6 لا يقسم العدد 3 ولا يقسم العدد4 ، لأنّ العدد 6 ليس أوّليّاً نسبيّاً لا مع 3 ولا مع 4 .

نلاحظ أنّ كلّ ما تقدّم من مبرهنات وخواصّ يتعلّق بالقاسم المشترك الأكبر لعددين . لأنّه في الواقع هو الأساس الذي يُردُّ إليه كلّ ما يتعلّق بالقاسم المشترك الأكبر لأكثر من عددين ، والمبرهنة الأساسيّة التالية سوف توضّح هذا الأمر ، وتبيّن لنا أنّ حساب القاسم المشترك الأكبر لـ m عدد صحيح (ليست جميعها أصفاراً) يرد إلى حساب القاسم المشترك الأكبر لـ (m-1) عدداً ، أحدهما يمثّل القاسم المشترك الأكبر لعددين .

مبرهنة: (حساب القاسم المشترك الاكبر لأكثر من عددين)

إذا كانت $a_1,a_2,.....,a_m$ أعداداً صحيحة ليست جميعها أصفارا ،فإنّه يتحقق : $(a_1,a_2,.....,a_m)=(a_1,a_2,...,a_{m-2},(a_{m-1},a_m))$

حيث a_{m-1}, a_m ليس كلاهما صفرا.

البرهان : بقراءة جيّدة للمساواة الواردة في نصّ المبرهنة ، ندرك أنّ المطلوب هو إثبات ما يلي :

العنصر الأكبر في مجموعة القواسم المشتركة الموجبة للأعداد $a_1,a_2,.....,a_m$ يساوي العنصر الأكبر في مجموعة القواسم المشتركة الموجبة للأعداد $a_1,a_2,.....,a_{m-2},(a_{m-1},a_m)$ ،وبما أنّ مجموعتي القواسم المشتركة الموجبة منتهيتين فإنّه يكفي البرهان على أنّ:

المجموعة $D(a_1,a_2,.....,a_m)$ (مجموعة القواسم المشتركة الموجبة للأعداد $a_1,a_2,.....,a_m$) مساوية للمجموعة $D(a_1,a_2,.....,a_{m-2},(a_{m-1},a_m))$ (مجموعة القواسم المشتركة الموجبة للأعداد $a_1,a_2,.....,a_{m-2},(a_{m-1},a_m)$).

وهذا صحيح لأنّ: $D(a_1,a_2,.....,a_{m-2},(a_{m-1},a_m))= D(a_1)\cap D(a_2) \cap .....\cap D(a_{m-2}) \cap D((a_{m-1},a_m))$

وبما أنّ $D((a_{m-1},a_m))=D(a_{m-1}) \cap D(a_m)$ حسب نتيجة لمبرهنة سابقة فإنّه ينتج المساواة المطلوبة وهي:

$D(a_1,a_2,.....,a_{m-2},(a_{m-1},a_m))= D(a_1)\cap D(a_2) \cap .....\cap D(a_{m-2}) \cap D(a_{m-1}) \cap D(a_m) = D(a_1,a_2,.....,a_m)$

مثال (1): لنوجد (260,112,72) ،حسب المبرهنة السابقة لدينا:

$$(260,112,72) = \left(260,(112,72)\right) \dots\dots (1)$$

$$= \left(260,(\overline{112},72)\right) = \left(260,(40,72)\right) = \left(260,(40,\overline{72})\right) = \left(260,(40,32)\right) = \left(260,(\overline{40},32)\right) = \left(260,(8,\overline{32})\right)$$

$$= (260,8) = (\overline{260},8) = (4,8) = 4$$

أو بطريقة أخرى ، نقوم أولاً بحساب (112,72) مستخدمين خوارزمية إقليدس ، فنجد :

$$112,72 \overset{\text{خ،ق}}{\Rightarrow} 112 = 72 + 40$$
$$72,40 \overset{\text{خ،ق}}{\Rightarrow} 72 = 40 + 32$$
$$40,32 \overset{\text{خ،ق}}{\Rightarrow} 40 = 32 + 8$$
$$32,8 \overset{\text{خ،ق}}{\Rightarrow} 32 = 4(8) + 0 \quad \Rightarrow (112,72) = 8$$

بالتعويض في (1) نجد أنّ المسألة تتحول إلى حساب القاسم المشترك الأكبر لعددين ،أيّ أنّ: (260,8)=(260,112,72)

لنحسب (260,8) باستخدام خوارزمية إقليدس مرّة أخرى فنجد:

$$260,8 \overset{\text{خ،ق}}{\Rightarrow} 260 = 32(8) + 4 \qquad (*)$$
$$8,4 \overset{\text{خ،ق}}{\Rightarrow} 8 = 2(4) + 0 \qquad \Rightarrow (260,8) = 4$$

وبالنتيجة نحصل على أنّ 4=(260,112,72)

ملاحظة :إنّ تعميم المبرهنة (العدد (a,b) هو تركيب خطّي للعددينa,b)كلاسيكي ويتم بالإستقراء ،ويتمّ الحصول على تركيب خطّي لهذه الأعداد باستخدام الفكرة نفسها من أجل عددين(ولكن على أكثر من مرحلة) ، في المثال السابق يمكننا إيجاد الأعداد الصحيحة x_0,y_0,z_0 بحيث $(a,b,c)=ax_0+by_0+cz_0$ بخطوات معاكسة لخوارزميّة إقليدس ، انطلاقاً من المساواة قبل الأخيرة الحاوية على الباقي الممثّل للقاسم المشترك الأكبر ،الذي حصلنا عليه ،وفي مثالنا انطلاقاً من المساواة (*)، فنجد:

$$4=260-32(8)=260-32(40-32)=260-32(40)+(32)(32)=260-(32(40)+32(72-40)$$
$$=260-64(40)+32(72)=260-64(112-72)+32(72)=260-64(112)+96(72)$$

ومنه نجد أنّ $x_0 = 1$, $y_0 = -64$, $z_0 = 96$.

ملاحظة ومثال: من الطبيعي أن نحصل في بعض الأمثلة على أنّ القاسم المشترك الأكبر لأكثر من عددين هو الواحد ،ولكن في هذه الحالة ليس من الضّروريّ أن يكون كلّ عددين منهما أوليّين نسبيّاً .

مثال ذلك لدينا : (35,21,15)=(35,(21,15))=(35,3)=1

ونلاحظ أنّ: (21,15)=3 , (35,15)=5 , (35,21)=7 وهذا يدعونا لتقديم التعريف الآتي:

تعريف (أعداد أوليّة تبادليّاً (أو تشاركيّاً) ، أعداد أوليّة نسبيّاً مثنى مثنى)

نقول عن الأعداد الصحيحة $a_1,a_2,\ldots,a_m$ ، التي ليست جميعها أصفاراً ، إنّها أوليّة تشاركيّا (أو تبادليّاً)(mutually prime)إذا كان $(a_1,a_2,\ldots,a_m)=1$

ونقول إنّها أوّليّة نسبيّا مثنى مثنى(relatively prime in pairs) إذا كان $\forall\ 1 \le I \ne j \le m\ \ (a_i\ ,\ a_j) = 1$.

- بالطبع الأعداد الأوليّة نسبيّاً مثنى مثنى تكون أوّليّة تشاركيّاً والعكس ليس صحيح كما وجدنا في المثال السابق لهذا التعريف.

مثال:الأعداد 25,21,4 أوّليّة نسبيّاً مثنى مثنى لأنّ: (21,4)=1 , (25,4)=1 , (25,21)=1

ملاحظة: في الفقرة الآتية نتعرّف على المفاهيم والرموز الموافقة لتلك المتعلقة بمجموعات القواسم الموجبة :

وهي: $[D(a) = \quad D(a,b) = D(a) \cap D(b) = \cdots \quad \operatorname{Max} D(a,b) = \gcd(a,b)]$
$[M(a) = \quad M(a,b) = M(a) \cap M(b) = \cdots \quad Min\ M(a,b) = lcm(a,b)]$

المضاعف المشترك الأصغر(l.c.m = least common muptiple)

إنّ مفهوم مضاعف عدد يرتبط بشكل وثيق بمفهوم القسمة ، فعندما قلنا إنّ العدد الصحيح b يعني وجود عدد صحيحc بحيث b=ac فإنّ هذه المساواة تعني أيضا أنّ العدد b هو مضاعفا للعدد a ، وبالتالي الرمز نفسه a|b قرأناه من اليسار إلى اليمين aيقسم b،ومن اليمين إلى اليسار b، مضاعفاً لـ a ،نلاحظ أنّه في كلّ مرة يأخذ العدد الصحيح c قيمة جديدة ، نحصل على مضاعفاً جديداً b للعددa،وبالتالي نستطيع تعريف مجموعة مضاعفات العدد الصحيح a بأنّه $\{ax; x \in \mathbb{Z}\}$ والتي نرمز لها بالرمز $a\mathbb{Z}$ أي أن:

$$a\mathbb{Z} = \{ax | x \in \mathbb{Z}\} = \{0, a(\pm 1), a(\pm 2), a(\pm 3), \ldots\} = \{0, \pm a, \pm 2a, \pm 3a, \ldots.\}$$

من الواضح أنّه عندما a=0 فإنّ مجموعة مضاعفاته تتألف من عنصر واحد هو الصفر،وفيما عدا ذلك تكون مجموعة المضاعفات لعدد مجموعة غير منتهية،لذلك في دراستنا لمضاعفات عدد نفترض أنّ هذا العدد يختلف عن الصفر .

عندما a=2 فإنّ مجموعة مضاعفات العدد2هي :$2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \ldots.\}$ وهي مجموعة الأعداد الزوجية السالبة والموجبة ،بالإضافة إلى الصفر،الذي يعتبر مضاعفا لأي عدد صحيح . من الطبيعي أنّ نهتمّ بالمضاعفات الموجبة لعدد صحيح مختلف عن الصفر ،وذلك لانّه من الواضح أنّ كلّ مضاعف موجب x لعدد صحيح $a \ne 0$ يقابله مضاعف سالب هوx- لذلك العدد .

سوف نرمز بـ M(a) لمجموعة المضاعفات الموجبة للعدد الصحيح a≠0 ، فإذا كان موجبا فإنّ $M(a)=\{a,2a,3a,\ldots\} = a\mathbb{Z}^+ = |a|\mathbb{Z}^+$.

وإذا كان a سالبا فإنّ :$(-a)\ \mathbb{Z}^+ = |a|\mathbb{Z}^+$. أي أنّه بشكل عامّ $M(a)=|a|\mathbb{Z}^+$، مثلا : $M(3)=3\mathbb{Z}^+=M(-3)=|-3|\mathbb{Z}^+$.

- إذا كانت M(a),M(b) مجموعتي المضاعفات الموجبة للعددين المختلفين عن الصّفر a , b ،فإنّ مجموعة تقاطعهما تمثّل مجموعة المضاعفات المشتركة

الموجبة لهما ،والتي نرمز لها بـ M(a,b)،أي أنّ : $M(a,b)=M(a)\cap M(b)$.
بما أنّ هذه المجموعة جزئية من مجموعة الأعداد الصحيحة الموجبة، وغير خالية (لماذا؟) فإنّها تملك عنصراً أصغر ، وذلك حسب مبدأ الترتيب الحسن ، نسمّي هذا العنصر الأصغر بالمضاعف المشترك الأصغر للعددين غير الصفريّين a , b (least common multiple) ونرمز له بالرمز lcm(a , b) أو اختصاراً [a , b]،

فمثلا إذا كان $a = 4 , b = 6$ فإنّ: $M(4,6)=M(4)\cap M(6)=\{12,24,...\}$ $M(6)=\{6,12,18,24,30,....\}$ $M(4)=\{4,8,12,16,20,24,....\}$
$lcm(4,6)=[4,6]=12$.

من الطبيعي تعميم مفهوم المضاعفات المشترك الأصغر لعددين على ثلاثة أعداد أو أكثر كما يأتي:
إذا كانت $a_1,a_2,.....a_n$ أعدادا صحيحة كلّا منها مختلف عن الصفر ، وكانت $M(a_1),M(a_2).....M(a_n)$ مجموعة المضاعفات الموجبة لها على الترتيب ، فإنّ مجموعة التقاطع $M(a_1) \cap M(a_2) \cap ... ... \cap M(a_n)$(والتي نرمز لها $M(a_1,a_2,.....,a_n)$) تمثّل مجموعة المضاعفات المشتركة الموجبة للأعداد $a_1,a_2,.....a_n$، والعنصر الأصغر في هذه المجموعة (الموجود حسب مبدأ الترتيب الحسن) يسمّى المضاعف المشترك الأصغر للأعداد $a_1,a_2,.....a_n$ ونرمز له بالرمز $lcm(a_1,a_2,.....a_n)$ أو اختصاراً $[a_1,a_2,.....a_n]$ ، فمثلا إذا كانت $a_3 = 9 , a_2 = 6 , a_1 = 4$ فإنّ:

$M(4)=\{4,8,12,16,20,24,28,32,36,.....\}$
$M(6)=\{6,,12,18,24,30,36,.....\}$
$M(9)=(9,18,27,36,45,54,63,.....,.....\}$

وتكون مجموعة المضاعفات المشتركة الموجبة لهذه الأعداد الثلاثة هي $M(4,6,9)=M(4)\cap M(6)\cap M(9)=\{36,72,...\}$
والعنصر الأصغر فيها 36 هو المضاعف المشترك الأصغر للأعداد 4,6,9 أي أنّ $[4,6,9] = 36$.
بالاعتماد على ما تقدّم نستطيع تقديم مفهوم المضاعف المشترك الأصغر لعددين أو أكثر الذي بيّنا وجوده ،كما يلي:

تعريف: (المضاعف المشترك الأصغر لعددين lcm(a , b))

إذا كان a , b عددين صحيحين كلّ منهما مختلف عن الصفر ،فإنّنا نقول عن العدد الصحيح الموجب m إنّه المضاعف المشترك الأصغر للعددين a , b ونرمز له lcm(a , b) أو اختصارا [a , b] ، إذا (وفقط إذا) تحقق الشرطان:

(1) m مضاعفاً مشتركاً لـ a , b أي أن $a \mid m \wedge b \mid m$.

(2)إذا كان cعدداً صحيحا موجباً بحيث $a \mid c \wedge b \mid c$ (أي إذا كان c مضاعفاً مشتركاً موجباً آخر للعددين a , b) ، فإنّ $m \leq c$.

(وكتطبيق على هذا التعريف سوف نبرهن لاحقا على مبرهنة نسميها مبرهنة الربط بين [a,b]و(a,b))

تعريف : (المضاعف المشترك الأصغر لأكثر من عددين)

إذا كانت $a_1,a_2,...,a_n$ أعداداً صحيحة ، كلّ منها مختلف عن الصفر ، فإنّنا نقول عن العدد الصحيح الموجب m إنّه المضاعف المشترك الأصغر للأعداد $a_1,a_2,.....,a_n$ ، ونرمز له بالرمز $lcm(a_1,a_2,.....,a_n)$ أو اختصاراً $[a_1,a_2,.....,a_n]$ إذا (وفقط إذا) تحقق الشرطان:

(1) $a_i \mid m$ لكلّ $I =1,2,....n$.

(2) إذا كان c عددا صحيحا موجبا آخر بحيث $a_i \mid c$ لكلّ $I = 1,2,....,n$ فإنّ $m \leq c$.

إنّ دراسة خواصّ المضاعف المشترك الأصغر لعددين ، وحساب ذلك المضاعف يعتمد على خاصّة هامّة جدا تربط بينه وبين القاسم المشترك الأكبر لنفس العددين ، ومضمون هذه الخاصّة يمكن ملاحظته مباشرة من الجدول الآتي :

a	b	(a,b)	[a,b]	(a,b)+[a,b]	[a,b]-(a,b)	(a,b)[a,b]
6	1	1	6	7	5	6
6	2	2	6	8	4	12
6	3	3	6	9	3	18
6	4	2	12	14	10	24
6	5	1	30	31	29	30
6	6	6	6	12	0	36
6	7	1	42	43	41	42

من الجدول السّابق نلاحظ انتظام الأعداد ، فقط ،في العمود الأخير الممثّل للجداء [a , b](a , b) حيث نلاحظ تحقق المساواة : (a , b)[a , b]=a . b
(عند الشرط a>0 و b>0) ، فهل يمكن تعميم هذه الملاحظة لتصبح مبرهنة ؟ الجواب في المبرهنة الآتية:

مبرهنة: (الربط بين (a , b) و [a . b])

إذا كان a , b عددين صحيحين موجبين فإنّه يتحقق [a , b](a , b) = a . b أي أن $[a,b]=\frac{a.b}{(a,b)}$

البرهان: إنّ المساواة المطلوب إثباتها هي $[a,b]=\frac{a.b}{(a,b)}$ ، وبالتالي يصبح المطلوب إثبات أنّ العدد الصحيح الموجب m = $\frac{a.b}{(a,b)}$ هو المضاعف المشترك الأصغر للعددين a , b ، نلاحظ أوّلا من كتابة العدد m بالشكلين $a.\frac{b}{(a,b)} = b.\frac{a}{(a,b)}$ =m أنّه مضاعف مشترك لـ a , b ، لأنّ كلّا من $\frac{b}{(a,b)}$ و $\frac{a}{(a,b)}$ عدد صحيح . وثانيا : إذا كان c عددا صحيحا موجبا بحيث b|c و a|c فإنّه يجب البرهان على أنّ m ≤ c أو أنّ $\frac{c}{m}$ عدداً صحيحاً ،بما أنّ (a,b) يكتب بشكل تركيب خطي لـ a , b أي أنّ (a , b) = a X + b y ، فإن $\frac{c}{m}=\frac{c(a,b)}{a.b}=\frac{c(ax+by)}{a.b}=\frac{cx}{b}+\frac{cy}{a}=\frac{c}{b}x+\frac{c}{a}y$
وبما أنّ كلّا من $\frac{c}{b}$ و $\frac{c}{a}$ عدد صحيح فإنّ $\frac{c}{b}x+\frac{c}{a}y$ يكون عدداً صحيحاً أي أنّ m|c ومنه نجد أنّ m ≤ c (لأنّ كلّا من mوcعدد صحيح موجب).

نتيجة:من المبرهنة السّابقة ينتج مباشرة أن: $(a,b)=1 \Leftrightarrow [a,b]=a.b$.

كتطبيق على المبرهنة السابقة نأخذ المثال :

مثال:لإيجاد [72,112] من الطبيعي أن نوجد أوّلاً (72,112)،وقد وجدنا أنّه مساوٍ للعدد 8=(72,112) ،ومن علاقة الربط نجد أنّ:

$[72,112]=\frac{72\times112}{8}=9\times112=1008$

ملاحظة ومثال : لايمكن تعميم المبرهنة السابقة على أكثر من عددين أي أنّ [a, b , c] (a , b ,c) ≠ a .b .c . ونوضّح ذلك بالمثال الآتي :[6,10,15]=30 ، (6,10,15)=1 ونلاحظ أنّ (6,10,15)[6,10,15]=30 ≠ 6×10×15=900

يتوجب على الطالب البرهان على خواصّ تتعلّق بالمضاعف المشترك الأصغر مشابهة لخواصّ القاسم المشترك الأكبر. فمثلاً ، نعلم أنه إذا كان a |b فإنّ |a|= (a, b)، فماذا عن [a , b] ؟ كذلك نعلم أن 1 = (1,a) ماذا عن [1,a] ؟ وهكذا بقية الخواص .

للبرهان على أنّ m≤c يكفي البرهان على أنّ m|c أي أنّ c=m□ .لدينا $\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$ وبالتالي يوجد $x_0,y_0\in z$ بحيث:

$$1=\frac{a}{(a,b)}x_0+\frac{b}{(a,b)}y_0 \Rightarrow c=\frac{a.c}{(a,b)}x_0+\frac{b.c}{(a,b)}y_0 \xrightarrow[a|c\Rightarrow c=a\alpha \;\&\; b|c\Rightarrow c=b\beta]{}$$

$$\frac{a.b}{(a,b)}\beta x_0+\frac{b.a}{(a,b)}\alpha y_0=m\beta x_0+m\alpha y_0=m(\beta x_0+\alpha y_0)\Rightarrow m|c\Rightarrow m\le c$$

تمهيدية: (تعميم للمبرهنة السابقة على الأعداد الصّحيحة السّالبة)

(1)إذا كان a عدداً صحيحاً مختلفاً عن الصّفر فإنّ |a|=[a,1]

(2)من أجل كلّ عددين صحيحين مختلفين عن الصّفر a, b يتحقّق :[a, b] = [|a|,|b|]

(3) إذا كان a ,b عددين صحيحين مختلفين عن الصّفر فإنّه يتحقّق: |a .b| = [a , b](a , b) أيّ أنّ [a , b] = $\frac{|a.b|}{(a,b)}$

البرهان:

(1)من تعريف المضاعف المشترك الأصغر يتّضح مباشرة أنّ |a|=[a,1]

(2) للبرهان على المساواة [|a|,|b|]=[a,b] نفرض أنّ [a,b]=m ثمّ نبرهن على أنّ m=[|a|,|b|]

أوّلاً: بما أنّ [a,b]=m فإنّ a|m وb|m وبالتالي ينتج أنّ |a| | m و |b| | m ، وذلك بالاستفادة من خواص القسمة .

ثانياً: ليكن c عدداً صحيحاً موجباً يحقق |a| | c و |b| | c ولنبرهن على أنّ m ≤ c . بما أنّ |a| | a و لدينا |a| | c فإنّ a|c
كذلك |b| | b و لدينا |b| | c فإنّ b|c ، ومنهما ينتج $[a,b]\le c \Leftarrow m\le c$.

(3) بما أن$a,b\in\mathbb{Z}-\{0\}$ فإنّ كلّاً من |a| , |b| من $\mathbb{Z}^+$ ، وبتطبيق مبرهنة الرَّبط عليهما ، نجد أنّ [|a| , |b|] = $\frac{|a|.|b|}{(|a|,|b|)}$ ولكن لدينا

(|a|,|b|)=(a,b), [|a|,|b|]=[a,b] ، وبالتالي ينتج $[a,b]=\frac{|a.b|}{(a,b)}$.

مبرهنة:

ليكن a,b عددين صحيحين مختلفين عن الصّفر ، عندئذ يتحقّق :

العدد الصّحيح m يكون مضاعفاً مشتركاً للعددين a,b ،إذا وفقط إذا كان m مضاعفاً للعدد [a,b].وبشكل رمزي[a,b]|m ⇔ [a|m ∧b|m]

البرهان: ($\overset{\text{(1) طريقة}}{\Longleftarrow}$) (دون استخدام علاقة الرّبط) بما أنّ m مضاعفاً مشتركاً لـa,b فإنّ $[a,b]\leq m$ (حسب تعريف [a,b]) وبتطبيق خوارزميّة القسمة على العددين ,m,[a,b] فإنّه يوجد عددان صحيحان وحيدان q,r بحيث $m=q[a,b]+r;\ 0\leq r<[a,b]$ ،لنبرهن على أنّ r=0(عندئذٍ نحصل على المطلوب) لذلك نفرض أنّ $r\neq 0$ ،عندئذٍ $0<r<[a,b]$ ويحقّق :

$$r=m-q[a,b]=\begin{Bmatrix}\propto_1 a-q\propto_2 a=(\propto_1-q\propto_2)a\\ \beta_1 b-q\beta_2 b=(\beta_1-q\beta_2)b\end{Bmatrix}\Rightarrow a|r\wedge b|r\Rightarrow$$ (ومن كون a|[a,b] , b|[a,b])

$$\Rightarrow r=0\Rightarrow m=q[a,b]\Rightarrow [a,b]|m$$ (تناقض مع كون [a,b] المضاعف المشترك الأصغر لـ a,b)

($\overset{\text{(2) طريقة}}{\Longleftarrow}$)ليكن a|m و b|m ولنبرهن على أنّ [a,b]|m ،لذلك يكفي البرهان على أنّ $\frac{m}{[a,b]}\in z$ وبما أنّ [a,b]=[|a|,|b|] فإنّه يمكن اعتبار كلّاً من a وb موجباً ولدينا: $\frac{m}{[a,b]}=\frac{m(a,b)}{[a,b](a,b)}=\frac{m(ax+by)}{a.b}=\frac{m}{b}x+\frac{m}{a}y\in\mathbb{Z}$ (لأنّ كلّاً من $\frac{m}{b}$ و $\frac{m}{a}$ عدد صحيح من الفرض ، وكذلك كلّاً من x , y عدد صحيح) ، إذاً $\frac{m}{[a,b]}$ عدد صحيح ، وبالتّالي نجد أنّ [a,b]|m.

(⇒)بما أنّ b|[a,b] وa|[a,b] ، وذلك من تعريف المضاعف المشترك الأصغر لعددين ، وبما أنّه بالفرض [a,b]|m فإنّه ينتج من خاصّة التّعدي لعلاقة القسمة أنّ : a|m و b|m ،وهو المطلوب.

نتيجة:

بقراءة جيّدة للتكافؤ الوارد في المبرهنة الأخيرة ، وباستخدام رمز مجموعة المضاعفات الموجبة لعدد ، ورمز مجموعة المضاعفات المشتركة لعددين أو أكثر نستطيع كتابة :$m\in M([a,b])\Leftrightarrow m\in M(a,b)$ وحسب مفهوم تساوي مجموعتين ينتج أنّ :

M([a,b])=M(a,b) أي أنّ : $M([a,b])=M(a)\cap M(b)$ ، وهذه النتيجة الهامّة جدّاً سوف تستخدم في برهان المبرهنة الآتية:

مبرهنة: (حساب $[a_1,a_2,.....,a_m]$)

إذا كانت $a_1,a_2,.....,a_m$ أعداداً صحيحة ،كلاً منها يختلف عن الصّفر ،فإنّه يتحقق :$[a_1,a_2,.....,a_m]=[a_1,a_2,.....,a_{m-2},[a_{m-1},a_m]]$

البرهان: لبرهان المساواة :$[a_1,a_2,.....,a_m]=[a_1,a_2,.....,a_{m-2},[a_{m-1},a_m]]$ التي طرفها الأيسر هو العنصر الأصغر في مجموعة المضاعفات المشتركة الموجبة للأعداد $a_1,a_2,.....,a_m$، وطرفها الأيمن هو العنصر الأصغر في مجموعة المضاعفات المشتركة الموجبة للأعداد $a_1,a_2,.....,a_{m-2},[a_{m-1},a_m]$. يكفي البرهان على المساواة بين مجموعتي المضاعفات المشتركة السابقتين ، أي البرهان على المساواة :

$$M(a_1,a_2,.....,a_m)=M(a_1,a_2,.....,a_{m-2},[a_{m-1},a_m])$$

لدينا : $M(a_1,a_2,.....,a_{m-2},[a_{m-1},a_m])=M(a_1)\cap M(a_2)\cap.....\cap M(a_{m-2})\cap M([a_{m-1},a_m])$

وحسب النتيجة الأخيرة نجد أنّ:

$$=M(a_1)\cap M(a_2)\cap.....\cap M(a_{m-2})\cap M(a_{m-1})\cap M(a_m)=M(a_1,a_2,.....,a_m)$$

كتطبيق على المبرهنة السّابقة لنأخذ بعض الأمثلة:

مثال(1): احسب [260,112,72]

بالاستفادة من المبرهنة السّابقة ، نستطيع كتابة [[112,72],260]=[260,112,72] ، وقد وجدنا في مثالٍ سابق أنّ [112,72]=1008 ، بالتعويض في المساواة السّابقة نحصل على : (1) .....[260,1008]=[260,112,72] ، ولحساب المضاعف المشترك الأصغر لعددين ، بشكل عام ، نحسب **أوّلاً** القاسم المشترك الأكبر لهما ، لذلك نحسب (260,1008) كمايلي :

$$\left.\begin{array}{rcl}228,32 & \overset{\text{خ.ق}}{\rightarrow} & 228=7(32)+4\\ 32,4 & \overset{\text{خ.ق}}{\rightarrow} & 32=8(4)+0\end{array}\right\}\Rightarrow(1008,260)=4$$

$$1008\ ,260\ \overset{\text{خ.ق}}{\rightarrow}\ 1008=3(260)+228$$

$$260,228\ \overset{\text{خ.ق}}{\rightarrow}\ 260=1(228)+32$$

وثانياً نستخدم علاقة الرّبط بينهما ، فنحصل على :$[260,1008]=\frac{260\times1008}{4}=65\times1008=65520$

بالتعويض في العلاقة (1) نحصل على : 65520 = [260,112,72] .

تمارين (للفصل الثاني)

الفصل الثاني(القسمة وخوّاصّها وخوارزميّة القسمة،(a,b)و[a,b] وتعميمهما)

(1) أثبت أنّ $2|(n^2-n)$ لكلّ عدد صحيح n .

(2) أثبت أنّ $3|n(n+1)(n+2)$ لكلّ عدد صحيح n.

(3) أثبت أنّ $6|n^3-n$ لكلّ عدد صحيح n .

(4) أثبت أنّ $2^{3n}-1$ يقبل القسمة على 7 لكلّ $n \geq 1$.

(5) أثبت أنّ 8 يقسم $3^{2n}+7$ لكلّ $n \geq 1$.

(6) أثبت أنّ مرتبة الآحاد للعدد 16^n هي 6 لكلّ $n \geq 1$.

(7) أثبت أنّ $7^{2n}+16n-1$ يقبل القسمة على 64 لكلّ $n \geq 1$.

(8) برهن على أنّه إذا كان a,b عددين ليس كلاهما صفراً فإنّ المجموعة $T = \{ax + by \,|x, y \in z\}$ هي بالضّبط مضاعفات العدد d=(a,b)

(9) برهن على أنّ (ma,mb)=m(a,b) وحيث m>0 .

(10) إذا كان a,b عددين أوّليّين نسبيّاً وكان c عدداً يقسم مجموعهما (a+b) فبرهن على انّ (c,a)=(c,b)=1 .

[التمرين بشكل رمزي ، برهن الاقتضاء : $(a,b)=1 \wedge c|(a+b) \Rightarrow (c,a)=(c,b)=1$] .

(11)(a) إذا كان (a,c)=(b,c)=1 ، فأثبت أنّ (a.b,c)=1

(b) إذا كانت $a_1,a_2,\ldots..,a_m$ أعداداً أوّليّة نسبيّاً مثنى مثنى فبرهن على أنّ: $[a_1,a_2,\ldots..,a_m] = a_1,a_2,\ldots..,a_m$.

(12) إذا كانت a,b,n أعداداً صحيحة موجبة فاثبت أنّ:1) $(a,b)=1 \Rightarrow (a^n,b^n)=1$ (2 $a^n \mid b^n \Leftrightarrow a \mid b$

(13)(تمرين محلول): ليكن a,b عددين صحيحين موجبين حيث: $a= p_1^{a_1}.p_2^{a_2}.\ldots..p_n^{a_n} \wedge b = p_1^{b_1}.p_2^{b_2}.\ldots..p_b^{b_n}$

وإذا كان
$$\left.\begin{array}{l} 0 \leq a_i , b_i \quad \forall\ 1 \leq i \leq n \ (1) \\ m_i = \min\{a_i, b_i\} \ \forall\ 1 \leq i \leq n \ (2) \\ M_i = Max\{a_i, b_i\} \ \forall\ 1 \leq i \leq n \ (3) \end{array}\right\}$$

فاثبت مايلي :

1) $a|b \Leftrightarrow a_i \leq b_i$ لكلّ i=1,2,…,n ($\Leftrightarrow$ كلّ قاسم أوّلي لـa يجب أن يقسم b،ويتكرّر ظهوره في b على الأقلّ عدد المرّات نفسها في a).

2) $(a,b) = p_1^{m_1}.p_2^{m_2}.\ldots..p_n^{m_n}$.

3) $[a,b] = p_1^{M_1}.p_2^{M_2}.\ldots..p_n^{M_n}$.

الحلّ : [1] إذا كان $a|b$ فإنّ $b = a.c \ ; \ c \in \mathbb{Z}$ وبالتالي كلّ ظهور لعدد أوّلي في تحليل a يجب أن يظهر في تحليل b وعلى الأقلّ عدد المرّات نفسها (هنا نستخدم حقيقة أنّ التحليل وحيد ماعدا التّرتيب) وبالتّالي فإنّ $a_i \leq b_i$ لكلّ $1 \leq i \leq n$.

العكس: $\left[b = p_1^{b_1}.p_2^{b_2}.\ldots..p_b^{b_n} = \left(p_1^{b_1-a_1}.p_2^{b_2-a_2}.\ldots..p_b^{b_n-a_n}\right)\left(p_1^{a_1}.p_2^{a_2}.\ldots..p_n^{a_n}\right) = c.a \ ; \ c \in \mathbb{Z} \Rightarrow a|b\right]$

[2] بما أنّ m_i أصغر العددين a_i, b_i لكلّ $1 \leq i \leq n$ فإنّ $p_1^{m_1}.p_2^{m_2}.\ldots..p_n^{m_n}$ قاسماً لكلّ من a , b حسب [1] .

لنفرض الآن أنّ d هو أي قاسم مشترك للعددين a , b فإنّه حسب [1] العدد d يكتب بالشّكل $d = p_1^{r_1}.p_2^{r_2}.\ldots..p_n^{r_n}$ وحيث $r_i \leq a_i \ \wedge \ r_i \leq b_i$ لكلّ $1 \leq i \leq n$ وبالتالي

$r_i \leq m_i$ لكلّ $1 \leq I \leq n$ ومنه $d|p_1^{m_1}.p_2^{m_2}.\ldots..p_n^{m_n}$ ومنه ينتج أنّ $p_1^{m_1}.p_2^{m_2}.\ldots..p_n^{m_n}$ هو القاسم المشترك الأكبر للعددين a , b ، أيّ أنّ $(a , b) = p_1^{m_1}.p_2^{m_2}.\ldots..p_n^{m_n}$ وحيث $m_i = \min\{a_i, b_i\}$.

[3] بما أنّ M_i أكبر العددين a_i , b_i لكلّ $1 \leq i \leq n$ فإنّ $a_i \leq M_i \ \wedge \ b_i \leq M_i$ لكلّ $1 \leq i \leq n$ وبالتّالي العدد $p_1^{M_1}.p_2^{M_2}.\ldots..p_n^{M_n}$ ، مضاعفاً لكلّ من a , b حسب [1] .

نفرض الآن أنّ M هو أي مضاعف مشترك للعددين a,b أي أن $(a|M , b|M) \xleftarrow{\text{حسب}[1]} M$ يكتب بالشّكل $M = p_1^{S_1}.p_2^{S_2}.\ldots p_n^{S_n}$ وحيث $a_i \leq S_i \ \wedge \ b_i \leq S_i \quad \forall\ 1 \leq i \leq n$

وبما أنّ $M_i = \text{Max}\{a_i, b_i\}$ فإنّ $M_i \leq S_i$ لكلّ $1 \leq i \leq n \Longleftarrow M \mid p_2^{M_2} \ldots\ldots p_n^{M_n}$

وبالتالي ينتج أنّ $p_1^{M_1} p_2^{M_2} \ldots\ldots p_n^{M_n}$ هو المضاعف المشترك الأصغر للعددين a , b ، أي أنّ

$[a,b]=p_1^{M_1} p_2^{M_2} \ldots\ldots p_n^{M_n}$; $M_i=\text{Max}\{a_i, b_i\}$; $a= p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ و $b = p_1^{b_1} p_2^{b_2} \ldots p_b^{b_n}$.

مثال:

$(75,900)=(3 \times 5^2, 2^2 \times 3^2 \times 5^2) = 3 \times 5^2 = 75$

$(900,440)=(2^2 \times 3^2 \times 5^2, 2^3 \times 5 \times 11) = 2^2 \times 5 = 20$

$[900,440]=[2^2 \times 3^2 \times 5^2, 2^3 \times 5 \times 11] = 2^3 \times 3^2 \times 5^2 \times 11 = 19800.$

تعريف (عدد أوّلي ، عدد مؤلّف composite number)
نقول عن العدد الصّحيح P إنّه عدد أوّلي (Prime Number) إذا كان P>1 ، وكانت القواسم الموجبة له هي العدد واحد والعدد نفسه فقط .
- إذا كان العدد الصّحيح n>1 ليس أوّلياً فإنّنا نسميّه عدداً مؤلّفاً (composite number)
ملاحظات ونتائج: من التّعريف ينتج مباشرة:
1) العدد 1 ليس أوّليّاً ولا مؤلّفاً.
2) العدد n يكون مؤلّفاً ⇔ n يكتب بالشّكل n = a . b وحيث 1< a <n ، 1< b <n. (أو حيث 1 < a ≤ b < n) .
3) في دراسة الأعداد الأوّلية نتكلّم عن القواسم الموجبة فقط إذا لم يصرّح بغير ذلك .
مبرهنة (شطر المبرهنة الأساسيّة في الحساب)
كلّ عدد صحيح n>1 ، إمّا أن يكون أوّليّاً ، أو حاصل ضرب عدد منته من الأعداد الأوّليّة ،
أو بعبارة مكافئة (كلّ عدد صحيح n>1 يكتب كحاصل ضرب عدد منته من الأعداد الأوّليّة)
البرهان : لقد برهنّا على ذلك كتطبيق على الصّيغة الثانية للاستقراء الرّياضي.
نتائج (من المبرهنة الأساسيّة في الحساب)
(1) كلّ عدد صحيح n>1 يكون له قاسم أوّلي.
(2) كلّ عدد مؤلّف n>1 يكون له قاسم أوّلي P ≤ $\sqrt{n}$ بعبارة رمزيّة :

$$\left(n>1 \text{ مؤلّف} \overset{n>1}{\Longrightarrow} \exists \text{عدد أوّلي } p \le \sqrt{n} \wedge p \middle| n\right)$$

(3) وبالنّفي المنطقي للبند(2) نجد أنّه ، إذا كان n>1 عدداً صحيحاً ليس مضاعفاً لأيّ عدد أوّلي p ≤ $\sqrt{n}$ (أو لا يملك قواسم أوّليّة p ≤ $\sqrt{n}$) فإنّ n يكون أوّليّا. وبعبارة مكافئة: إذا كان العدد الصّحيح n>1 لا يقبل القسمة على أي عدد أوّلي p ≤ $\sqrt{n}$ فإنّ العدد n يكون أوّليّاً.
البرهان:(1) إذا كان العدد الصّحيح n>1 أوّليّاً فإنّه يقسم نفسه ويتحقّق المطلوب .أمّا إذا كان العدد الصّحيح n>1 ليس اوّليّاً فإنّه يكون حاصل ضرب عدد منته من الأعداد الأوليّة والتي كلّ منها يكون قاسماً أوّليّاً للعدد n>1 .
(2)إذا كان العدد الصّحيح n>1 مؤلّفاً فإنّه يكتب بالشّكل n = a .b وحيث 1< a ≤ b < n ومن ذلك ينتج $a^2 \le a . b = n$ ومنه a ≤ $\sqrt{n}$، وبما أنّ العدد الصّحيح a>1 فإنّه يوجد قاسم أوّلي وليكن P (حسب(1)) وبالتّالي نستطيع كتابة P ≤ a ، P|a ، وبما أنّ a|n فإنّه حسب خاصّة التّعدي للقسمة ينتج أنّP|n ومن كون P ≤ a , a ≤ $\sqrt{n}$ فإنّ P≤$\sqrt{n}$. وإذاً يوجد عدد أوّليP يقسم n وأصغر من $\sqrt{n}$ أو يساويه.
(3) ينتج مباشرة من (2) بالنّفي المنطقي،ويمكن البرهان بأن نفرض جدلاً أنّ العدد الصّحيح n>1 ليس أوّليّاً ، وبالتالي يكون مؤلّفاً ،وحسب (2) يكون للعدد n قاسم أوّلي p ≤ $\sqrt{n}$،إذاً الفرض الجدلي ليس صحيحاً ويتحقّق أنّ n عدد أوّلي.

اختبار أولية عدد: تساعد النتيجة (3) في صيغة اختبار عملي لمعرفة إذا كان عدد ما (صغير نسبياً) أولياً أم لا . وذلك باختبار " إذ كان العدد n>1 لا يقبل القسمة على أي عدد أولي p ≤ $\sqrt{n}$ فإن n أولي وإلا فلا ".

مثال: لمعرفة إذا العدد 103 أولياً أم لا؟ نلاحظ أن 10 < $\sqrt{103}$ < 11 وبالتالي الأعداد الأولية الأصغر من $\sqrt{103}$ هي 2,3,5,7 ونلاحظ أن 103 لا يقبل القسمة عل أي منها ، إذاً العدد 103 أولي .
قاعدة1: (مرشحة إراتوستينس The Sieve Of Eratosthenes).
إنّ النتيجة الثالثة أيضاً ترشد إلى طريقة لإيجاد الأعداد الأوّليّة الواقعة الواقعة في مجال محدد من الأعداد الصحيحة ، فإذا أردنا إيجاد جميع الأعداد الأوّليّة التي أصغر من 100 فإنّنا نكتب جميع الأعداد من 2 إلى 100 . نلاحظ أنّ العدد 2 أوّلي لذلك نضع دائرة حوله ثم نشطب جميع مضاعفاته من القائمة ،والتي هي الأعداد الزوجية ،لأنّها جميعها مؤلّفة ، إنّ العدد التّالي في القائمة الذي لم يتمّ شطبه هو العدد 3 وهو أوّلي ، لذلك نضع دائرة حوله ، ثم نشطب جميع مضاعفاته من القائمة ،لأنّ جميعها مؤلّفة . نلاحظ أنّه عند نهاية كلّ خطوة من هذه العمليّة يكون أصغر عدد من القائمة لم توضع حوله دائرة ، أو لم يشطب ،هو عدد أوّلي ،لأنّه إذا لم يكن عدداً أوّليّاً فإنّ له قاسم أوّلي أصغر منه ،أي أنّه مضاعف لعدد أوّلي أصغر منه ، وقد تمّ شطب كلّ المضاعفات في خطوة سابقة . باستخدام النتيجة (3) نلاحظ أنّه يكفي شطب مضاعفات الأعداد الأوّليّة P ≤ $\sqrt{100}$ = 10، وفي الحالة المدروسة P=2,3,5,7 . عند متابعة الطّريقة السّابقة نحصل على الأعداد الأوّليّة التي أصغر من 100 وهي :
2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97والتي عددها 25 .

تمرين وملاحظة: باستخدام مرشحة إراتوستينس بيّن أنّه يوجد عشرة أعداد أوّليّة بين العددين 100,150 ، أوجدها. (للتأكد الجواب هو : 101,103,107,109,113,127,131,137,139,139).

- وأنّه يوجد ثمانية أعداد أوّليّة بين العددين 1000,1050 .أوجدها. (وهي: 1009,1013,1019,1021,1031,1033,1039,1049) .
- وأنّه يوجد أربعة أعداد أوّليّة فقط بين العددين 10050,10000 (وهي: 10007,10009,10037,10039) .

قد يتبادر للّذهن استنتاج خاطئ من ظاهرة أنّ الأعداد الأوّليّة بين عددين الفرق بينهما ثابت (مثلاً خمسون) تتناقص كلّما كبر هذين العددين ،وبالتّالي قد نتوصّل إلى تصوّر خاطئ بأنّ مجموعة الأعداد الأوليّة منتهية وقد كثرت البراهين على وجود عدد غير منته من الأعداد الأوّليّة ،نقدّم واحداً منها في المبرهنة الآتية:

<u>مبرهن</u>: الأعداد الأوّليّة غير منتهية.(أو يوجد عدد غير منته من الأعداد الأوّليّة).

<u>البرهان(فكرة البرهان</u>:إثبات أنّه من أجل كلّ عدد صحيح موجب n يوجد عدد أوّلي q_nأكبر من n)

من أجل كلّ عدد صحيح n≥1 نضع $Q_n = n! + 1$ ، بملاحظة أنّ العدد $Q_n > 1$ ،فإنّه حسب النتيجة (1)، يوجد قاسم أوّلي q_n للعدد Q_n ، (أي أن $|Q_n$ (q_n) . لنبرهن على أنّ $q_n > n$ ، لذلك نفرض جدلاً أنّ $q_n \leq n$ ، في هذه الحالة يكون $q_n|n!$ ،(لأنّ q_n يكون أحد العوامل 2...(n-1)n=(n!)) ، وبما أنّ q_n يقسم كلّاً من Q_n و n! فهو يقسم أي تركيب خطّي لهما ،أي أنّ $q_n|(Q_n - n!)$ وبالتالي $q_n|1$ وهذا غير ممكن إذاً $q_n > n$ لكلّ n≥1 . وبالتالي نجد أنّه من أجل كلّ عدد صحيح موجب n يوجد عدد أوّلي q_n أكبر منه ،إذاً عدد الأعداد الأوّلية غير منته.

<u>مبرهنة</u>: (وجود على الأقلّ n عدد صحيح متتالي مؤلّف). لكلّ عدد صحيح موجب n ،يوجد على الأقلّ n من الأعداد الصّحيحة المؤلّفة المتتالية الموجبة .

<u>البرهان</u>:إنّ الأعداد الصّحيحة المتتالية: $(n+1)! + 2 , (n+1)! + 3 , \dots , (n+1)! + (n+1)$ ، والتي عددها n جميعها مؤلّفة وذلك لأنّه من أجل كلّ $2 \leq k \leq n+1$ فإنّ $k|(n+1)!$ ،وبما أنّ العدد k يقسم نفسه فإنّ $k \mid (n+1)! + k$ لكلّ $2 \leq k \leq n+1$ ، وهذا يبيّن أنّ جميع الأعداد $((n+1)! + 2,(n+1)! + 3, \dots , (n+1)! + (n+1))$ مؤلّفة.

<u>ملاحظة وتعريف</u> : إنّ وجود أزواج من الأعداد الأوّليّة الفرق بينهما 2 ،والتي تسمّى أعداد أوّلية توأمية مثل (101,103) ، (3,5) ، بالإضافة إلى وجود عدد غير منته من الأعداد الأوّليّة ، وما تضمّنته المبرهنة الأخيرة من وجود أي عدد نريد من الأعداد الصّحيحة الموجبة المتتالية المؤلّفة ، إنّ كل ذلك ، يبيّن عدم الانتظام في توزّع الأعداد الأوّليّة بين الأعداد الصّحيحة الموجبة ، سنقدّم للمبرهنة الأساسيّة في الحساب التمهيدية الآتية:

<u>تمهيدية</u>: (العدد الأوّلي إذا قسم جداء عددين أو أكثر فإنّه يقسم واحداً منها على الأقلّ)

(a) إذا كان P عددا أوّليّاً يقسم حاصل ضرب العددين a,b فإنّه يقسم أحدهما على الأقلّ .أي أنّه بشكل رمزي :

$$P \mid a.b \xrightarrow{P \text{ عدد أوّلي}} P \mid a \ \vee \ p \mid b$$

(b) إذا كان p عدداً أوّليّاً يقسم حاصل ضرب الأعداد $a_1, a_2, .., a_n$ ، فإنّ p يقسم أحد هذه الأعداد على الأقلّ ، وبشكل رمزي :

$$(p \mid a_1.a_2 \dots a_n \xrightarrow{P \text{ عدد أوّلي}} p \mid a_1 \vee \ p \mid a_2 \ \vee \ \dots \ \vee \ p \mid a_n)$$

(c) إذا كان p عدداً أوّليّاً يقسم a^n (حيث a عدد صحيح و n عدد صحيح موجب) فإنّ p يقسم a.

<u>البرهان</u> : (a) نفرض أنّ $p \nmid a$ ولنبرهن على أنّ $p \mid b$ ،بما أنّ p عدد أوّلي و $p \nmid a$ فإنّ (p,a)=1 ، وبما انّ $p \mid a.b$ فإنّه حسب تمهيدية إقليدس يكون $p \mid b$.

(b) نبرهن ذلك بالاستقراء :أولاً إذا كان n=2 فإنّ الخاصّة صحيحة حسب (a). ثانياً نفرض أنّه إذا قسم العدد الأوّلي p حاصل ضرب k من الأعداد الصّحيحة فإنّه يقسم واحداً منها على الأقّل،ولنبرهن على أنّه إذا قسم العدد الأوّلي p حاصل ضرب (k+1) من الأعداد الصّحيحة فإنّه يقسم واحداً منها على الأقلّ.

$$P|a_1.a_2 \dots .. a_k.a_{k+1} \Rightarrow p|(a_1a_2 \dots a_k)a_{k+1}$$

$$\underset{(a)}{\Rightarrow} p|(a_1.a_2 \dots .. a_k) \vee p|a_{k+1} \xrightarrow[\text{فرضيّة الإستقراء}]{} (p|a_1 \vee p|a_2 \vee \dots .. \vee p|a_k) \vee p|a_{k+1}$$

$$\Rightarrow p \text{ يقبل القسمة على } a_1, a_2, \dots, a_k, a_{k+1} \text{ أحد الأعداد}$$

<u>مبرهنة</u> (المبرهنة الأساسيّة في الحساب)

كلّ عدد صحيح n>1 يكتب بشكل وحيد (باستثناء الترتيب) كحاصل ضرب عدد منته من الأعداد الأوّليّة .

أو بعبارة مكافئة كلّ n>1 إمّا أن يكون أوّليّاً أو أنّه يكتب بشكل وحيد (باستثناء الترتيب) كحاصل ضرب عدد منته من الأعداد الأوّليّة .

<u>البرهان</u> لقد برهنّا سابقاً على أنّ كلّ عدد صحيح n>1 إمّا أن يكون أوّليّاً ،أو أنّه يكتب كحاصل ضرب عدد منته من الأعداد الأوّليّة ، وذلك كتطبيق على الصّيغة الثّانية للاستقراء الرّياضي ، وبالتّالي علينا فقط إثبات أنّ n يكتب بشكل وحيد. وسوف نستخدم أيضاً المبدأ الثّاني للاستقراء الرّياضي على أنّ n .

(1) من أجل n=2 ،فمن الواضح أنّ العدد الأوّلي 2 يحقّق وحدانيّة الكتابة كما وردت في نصّ المبرهنة.

(2) نفرض أنّ كلّ من الأعداد 2,3,...,k يحقّق نصّ المبرهنة، ولنبرهن على أنّ العدد k+1 يكتب بشكل وحيد (باستثناء التّرتيب) كحاصل ضرب عدد منته من الأعداد الأوّليّة.

إذا كان العدد K+1 أوّليّا فيتحقّق المطلوب ، أمّا إذا كان k+1 عدداً مؤلّفاً ، فإنّنا نفترض أنّه يكتب كحاصل ضرب عدد منته من الأعداد الأوّليّة بطريقتين ،أي أنّ: $k+1 = p_1.p_2 \dots .p_t = q_1.q_2 \dots .q_s$. ثمّ نبرهن على تساوي التّحليلين : بما أنّ $p_1|q_1.q_2 \dots .q_s$ ، و p_1 عدد أوّلي ، فإنّه حسب التمهيديّة السّابقة ، العدد p_1 يقسم أحد الأعداد $q_1, q_2, \dots, q_s$ وليكن q_i وحيث $1 \leq i \leq s$ ، وبالطّبع يمكن إعادة ترتيب الأعداد $q_1.q_2 \dots .q_s$ بحيث يكون $p_1|q_1$ ، وبما أنّ قواسم العدد الأوّلي q_1 هي فقط q_1 و1 وبما أنّ $p_1 \neq 1$ فإنّ $p_1 = q_1$ ،

وبالتالي فإنّه يمكن كتابة : $\frac{k+1}{p_1} = p_2.p_3 \dots .p_t = q_2.q_3 \dots q_s; 1 < \frac{k+1}{p_1} < k+1$ ، وبتطبيق فرضيّة الاستقراء على العدد $\frac{k+1}{p_1}$ فإنّ الطريقتين السّابقتين لكتابة $\frac{k+1}{p_1}$ متطابقتان (باستثناء التّرتيب) ، وعليه فإنّ s=t ، وبالتّالي فإنّ طريقتي تحليل العدد k+1 إلى عوامل أوّليّة متطابقتان .

ملاحظات وتعريف:

(1)إذا كانت العوامل الأولية المختلفة للعدد الصحيح n>1 هي $p_1, p_2, \dots, p_k$ ، وعدد تكرار p_i هو m_i لكل $1 \le i \le k$ فإننا نستطيع كتابة العدد n>1 بالشكل $n = p_1^{m_1}.p_2^{m_2} \dots .p_k^{m_k}$.ونسمي التحليل السابق الصورة القياسية لتحليل العدد n>1 إلى قوى عوامله الأولية المختلفة.

(2)إن أهمية المبرهنة الأساسية في الحساب ترجع إلى أن تحليل العدد الصحيح ى إلى حاصل ضرب أعداد أولية هو تحليل وحيد . وبالطبع توجد مجموعات كثيرة من الأعداد التي لا تتحقق فيها هذه الخاصة المهمة.والمثال الآتي يبين ذلك:

مثال: إذا كانت E ترمز لمجموعة الأعداد الصحيحة الزوجية ، واتفقنا على القول بأن العدد الزوجي يكون أولياً في E إذا لم نستطع كتابته كحاصل ضرب عددين من المجموعة E . فإن كل من الأعداد ...2,6,10,14, ، يكون عدداً أولياً في E بينما الأعداد ...4,8,12, ليست أوّلية في E . من السّهل التّحقّق من أنّ العدد 60 يكتب بطريقتين مختلفتين : $60 = 2(30) = 6(10)$ ، كحاصل ضرب عددين أوّليين في E .

أمثلة: (استخدام الوحدانيّة في المبرهنة الأساسيّة في الحساب).

(1) للبرهان على أنّ العدد $\sqrt[3]{10}$ ليس صحيحاً ، نفرض جدلاً أنّ $a=\sqrt[3]{10}$ عدد صحيح ، ومنه $a^3=10=2\times5$ وهذا غير ممكن ، لأنّ للعدد 10 تحليل واحد فقط إلى عوامله الأوّليّة.

(2) للبرهان على أنّ العدد $\log_{10} 2$ ليس نسبيّاً ، نفرض جدلاً أنّه عدد نسبي وأنّه يكتب بالشّكل $\log_{10} 2 = \frac{a}{b}$ وحيث a,b عددان صحيحان و $b \neq 0$ ومنه: $b.\log_{10} 2=a \Rightarrow \log_{10} 2^b = a \Rightarrow 2^b = 10^a = 2^a \times 5^a$ والكتابة الأخيرة غير صحيحة ، حسب وحدانيّة تحليل عدد صحيح إلى عوامل أوّليّة ،إذاً الفرض الجدلي ليس صحيحاً والعدد $\log_{10} 2$ ليس نسبيّاً.

- تطبيقات على المبرهنة الأساسيّة في الحساب :

1)مبرهنة:(تستخدم في مبرهنة لاحقة)

إذا كان a , b عددين صحيحين موجبين أوّليّين نسبيّاً وكان $a . b = c^n$ ، فإنّه يوجد عددان صحيحان d , e أوّليّان نسبيّاً بحيث $a = d^n$ ، $b = e^n$ ، وبشكل رمزيّ :

$$a>0 , b>0 , (a , b)=1 \ \wedge \ a . b = c^n \implies \exists d , e \in \mathbb{Z} ; a = d^n \ \wedge \ b = e^n$$

البرهان: - إذا كان أحد العددين a , b مساوياً للواحد ، وليكن a=1 ، فإنّنا نأخذ e = c , d = 1 ويتمّ المطلوب ، لذلك نستطيع أن نفرض أنّ كلّاً من a , b أكبر من الواحد ،ثم نكتب كلّاً منها على الصّورة القياسيّة :

$$a=p_1^{a_1}.p_2^{a_2} \dots .p_r^{a_r} \ \wedge \ b=p_{r+1}^{a_{r+1}}.p_{r+2}^{a_{r+2}} \dots .p_{r+s}^{a_{r+s}}$$

وحيث : $p_1 < p_2 < \dots < p_r \ \wedge \ p_{r+1} < p_{r+2} < \dots < p_{r+s}$ أعداد أوّليّة. وبما أنّ (a , b)=1 فإنّ جميع هذه الأعداد الأوليّة مختلفة. لنفرض الآن أنّ الصّورة القياسيّة لتحليل العدد c هي :

$$c = q_1^{b_1}.q_2^{b_2} \dots .q_k^{b_k} \ ; \ q_1 < q_2 < \dots . < q_k \ (q_i \text{ أعداد أوّليّة})$$

بما أنّ $a . b = c^n$ ، فإنّنا نكتب : $a . b = p_1^{a_1}.p_2^{a_2} \dots .p_{r+s}^{a_{r+s}} = q_1^{nb_1}.q_2^{nb_2} \dots .q_k^{nb_k} = c^n$ بعد ترتيب وإعادة ترقيم الطّرف الأيسر بحيث $p_1 < p_2 < \dots < p_{r+s}$ ، ثمّ باستخدام وحدانيّة التحليل في المبرهنة الأساسيّة نجد أنّ :

$$K = r + s \ , \ p_i = q_i \ , a_i = nb_i \ \forall \ 1 \le i \le r + s$$. وبالتالي نستطيع كتابة ما يأتي :

$a . b = p_1^{nb_1}.p_2^{nb_2} \dots .p_r^{nb_r}.p_{r+1}^{nb_{r+1}} \dots p_{r+s}^{nb_{r+s}}$. (وبعد إعادة الترتيب والترقيم عند الضّرورة) نأخذ:

$d=p_1^{b_1}.p_2^{b_2} \dots .p_r^{b_r}$ ، $e = p_{r+1}^{b_{r+1}}.p_{r+2}^{b_{r+2}} \dots .p_{r+s}^{b_{r+s}}$. فنحصل على أنّ $a=d^n$, $b=e^n$ نلاحظ أنّ (d , e) = 1 ، لأنّ $(p_i, p_j) = 1$ لكلّ $i \neq j$ ، وبالتّالي $(p_i^{b_i}, p_j^{b_j}) = 1$ لكلّ $I \neq j$.

تمرين: إذا كان $a_1|b_1$ و $a_2|b_2$ فبيّن صحّة أو عدم صحّة مايلي :
$$\begin{matrix} a_1.a_2|b_1.b_2 & (1) \\ (a_1+a_2)|(b_1+b_2) & (2) \end{matrix}\}$$

(9)(برهان: إقليدس لوجود عدد غير منته من الأعداد الأوّلية)

(a) إذا كانت $p_1, p_2, \dots, p_k$ أعداداً أوّليّة وكان $p \mid p_1, p_2, \dots, p_{k+1}$ ، وحيث p عدد أوّلي ، فبرهن على أنّ p يجب أن يكون مختلفاً عن الأعداد $p_1, p_2, \dots, p_k$.

(b) استخدم الفقرة (a) لإثبات وجود عدد غير منته من الأعداد الأوّليّة.

(10)إذا كان p ∤ n لجميع الأعداد الأوّليّة $p \le \sqrt[3]{n}$ فأثبت أنّ n إمّا أوّلياً ،أو أنّه حاصل ضرب عددين أوّليّين فقط.

(a) (11)إذا كان n>2 فبرهن على وجود عدد أوّلي p يحقق n< p < n! .

(b) هل تستطيع أن تستنتج من (a) وجود عدد غير منته من الأعداد الأوّليّة ؟.

(12) إذا كان p≠3 عدداً أوّلياً فأثبت أنّه لا يمكن أن يكون العددان p+2, p+4 أوّليّين في الوقت نفسه.

(13) إذا كان p , q عددين أوّليّين وكان $5 \le q \le p$ فأثبت أنّ $24 \mid (p^2 - q^2)$.

(14) إذا كان $2^k + 1$ عدداً أوّلياً فأثبت أنّ العدد k يجب أن يكون على الصّورة :$k=2^n; n \in z$.

(15) إذا كان $2^k - 1$ عدداً أوّلياً فأثبت أنّ k عدد أوّلي ، هل العكس صحيح ؟

(16) إذا كان 2|m≤0 وكان (210n+m) عدداً أوّلياً فأثبت أنّ m عدد أوّلي .

(18) لتكن f كثيرة الحدود المعرّفة كالتّالي :$f(n) = n^2 + n + 41$وحيث n من $\mathbb{Z}$.

(a) بيّن أنّ *f(n)*عدد أوّلي لكلّ 39≤n≤0 .

(b) بيّن أنّ*f(41), f(40)* عددان مؤلّفان .

(19) برهن على استحالة وجود كثيرة حدود من الدّرجة k≥1 بحيث *f(n)* عدد أوّلي لكلّ n≥1 .

(20) إذا كان n عدداً صحيحاً بحيث n|(n-1)!+1 فأثبت أنّ n يجب أن يكون عدداً أوّلياً .

<u>أعداد فيرما</u>: (Fermat Numbers)

ولد العالم بيير فيرما (Pierre de Fermat) بمدينة تولوز الفرنسيّة سنة 1601 وتوفّي سنة 1665 ، وهو محامي وقاضي إلّا أنّه كان مهتمّاً بالرّياضيات ، وعُرف في الوسط الرّياضي بمراسلاته لعلماء عصره من الرّياضيّين . على الرّغم من أنّه لم ينشر أي بحث في مجلّة علميّة إلّا أنّ إنجازاته كانت عظيمة لاسيما في نظريّة الأعداد التي يعتبر بحقّ مؤسّسها بمفهومها الحديث . وسوف نورد فيما يلي بعضاً من اكتشافاته:

(1)<u>مبرهنة فيرما الصّغرى:</u>

لقد أورد فيرما بدون برهان الحقيقة الآتية (التي برهنها أولر (Euler) عام 1763):

((إذا كان p عدداً أوّليّاً وكان a عدداً صحيحاً أوّلي نسبيّاً مع p فإنّ العدد $(a^{p-1} - 1)$ يقبل القسمة على p))

وسوف نقوم لاحقاً بدراسة هذه المبرهنة ، والتي ستكتب رمزيّا بالشّكل:

$$\forall\, a \in \mathbb{Z}\ ;\ (a, p) = 1 \underset{p \text{ أولي}}{\Longrightarrow} p \mid (a^{p-1} - 1)$$

(2)<u>مبرهنة فيرما الكبرى:</u>

"إنّ الحدس التّالي لفيرما" :

((لا يوجد حلّ (غير الحلّ <u>التافه</u>)(الحلول التي تحقق x.y.z=0) للمعادلة $x^n + y^n = z^n$ لكل 2<n))

يعرف بمبرهنة فيرما الكبرى (Fermat's last theorem) والذي لم يبرهن عليها إلّا في العقد الأخير من القرن العشرين.

(3) ((لا يوجد حلّ غير الحلّ التافه للمعادلة $x^4 + y^4 = x^2$)).

وقد برهن فيرما على هذه الحقيقة بطريقة تنسب له وتعرف بطريقة فيرما <u>المتناقصة بلا نهاية.</u>).

(4) كل عدد أولي فردي يمكن كتابته بطريقة وحيدة كفرق بين مربعين صحيحين.

البرهان: إذا كان p عدداً أولياً فردياً ، فإنه من السهل التحقق من كتابته على الشكل: $p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2$.

وللبرهان على وحدانية هذه الكتابة ، نفرض أن $p = x^2 - y^2$ ، ومنه نجد أن: $y = \frac{p-1}{2}$, $x = \frac{p+1}{2}$.

(5)تمهيديّة (لطريقة فيرما في التّحليل) :

إذا كان m عدداً صحيحاً فرديّاً موجباً فإنّه يتحقّق :

m يكتب كحاصل ضرب عددين موجبين ، إذا وفقط إذا ،أمكن كتابة m كفرق بين مربعيّ عددين صحيحين .

<u>البرهان:</u>

إذا كان m = a . b عدداً فرديّاً ، وحيث كلّ من a , b عدد موجب ، فإنّ كلاًّ من a , b يكون عدداً فرديّاً ، وعليه نستطيع كتابة : m = a . b = $\left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$.

<u>وبالعكس :</u>

إذا كان $m = a^2 - b^2$ ، فإنّنا نستطيع أخذ β=|b| ,∝=|a| وبما أنّ عدد فردي موجب فإنّ $0<\beta<\propto$ ، ويتحقّق :$m = \propto^2 - \beta^2 = (\propto + \beta)(\propto - \beta)$ ، وهذا يعني أنّ العدد m كتب كحاصل ضرب عددين موجبين .

طريقة فيرما لتحليل عدد فردي موجب m:

من التكافؤ الوارد في التمهيديّة السّابقة نلاحظ أنّه لتحليل عدد فردي موجب m إلى حاصل ضرب عددين موجبين فإنّه يكفي (ويلزم) أن نكتب m كفرق بين مربعين، أي نبحث عن حلّ للمعادلة $m = x^2 - y^2$ والتي تكتب بالشّكل : $y^2 = x^2 - m$ ، لذلك نبحث عن مربّع كامل على الصّورة $x^2 - m$ ، والذي يجب أن يكون غير سالب أي أنّ x تحقّق : $x^2 - m \geq 0 \Rightarrow x^2 \geq m \Rightarrow x \geq \sqrt{m}$. وهذا يعني البحث عن مربّع كامل $x^2 - m$ وحيث قيم x تحقّق $x \geq \sqrt{m}$ ، فإذا رمزنا بـ t لأصغر عدد صحيح يحقق $t \geq \sqrt{m}$ فإنّنا نبحث عن مربّع كامل من بين حدود المتتالية:

$$t^2 - m \ , \ (t+1)^2 - m \ , \ \ldots.$$

وهذا البحث يجب أن ينتهي بالتّأكيد لأنّ تحليل العدد m = m .1 يؤدّي إلى أنّ $m = \left(\frac{m+1}{2}\right)^2 - \left(\frac{m_1}{2}\right)^2$.

مثال (1) لتحليل العدد الفردي الموجب m=327 نلاحظ أوّلاً أنّ $18 < \sqrt{327} < 19$ ، لذلك نبحث عن مربّع كامل بين حدود المتتالية التي تبدأ بالحدّ $t^2 - m$ ، وحيث t أصغر عدد صحيح يحقّق $t \geq \sqrt{m}$ ، أي أن t = 19 ، ومنه نجد :

$$t=19 \Rightarrow 19^2 - 327 = 34 \neq a^2$$

$$20^2 - 327 = 73 \neq a^2$$

.....

$$(56)^2 - 327 = 2809 = (53)^2$$

$$\Rightarrow 327 = (56)^2 - (53)^2 = (56-53)(56+53) = 3(109)$$

وبما أنّ كلّاً من 3 و109 عدد أوّلي فنكون قد حلّلنا العدد 327 إلى عوامله الأوّليّة.

مثال(2): لتحليل العدد 476572 إلى عوامله الأوّليّة نلاحظ أوّلاً أنّه يكتب بالشّكل : 476572=4×119143 ثمّ نعتمد في تحليل العدد الفرديّ 119143 طريقة فيرما . نلاحظ أوّلاً أنّ $345 < \sqrt{119143} < 346$ ، لذلك نبحث عن مربّع كامل في المتتالية التي تبدأ بالحدّ الأوّل:

$$(346)^2 - 119143 = 573 \neq y^2 (347)^2 - 119143 = 1266 \neq y^2$$

.....

$$(352)^2 - 119143 = 4761 = (69)^2 \Longrightarrow$$

$$119143 = (352)^2 - (69)^2 = (352-69)(352+69) = 283 \times 421$$

بما أنّ كلّاً من 421,283 عدد أوّلي (تحقّق من ذلك) ، فإنّ العدد المعطى يحلّل إلى عوامله الأوّليّة بالشّكل : $476572 = 2^2 \times 283 \times 421$.

ملاحظة : للتحقّق من أنّ 283 عدد أوّلي نلاحظ أنّ $\sqrt{283} = 16.822$ وأنّ الأعداد الأوّليّة التي أصغر من $\sqrt{283}$(أو تساويه) هي: 2,3,5,7,11,13 ، وبما أنّ 283 لا يقبل القسمة على أيّ منها فإنّه يكون أوّليّاً حسب نتيجة . وبالطريقة نفسها نلاحظ أنّ $\sqrt{421} = 20.518$. وأنّ الأعداد الأوليّة الأصغر من $\sqrt{421}$ (أو تساويه) هي: 2,3,5,7,11,13,17,19 ، وأنّ أي منها لا يقسم 421 وبالتالي 421 أوّلي.

ملاحظة: (نبيّن فيها أنّ طريقة فيرما في تحليل عدد صحيح فردي ليست عمليّة دائماً .)

مثال ذلك: العدد 8359=643×13 ، الذي يحقّق $91 < \sqrt{8359} < 92$. نلاحظ أوّلاً أنّه إذا أردنا التحقّق فيما إذا كان هذا العدد أوّلي أم لا ، يلزمنا كلّ الأعداد الأوّليّة الأصغر من 91 ، وهي كثيرة ، لذلك من الطبيعي اللجوء ثانياً إلى استخدام طريقة فيرما في التحليل فيكون العدد t الموصوف في هذه الطريقة هو t=92 عند ذلك نبحث عن مربّع كامل في حدود المتتالية $t^2 - m, (t+1)^2 - m, \ldots$ ، ومنه

$$t^2 - m = (92)^2 - 8359 = 105 \neq a^2$$

$$= (93)^2 - 8359 = 290 \neq a^2 \quad = (94)^2 - 8359 = 477 \neq a^2 = (95)^2 - 8359 = 666 \neq a^2$$
$$= (96)^2 - 8359 = 857 \neq a^2$$

.... الطريق طويل جدا ...

$$= (328)^2 - 8359 = 99225 = (315)^2 \Rightarrow 8359 = (328)^2 - (315)^2 = (328+315)(328-315)$$

(إنّ كلّ من 13 و 643 عدد اوّلي) (13)(643)=8359

ملاحظة: في طريقة فيرما لتحليل عدد فردي إلى جداء عددين نبحث عن مربّع كامل في المتتالية :

$$u_0 = x_0^2 - m \ , u_1 = (x_0+1)^2 - m \, , u_2 = (x_0+2)^2 - m, \ldots \ldots$$

وحيث x_0 أصغر عدد صحيح أكبر أو يساوي $\sqrt{m}$. بملاحظة أنّ : $u_1 - u_0 = 2x_0 + 1 \, , u_2 - u_1 = 2x_0 + 3, \ldots \ldots$

فإنّنا نجد أنّ $u_i - u_{i-1} = [(x_0+i)^2 - m] - \left[\left(x_0 + (i-1)\right)^2 - m\right] = (x_0+i)^2 - (x_0+i-1)^2$

$$= [(x_0+i) - (x_0+i-1)][(x_0+i) + (x_0+i-1)] = 2x_0 + 2i - 1 = 2(x_0+i)$$

$$u_i = u_{i-1} + 2(x_0 + i) - 1 \qquad \forall\ i = 1,2,\dots\dots \quad ; u_0 = x_0^2 - m$$

وهذه الصّيغة تبسّط الحسابات بشكل كبير .

.

مثال: لدينا $4<\sqrt{19}<5$ وبالتالي $x_0 = 5$.

طريقة فيرما	طريقة د.نادر
نبحث في حدود المتتالية التالية عن مربّع كامل	نبحث عن مربّع كامل في المتتالية
$u_0 = x_0^2 - m = 25 - 19 = 6$ $u_1 = (x_0+1)^2 - m = 6^2 - 19 = 17 u_2 = (x_0+2)^2 - m$ $= 7^2 - 19 = 30$ $u_3 = (x_0+3)^2 - m = 8^2 - 19 = 45$ $u_4 = (x_0+4)^2 - m = 9^2 - 19 = 62 u_5 = (x_0+5)^2 - m$ $= 10^2 - 19 = 81$ $= 9^2 \Longrightarrow \qquad \Longrightarrow$ $19 = 10^2 - 9^2 = (10-9)(10+9) = 1 \times 19$	$u_0 = x_0 - m = 25 - 19 = 6 u_1 = 6 + 2(5+1) - 1 = 17$ $u_2 = 17 + 2(5+2) - 1 = 30 u_3 = 30 + 2(8) - 1$ $= 45 u_4 = 45 + 2(4) - 1 = 62 u_5$ $= 62 + 2(10) - 1 = 81$ $= 9^2 \Longrightarrow \qquad \Longrightarrow$ $((x_0+5)^2 - m = 9^2 \Rightarrow m = 19 = 10^2 - 9^2 = 1 \times 19$

ملاحظة: من أجل كلّ عدد فردي m فإنّ العددين الصّحيحين المتتاليين $\frac{m-1}{2}, \frac{m+1}{2}$ يحقّقان :

$$\left.\begin{aligned} m &= \frac{m+1}{2} + \frac{m-1}{2} \\ 1 &= \frac{m+1}{2} - \frac{m-1}{2} \end{aligned}\right\} \Rightarrow m = m \times 1 = \left(\frac{m+1}{2} + \frac{m-1}{2}\right)\left(\frac{m+1}{2} - \frac{m-1}{2}\right) = \left(\frac{m+1}{2}\right)^2 - \left(\frac{m-1}{2}\right)^2$$

أي أنّ $m=\left(\frac{m+1}{2}\right)^2 - \left(\frac{m-1}{2}\right)^2$ وبالتالي إذا أدّت طريقة فيرما في التّحليل إلى الشّكل m=m.1 فقط فإنّ m أوّليّ .

ممثّلاً بالنسبة لأعداد فيرما (الفرديّة) $F_m = 2^{2^m} + 1$ نلاحظ أنّ $\left[2^{2^m}\right]^{\frac{1}{2}} = 2^{\frac{1}{2}2^m} = 2^{2^{m-1}}$

$$2^{2^{m-1}} = \left[\left(2^{2^m}\right)^{\frac{1}{2}} < \sqrt{F_m} < x_0 ,\ 2^{2^m} < 2^{2^m} + 1\right.,$$

سؤال :هل هذه العبارة صحيحة [فيكون x_0 المرتبط بالعدد F_m هو $2^{2^{m-1}} + 1$ ، أي انّه F_{m-1}]

البرهان: من اجل كلّ عدد صحيح موجب a يتحقّق $a^2 < a^2 + 1 < a^2 + 2a + 1 = ((a+1)^2)$ أي $a < \sqrt{a^2+1} < a+1$

ومنه $2^{2^{m-1}} < \sqrt{F_m} < 2^{2^{m-1}} + 1 = x_0$.

إذا صحّ ذلك .فإنّه قد يكون ممكناً الرّبط بين كلّ عدد فيرما والّذي يسبقه؟!! بالنّسبة لتحليله إلى عوامله الأوّليّة .

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$

$2<\sqrt{5}<3$ $4<\sqrt{17}<5$ $16<\sqrt{257}<17$ $256<\sqrt{F_4}<257$

تمارين (على فقرة أعداد فيرما)

(1) استخدم طريقة فيرما لتحليل كلّ مما يلي : 81518057 , 40273 , 34417 , 6077 , 977 .

(2) أثبت أنّ مرتبة الآحاد للعدد F_n هي 7 لكلّ n≥2 (بالاستقراء) .

(3) أثبت أنّ F_4 عدد أوّلي .

(4) أثبت انّ العدد F_7 مؤلّف.

(5) أوجد عدد المراتب العشريّة في العدد F_8.

(6) استخدم طريقة فيرما للتحليل العدد $2^{11} - 1$.

(6)أعداد فيرما .(تعريف):

لقد لاحظ فيرما أنّ جميع الأعداد : $(2)^{2^0} + 1 = 3$, $(2)^{2^1}+1=5$, $(2)^{2^2} + 1 = 17$, $(2)^{2^3} + 1 = 257$, $(2)^{2^4} + 1 = 65537$

هي أعداد أوّليّة ، لذلك توقّع أن تكون جميع الأعداد التي تكتب يمكن كتابتها على الصّورة $\forall n \geq 0$ $F_n = (2)^{2^n} + 1$ أعداد أوّليّة ، والتي تسمّى حاليّاً أعداد فيرما (Fermat's numbers) ، ومن الواضح أنّها أعداد فرديّة ، ولقد كتب إلى العالم مرسين ((Mersenne)) بأنّ جميع محاولاه للمبرهنة على هذا التوقّع باءت بالفشل . وهذا طبيعي لأنّ هذا التوقّع لم يكن صحيحاً ، وهو الحدس الوحيد لفيرما الذي أخطأه .ولقد استطاع العالم الرّياضي الكبير أولر حلّ هذه

المشكلة عام 1732 حيث وجد أنّ العدد $f_5 = (2)^{2^5} + 1 = 4294967297$ يقبل القسمة على العدد 641 ،وسوف نقدّم برهاناً لذلك في المبرهنة التالية.

مبرهنة (F_5 ليس أوّلي) العدد *641* يقسم العدد F_5.

البرهان: لدينا

1) $2^{2^5} = 2^{32} = 2^4 \times 2^{28}$

2)641=16+625=$2^4 \times 5^4 \Rightarrow 2^4 = 641 - 5^4$

$$\Rightarrow 2^{32} = 2^4 \times 2^{28} = (641 - 5^4)2^{28} = 641\ 2^{28} - 5^4.2^{28} = 6412^{28} - 5^4(2)^{7^4}$$

3) 641=640+1=$5 \times 2^7 + 1 \Rightarrow 5 \times 2^7 = 641 - 1$

ومنه 4)$2^{32} = 641 \times 2^{28} - (5 \times 2^7)^4 = 641 \times 2^{28} - (641 - 1)^4 = 641\ k - 1\ ; k \in z$

ومنه نجد أنّ $F_5 = 2^{23} + 1 = 641k$

ملاحظة: إنّ أعداد فيرما F_n كبيرة جداً عندما تكون n≥6 .وعليه ننصح بعدم إجراء حسابات لمثل هذه الأعداد على الحاسبات العاديّة ، فمثلاً عند كتابتنا لعدد فيرما F_{15} على حاسب ذو قدرة عالية احتجنا إلى صفحتين كاملتين لطباعة هذه العدد وعند إحصائنا لعدد أرقام العدد F_{15} كان العدد هو 9870 رقماً.

على الرّغم من كلّ ذلك فقد وجد أنّ F_n عدداً مؤلّفاً لجميع قيم n وحيث 5≤n≤32 ،وكذلك وجد على الأقلّ 47 قيمة أخرى للعدد *n* حيث كان F_n عدداً مؤلّفاً وأكبر هذه القيم n=3310 ، لقد تمّ في العام *1905* البرهان على أنّ العدد F_7 مؤلّف وذلك بدون معرفة عوامله الأوّليّة ، إلى أن استطاع بيلارت (Billhart) وموريس(Morrison) تحليل F_7 إلى عوامله الأوّليّة في العام 1971 بالاستعانة في الحاسوب فوجد أنّ :

$$F_7 = (59649589127497217)(5704689200685129054721)$$

أمّا العدد F_8 فقد تمّ تحليله إلى عوامله الأوّليّة في العام *1981* . وفي العام *1993* تمّ لمجموعة من العلماء تحليل كلّاً من F_{19}, F_{21}, F_{22} .ومن الجدير بالذّكر أنّ حدس فيرما بالنّسبة لأعداده انقلب راساً على عقب حيث يتوقّع اليوم عدم وجود أعداد فيرما أوّليّة بعد العدد F_4 .على الرّغم من ذلك فإنّ لأعداد فيرما أهميّة خاصّة حيث أنّها أوّليّة نسبيّاً مثنى مثنى وهذا مانقدّم في المبرهنة التي نمهّد لها بما يلي:

تهميديّة: إنّ أعداد فيرما تحقّق المساواة : $\forall m \geq 1 \quad F_0, F_1, F_2 \ldots F_{m-1} = F_{m-2}$

البرهان: (بالاستقراء على m)

- من اجل m=1 لدينا $F_1 - 2 = 5 - 2 = 3 = F_0$ وبالتّالي المساواة صحيحة من أجل m=1 .

- نفرض صحّة المساواة من أجل m=k ، أي نفرض صحّة المساواة :$F_0.F_1 \ldots \ldots F_{k-1} = F_k - 2$ ونبرهن على صحّة المساواة من اجل m=k+1 ، أي نبرهن على صحّة المساواة :$F_0.F_1 \ldots \ldots .F_{k-1}.F_k = F_{k+1} - 2$ من فرضيّة الاستقراء نستطيع كتابة :

$$F_0.F_1 \ldots \ldots .F_{k-1}.F_k = (F_k - 2)F_k = (2^{2^k} - 1)(2^{2^k} + 1) = \left(2^{2^k}\right)^2 - 1 = 2^{2^{k+1}} - 1 = F_{k+1} - 2$$

مبرهنة(اعداد فيرما اوّليّة نسبيّاً مثنى مثنى) إنّ أعداد فيرما اوّليّة نسبيّاً مثنى مثنى أي أنّ: $\forall m \neq n \quad ; \quad m, m \geq 0 \quad (F_m, F_n) = 1$

البرهان: بما أنّ m≠n . فإنّه بالإمكان أن نفرض انّ m<n وباستخدام التمهيديّة الاخيرة نجد أنّ :$F_0F_1 \ldots F_mF_{m+1} \ldots F_{n-1} = F_n - 2$

إذا كان $(F_m, F_n) = d$ فإنّ d يقسم كلاً من F_m, F_n وبالتالي فهو يقسم اي تركيب خطّي لهما ، وعليه فإنّ :

$d|[F_n - (F_0F_i..F_{m-1})F_m(F_{m+1} \ldots F_{n-1})] = 2$ ، ومنه d|2 ، وهذا يعني أنّ العدد غمّا ان يكون مساوياً 2 وهذا غير ممكن (لأنّ أعداد فيرما كلّها أعداد فرديّة) أو مساوٍ للعدد 1 وهذا هو المطلوب.

نتيجة: يوجد عدد غير منته من الأعداد الأوليّة .

البرهان: بما أنّ كلّ عدد فيرما $F_m > 1$ فإنّه يوجد قاسم أوّلي p_m للعدد F_m . إذاً لكلّ عدد فيرما F_m يوجد قاسم أوّلي له p_m ، وبما أنّ $(F_m, F_n) = 1$ فإنّه ينتج أنّ $p_m \neq p_n$ لكلّ m≠n ، وهذا يعني وجود عدد غير منته من الأعداد الأوّليّة .

المعادلات الديوفنتية الخطيّة (Linear Diofantine Equations)

إنّ المعادلات الديوفنتيّة الخطيّة تنسب إلى العالم الرياضي اليوناني ديوفانتس (Diophantus) الذي عاش في القرن الثّالث قبل الميلاد ، وقد اشتهر هذا العالم بكتابة علم الحساب (Arithmetica) ويلقّبه بعض المؤرّخين بأبي الجبر لأنّه عالج في كتاباته بعض المسائل الجبريّة ، التي تعتبر اليوم مسائل في نظريّة الأعداد ، لذلك نعتقد أنّ العالم الرّياضي محمّد بن موسى الخوارزميّ الذي عاش في الفترة 780 إلى 850 ميلادي وهو صاحب الكتاب المشهور (الجبر والمقابلة) هو أحقّ من كلّ من سبقوه بلقب أبي الجبر ، لأنّه بحقّ أوّل من عالج مسائل جبريّة .

إنّ حلّ المعادلات الديوفنتيّة الخطيّة بطريقة عامّة ينسب إلى ديوفانتس ، على الرّغم من أنّه لم يقدّم في الواقع حلّاً عامّاً لها . لأنّه كان يكتفي بإيجاد حلّ واحد للمعادلة في أغلب الأحيان ، فضلاً عن أنّه لم يستخدم الأعداد الصّحيحة السّالبة، وكانت الطّرائق الّتي يتّبعها في الحلّ خاصّة جداً بحيث لا يمكن استخدامها في حلّ معادلة مشابهة .

في الحقيقة، إنّ أوّل من وضع حلّاً عامّاً للمعادلات الديوفنتيّة الخطيّة بمجهولين هو العالم الهندي اريابهاتا (Aryabhatata) الذي ولد عام 476 قبل الميلاد ، ولقد وضع العالم الفرنسي باشيه (Bachet) الذي عاش في الفترة من 1581 إلى 1638 ميلادي ، الحلّ العامّ للمعادلة الديوفنتيّة الخطيّة ، علماً بأنّه لم يكن على علم بطريقة أريابهاتا.

سوف نقدّم الآن مفهوم المعادلات الديوفنتيّة الخطيّة بمجهولين او اكثر ، ثم دراسة الشّرط اللّازم والكافي لوجود حلول لمثل هذه المعادلات.

تعريف (المعادلة الديوفنتيّة الخطيّة بمجهولين او أكثر)

(a) كلّ معادلة من الشّكل $ax+by=c$ وحيث a,b,c اعداد صحيحة تسمّى معادلة ديوفنتيّة خطيّة بالمجهولين الصّحيحين x,y . ودراسة حلول هذه المعادلة يعني إيجاد جميع الأزواج (x,y) . ودراسة حلول هذه المعادلة يعني إيجاد جميع الأزواج (x,y) من الأعداد الصّحيحة التي تتحقّق من اجلها المعادلة .

(b) كلّ معادلة من الشّكل $a_1x_1+a_2x_2+\cdots+a_mx_m=c$ وحيث $a_1,a_2,\dots a_m,c$ اعداد صحيحة تسمّى معادلة ديوفنتيّة خطيّة بالمجاهيل الصّحيحة $x_1,x_2,\dots,x_m$ وبالطّبع ، دراسة حلول هذه المعادلة يعني إيجاد جميع الميميّات $(x_1,x_2,\dots,x_m)$ من الأعداد الصّحيحة التي تتحقّق من أجلها المعادلة.

مثال(1) إنّ المعادلة $65x+72y-40$ حلّاً (حلولاً) مثل الزّوج $(x,y)=(20,-15)$ لأنّ 40=(-15)72+(20)56 .

أمّا عن معرفة متى يكون لمثل هذه المعادلات حلّ وعن كيفيّة إيجاد هذا الحلّ ، والاكثر من ذلك ، كيفيّة إيجاد جميع حلول هذه المعادلة (عند وجودها) فإنّ كلّ ذلك تجيب عنه هذه الفقرة، المبرهنة التّالية تقدّم لنا الشّرط اللازم والكافي لوجود حلول للمعادلة الديوفنتيّة الخطيّة بمجهولين .

ميرهنة: (a) المعادلة الديوفنتيّة الخطيّة $ax+by=c$ (1) يكون لها حلّ ، إذا وفقط إذا كان (a,b) يقسم c .

(b) *إذا كان* x_0,y_0 حلّاً للمعادلة الخطيّة (1) فإنّ الحلّ العام لهذه المعادلة هو $x=x_0+\frac{b}{(a,b)}k \quad \wedge \quad y=y_0-\frac{a}{(a,b)}k \;;\; k\in z$

البرهان: لنفرض أوّلاً انّ (a,b)=d|c ، عند ذلك يوجد عدد صحيح m بحيث c=md ، وبما أنّ القاسم المشترك الأكبر لعددين يكتب بشكل تركيب خطّي لهما فإنّه يوجد عددان صحيحان s,t بحيث d=as+bt . وبضرب الطّرفين بالعدد الصّحيح m فإنّنا نجد أنّ c=m.d=a(m.s)+b(m.t) وهذا يعني أنّ y=mt و x=ms حلّاً للمعادلة $ax+by=c$.

لبرهان العكس ، نفرض أنّ x_0,y_0 حلّ للمعادلة $ax+by=c$ وهذا يعني أنّ $ax_0+by_0=c$ وبما أنّ d يقسم كلّ من a,b فإنّ d يقسم أي تركيب خطّي لهما ، وبالتّالي فإنّ dيقسم $c=ax_0+by_0$.

ملاحظة ونيجة: لقد وجدنا سابقاً كيفيّة إيجاد عددين صحيحين s,t بحيث (a,b)=a.s+b.t ، ذلك باتبّاع خطوات معاكسة لخوارزمية إقليدس عند حساب (a,b) ، فإذا كان (a,b)|c فإنّ $\frac{c}{(a,b)}$ يكون عدداً صحيحاً بضربه بطرفي المساواة السابقة فإنّنا نحصل على ما يأتي : $c=a\frac{c.s}{(a,b)}+b\frac{c.t}{(a,b)}$

وهذا يعني أنّنا حصلنا على حلّ $x_0=\frac{c.s}{(a,b)}\;,y_0=\frac{c.t}{(a,b)}$ للمعادلة الديوفنتيّة الخطيّة $ax+by=c$ (عند تحقّق الشرط (a,b)|c) ،

وذلك أوّلاً: باستخدام خوارزميّة اقليدس في حساب (a,b)، فإذا كان (a,b)|c فإنّ للمعادلة حلّ ،عند ذلك ننتقل إلى:

ثانياً: نوجد العددين الصّحيحين s,t بحيث (a,b)=a.s+b.t.

وثالثاً:وأخيرا: نضرب طرفي المساواة الاخيرة بالعدد الصّحيح $\frac{c}{(a,b)}$ فنحصل على حل.

مثال(1): لإيجاد حلّ للمعادلة $28x+36y=20$ ، نحسب أوّلاً (28,36) فنجد

$$36,28 \xrightarrow{\text{خ.ق}} 36=1(28)+8$$

$$28,8 \xrightarrow{\text{خ.ق}} 28=3(8)+4$$

$$8,4 \xrightarrow{\text{خ.ق}} 8=2(4)+0 \qquad \Longrightarrow (36,28)=4|20 \qquad \Longrightarrow \text{للمعادلة حلّ}$$

ثانياً: لإيجاد الحلّ نكتب العدد 4 كتركيب خطّي للعددين 36,28 ، وذلك بخطوات معاكسة

لخوارزميّة إقليدس انطلاقاً من المساواة قبل الأخيرة (في الخوارزميّة) فنجد 4=(28)-3(36) = 28-3(36-28) = 4(28)-3(8) = 28-4 وبذلك نحصل على المساواة 4=4(28)-3(36)

ثالثاً بضرب طرفي المساواة الأخيرة بالعدد 5 فإنّنا نحصل على المساواة :20=20(28)-15(36) بالمقارنة مع المعادلة الديوفنتيّة المعطاة نجد أنّنا حصلنا على الحلّ $x=20,\quad y=-15$.

ننتقل الآن إلى مسألة إيجاد جميع الحلول لمعادلة ديوفنتيّة خطيّة بمجهولين . وهذه الحلول ، كما ستبيّنه المبرهنة الآتية ،لها شكل عامّ مشترك ، لذلك نسمّي هذه الحلول بالحلّ العامّ للمعادلة (بدلالة حلّ خاصّ).

ميرهنة: (الحلّ العامّ للمعادلة الديوفنتيّة الخطيّة بمجهولين)

إذا كان x_0,y_0 حلّاً للمعادلة الديوفنتيّة الخطيّة (1) $ax+by=c$ (المحقّقة بالطبع للشّرط (a,b)|c) فإنّ الحلّ العام للمعادلة يكون على الصّورة :

$$x=x_0+\frac{b}{(a,b)}k \;\;;\;\; y=y_0-\frac{a}{(a,b)}k \qquad \forall k\in z$$

البرهان: لنبرهن أوّلاً على أنّه من أجل كلّ عدد صحيح k فإنّ $x=x_0+\frac{b}{(a,b)}k \;\;;\;\; y=y_0-\frac{a}{(a,b)}k$ يكون حلّاً للمعادلة : بالتعويض في الطّرف الأيسر من المعادلة $ax+by=c$ نجد : $a\left(x=x_0+\frac{b}{(a,b)}k\right)+b\left(\;y=y_0-\frac{a}{(a,b)}k\;\right)=ax_0+by_0$ وبما أنّ x_0,y_0 حلّاً فإنّنا نجد أنّ $ax_0+by_0=c$ ، ويتحقّق المطلوب .

- لنبرهن ثانياً على أنّ كل حلّ للمعادلة يكتب بالصّورة المذكورة في نصّ المبرهنة :

إذا كان x_1,y_1 حلّاً آخر للمعادلة فإنّ المطلوب إثبات وجود عدد صحيح k_1 بحيث $x_1=x_0+\frac{b}{(a,b)}k_1\;,\;\; y_1=y_0-\frac{a}{(a,b)}k_1$ بملاحظة التكافؤات التالية: $\frac{b}{(a,b)}|(x_1-x_0) \iff x_1-x_0=\frac{b}{(a,b)}k_1 \iff x_1=x_0+\frac{b}{(a,b)}k_1$ فإنّه يلزم ويكفي البرهان على علاقة القسمة الأخيرة الواردة في تلك التكافؤات.

بما أنّ كلّ من الزّوجين $(x_0,y_0),(x_1,y_1)$ حلّا للمعادلة (1) فإنّنا نحصل على المساواة : $ax_0+by_0=ax_1+by_1$ ومنه نحصل على المساواة $a(x_1-x_0)=b(y_1-y_0)$ (*) وبقسمة الطّرفين على (a,b) نحصل على $\frac{a}{(a,b)}(x_1-x_0)=\frac{b}{(a,b)}(y_1-y_0)$ وهذا يعني أنّ $\frac{b}{(a,b)}|\frac{a}{(a,b)}(x_1-x_0)$ وبما أنّ $\left(\frac{b}{(a,b)},\frac{a}{(a,b)}\right)=1$ فإنّه حسب تمهيديّة إقليدس ينتج أنّ $\frac{b}{(a,b)}|(x_1-x_0)$ ومنه يوجد عدد صحيح k_1 بحيث $x_1-x_0=\frac{b}{(a,b)}k_1$ (4) ومنه نجد أنّ $x_1=x_0+\frac{b}{(a,b)}k_1$ بتعويض (4) في (*) نجد :

$$a\left[\frac{b}{(a,b)}k_1\right]=b(y_0-y_1)\Rightarrow\frac{ak_1}{(a,b)}=(y_0-y_1)\Rightarrow y_1=y_0-\frac{a}{(a,b)}k_1$$

مثال (2) أوجد الحلّ العامّ للمعادلة الديوفنتيّة $28x+36y=20$ لقد وجدنا في المثال (1) حلّاً لهذه المعادلة هو $x_0=20\,,y_0=-15$ وبالتّالي يكون الحلّ العام لهذه المعادلة (حسب المبرهنة السّابقة) على الشّكل : $\forall k\in z$

$$\left.\begin{aligned}x&=x_0+\frac{b}{(a,b)}k=20+\frac{36}{4}k=20+qk\\y&=y_0-\frac{a}{(a,b)}k=-15-\frac{28}{4}k=-15-7k\end{aligned}\right\}$$

سؤال: هل توجد قيم موجبة لكلّ من x,y تكون حلّاً؟؟ (الجواب لا يوجد).

ملاحظة ومثال(3): في المسائل العمليّة توجد شروط إضافيّة على حلول المعادلات الديوفنتيّة ، مثل أن تكون جميع المتغيّرات موجبة ، أو أن تكون على أحد المجاهيل قيود محدّدة ، عند ذلك نبحث عن قيم k الصّحيحة (إن وجدت) بحيث تتحقق مثل هذه الشّروط.

فمثلاً إذا طلب إيجاد جميع الحلول الصّحيحة الموجبة للمعادلة الديوفنتيّة $18x+7y=302$ فإنّه باستخدام خوارزميّة إقليدس ، نوجد (18,7) ، على الرّغم من انّه من الواضح أنّه مساوٍ للواحد .

$$18,7\xrightarrow{\text{خ.ق}}18=2(7)+4$$
$$7,4\xrightarrow{\text{خ.ق}}7=1(4)+3$$
$$4,3\xrightarrow{\text{خ.ق}}4=1(3)+1$$
$$3,1\xrightarrow{\text{خ.ق}}3=3(1)+0\}\Rightarrow(18,7)=1|302\Rightarrow$$ للمعادلة حلّ

من العلاقة قبل الأخيرة وما قبلها من علاقات نكتب : $1=4-3=4-(7-4)=2(4)-7=2[18-2(7)]-7=2(18)-5(7)\Rightarrow1=2(18)-5(7)$

بضرب طرفي المساواة الأخيرة بالعدد 302 نحصل على المساواة : 302=604(18)-1510(7) ومنه نحصل على الحلّ . $x_0=604,\ y_0=-1510$

وحسب المبرهنة الأخيرة نجد انّ الحلّ العام يكتب بالشّكل :$k\in z$; x=604+7k , y=-1510-18k ولإيجاد الحلول الموجبة نكتب :

$x=604+7k>0\Rightarrow k>-\frac{604}{7}=-86.29$, $y=-1510-18k>0\Rightarrow k<-\frac{1510}{18}=-83.89$

وبالتالي القيم الموجبة لكلّ من Xو Y تنتج من قيم k الصّحيحة المحقّقة : 86.29-<k<-83.89 أيّ القيم 84-,85-,86-=k والتي توافقها الحلول الموجبة :

(x,y)=(2,38),(9,20),(16,2)

تمرين: برهن أنّ للمعادلة الديوفنتيّة 15x+18y=51 حلّاً وحيداً موجباً ثمّ أوجده (الجواب: (1,2)).

دراسة المعادلات الديوفنتيّة الخطيّة بأكثر من مجهولين :

مبرهنة : القاسم المشترك الأكبر لأكثر من عددين يكتب بشكل تركيب خطّي لتلك الأعداد)

من أجل الأعداد الصّحيحة $a_1,a_2,\dots a_m$ التي ليست جميعها أصفاراً ، توجد أعداد صحيحة $b_1,b_2,\dots,b_m$ بحيث :

$\forall m\geq2\,.\,(a_1,a_2,\dots a_m)=a_1b_1+a_2b_2+\cdots+a_mb_m$ (الطرف الأيمن من المساواة الأخيرة يسمّى تركيباً خطيّاً للأعداد $a_1,a_2,\dots a_m$ في $\mathbb{Z}$)

البرهان:بالإستقراء على m.

(1) من أجل m=2 نعلم أنّ (a_1,a_2) يكتب بشكل تركيب خطّي للعددين a_1,a_2 حسب مبرهنة سابقة.

(2) نفرض صحّة المبرهنة من أجل m=k (أي من أجل كلّ $a_1,a_2,\dots a_k$ عدد صحيح ليست جميعها أصفاراً توجد أعداد صحيحة $b_1,b_2,\dots b_k$ بحيث:$(a_1,a_2,\dots a_k)=a_1b_1+a_2b_2+\cdots+a_kb_k$) ونبرهن على صحّتها من أجل m=k+1 ، أي نفرض أنّ $a_1,a_2,\dots a_k,a_{k+1}$ أعداد صحيحة ليست جميعها أصفاراً ونبرهن على وجود أعداد صحيحة $b_1,b_2,\dots,b_{k+1}$ بحيث $(a_1,a_2,\dots a_{k+1})=a_1b_1+a_2b_2+\cdots+a_{k+1}b_{k+1}$

حسب مبرهنة حساب القاسم المشترك الأكبر لأكثر من عددين ، نستطيع كتابة :$(a_1,a_2,\dots a_k)=(a_1,a_2,\dots a_{k-1},(a_k,a_{k+1}))$ الطّرف الأيمن يتألّف من k عدد ليست جميعها أصفاراً ، وبالتّالي حسب فرضيّة الإستقراء يوجد أعداد صحيحة $b_1,b_2,\dots,b_{k-1},c_k$ بحيث :

$$(a_1,a_2,\dots a_{k-1},(a_k,a_{k+1}))=a_1b_1+a_2b_2+\cdots+a_{k-1}b_{k-1}+(a_k,a_{k+1})c_k$$

نحصل على $xc_k=b_k\,,yc_k=b_{k+1}$ بوضع x,y عددين صحيحين ، وحيث $=a_1b_1+a_2b_2+\cdots+a_{k-1}b_{k-1}+(a_kx+a_{k+1}y)c_k$

المساواة المطلوبة : $a_1,a_2,\dots,a_{k-1},a_k,a_{k+1}=a_1b_1+a_2b_2+\cdots+a_{k-1}b_{k-1}+a_kb_k+a_{k+1}b_{k+1}$

مبرهنة: يوجد حلّ للمعادلة الديوفنتيّة الخطيّة $a_1x_1+a_2x_2+\cdots+a_mx_m=c$ حيث $c_2\leq m$ إذا وفقط إذا كان $(a_1,a_2,\dots,a_m)|c$.

البرهان: ليكن $d=(a_1,a_2,\dots,a_k)$ ، إذا كان d|c ف إنّه يوجد عدد صحيح r بحيث c=d.r وحسب المبرهنة السّابقة توجد أعداد صحيحة $b_1,b_2,\dots,b_m$ بحيث : $d=a_1b_1+a_2b_2+\cdots+a_mb_m$ وبضرب طرفي المساواة الأخيرة بالعدد اصّحيح r نحصل على المساواة :

$c=a_1(b_1r)+a_2(b_2r)+\cdots+a_m(b_mr)$ والتي تبيّن أنّ $x_1=b_1r\,,x_2=b_2r\,,\dots,x_m=b_mr$ حلّاً للمعادلة المفروضة .

العكس : نفرض أنّ $b_1,b_2,\dots,b_m$ حلّاً للمعادلة المفروضة ، وبالتّالي تتحقق المساواة :$a_1b_1+a_2b_2+\cdots+a_mb_m=c$ وبما أنّ $d|a_i$ لكلّ 1≤i≤m ، فإنّ d يقسم أي تركيب خطّي للاعداد $a_1,a_2,\dots,a_m$ ، وبالتّالي فإنّ $d|a_1b_1+a_2b_2+\cdots+a_mb_m$ أي انّ d|c .

ملاحظة وخوارزميّة: يمكن إيجاد حلّ معادلة ديوفنتيّة خطيّة بأكثر من مجهولين بنفس طريقة حلّ المعادلة بمجهولين ، وذلك بحساب $(a_1, a_2, \dots, a_m)$ ومن خوارزميّة ،تعتبر تعميماً لخوارزميّة إقليدس في حساب (a,b) ، وذلك وفق مايلي:

نفرض أنّ الأعداد $a_1, a_2, \dots, a_m$ غير سالبة ، وليست جميعها أصفاراً (وهذا لا يؤثّر على عموميّة الخوارزميّة)(لماذا؟). ثمّ نتّبع الخطوات التّالية :

(1) نختار أصغر عدد موجب من بين الأعداد $a_1, a_2, \dots, a_m$ ولنفرض أنّه a_1 (قد يوجد أكثر من عدد بهذه الصّفة نختار احدها).

(2) نستخدم خوارزميّة القسمة (لكتابة الأعداد $a_2, a_3, \dots, a_m$; $a_1 \le a_i \ \forall i = 2,3, \dots m$ بدلالة a_1) فنحصل على :

$$a_1, a_2, \dots, a_m \xrightarrow{\text{خ.ق}} \begin{aligned} a_2 &= a_1 q_2 + r_2^{(1)} \ ; \ 0 \le r_2^{(1)} < a_1 \\ a_3 &= a_1 q_3 + r_3^{(1)} \ ; \ 0 \le r_3^{(1)} < a_1 \\ &\dots \qquad\qquad \dots \qquad\qquad \dots \\ a_m &= a_1 q_m + r_m^{(1)} \ ; \ 0 \le r_m^{(1)} < a_1 \end{aligned}$$

لاحظ أنّ $(a_1, a_2, \dots, a_m) = (a_1, r_2^{(1)}, \dots, r_m^{(1)}) = (r_1^{(1)}, r_2^{(1)}, \dots, r_m^{(1)})$ حيث افترضنا أنّ $a_1 = r_1^{(1)}$. نكرّر الخطوتين (1)و(2) السّابقتين بالنّسبة للأعداد $r_1^{(1)}, r_2^{(1)}, \dots, r_m^{(1)}$ ، ونستمرّ في ذلك مع ملاحظة أنّ الأعداد في كلّ خطوة هي أصغر من أصغر الأعداد في الخطوة التي تسبقها ، وبالتّالي لابدّ من الوصول في نهاية المطاف إلى أنّ : $\left(r_1^{(k)}, 0, \dots, 0\right) = r_1^{(k)} = \left(r_1^{(k-1)}, r_2^{(k-1)}, \dots, r_m^{(k-1)}\right)$ مع ملاحظة أنّ بعض الأعداد $r_i^{(k-1)}$ أصفاراً ، ومن ذلك نحصل أخيراً على أنّ : $(a_1, a_2, \dots, a_m) = r_1^{(k)}$

لماذا الناتج هو $r_1^{(k)} \neq 0$ هو $(a_1, a_2, \dots, a_m)$ ؟ نوضّح ذلك كما يلي :

$(a_1, a_2, a_3) = \left((a_1, a_2), a_3\right) = (a_1, a_3, \overline{a_2}) = \left((a_1, \overline{a_3}), \overline{a_2}\right) = (a_1 \overline{a_2}, \overline{a_3})$; وحيث $\overline{a_2}, \overline{a_3}$ هو باقي قسمة كلّ من a_3وa_2 على a_1 وحيث $a_1 \le a_i$

(قدّمنا شرط للخوارزميّة السّابقة على المثال)

مثال: لنستخدم الخوارزميّة السّابقة في إيجاد (119,38,95) ثمّ في حلّ المعادلة الديوفنتيّة الخطيّة 119x+38y+95z=c وحيث c أي عدد صحيح .

لحساب (119,38,95) ، نلاحظ اوّلاً أنّ أصغر هذه الاعداد هو 38 لذلك نكتب :

$$119,38,95 \xrightarrow{\text{خ.ق}} 119 = 3(38) + 5 \ \& \ 95 = 2(38) + 19 \Longrightarrow (119,38,95) = (5,38,19)$$

$$5,38,19 \xrightarrow{\text{خ.ق}} 38 = 7(5) + 3 \ \& \ 19 = 3(5) + 4 \Longrightarrow (5,38,19) = (5,3,4)$$

$$5,3,4 \xrightarrow{\text{خ.ق}} 5 = 1(3) + 2 \ \& \ 4 = 1(3) + 1 \Longrightarrow (5,3,4) = (2,3,1) = 1 | c \ \forall c \in z$$

$$5,3,1 \xrightarrow{\text{خ.ق}} 3 = 3(1) + 0 \ \& \ 2 = 2(1) + 0$$

مّما تقدّم نجد أوّلاً أنّ 1=(1,0,0)=(119,38,95) وهو يقسم أي عدد صحيح c ، وبالتّالي للمعادلة الديوفنتيّة المعطاة حلّ نحصل علي بكتابة هذا القاسم المشترك الأكبر (وهنا الواحد) من المعادلة التي يظهر فيها كباقي قسمة ، وهنا المعادلة الأخيرة ، فنكتب :$1 = 4 - 3 = 19 - 3(5) - [38 - 7(5)]$
$= 19 + 4(5) - 38 = 95 - 2(38) + 4[119 - 3(38)] - 38 = (95) - 15(38) + 4(119) = 1$

بضرب طرفي المعادلة بالعدد الصّحيح c نحصل على المساواة: $c = c(95) - 15c(38) + 4c(119)$ بالمقارنة مع المعادلة المفروضة $119x + 38y + 95z = c$ نحصل على الحلّ: $x = 4c \ , y = -15c \ , z = c$.

من أجل c=1 مثلاً ،نحصل على الحلّ $x = 4 \ , y = -15 \ , z = 1$ للمعادلة $119x + 38y + 95z = 1$

طريقة أولر في حلّ المعادلات الديوفنتيّة الخطيّة:

تعتمد طريقة أولر في حلّ معادلة ديوفنتيّة خطيّ بمجهولين أو أكثر ، على حقيقة أنّ العمليّات الحسابيّة من جمع وطرح وضرب على الأعداد الصّحيحة مغلقة. وسوف نقوم بشرح هذه الطريقة على معادلة ديوفنتيّة خطيّة بمجهولين $a_1 x_1 + a_2 x_2 = c$ وحيث $(a_1, a_2) | c$ لضمان وجود حلّ لهذه المعادلة ، وذلك بتقديم المثال التالي:

مثال: (شرح طريقة أولر في إيجاد حلول لمعادلة ديوفنتيّة خطيّة بمجهولين)

أوجد جميع حلول المعادلة $-15x_1 + 21x_2 = 66$

بما أنّ 66|3=(-15,21) ، فإنّ للمعادلة المفروضة حلّ ، (وبالتالي حلول) ، لإيجاد جميع هذه الحلول نقسّم أوّلاً طرفي المساواة على القاسم المشترك الأكبر 3 ، فنحصل على المعادلة المكافئة : $-5x_1 + 7x_2 = 22$ ثمّ نتّبع الخطوات التالية:

(1) نختار المجهول الذي معامله بالقيمة المطلقة أصغر المعاملات الأخرى ، في مثالنا نختار x_1 لأنّ |7|>|-5| .

(2) نبقي الحدّ الذي فيه المجهول المختار في الخطوة (1) في الطّرف الأيسر ، وننقل بقيّة الحدود إلى الطّرف الأيمن فنحصل على المعادلة : $-5x_1 = 22 - 7x_2$.

(3) نقسّم طرفي المعادلة الأخيرة على معامل x_1 وهو 5- فنحصل على المعادلة : $x_1 = x_2 + \frac{2}{5}x_2 - 4 - \frac{2}{5}$ لاحظ انّ المقدار $\frac{2}{5}x_2 - \frac{2}{5}$ يجب أن يكون عدداً صحيحاً كي يكون للمعادلة حلّ .

(4) نفرض أنّ $t_1 = \frac{2}{5}x_2 - \frac{2}{5}$ ، ثمّ نصلح هذه المعادلة (بضرب الطرفين بـ5)لتأخذ الشّكل :$2x_2 - 5t_1 = 2$

وهي معادلة ديوفنتيّة خطيّة جديدة بمجهولين .

(5) نطبّق الخطوات (1)و(2)و(3) على المعادلة الديوفنتيّة التي حصلنا عليها في الخطوة (4) فنحصل على :

$2x_2 = 5t_1 + 2 \Rightarrow x_2 = 2t_1 + \frac{1}{2}t_1 + 1$.

(6) نطبّق الخطوة (4) على المعادلة في الخطوة (5) وذلك بأن نفرض $\frac{1}{2}t_1 = t_2$ ومنه $t_1 = 2t_2$ نتوقّف هنا ، لأنّ أصغر معامل لمتغيّر أصبح يساوي 1(أو 1-) وهو معامل t_1 ، نعوّض في معادلة الخطوة (5) فنحصل على : $x_2 = 2t_1 + \frac{1}{2}t_1 + 1 = 5t_2 + 1$ ومن معادلة الخطوة (3) نحصل بالتّعويض على : $x_1 = 5t_2 + 1 - 4 + 2t_2 = 7t_2 - 3$ وحيث t_2 ليس عليه أي شروط سوى أن يكون عدداً صحيحاً وبالتّالي الحلّ العامّ للمعادلة هو :

$\forall t_2 \in z:\quad x_2 = 5t_2 + 1 \quad , \quad x_1 = 7t_2 - 3$

تمرين: احسب الحلّ العامّ للمعادلة الواردة في المثال السّابق ،وذلك بإيجاد حلّ خاصّ ثمّ إيجاد الحلّ العام وذلك بالطّريقة المتّبعة سابقاً ،ثمّ تأكّد من صحّة الحلّ الذي وجدناه بطريقة اولر.

مثال: (طريقة أولر لحلّ معادلة ديوفنتيّة خطيّة بأكثر من مجهولين)

أوجد جميع الحلول للمعادلة : $7x + 3y - 20z = 23$.

الحلّ: نلاحظ أوّلاً أنّ 23|1=(7,3,-20) وبالتّالي للمعادلة حلّ لإيجاده نتبّع الخطوات التالية :

(1) إنّ أصغر المعاملات بالقيمة المطلقة هو 3 ، لذلك نكتب المعادلة المكافئة التالية: $3y = 23 - 7x + 20z$.

(2) نقسّم الطرفين على 3 ، فنحصل على المعادلة المكافئة التّالية :$y = 7 + \frac{2}{3} - 2x - \frac{1}{3}x + 6z + \frac{2}{3}z$

$$= 7 - 2x + 6z + \frac{2}{3} - \frac{1}{3}x + \frac{2}{3}z$$

(3) نضع الجزء الكسري مساوٍ t_1 ، أي نكتب : $t_1 = \frac{2}{3} - \frac{1}{3}x + \frac{2}{3}z$ ومنه نكتب : $x = 2 - 3t_1 + 2z$ ، نتوقّف عند هذه الخطوة ، لانّ أحد المجاهيل معامله 1 ، وهو x ، ومنه نجد : $x = 2 - 3t_1 + 2z$ ، ومن المعادلة في الخطوة (2) نجد أنّ $y = 7 - 2x + 6z + t_1$

$$7 - 2(2 - 3t_1 + 2z) + 6z + t_1 \qquad \Longrightarrow \qquad y = z + 7t_1 + 2z$$

ونضع $z = t_2$ حيث t_2 اي عدد صحيح وبالتّالي نحصل على الحلّ العام : $\forall\ t_1, t_2 \quad , y = z + 7t_1 + 2z, \quad z = t_2 \quad x = 2 - 3t_1 + 2z$

ملاحظة: إنّ طريقة اولر المبيّنة في المثال السّابق ، تؤدّي دائماً إلى الحصول على معادلة ،معامل أحد متغيّراتها يساوي الواحد ، والتي منها نحصل على الحلّ العام بالتّعويض العكسي.

تمارين (معادلات ديوفنتّة خطيّة)

(1) احسب ما يلي : (238,1190,334) , (1150,2344,228,96) , (1050,34,102)

[2] أوجد (إن أمكن) جميع حلول كلّ من المعادلات الديوفنتيّة الآتية :

(1) 12x+10y=32

(2) 22x+5y=18

(3) 60x+18y=97

(4) 86x+10y=500

(5) 207x+246y=15

(6) 2x+5y=51

(7) 6x+255y=137

(8) 111x+69y=9000

[3] أوجد (إن أمكن) جميع حلول كلّ من المعادلات الديوفنتيّة الآتية :

(1) 6x+24y-41z=91

(2) 15x+12y+30z=24

(3) 5x-2y-4z=10

[4] اشترى طالب مائة من المساطر والاقلام والأقلام و الاوراق و الاوراق بقيمة إجمالية مقدارها مائة ليرة سورية وكانت الأسعار على النّحو الآتي :

3 ليرات لكلّ قلم ، 2 ليرة لكلّ مسطرة. كلّ خمسة أوراق بليرة واحدة . ماعدد ما اشتراه من كلّ نوع؟

(5) شقّة سكنيّة فيها نوعان من الغرف ، غرف جيّدة أجرة كلّ منها 1230 ليرة سوريّة في الشّهر ، وغرف عاديّة أجرة كلّ غرفة منها 870 ل.س في الشّهر، فإذا كانت جميع الغرف في الشّقة مؤجّرة وكان الدّخل الكلّي للشقّة 87330 ل.س شهريّا فكم غرفة من كلّ نوع موجود في الشّقة .

كتمهيد لنظريّة الأعداد الأوّليّة ، التي سترد قريباً ، إذا أمكن بيان أنّ في قرب (جوار) لـ n ، أنّ متوسّط المسافة بين عددين أوّليّين متتاليين تكون متقاربة مع $\log n$. للتوضيح ، لنختار مجالاً طوله 200 ، مركزه n=1000 ، بالعودة إلى جدول الأعداد الأوّليّة يمكن التأكّد أنّه يوجد 28 عدد أوّلي في هذا المجال وأنّ متوسّط المسافة بين عددين أوّليّين متتاليين هو 6.8 . ومن جهة أخرى لدينا $\log 1000 \approx 6.9$.

تعريف: (تابع التعداد الأوّلي Prime Counting Function)

إذا كان $x > 0$ عدد حقيقي موجب ، عندئذٍ نرمز ب $\pi(x)$ للتابع الذي يعطي عدد الأعداد الأوّليّة $p \geq x$ ، ونسمّيه تابع التعداد الأوّلي (Prime Counting Function) $\pi(x) = |\{p \leq x | p$ عدد أوّلي$\}$ ، فمثلاً بما أنّ الأعداد الاوّليّة الأصغر من 10 أو تساويه هي 2,3,5,7 فنجد أنّ $\pi(10) = 4$. أيضاً ، بما أنّ الأعداد الأوّليّة حتّى الـ 30 هي 2,3,5,7,11,13,17,19,23,29, نجد أنّ $\pi(30) = 10$.

- حسب مبرهنة (عدد الأعداد الأوّليّة غير منته) نجد أنّ $\pi(x)$ يسعى إلى ∞ .(أي أنّ $\begin{pmatrix} \pi(x) \longrightarrow \infty \\ x \longrightarrow \infty \end{pmatrix}$).

الجدول الآتي يبيّن أنّ $\pi(10^n)$ يكبر مع n

n	$\pi(10^n)$	n	$\pi(10^n)$
1	4	10	455051511
2	25	11	4118054813
3	168	12	37607912018
4	1229	13	346065536839
5	9592	14	3204941750802
6	78498	15	29844570422669
7	664579	16	279238341033925
8	5761455	....	
9	50847534	20	2220819602560918840

إذا كان x عدداً صحيحاً موجباً وكبيراً ، نريد استخدام تقريب (تقدير) لـ $\pi(x)$ ، لعدد كلّ الأعداد الأوّليّة $p \geq x$. ماذا يعني القول بأنّ تابع ما يصبح تقريب جيّد (good estimate) لتابع آخر ؟ الجواب في التعريف الآتي :

تعريف: ليكن $f(x), g(x)$ تابعين بالمتغيّر الحقيقي x معرّفان من أجل x>0 . نقول إنّ $f(x)$ مقارب ل $g(x)$ ونكتب $f(x) \sim g(x)$ إذا كان $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

- إذا تحقّق ذلك ، فإنّه يبدو من المعقول استخدام $g(x)$ كتقريب لـ $f(x)$ من أجل x كبيرة .

الآن نحن جاهزون لتقديم واحدة من أهمّ النّظريّات في نظريّة الأعداد :

مبرهنة. (Prime Number Thorem)

إنّ $\pi(x) \sim \frac{x}{\log x}$ أي أنّ $\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$

إنّ مبرهنة عدد أوّلي، التي تسمح لنا باستخدام $(x/\log x)$ كتقدير (كتقريب) لقيم $\pi(x)$ ، تمّ طرحها كتخمين في العالم 1790 من قبل كلٍّ من Gauss و Legender بشكل منفصل . أوّل برهان كامل لها ، اعتمد على التحليل المركّب ، قُدِّمَ في العام 1896 بشكل منفصل من قبل كلّ من Hadamard و De la vallee Poussin ، وفي العام 1949 قدّم selberg and Erdos برهاناً يستخدم فقط التحليل الحقيقي .

- ليكن $f(x) = \pi(x) \log x/x$. إنّ تقارب f(x) إلى 1 بطيئ . مثلاً ، $f(10^{20}) = 1.023$ هذا يعني أنّ خطأ نسبي مقداره % 2.3 ينتج عندما $\pi(10^{20})$ يقدر بـ $10^{20}/\log 10^{20}$.

تقريب أفضل لـ $\pi(x)$ قدم بما يعرف بالتكامل اللوغاريتمي (so-called logarithmie integeral) $li(x) = \int_2^x \frac{dt}{log\ t}$.

الفصل الرابع : التطابقات (Congruences)

مقدمة:

إن التطابق هو تعبير حديث لقابلية القسمة، وهو ينطوي على معلومات قيمة وطرق سهلة للبرهان، وعلى مسائل جدبدة وعملية بالإضافة إلى ذلك فإن التطابق مفهوم حديث لأنه يمثّل علاقة تكافؤ على مجموعة الأعداد الصحيحة، ويتحول بسهولة إلى مساواة في $\mathbb{Z}$ ، وهذا ما يجعله أكثر ديناميكية في الاستعمال . إن مفهوم التطابق ظهر في ألمانيا، وكان صاحبه العالم المعروف كارل فريدريك غاوس(Karl Friedrich Gauss) الذي عاش في الفترة 1777-1855 ، وقد قدم هذا المفهوم في كتابه (Disquisitiones Arithmeticae) وكان عمر غاوس لا يتجاوز الرابع والعشرين، ويعتبر هذا الكتاب أساس نظرية الأعداد في مفهومها الحديث . وقد اشتغل غاوس في الفيزياء والفلك بالإضافة إلى الرياضيات وهو صاحب القول المشهور "الرياضيات ملكة العلوم ، ونظرية الأعداد ملكة الرياضيات " ولقد عرف في زمانه "بأمير الرياضيات" . بعد هذه المقدمة التاريخية، نقدم مفهوم التطابق بشكله الحديث .

تعريف (التطابق على $\mathbb{Z}$ بواسطة عدد صحيح موجب n)

ليكن n عدداً صحيحاً موجباً، و a،b عددين صحيحان، نقول إن العدد a يطابق العدد b قياس n ونرمز لذلك بالرمز $a \equiv b(mod\ n)$ ،إذا (وفقط إذا) كان $n|(a-b)$، أما إذا كان $n \nmid (a-b)$ فإننا نقول إن a لا يطابق b قياس n ونكتب $a \not\equiv b(mod\ n)$.

ملاحظة :إن مفهوم التطابق يكتب رمزيا كما يلي $a \equiv b(mod\ n) \Leftrightarrow n|(a-b)$ ، ومن تعريف قابلية القسمة نستطيع أن نكتب :

$$a \equiv b(mod\ n) \Leftrightarrow n|(a-b) \Leftrightarrow a-b=kn\ ;k \in \mathbb{Z} \Leftrightarrow a-b \in n\mathbb{Z} \Leftrightarrow a=b+kn\ ;k \in \mathbb{Z}$$

التكافؤات السابقة سوف نسميها تكافؤات التطابق .

مبرهنة: إن كل عدد صحيح a يطابق عدداً واحداً من المجموعة $\mathbb{Z}_n$ = {0,1,2,.....,n-1} ، وبالتحديد a يطابق باقي قسمته على n قياس n .

البرهان: حسب خوارزمية القسمة ، من أجل العددين a , n ، يوجد عددان صحيحان وحيدان q , r بحيث : $0 \le r < n\ ;\ a=qn+r$ ، وحسب مكافئات التطابق نجد أن $a \equiv r(mod\ n)$.

الوحدانية : إذا فرضنا وجود عدد آخر r` من $\mathbb{Z}_n$ بحيث $a \equiv r`(mod\ n)$ فإن $0 \le r' < n$ ويتحقق:

$$n|a-r \wedge n|a-r` \Rightarrow n|(a-r)-(a-r`)=r`-r \Rightarrow n||r`-r| \Rightarrow |r-r`|=0$$
$$\Rightarrow r=r`\ ;0 \le |r-r`| < n$$

مبرهنة : (علاقة التطابق هي علاقة تكافؤ)

إذا كان a , b , c أعداداً صحيحة ، وكان n عددا صحيحاً موجباً فإنه يتحقق :

1- $a \equiv a(mod\ n)$ ، (أي أن التطابق علاقة انعكاسية).

2- $a \equiv b(mod\ n) \Rightarrow b \equiv a(mod\ n)$. (أي أن التطابق علاقة تناظرية).

3- $a \equiv b(mod\ n) \wedge b \equiv c(mod\ n) \Rightarrow a \equiv c(mod\ n)$ ،(أي أن التطابق علاقة متعدية).

4- إن علاقة التطابق قياس n على $\mathbb{Z}$ هي علاقة تكافؤ.

البرهان :

1- بما أن $a-a=0=0.n$ ، وبما أن الصفر مضاعف لكل عدد صحيح n ، فإنه ينتج أن $n|(a-a)$ ، وبالتالي $a \equiv a(mod\ n)$

2- لدينا $a \equiv b(mod\ n) \Rightarrow n|(a-b) \Rightarrow n|(b-a) \Rightarrow b \equiv a(mod\ n)$.

3- $a \equiv b(mod\ n) \wedge b \equiv c(mod\ n) \Rightarrow n|(a-b) \wedge n|(b-a) \Rightarrow n|(a-b)+(b-c)$
$\Rightarrow n|(a-c) \Rightarrow a \equiv c(mod\ n)$

4- واضح من البنود الثلاثة السابقة.

مبرهنة: (العمليات الحسابية على التطابقات)

إذا كانت a , b , c , d أعداداً صحيحة ، وكان n عددا صحيحاً موجباً ، بحيث $c \equiv d(mod\ n)$ و $a \equiv b(mod\ n)$ فإنه يتحقق:

1- $a+c \equiv b+d(mod\ n)$

2- $a-c \equiv b-d(mod\ n)$

3- $a.c \equiv b.d(mod\ n)$

البرهان : بما أن $a \equiv b(mod\ n)$ فإن $n|(a-b)$ ، وبما أن $c \equiv d(mod\ n)$ فإن $n|(c-d)$ ، وبالتالي فإن n يقسم كل تركيب خطي للعددين $(c-d)$ و $(a-b)$ وبالتالي فإن :

1- n يقسم مجموعهما أي أن $n|(a+c)-(b+d)$ ومنه $a+c \equiv b+d(mod\ n)$

2- n يقسم الفرق بينهما أي أن $n|(a-c)-(b-d)$ ومنه $a-c \equiv b-d(mod\ n)$

3- n يقسم التركيب الخطي لهما $c(a-b)+b(c-d)$ والذي يساوي $ca-bd$ أي أن $n|(ca-bd)$ وبالتالي $ca \equiv bd(mod\ n)$.

نتيجة (1): ليكن $a \equiv b(mod\ n)$ ، وبما أن كل عدد صحيح c يحقق $c \equiv c(mod\ n)$ ، فإنه ينتج من المبرهنة السابقة مباشرة أن :

1- $a+c \equiv b+c(mod\ n)$

2- $a-c \equiv b-c(mod\ n)$

3- $a\ .\ b \equiv b\ .\ c(mod\ n)$

ونلخص البنود الثلاثة بقولنا إن اضافة أو طرح أو ضرب أي عدد صحيح c الى طرفي تطابق $a \equiv b(mod\ n)$ يبقي التطابق صحيحاً.

نتيجة (2): (تعميم للبندين 1 و 3 من المبرهنة الأخيرة)

اذا كانت $a_1, b_1, a_2, b_2, \dots, a_m, b_m$ أعداداً صحيحة ، وكان n عدداً صحيحاً موجباً بحيث : $\forall\ 1 \le i \le m \quad a_i \equiv b_i (mod\ n)$ ، فإنه يتحقق:

1- $a_1 + a_2 + \dots + a_m \equiv b_1 + b_2 + \dots + b_m (mod\ n)$ ، أي بشكل مختصر ، $\sum_{i=1}^{m} a_i \equiv \sum_{i=1}^{m} b_i\ (mod\ n)$.

2- $a_1 . a_2 . \dots . a_m \equiv b_1 . b_2 . \dots . b_m (mod\ n)$ أي بشكل مختصر ، $\prod_{i=1}^{m} a_i \equiv \prod_{i=1}^{m} b_i\ (mod\ n)$.

البرهان:(بطريقة الاستقراء الرياضي)

1- من أجل $m = 2$ ، فإن العبارة صحيحة ، حسب مبرهنة العمليات الحسابية على التطابقات ، لنفرض الآن صحة التطابق 1 من أجل $m = k$ ولنبرهن على صحته من أجل $m = k + 1$. من فرضية الاستقراء لدينا $a_1 + a_2 + \dots\dots\dots + a_k \equiv b_1 + b_2 + \dots\dots\dots + b_k (mod\ n)$ أي أنه لدينا $\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i\ (mod\ n)$ ، ومن الفرضيات الواردة في نص المبرهنة ، لدينا $a_{k+1} \equiv b_{k+1} (mod\ n)$ ، وحسب مبرهنة العمليات الحسابية على التطابقات $\sum_{i=1}^{k+1} a_i \equiv \sum_{i=1}^{k} a_i + a_{k+1} \equiv \sum_{i=1}^{k} b_i + b_{k+1} (mod\ n)$ وبالتالي فإن $\sum_{i=1}^{k+1} a_i \equiv \sum_{i=1}^{k} b_i\ (mod\ n)$.

2- من أجل $m = 2$ ، فإن العبارة صحيحة حسب مبرهنة العمليات الحسابية على التطابقات ، لنفرض صحة التطابق 2 من أجل $m = k$ ، ولنبرهن على صحته من أجل $m = k + 1$ ، من فرضية الاستقراء لدينا $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i\ (mod\ n)$ ومن الفرضيات الواردة في نص المبرهنة ، لدينا $a_{k+1} \equiv b_{k+1} (mod\ n)$ ، وحسب مبرهنة العمليات الحسابية على التطابقات نجد $\prod_{i=1}^{k} a_i . a_{k+1} \equiv \prod_{i=1}^{k} b_i . b_{k+1} (mod\ n)$ ، وبالتالي فإن $\prod_{i=1}^{k+1} a_i \equiv \prod_{i=1}^{k+1} b_i\ (mod\ n)$ ويتم المطلوب .

نتيجة (3) : إذا كان $a \equiv b (mod\ n)$ ، فإن $a^m \equiv b^m (mod\ n)$ لكل $1 \le m$.

البرهان : ينتج مباشرة من البند الثاني من النتيجة 2 بأخذ الحالة الخاصة $a_i = a$ و $b_i = b$ لكل $1 \le i \le m$.

ملاحظة: في النتيجة 1 ، وجدنا أنه إذا كان $a \equiv b (mod\ n)$ فإن $a . c \equiv b . c (mod\ n)$ لكل عدد صحيح c ومن الطبيعي أن نتساءل إذا كان العكس صحيحاً ؟ والجواب يكون بالنفي ، الذي يوضحه المثال الآتي:

مثال : إن $14 \equiv 8 (mod\ 6)$ التي تكتب بالشكل $7.2 \equiv 4.2 (mod\ 6)$ ، نلاحظ أن طرفي التطابق يقبل القسمة على 2 ، وعلى الرغم من ذلك فإن ناتج قسمتهما على العدد 2 لا يتطابقان قياس 6 ، لأن $7 \not\equiv 4 (mod\ 6)$.

مبرهنة : (شرط إجراء قسمة طرفي تطابق على عدد صحيح)

إذا كان a , b , c أعداداً صحيحة ، وكان n عدداً صحيحاً موجبا ، فإنه يتحقق: $a . c \equiv b . c (mod\ n) \iff a \equiv b (mod\ \frac{n}{(c,n)})$

البرهان: ($\Longleftarrow$)إذا كان $a \equiv b (mod\ \frac{n}{(c,n)})$ ، فإنه يوجد عدد صحيح k بحيث $a - b = \frac{n}{(c,n)} k$ ومنه $a\ c - b\ c = \left(\frac{c}{(c,n)} k\right) n$ وهذا يعني أن $a . c \equiv b . c (mod\ n)$

($\Rightarrow$) إذا كان $a . c \equiv b . c (mod\ n)$ ، فإنه يوجد عدد صحيح k بحيث $a\ c - b\ c = k\ n$ ، ومنه $(a - b)c = k\ n$ وبقسمة الطرفين على (c, n) نحصل على المساواة $(a - b)\frac{c}{(c,n)} = k\frac{n}{(c,n)}$ ، وهذا يبين أن $\frac{n}{(c,n)} | (a - b).\frac{c}{(c,n)}$ ، وبما أن $1 = \left(\frac{c}{(c,n)}\ ,\ \frac{n}{(c,n)}\right)$ ، فإنه ينتج حسب تمهيدية اقليدس $\frac{n}{(c,n)} | (a - b)$ ، وبالتالي $a \equiv b (mod\ \frac{n}{(c,n)})$.

نتيجة: في الحالة الخاصة إذا كان $(c, n) = 1$ ، فإنه يتحقق: $a\ c \equiv b\ c (mod\ n) \iff a \equiv b (mod\ n)$

فإذا كان $n = p$ عددا أوليا ، فإن أي عدد صحيح c لا يقبل القسمة على p يكون أوليا نسبيا مع p ، وبالتالي ينتج :

- من أجل كل عدد أولي p وأي عدد صحيح c لا يقبل القسمة على p يتحقق $a\ c \equiv b\ c (mod\ p) \iff a \equiv b (mod\ p)$

مبرهنة : (تغيير قياس التطابق)

إذا كان $a \equiv b (mod\ n)$ وكان $m | n$ فإن $a \equiv b (mod\ m)$. وبشكل رمزي $[a \equiv b (mod\ n) \ \wedge \ m | n \Longrightarrow a \equiv b (mod\ m)]$

البرهان : بما ان $a \equiv b (mod\ n)$ فإن $n | (a - b)$ ، وبما أن $m | n$ فإنه ينتج حسب خاصة التعدي للقسمة ، $m | (a - b)$ وهذا يعني أن $a \equiv b (mod\ m)$.

ملاحظة ومثال: من الطبيعي أن نتساءل عمّا إذا كان العكس صحيحاً ؟ أي إذا كان $a \equiv b (mod\ m)$ وكان $m | n$ فهل $a \equiv b (mod\ n)$ ؟ الإجابة هنا بالنفي ومثال ذلك ، إن $5 \equiv -3 (mod\ 2)$ ، والعدد 6 مضاعف للعدد 2 ، إلا أن $5 \not\equiv -3 (mod\ 6)$.

ملاحظة ومثال : إذا كان $a \equiv b (mod\ m_1)$ ، وكان $a \equiv b (mod\ m_2)$ ، فهل $a \equiv b (mod\ m_1 . m_2)$ ؟

الجواب في المثال التالي : $17 \equiv 5 (mod\ 6)$ و $17 \equiv 5 (mod\ 4)$ ولكن $17 \not\equiv 5 (mod\ 24)$. في الحقيقة سوف نقدم مبرهنة تؤكد أنّ $17 \equiv 5 (mod\ [6,4])$ ، ولكن قبل ذلك نحتاج إلى التمهيدية الآتية :

تمهيدية : إذا كان $[a_1, a_2, \dots\dots\dots, a_m] | c$ ، فإنّ $a_1 | c\ ,\ a_2 | c\ ,\ \dots\ ,\ a_m | c$ لكل عدد صحيح $2 \le m$ ، والعكس صحيح ، أي أنّه إذا كان $[a_1, a_2, \dots\dots\dots, a_m] | c$ فإنّ $a_i | c$ لكل $1 \le i \le m$.

البرهان :من أجل $m = 2$ وجدنا في مبرهنة سابقة التكافؤ التالي $[a_1, a_2] | c \iff a_1 | c \ \wedge \ a_2 | c$ ، وبالتالي القضية محققة من أجل $m = 2$ ، لنفرض صحّة القضية من أجل $2 \le m = k$ ، ولنبرهن على صحتها من أجل $m = k + 1$ ، فإذا كان $a_1 | c, a_2 | c, \dots\dots\dots, a_{k+1} | c$ فإنه يتحقق $[a_1, a_2, \dots\dots\dots, a_{k-1}, [a_k, a_{k+1}]] | c$ ، وحسب فرضية الاستقراء ، فإنه يتحقق $a_1 | c, a_2 | c, \dots\dots\dots, a_{k-1} | c, [a_k, a_{k+1}] | c$ وبالتالي يتحقق $[a_1, a_2, \dots\dots\dots, a_{k-1}, [a_k, a_{k+1}]] = [a_1, a_2, \dots\dots\dots, a_{k-1}, a_k, a_{k+1}]$ لأنه حسب مبرهنة $[a_1, a_2, \dots\dots\dots, a_{k-1}, a_k, a_{k+1}] | c$.

إن العكس صحيح ، لأنه إذا كان $[a_1, a_2, \dots\dots\dots, a_m] | c$ ، ولدينا $a_i | [a_1, a_2, \dots\dots\dots, a_m]$ لكل $1 \le i \le m$ فإنّ $a_i | c$ لكل $1 \le i \le m$ وذلك حسب خاصة التعدي لعلاقة القسمة ، وبذلك يتحقق المطلوب .

مبرهنة (1): إذا كان a, b عددين صحيحين ، وكانت $n_1, n_2, \dots\dots\dots, n_k$ أعداداً صحيحة موجبة ، فإنّه يتحقق:

$a \equiv b (mod\ n_i)\ ,1 \le i \le k \iff a \equiv b (mod\ [n_1, n_2, \dots\dots\dots, n_k])$.

البرهان: نلاحظ بسهولة أن:

$$a \equiv b(mod\, n_i)\ \forall\, 1 \le i \le k \iff n_i|(a-b)\ \ \forall\ 1 \le i \le k \iff [n_1, n_2, \dots\dots\dots, n_k]|(a-b) \iff$$

$$a \equiv b(mod\ [n_1, n_2, \dots\dots\dots, n_k])$$

<u>مبرهنة (2)</u>:

1- إذا كانت $(a,c) = (b,c) = 1$ فإنّ $(ab,c) = 1$.

2-إذا كانت $a_1, a_2, \dots\dots\dots, a_m$ أعداداً أولية نسبيا مثنى مثنى ، فإنّه يتحقق :

$[a_1, a_2, \dots\dots\dots, a_m] = a_1.a_2.\dots\dots\dots.a_m\ \ \forall\ m \ge 2$.

<u>البرهان :</u> 1-(طريقة أولى) بما انّ $(a,c) = 1$ ، فإنّه يوجد عددان صحيحان x_1, y_1 بحيث $1 = ax_1 + cy_1$ ، كذلك ، بما أنّ $(b,c) = 1$ فإنّه يوجد عددان صحيحان x_2, y_2 بحيث $1 = ax_2 + cy_2$ ، بضرب المساوتين السابقتين نجد أنّ :

$$1 = (ax_1 + cy_1)(ax_2 + cy_2) = (ab)x_1x_2 + c(ax_1y_2 + by_1x_2 + cy_1y_2)$$

وهذا يعني ، حسب مبرهنة سابقة أنّ ، $(ab,c) = 1$.

(طريقة ثانية) نفرض جدلاً أنّ $(ab,c) = d > 1$ ، وبالتالي يوجد قاسم أولي p لكل من $ab\ , c$ أي أنّ

$$p|ab\ \wedge\ p|c \Longrightarrow (p|a\ \vee\ p|b)\ \wedge\ p|c \implies (p|a\ \wedge\ p|c)\ \vee (p|b\ \wedge\ p|c) \implies (a,c) \ne 1\ \ \vee\ \ (b,c) \ne 1$$

وهذا يتناقض مع الفرض .

2- نعلم أنّه من أجل $m = 2$ يتحقق: $[a_1, a_2] = a_1.a_2 \iff (a_1, a_2) = 1$ ، أي أنّ البند 2 محقق من أجل $m = 2$ ،

لنفرض صحّة البند 2 من أجل $2 \le m = k$ ، ولنبرهن على صحّته من أجل $m = k + 1$.

لدينا $[a_1, a_2, \dots\dots\dots, a_k, a_{k+1}]$=$[a_1, a_2, \dots\dots\dots, a_{k-1}, [a_k, a_{k+1}]] = [a_1, a_2, \dots\dots\dots, a_{k-1}, a_ka_{k+1}]$

لأنّ $[a_k, a_{k+1}] = a_ka_{k+1}$ عندما $(a_k, a_{k+1}) = 1$ ، وبما أنّ $(a_i, a_k) = (a_i, a_{k+1}) = 1$ لكل $1 \le i \le k-1$ (حسب الفرض بأنّ الأعداد المفروضة أوليّة نسبيّاً مثنى مثنى) فإنّه حسب البند الأوّل ينتج أنّ $(a_i, a_ka_{k+1}) = 1$ لكل $1 \le i \le k-1$ ، وبالتالي فإنّ الأعداد $a_1, a_2, \dots\dots\dots, a_{k-1}, a_ka_{k+1}$ ، والتي عددها k ، تكون أوليّة نسبيّاً مثنى مثنى ، وحسب فرضية الاستقراء ، فإنّه يتحقق أنّ $[a_1, a_2, \dots\dots\dots, a_{k-1}, a_ka_{k+1}]$=$a_1.a_2.\dots\dots\dots.a_{k-1}.a_ka_{k+1}$ وبالتالي يتحقق المطلوب .

<u>نتيجة(1):</u> إذا كانت الأعداد الصحيحة الموجبة $n_1, n_2, \dots\dots\dots, n_k$ أوليّة نسبيّاً مثنى مثنى فإنّه يتحقق

$$a \equiv b(mod\, n_1.n_2.\dots\dots\dots.n_k) \iff a \equiv b(mod\, n_i)\ \ ,1 \le i \le k$$

<u>البرهان:</u> ينتج مباشرة من المبرهنة 1 والبند الثاني من المبرهنة 2 .

<u>نتيجة(2):</u> إذا كان $n = p_1^{r_1}p_2^{r_2} \dots\dots\dots p_k^{r_k}$ ، تحليلاً للعدد الموجب n إلى قوى عوامله المختلفة ، فإنّه يتحقق :

$$a \equiv b(mod\, n) \iff a \equiv b\left(mod\, p_i^{r_i}\right)\ \ ,1 \le i \le k$$

<u>البرهان:</u> نلاحظ أنّ الأعداد $p_1^{r_1}, p_2^{r_2}, \dots, p_k^{r_k}$ أوليّة نسبيّاً مثنى ، وحاصل ضربها يساوي العدد n ، فإنّه بالتطبيق المباشر للنتيجة 1 ، نحصل على المطلوب.

<u>مثال:</u> إن ايجاد عدداً صحيحاً x ، له نفس باقي القسمة *2* على كل من الأعداد 3,4,7 ، يكافئ إيجاد حلّ للتطابقات الآتية :

$$\left.\begin{matrix} x \equiv 2(mod\ 3) \\ x \equiv 2(mod\ 4) \\ x \equiv 2(mod\ 7) \end{matrix}\right\} \iff x \equiv 2(mod 84) \implies x = 86$$

<u>تعريف:</u>(نظير ضربي لعدد صحيح قياس n)

ليكن nعدداً صحيحاً موجباً ، و a عدداً صحيحاً ، نقول عن عدد صحيح b (إن وجد) إنّه نظير ضربي للعدد a قياس n إذا تحقق $a.b \equiv 1(mod\, n)$

<u>مثال:</u> العدد $b = 2$ هو نظير ضربي للعدد $a = 8$ قياس العدد صحيح الموجب 15 لأنّ $2 \times 8 \equiv 1(mod\ 15)$.

<u>ملاحظة</u> ومثال: ليس لكل عدد صحيح نظير ضربي قياس n ، فمثلاً إذا كان $n = 4$ و $a = 2$ ، فإنّ للعدد 2 نظير ضربي b قياس 4 إذا وفقط إذا تحقق $2.b \equiv 1(mod\, 4) \iff 2b - 1 = 4m\ ;\ m \in \mathbb{Z} \iff 2b - 4m = 1$ ، والمساواة في الطرف الأيمن تمثّل معادلة ديوفنتيّة خطيّة بالمجهولين b, m والتي ليس لها حلّ لأنّ $2 = (2, -4) \nmid 1$ ، أو بكل بساطة لأنّ الطرف الأيسر زوجي دوماً .

<u>مبرهنة:</u> ليكن n عدداً صحيحاً موجباً ، إنّ العدد الصحيح a يكون له نظير ضربي قياس n إذا وفقط إذا كان $(a,n) = 1$.

<u>البرهان:</u> (يعتمد على الخاصة $(a,b) = 1 \iff \exists x, y \in \mathbb{Z}\ , ax + by = 1$)

($\Longrightarrow$) بما أنّ $(a,n) = 1$ ، فإنّه يوجد عددان صحيحان x, y بحيث $ax + ny = 1$ ، ومنه $ax = 1 + n(-y)$ ، وهذا يعني أنّ $ax \equiv 1(mod\, n)$ وبالتالي x نظير ضربي لـ a قياس n .

($\Longleftarrow$) إذا كان b نظيراً ضربياً قياس n للعدد a فإنّه يتحقق $ab = 1(mod\, n)$ وبالتالي $ab = 1 + kn$ وحيث k عدد صحيح ، ومنه $ab + n(-k) = 1$ ، وهذا يعني حسب مبرهنة أنّ $(a,n) = 1$.

<u>نتيجة:</u> (طريقة إيجاد نظير ضربي)

من برهان المبرهنة السابقة ، نلاحظ أنّه لإيجاد نظيراً ضربياً لعدد a قياس n ، وحيث $(a,n) = 1$ ، فإنّه علينا كتابة العدد 1 بشكل تركيب خطي للعددين الأوليين نسبياً a, n باستخدام خوارزمية اقليدس ، وذلك بكتابة الخطوات المعاكسة لإيجاد (n, a) ، باستخدام خوارزمية القسمة لدينا نجد :

$$25,17 \xrightarrow{\text{خ.ق}} 25=1(17)+8$$
$$17,8 \xrightarrow{\text{خ.ق}} 17=2(8)+1 \quad \Longrightarrow \quad (25,17)=1$$
$$8,1 \xrightarrow{\text{خ.ق}} 8=8(1)+0$$

وبما أنّ $1=(25,17)$ فإنّ للعدد 17 نظير ضربي قياس 25 ، لإيجاده ، نكتب الواحد كتركيب خطي للعددين 25,17 ، وذلك انطلاقاً من العلاقة قبل الأخيرة من خوارزمية اقليدس ، فنجد $1=17-2(8)=17-2(25-17)=3(17)-2(25)$

$$\Longrightarrow \quad 3(17)=1+2(25) \quad \Longrightarrow \quad 3(17)\equiv 1(mod\ 25) \quad \Longrightarrow$$

العدد 3 نظير ضربي للعدد 17 قياس 25 .

- هل يوجد نظير ضربي آخر للعدد 17 قياس 25 ، حدد واحداً إن وجد ؟.

أمثلة على التطابقات:

مثال(1): يمكن اثبات أنّ العدد $F_5=2^{32}+1\equiv 0(mod\ 641)$ ، ليس أولياً . وذلك بأن نحسب أولاً $2^{32}=2^{2^5}$ ، لدينا $2^8=256$ وبالتالي

$$2^8\equiv 256(mod\ 641) \quad \Longrightarrow \quad (2^8)^2=2^{16}=(256)^2=65536\equiv 154(mod\ 641) \quad \Longrightarrow$$
$$2^{32}=(2^{16})^2\equiv (154)^2=23716\equiv 640(mod\ 641) \quad \Longrightarrow \quad F_5=2^{32}+1\equiv 0(mod\ 641) \quad \Longrightarrow \quad 641|F_5$$

تمرين: باستخدام طريقة المثال(1) برهن على صحّة ما يلي :

(a) $6^{48}\equiv 1(mod\ 13)$

(b) $6^{44}\equiv 1(mod\ 89)$

(c) $2^{644}\equiv 1(mod\ 645)$ (لاحظ أنّ $(2,645)=1$)

مثال(2): أوجد باقي قسمة العدد $\sum_{k=1}^{1000} k!$ على 24 .

بما أنّ $4!=24\equiv 0(mod\ 24)$ ، وبملاحظة أنّ $\sum_{k=1}^{1000} k!=1!+2!+3!+4!+5!+\cdots\ldots\ldots+(1000)!$

فإنّ $k!\equiv 0(mod\ 24)$ لكل $4\leq k$ ، وبالتالي $\sum_{k=1}^{1000} k!=1+2+6+\sum_{k=4}^{1000} k!\equiv 9(mod\ 24)$

وبالتالي العدد 9 هو باقي قسمة $\sum_{k=1}^{1000} k!$ على 24 .

مثال(3): أوجد أصغر عدد صحيح موجب k بحيث $31|\ (33(26)^2-k)$.

بما أنّ ، $31|\ (33(26)^2-k) \quad \Leftrightarrow \quad 33(26)^2\equiv k(mod\ 31)$ ، فإنّ المطلوب إيجاد باقي القسمة $33(26)^2$ للعدد 31 على العدد 31 الذي يحقق $0\leq k<31$ وبما أنّ:

$$33\equiv 2(mod\ 31) \quad \wedge \quad (26)^2=(31-5)^2=(31)^2-10(31)+5^2\equiv 25(mod\ 31)\Rightarrow$$
$$33(26)^2=2(25)=50\equiv 19(mod\ 31)\Rightarrow k=19$$

اختبارات خاصّة بقابلية القسمة: إحدى التطبيقات الهامة لعلاقة التطابق ، هو إيجاد اختبارات تتعلق بقابلية قسمة الأعداد الصحيحة على بعض الأعداد المعيّنة .

تمهيدية(1): من أجل كل عددين صحيحين موجبين k,n وحيث $1\leq k\leq n$ يتحقق:

1- $10^n\equiv 0(mod\ 2^k)$

2- $10^n\equiv 0(mod\ 5^k)$

البرهان: بما أنّ $10=2\times 5$ فإنّ $10^k=2^k\times 5^k$ لكل $1\leq k$ ، وبالتالي فإنّ يتحقق $5^k|10^k$ و $2^k|10^k$ لكل $1\leq k$ ، ومنه ينتج أنّ $5^k|10^n$ و $2^k|10^n$ لكل $n\geq k$ ، وهذا يعني أنّ $10^n\equiv 0(mod\ 5^k)$ و $10^n\equiv 0(mod\ 2^k)$ لكل $1\leq k\leq n$.

مبرهنة: ليكن N عددا صحيحا تمثيله العشري $N=(a_m.a_{m-1}.\ldots\ldots\ldots.a_1.a_0)_{10}$ ، وحيث a_k أعداد صحيحة تحقق $0\leq a_k\leq 9$ لكل عدد صحيح k يحقق $0\leq k\leq m$ ولنفرض أنّ $S=\sum_{k=0}^{m} a_k$ و $T=\sum_{k=0}^{m}(-1)^k a_k$ وأنّ $N_k=(a_{k-1}.a_{k-2}.\ldots\ldots\ldots.a_1.a_0)$ عند ذلك يتحقق :

1- $2^k|N_k \quad \Leftrightarrow \quad 2^k|N$

2- $5^k|N_k \quad \Leftrightarrow \quad 5^k|N$

3- $3\,|S \quad \Leftrightarrow \quad 3\,|N$

4- $\{S\equiv N(mod\ 9) \quad \Leftrightarrow \quad [\,S\equiv 0(mod\ 9) \quad \Leftrightarrow \quad N\equiv 0(mod\ 9)]\} \quad \Leftrightarrow \quad [9\,|S \quad \Leftrightarrow \quad 9\,|N\,]$

5- $11\,|\,T \Leftrightarrow 11\,|N$.

البرهان: (2+1)- بما أنّ:

$$N = a_0 + 10\,a_1 + \cdots + 10^{k-1}a_{k-1} + 10^k a_k + \cdots + 10^m a_m = N_k + 10^k \sum_{i=k}^{m} 10^{i-1}\,a_i \Longrightarrow$$
$$N \equiv N_k(mod\ 10^k) \Longrightarrow \begin{cases} N \equiv N_k(mod\ 2^k) \Longrightarrow \left(N \equiv 0(mod\ 2^k) \Leftrightarrow N_k \equiv 0\ (mod\ 2^k)\right) \\ N \equiv N_k(mod\ 5^k) \Longrightarrow \left(N \equiv 0(mod\ 5^k) \Leftrightarrow N_k \equiv 0\ (mod\ 5^k)\right) \end{cases}$$

طريقة أخرى للبرهان على (1) :

$$2^k|N \Leftrightarrow N \equiv 0(mod\ 2^k) \Leftrightarrow \sum_{i=0}^{m} a_i 10^i \equiv 0(mod\ 2^k) \Leftrightarrow \sum_{i=0}^{k-1} a_i 10^i + \sum_{i=k}^{m} a_i\,10^i \equiv 0(mod\ 2^k)$$
$$\Leftrightarrow \sum_{i=0}^{k-1} a_i 10^i \equiv 0(mod\ 2^k)$$

وذلك لأنه من أجل كل $k \le i \le m$ يتحقق $10^i \equiv 0(mod\ 2^k)$ ومنه يتحقق $a_i 10^i \equiv 0(mod\ 2^k)$ وبالتالي يتحقق : $\sum_{i=0}^{m} a_i 10^i \equiv 0(mod\ 2^k)$ ، وبما أن $N_k = \sum_{i=0}^{k-1} a_i 10^i \equiv 0(mod\ 2^k)$ ، فإنه ينتج من التكافؤات السابقة أن: $2^k|N_k \Leftrightarrow 2^k|N$

ويتم البرهان على 2 بخطوات مماثلة للبرهان على 1 ، وذلك بإبدال 5^k مكان 2^k أينما وجدت .

(4+3): (قبل البدء بالبرهان يجب ملاحظة أنّه إذا كان $a \equiv b(mod\ n)$ فإنّه يتحقق التكافؤ $b \equiv 0(mod\ n) \Leftrightarrow a \equiv 0(mod\ n)$ ، الذي بدوره يكتب بالشكل $n|b \Leftrightarrow n|a$ ، ومن هنا نستطيع القول بأنّه للبرهان على التكافؤ الأخير يكفي أن نبرهن على التطابق الأول.

الآن لدينا $10 \equiv 1(mod\ 9)$ ومنه $10^k \equiv 1(mod\ 9)$ وبالتالي $a_k.10^k \equiv a_k(mod\ 9)$ وبأخذ المجموع للطرفين من $k = 0$ إلى $k = m$ نجد أنّ :

$\sum_{k=0}^{m} a_k.10^k \equiv \sum_{k=0}^{m} a_k\ (mod\ 9) \Longrightarrow N \equiv S(mod\ 9)$ ، ومن التطابق الأخير ينتج التكافؤ

$N \equiv 0(mod\ 9) \Leftrightarrow S \equiv 0(mod\ 9)$ ، والذي يكتب بالشكل: $9|N \Leftrightarrow 9|S$

يتم برهان 3 بنفس طريقة برهان 4 ، يكفي لذلك ملاحظة أن $10 \equiv 1(mod\ 3)$ وأن $10 \equiv 1(mod\ 9)$. ويمكن إثبات الاثنين معاً كما يأتي:

$$10 \equiv 1(mod\ 9) \Longrightarrow 10^i \equiv 1(mod\ 9)\ \forall\ i \ge 0 \Longrightarrow a_i 10^{\mathrm{i}} \equiv \mathrm{a_i}(\mathrm{mod}\ 9) \Longrightarrow \sum_{\mathrm{i=0}}^{\mathrm{m}} \mathrm{a_i} 10^{\mathrm{i}} \equiv \sum_{\mathrm{i=0}}^{\mathrm{m}} \mathrm{a_i}(\mathrm{mod}\ 9) \Longrightarrow$$

$$N \equiv S\ (mod\ 9) \begin{cases} \Longrightarrow [N \equiv 0(mod\ 9) \Leftrightarrow S \equiv 0\ (mod\ 9)] \\ {\scriptstyle 3|9} \\ \Longrightarrow N \equiv S\ (mod\ 3) \Longrightarrow [N \equiv 0\ (mod\ 3) \Leftrightarrow S \equiv 0\ (mod\ 3)] \end{cases}$$

5- لدينا $10 \equiv -1(m0d\ 11)$ وبالتالي $10^i \equiv (-1)^i(mod\ 11)$ ، وبضرب الطرفين بـ a_i نجد أنّ : $a_i 10^i \equiv (-1)^i a_i(mod\ 11)$ وبالجمع نجد $\sum_{i=0}^{m} a_i 10^i \equiv \sum_{i=0}^{m}(-1)^i a_i(mod\ 11)$ ،وهذا يعني أنّ $N \equiv T(mod\ 11)$ ، ومنه ينتج التكافؤ $11|N \Leftrightarrow 11|T$ ، أي أنّ $N \equiv 0(mod\ 11) \Leftrightarrow T \equiv 0(mod\ 11)$.

مثال: أوجد أكبر أس k للعدد 2 بحيث: $2^k|4157892348 = N$.

الحل:$8|2$ و $2^2|48$ و $4 = 2^2$ و $2^3 \nmid 348$ ، $8 = 2^3$ ، وبالتالي فإنّ $2^2|N$ و $2^3 \nmid N$ ، وينتج من ذلك أنّ $k = 2$.

مثال: أوجد أكبر أس k للعدد 5 بحيث : $5^k|7963625 = N$.

الحل:$25|5^2$ و $625|5^3$ و $3625 \nmid 5^4$ ، وبالتالي فإنّ $5^3|N$ و $5^4 \nmid N$ وبالتالي أكبر أس هو $k = 3$.

مثال: اختبر قابلية قسمة العدد $N = 894325734$ على كل من 3,9,11 .

الحل: بما أنّ $S = 4 + 3 + 7 + 5 + 2 + 3 + 4 + 9 + 8 = 45$ يقبل القسمة على 3 فإنّ N يقبل القسمة على 3 ، وكذلك S يقبل القسمة على 9 ، وبالتالي فإنّ N يقبل القسمة على 9 أيضاً . كذلك لدينا $T = 4 - 3 + 7 - 5 + 2 - 3 + 4 - 9 + 8$ لا يقبل القسمة على 11 ، فإنّ العدد N لا يقبل القسمة على 11 . إن كل ما تقدم من أمثلة يعتمد على التكافؤات الواردة في المبرهنة السابقة .

مبرهنة: (اختبار قابلية القسمة على 7,11,13)

ليكن n عدداً صحيحاً موجباً ، وليكن $r(n)$ باقي قسمة العدد n على 1000 و $q(n)$ ناتج هذه القسمة ، فإذا كان c يرمز إلى أحد الأعداد 7,11,13 فإنّه يتحقق التكافؤ : $c|n \Leftrightarrow c|\left(q(n) - r(n)\right)$.

البرهان: نلاحظ أولاً أنّ $1001 = 7 \times 11 \times 13$ ، وحسب المعطيات ، فإنّ العدد n يكتب بالشكل $n = 1000.q(n) + r(n)$ ، ومنه بإضافة $q(n)$ للطرفين وإجراء بعض الإصلاحات نجد $q(n) - r(n) = 1001.q(n) - n$ ، وبالتالي فإنّ $q(n) - r(n) \equiv -n(mod\ 1001)$ أي أنّ $q(n) - r(n) \equiv -n(mod\ 7 \times 11 \times 13)$ ، وبما أن $c = 7,11,13|\ 1001$ فإنه حسب مبرهنة يتحقق:

$$q(n) - r(n) \equiv -n(mod\ c) \Longrightarrow [q(n) - r(n) \equiv 0(mod\ c) \Leftrightarrow -n \equiv 0(mod\ c) \Leftrightarrow n \equiv 0(mod\ c)]$$

وهذا يعني تحقق التكافؤ: $c|n \Leftrightarrow c|\left(q(n) - r(n)\right)$.

مثال: اختبار قابلية قسمة العدد n=14824017659 على كل من الأعداد 7,11,13 .لدينا

$$14824017659 = 1000 \times 14824017 + 659 \implies q(n) - r(n) = 14824017 - 659 = 14823358 = n_1$$

من جديد نكتب العدد n_1 على الشكل :

$$n_1 = 14823358 \equiv 1000 \times 14823 + 358 \implies q(n_1) - r(n_1) = 14823 - 358 = 14465 = n_2$$

ثم نكتب العدد n_2 بالشكل:

$$n_2 = 14465 \equiv 1000 \times 14 + 465 \implies q(n_2) - r(n_2) = 14 - 465 = -451$$

وبما أنّ $11|-451$ وأنّ $7 \nmid -451$ وأنّ $13 \nmid -451$ فإنّه ينتج أنّ $11|n$ و $7 \nmid n$ و $13 \nmid n$.

تمارين:

1-إذا كان $a \equiv b(mod\ n)$ فأثبت أنّ $(a,n) = (b,n)$

2-أثبت $ab \equiv cd(mod\ n) \ \wedge \ b \equiv d(mod\ n) \ ; (b,n) = 1 \implies a \equiv c(mod\ n)$

3-أثبت $a \equiv b(mod\ n_1) \ \wedge \ b \equiv c(mod\ n_2) \implies a \equiv c(mod\ (n_1, n_2))$.

4 - أثبت: $(a$ $b|c \implies (a+c,b) = (a,b)$.

(b $(a\ , bc) = (a,b) \implies (a,c) = 1$.

5-أثبت صحّة كل من العلاقات الآتية : (a) $6^{48} \equiv 1(mod\ 13)$.

(b) $2^{44} \equiv 1(mod\ 89)$.

(c) $2^{644} \equiv 1(mod\ 645)$

6-استخدم الاستقراء الرياضي في إثبات ما يلي :(a) $\sum_{k=1}^{n-1} k \equiv 0(mod\ n)$ وحيث n فردي > 1

(b) $16^n \equiv 6(mod\ 10)$

(c) $6^n \equiv 1 + 5n(mod\ 25)$

(d) $2^{3n} \equiv 1(mod\ 7)$

(e) $3^{6n-3} \equiv -1(mod\ 7)$

(f) $5^{3n} \equiv 1(mod\ 31)$

(g) $2^{2n} \equiv 3n + 1(mod\ 9)$

(h) $(-4)^n \equiv 1 - 5n(mod\ 25)$

(i) $5^n \equiv 8n^2 - 4n + 1(mod\ 64)$

7-أثبت ما يلي: $a^2 \equiv \begin{cases} 0(mod\ 4) & ;a\text{زوجي} \\ 1(mod\ 4) & ;a\text{فردي} \end{cases}$

8-إذا كان a عدداً فردياً فأثبت أنّ : $a^2 \equiv 1(mod\ 8)$

9-إذا كان p عدداً أولياً ، وكان $a^2 \equiv b^2(mod\ p)$ ، فأثبت أنّ $a \equiv \pm b(mod\ p)$.

11-أثبت أنّ $a^3 \equiv a(mod\ 3)$ لكل عدد صحيح a .

12-إذا كان b, c نظيرين ضربيين للعدد a قياس n فأثبت أنّ $b \equiv c(mod\ n)$

[13] إذا كانت $a_1, a_2, \dots, a_t$ هي جميع الأعداد من $\mathbb{Z}_n = \{0,1,2, \dots, n-1\}$ التي تحقّق $1 \le i \le t$; $(a_i, n)=1$ ، فأثبت أنّ :

للعدد a نظير ضربي قياس n⇔ يوجد i بحيث $a \equiv a_i(mod\ n)$ وحيث $1 \le i \le t$.

[14] أوجد جميع الأعداد من $\mathbb{Z}_{12}$ التي لها نظير ضربي قياس 12.

[15] هل يوجد نظير ضربي للعدد 16 قياس 35 ؟ أوجده إن كان جوابك نعم.

[16] إذا كان $x \equiv y(mod\ n)$ فأثبت أنّ: $\forall\ a,b,c\ \in \mathbb{Z}\quad ax^2+bx+c \equiv ay^2+by+c(mod\ n)$.

[17] إذا كانت $f(x)=\sum_{k=0}^{m} c_k x^k$ كثيرة حدود ، بمعاملات من $\mathbb{Z}$ ، وإذا كان $a \equiv b(mod\ n)$ فأثبت أنّ $f(a) \equiv f(b)(mod\ n)$.

[18] إذا كانت $f(x)$ هي كثيرة الحدود في التمرين السّابق [17] فأثبت أنّ: $\forall t \in \mathbb{Z}\quad f(x) \equiv f(x+tn)(mod\ n)$.

[19] أوجد أكبر أسّ k للعدد 2 بحيث تقبل كلّ من الأعداد التالية القسمة على 2^k : 44444 , 1324804 , 81356822426 .

[20] أوجد أكبر أسّ k للعدد 5 بحيث تقبل كلّ من الاعداد التالية القسمة على 5^k : 55555 , 2566025 , 23455890 .

[21] اختبر قابلية قسمة كلّ من الأعداد التالية على أيّ من العددين 3 , 9 : 6743109 , 10763732 , 153456781 .

[22]اختبر قابليّة قسمة كلّ من الأعداد التّالية على ايّ من الأعداد 7,11,13: 6743109 , 10763732 , 1086320015 .

[23] برهن على أنّ العدد $2^{3n+2}+234235236237238239$ يقبل القسمة على 7 لكلّ n≥0 .

(a)[24] إذا علمت أنّ $10^3 \equiv 1(mod\ 37)$ ، فصمّم اختبارا لقابليّة القسمة على 37 .

(b) استخدم (a) لاختبار قابليّة قسمة الأعداد التالية على 37 :2688238145 , 20612573112607 , 101800771617212 .

(a)[25] إذا كان d | k فأثبت أنّ $2^{d-1}|2^{k-1}$.

(b) استخدم (a) لإثبات التمرين : إذا كان 2^{k-1}عدداً أوّلياً فأثبت أنّ العدد k أوّلي ، هل العكس صحيح؟

أنظمة الرواسب (Residue systems)

لقد وجدنا أنّ علاقة التطابق قياس عدد صحيح موجب n المعرّفة على $\mathbb{Z}$هي علاقة تكافؤ ، وبالتالي فإنّ هذه العلاقة تجزّئ المجموعة $\mathbb{Z}$ إلى n من المجموعات الجزئية غير المتقاطعة ، والتي كلّ منها صفّ تطابق قياس n ، وكلّ صفّ يتكوّن من جميع الأعداد المتطابقة قياس n ، فمثلاً : كلّ صفّ تطابق قياس 2 يكتب بالشّكل : $[a]=\{x \in \mathbb{Z}\mid x \equiv a(mod\ 2)\}=\{x \in \mathbb{Z}|x=a+2k;k \in z\} \Longrightarrow [a]=\{a+2k|k \in \mathbb{Z}\}$

وبالتالي فإنّ صفوف التطابق المختلفة قياس 2 هي: $[0]=\{2k;k \in \mathbb{Z}\}=\{\dots,-4,-2,0,2,4,6,\dots\}=2\mathbb{Z}$

$[1]=\{1+2k;k\ \in \mathbb{Z}\}=\{\dots,-5,-3,-1,1,3,5,7,\dots\}=2\mathbb{Z}+1$

وذلك لأنّ $\cdots=[\pm5]=[\pm3]=[1]$ و $\cdots=[\pm4]=[\pm2]=[0]$ وذلك حسب خواصّ صفوف التكافؤ .

لقد برهنّا سابقاً على أهمّ خواصّ التطابقات والتي من المفيد ذكرها هنا لأهميتها :

<u>مبرهنة</u> كلّ عدد صحيح يجب أن يطابق عدداً <u>واحداً فقط</u> من أعداد المجموعة $\mathbb{Z}_n=\{0,1,2,\dots\dots,n-1\}$ قياس n ، وبشكل أكثر تحديداً كلّ عدد صحيح x يطابق باقي قسمته $\bar{x}$ على n قياس n ، وبشكل رمزي نكتب : $\forall x \in \mathbb{Z}\,,\exists^1 a=\bar{x} \in \mathbb{Z}_n; x \equiv \bar{x}(mod\ n)$.

<u>ملاحظة (1)</u>: المبرهنة الأخيرة تبيّن وجود تطبيق $\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_n$ معرّف بالمساواة $\pi(x)=\bar{x}$ ، وهو غامر لأنّ كلّ عدد a من $\mathbb{Z}_n$ يكون عدداً صحيحاً ويحقّق 0≤a<n وبالتالي فإنّه يكتب بالشكل $\pi(a)=\bar{a}=a$ وبالتالي التطبيق π غامر .

<u>ملاحظة (2)</u>:المبرهنة الأخيرة تبيّن أنّ كلّ عدد صحيح يطابق عدداً واحدً فقط من المجموعة $\mathbb{Z}_n$ قياس n.وفي الحقيقة امجموعة $\mathbb{Z}_n$ ليست المجموعة الوحيدة التي تتمتع بهذه الميزة (سنبيّن ذلك لاحقاً) وهذا يقود إلى التعريف التالي :

<u>تعريف</u> (نظام رواسب تام قياس n : Complete residuesystem)

نقول إنّ المجموعة $A=\{r_1,r_2,\dots,r_n\}$ الجزئية من $\mathbb{Z}$ ، تمثّل <u>نظام رواسب تامّ</u> قياس n، إذا كان كلّ عدد صحيح يطابق عدداً واحداً فقط من عناصر المجموعة A قياس n .

(يمكن ذكر الشّرط بلغة التطبيقات بقولنا : إذا كانت علاقة التطابق من $\mathbb{Z}$ على A تطبيقاً غامراً .

<u>مثال (1)</u> : من المبرهنة الأخيرة والتعريف نلاحظ أنّ عناصر المجموعة $\mathbb{Z}_n$ تمثّل نظام رواسب تامّ قياس n ، وهو من أهمّ أنظمة الرواسب قياس n ، حيث عناصره تمثّل مجموعة بواقي قسمة الأعداد الصّحيحة على العدد الصّحيح الموجب n ، ولتمييزه عن غيره نسميّه نظام الرّواسب التّام الأساسي قياس n.

<u>مبرهنة</u> (اختبار عملي لكي تمثّل عناصر مجموعة جزئيّة A من$\mathbb{Z}$ نظام رواسب تامّ قياس n)

لتكن $A=\{a_1,a_2,\dots,a_n\}$ مجموعة جزئيّة من مجموعة الأعداد الصّحيحة ، عند ذلك يتحقّق :

عناصر المجموعة A تمثّل نظام رواسب تام قياس n إذا وفقط إذا تحقق $\forall\ 1 \le i \ne j \le n\quad a_i \not\equiv a_j(mod\ n)$ (أي أنّ عناصر A غير متطابقة مثنى مثنى)

البرهان : (⟸) نفرض أنّ A تمثّل نظام رواسب تامّ قياس n ، ولنفرض جدلاً وجود عددان مختلفان a_i,a_j من A بحيث $a_i \equiv a_j(mod\ n)$. بما أنّ $a_j \equiv a_j(mod\ n)$ فإنّه ينتج أنّ العدد الصّحيح a_j يطابق عددين مختلفين هما a_i,a_j وهذا مستحيل . إذاً الفرض الجدلي غير ممكن وبالتّالي يتحقق الشرط

المطلوب في الطرف الأيسر .

(⟹)(طريقة 1) بما أنّ $\mathbb{Z}_n$ نظام رواسب تامّ قياس n ، فإنّ كل عدد صحيح a_i من A يتطابق مع عنصر واحد فقط k_i من $\mathbb{Z}_n$ وهذا يعرّف تطبيقاً من A إلى $\mathbb{Z}_n$ ، وهذا التطبيق متباين (لأنّه إذا كان $a_i \neq a_j$ عنصرين مختلفين من A فإنّ صورتيهما k_i, k_j مختلفتان من $\mathbb{Z}_n$ ، وذلك لأنّه لو كان $k_i = k_j$ لكان $a_i \equiv a_j (mod\ n)$ ، وهذا يتناقض مع الفرض بأنّ $a_i \not\equiv a_j (mod\ n)$ لكلّ I ≠ j ، وبما أنّ المجموعتين A و z_n منتهيتين ولهما نفس العدد من العناصر فإنّ التطبيق المتباين بينهما يكون تقابلاً ، وبما أنّ كلّ عدد صحيح x يطابق عدداً واحداً فقط من $\mathbb{Z}_n$ ، فهو يطابق عنصراً واحداً فقط من A بواسطة التقابل المذكور.

(طريقة2):

$$\forall\, a_i \in \mathbb{Z}; 1 \le i \le n \xrightarrow{n\text{ نظام رواسب تام قياس } \mathbb{Z}_n} \exists^1 k_i \in \mathbb{Z}_n\ ;\ a_i \equiv k_i (mod\ n) \xrightarrow{\text{عناصر } A \text{ غير متطابقة مثنى مثنى}} k_i \neq k_j\ \forall\ 1 \le i \neq j \le n$$
$$\xrightarrow{\mathbb{Z}_n = \{k_1, k_2, \dots, k_n\}} \forall\ k_i \in \mathbb{Z}_n \exists^1 a_i \in A; k_i \equiv a_i\ (mod\ n)$$

وبما أنّ كلّ عدد صحيح x يتطابق مع عنصر واحد k_i من $\mathbb{Z}_n$ (لأنّ $\mathbb{Z}_n$ نظام تامّ) وكلّ عنصر k_i من $\mathbb{Z}_n$ يتطابق مع عنصر واحد a_i من A فإنّ كلّ عدد صحيح x يتطابق مع عنصر واحد a_i من A ، وبالتالي فإنّ A نظام راسب تامّ قياس n.

نستخدم المبرهنة السّابقة في إثبات النتائج الآتية :

نتائج :

(1) كلّ مجموعة مؤلّفة من n من الأعداد الصّحيحة المتتالية تمثّل نظام رواسب تامّ قياس n .

(2) إذا كانت $A = \{r_1, r_2, \dots, r_n\}$ نظام رواسب تامّ قياس n، وكان a عدداً صحيحاً أوّليّاً نسبيّاً مع العدد n ، فإنّ عناصر المجموعة : $B = \{ar_1 + b, ar_2 + b, \dots, ar_n + b\}$ تمثّل نظام رواسب تامّ قياس n لكلّ عدد صحيح b .

البرهان:

(1) لتكن b , b+1 , b+2 , … , b+(n-1) ، أعداد صحيحة متتالية عددها n ، ولنفرض جدلاً وجود عنصرين مختلفين منها b+j , b+i متطابقين قياس n . أي نفرض أنّ $0 \le i, j < n\ ;\ i \neq j\ ;\ b + i \equiv (b + j)(mod\ n)$ ، ومنه نجد أنّ $i \equiv j(mod\ n)$ وهذا يتناقض مع كون $\mathbb{Z}_n$ نظام رواسب تامّ قياس n .

(2) نفرض جدلاً وجود عنصرين مختلفين $ar_i + b\ , ar_j + b$ من المجموعة B ، بحيث : $ar_i + b \equiv (ar_j + b)(mod\ n); i \neq j$ ومن التطابق الأخير نجد انّ $ar_i \equiv ar_j (mod\ n)$ ، وبما أنّ (a ,n)=1 ، فإنّه (حسب مبرهنة قسمة طرفي تطابق) نستطيع تقسيم طرفي التطابق على a (دون تغيير n) فنحصل على $r_i \equiv r_j (mod\ n)$ ، وهذا غير ممكن لأنّ عناصر A تمثّل نظام رواسب تامّ قياس n . إذاً الفرض الجدلي غير صحيح ، وبالتالي المجموعة B التي عدد عناصرها n تحقّق $\forall\ i \neq j\ ;\ 1 \le i, j \le n\ \ ar_i + b \not\equiv ar_j + b (mod\ n)$ ، إذاً حسب المبرهنة الأخيرة نجد أنّ المجموعة B تمثّل نظام رواسب تامّ قياس n.

تعريف(نظام رواسب مختزل قياس n)

إذا كانت $A = \{r_1, r_2, \dots, r_n\}$ نظام رواسب تامّ قياس n ، فإننا نسمّي مجموعة الأعداد من A الأوّليّة نسبيّاً مع n نظام رواسب مختزل قياس n ، وبالتالي نظام الرّواسب المختزل قياس n هو المجموعة الجزئيّة S من نظام رواسب تامّ A قياس n ، المعرّفة بالشّكل $S = \{a \in A \mid (a, n) = 1\}$.

[في نظام الرّواسب التامّ قياس n الأساسي $\mathbb{Z}_n$ نكتب $S = \{a \in \mathbb{Z}_n | (a, n)\}$. لاحظ أنّ S في $\mathbb{Z}_n$ تمثّل العناصر القلوبة في الحلقة $\mathbb{Z}_n$ ، أي أنّ S هي الزمرة الضّربيّة في $\mathbb{Z}_n$)

مثال:نعلم انّ $\mathbb{Z}_{12} = \{0,1,2, \dots, 11\}$ نظام رواسب تامّ قياس 12 ، وأنّ مجموعة الأعداد من $\mathbb{Z}_{12}$ ،الأوّليّة نسبيّاً مع 12 ، هي {1,5,7,11}=S ، وهي تشكّل نظام الرّواسب المختزل قياس 12 الموافق لنظام الرواسب التامّ $\mathbb{Z}_{12}$. وإذا غيّرنا نظام الرّواسب التامّ قياس 12 ، وأخذنا الأعداد المتتالية $A = \{0, \pm1, \pm2, \pm3, \pm4, \pm5, 6\}$ ، التي تمثّل نظام رواسب تامّ قياس 12 ، فإنّ نظام الرّواسب المختزل قياس 12 الموافق هو $\{\pm1, \pm5\}$ ، وعدد عناصره أربعة أيضاً كما هو عدد عناصر S. سوف نرى في مبرهنة قادمة أنّ لجميع أنظمة الرواسب المختزلة قياس n العدد نفسه من العناصر ، وهذا العدد سوف يسمّى دالّة أولر أو تابع أولر(Euler's function).

تمهيدية:(1) إذا كان $a \equiv b\ (mod\ n)$ فإنّ $(a, n) = (b, n)$. (العكس ليس بالضّرورة صحيح)

(2) إذا كان $B = \{a_1, a_2, \dots, a_k\}$ نظام رواسب مختزل قياس n، وكان a عدداً صحيحاً أوّليّاً نسبيّاً مع n ، فإنّ a يتطابق مع عدد واحد فقط من المجموعة B قياس n.

البرهان: (1) بما أنّ $a \equiv b(mod\ n)$ ، فإنّ $a - b = qn\ ;\ q \in z$ ، ومنه $a = qn + b$ ، وبالتّالي : $(a, n) = (qn + b, n) = (b, n)$.

(2) ليكن A نظام الرواسب التامّ قياس n الموافق لـ B ، من اجل العدد الصّحيح a يوجد عدد وحيد b من A بحيث $a \equiv b(mod\ n)$ ، وبالتالي $(a, n) = (b, n)$ ، وبما أنّ $(a, n) = 1$ فإنّ $(b, n) = 1$ ، ومن تعريف نظام الرّواسب المختزل قياس n فإنّ b يكون من B ، وبما أنّ b يتطابق مع نفسه فقط في نظام الرّواسب التامّ A ، فإنّه بالتأكيد يكون كذلك في النّظام B.

مبرهنة وتعريف(دالّة اولر)

جميع أنظمة الرّواسب المختزلة قياس n، تملك نفس العدد من العناصر ، نرمز لهذا العدد بالرّمز φ(n) ونسمّيه دالّة اولر (أو تابع اولر Euler's function)

البرهان: نفرض وجود نظامي رواسب مختزلين قياس n هما : $B = \{b_1, b_2, \dots, b_s\}$, $A = \{a_1, a_2, \dots, a_t\}$ ، ومن التمهيدية السابقة نجد أنّ كلّ عدد من B يتطابق مع عدد واحد فقط من أعداد A ، وبما أنّه لا يوجد عددان متطابقان في أيّ نظام رواسب مختزل قياس n، فإنّنا نجد أنّه لا يمكن وجود

عددين من B يطابقان العدد نفسه من A ، قياس n ، وبالتّالي فإنّ عدد عناصر B اقلّ أو يساوي عدد عناصر A ، أيّ أنّ $s \le t$ ، وبالطريقة نفسها نبرهن على أنّ $t \le s$ ، ومن ثم نحصل على أنّ $t=s$.

ملاحظة: إذا أخذنا $\mathbb{Z}_n$ كنظام رواسب تامّ قياس n ، فإنّ نظام الرّواسب المختزل قياس n يكون $B = \{a \in \mathbb{Z}_n | (a,n) = 1\}$ ، وبالتالي فإنّ ϕ(n) هو عدد الأعداد الأوّليّة نسبيّاً مع n ، والتي اصغر من n وأكبر أو تساوي الصّفر . (إنّ B تمثّل الزّمرة الضّربيّة في الحلقة $\mathbb{Z}_n$ (حلقة بواقي القسمة على n).

مثال: إنّ الأعداد من $\mathbb{Z}_{12}$ الأوّليّة نسبيّاً مع 12 هي {1,5,7,11} وعددها 4 وبالتّالي ϕ(12)=4 .

- كذلك الأعداد من $\mathbb{Z}_9$ الأوّليّة نسبيّاً مع 9 هي {1,2,4,5,7,8} وعددها 6 وبالتالي ϕ(9)=6.

-ونلاحظ أنّه من أجل كلّ عدد صحيح n>1 فإنّ $\phi(n) \le n-1$ ، والمساواة تتحقق عندما يكون العدد n أوّليا ، لأنّه في هذه الحالة الأعداد من $\mathbb{Z}_n$ والأوّليّة نسبيّاً مع n هي كلّ الأعداد 1,2,...,n-1 والتي عددها (n-1).

ملاحظة: إنّ المجموعة {1,2,...,ϕ(n)} ، والتي عدد عناصرها يساوي عدد عناصر أي نظام رواسب مختزل قياس n ، تصلح دوماً لترقيم أي نظام رواسب مختزل قياس n.

مبرهنة: إذا كانت $A = \{a_1, a_2, \dots, a_n\}$ نظام رواسب تامّ قياس n ، وكانت $B = \{r_1, r_2, \dots, r_{\varphi(n)}\}$ مجموعة جزئيّة من A تمثّل نظام الرواسب المختزل الموافق قياس n، وإذا كان a عدداً صحيحاً أوّليّاً نسبيّاً مع n فإنّ المجموعة $B' = aB = \{ar_1, ar_2, \dots, ar_{\varphi(n)}\}$ تكون نظام رواسب مختزل قياس n.

(نلخّص المبرهنة السّابقة بقولنا : إذا ضربنا جميع عناصر نظام رواسب مختزل قياس n بعدد صحيح أوّليّ نسبيّاً مع n ، فإنّنا نحصل على نظام رواسب مختزل جديد قياس n).

البرهان: بما أنّ (a ,n)=1 فإنّه حسب نتيجة المجموعة $A' = aA = \{aa_1, aa_2, \dots, aa_n\}$ تمثل نظام رواسب تامّ قياس n ، وبما أنّ $B' \subseteq A'$ فإنّه يكفي أن نبرهن على انّ $(ar_i, n) = 1$ لكلّ $1 \le I \le \phi(n)$ ، نفرض جدلاً أنّ $(ar_i, n) > 1$ ، وبالتالي يوجد قاسم أوّلي P لهما أيّ $p \mid ar_i$ و $p \mid n$ ، وبالتالي يصبح لدينا : $p \mid n \wedge (p \mid a \vee p \mid r_i) \Longrightarrow (p \mid n \wedge p \mid a) \vee (p \mid n \wedge p \mid r_i)$ ، وكلاهما مستحيل لأنّ $(r_i, n) = (a, n) = 1$ ، إذاً الفرض الجدلي ليس صحيح ، وبالتالي $(ar_i, n) = 1$.

تمارين على أنظمة الرّواسب

1) أوجد نظام رواسب مختزل قياس 40.
2) أوجد نظامي رواسب مختزلين قياس 30.
3) هل يوجد نظام رواسب تامّ قياس 13 جميع عناصره قوى للعدد 3.
4) أوجد (إن أمكن) نظام رواسب مختزل قياس 13 جميع عناصره قوى للعدد 3.
5) إذا كان $B = \{a_1, a_2, \dots, a_{\varphi(n)}\}$ نظام رواسب مختزل قياس n ، فبيّن أنّه ليس بالضّرورة أن يكون $a_1 + 2, a_2 + 2, \dots, a_{\varphi(n)} + 2$ نظام رواسب مختزل قياس n.
6) إذا كان $A = \{a_1, a_2, \dots, a_p\}$ و $B = \{b_1, b_2, \dots, b_p\}$ ، نظامي رواسب تامّين قياس العدد الأوّلي P ، فبرهن على أنّه ليس بالضّرورة أن يكون $a_1b_1, a_2b_2, \dots, a_pb_p$ ، نظام رواسب تامّ قياس P.
7) إذا كان n عدداً فرديّاً ، وكان $A = \{a_1, a_2, \dots, a_n\}$ نظام رواسب تامّ قياس n ، فبرهن على أنّ : $a_1 + a_2 + \cdots + a_n \equiv 0 (mod\ n)$.

تطابقات خاصّة (مبرهنة أولر + مبرهنة ويلسن Wilson's theorem)

مبرهنة: (أولر Euler's theorem)

إذا كان n عدداً صحيحاً موجباً ، وكان a عدداً صحيحاً أوّلياً نسبيّاً مع n ، فإنّه يتحقّق $a^{\varphi(n)} \equiv 1 (mod\ n)$ ، حيث ϕ(n) ترمز لدالّة أولر

وبشكل رمزي نكتب $\forall (n,a) \in \mathbb{Z}^+ \times \mathbb{Z}\ ;\ (a,n) = 1 \Longrightarrow a^{\varphi(n)} \equiv 1 (mod\ n)$.

البرهان : نفرض أنّ $B = \{r_1, r_2, \dots, r_{\varphi(n)}\}$ نظام رواسب مختزل قياس n ، بما أنّ (a ,n)=1 ، فإنّه حسب مبرهنة سابقة نجد أنّ $B' = aB = \{ar_1, ar_2, \dots, ar_{\varphi(n)}\}$، تكون نظام رواسب مختزل قياس n ، وبالتالي كلّ عدد أوّلي نسبيّاً مع n يطابق عدداً وحيداً من عناصر B'، حسب تمهيديّة سابقة ، وبالتّالي كل عنصر r_i يطابق عدداً وحيداً ar_j قياس n ، ومن ذلك ينتج ϕ(n) تطابق بين عناصر B وعناصر B' ، وبضرب هذه التطابقات طرفاً لطرف نحصل على التطابق : $ar_1.ar_2 \dots .ar_{\varphi(n)} \equiv r_1.r_2 \dots r_{\varphi(n)} (mod\ n)$ ، ومنه نحصل على التطابق :

$a^{\varphi(n)}.r_1.r_2 \dots r_{\varphi(n)} \equiv r_1.r_2 \dots r_{\varphi(n)} (mod\ n)$ ، وبما أنّ $(n, r_i) = 1$ ، لكلّ $1 \le I \le \phi(n)$ ، فإنّ $\left(n, r_1.r_2..r_{\varphi(n)}\right) = 1$ (حسب مبرهنة) وبالتالي ، بتقسيم طرفي التطابق الأخير على $r_1.r_2 \dots r_{\varphi(n)}$ ، نحصل على المطلوب $a^{\varphi(n)} \equiv 1 (mod\ n)$.

نتائج:

1) (مبرهنة فيرما الصّغرى) إذا كان P عدداً أوّليّاً و a عدداً صحيحاً بحيث p † a فإنّه يتحقق : $a^{p-1} \equiv 1 (mod\ P)$.
2) إذا كان P عدداً أوّليّاً فإنّه ، لكلّ عدد صحيح a يتحقّق : $a^p \equiv a (mod\ P)$.
3) إذا كان (a ,n)=1 فإنّ $a^{\varphi(n)-1}$ نظير ضربي للعدد a قياس n .
4) إذا كان (a,n)=1 فإنّ الحلّ الوحيد للتطابق $ax \equiv b (mod\ n)$ هو $x \equiv b.a^{\varphi(n)-1} (mod\ n)$.

ملاحظة: النتيجة 2 تكتب بالشّكل : ($a^p \equiv a(mod\ P) \forall a \in z \Leftarrow$(P عدد أوّلي) . وبالتالي فإنّ نفي هذه القضيّة يكتب بالشّكل :
($a^p \not\equiv a(mod\ p) \Leftarrow$(P ليس أوّلي) لعدد صحيح محدد a .
وهذه تقدّم لنا طريقة للبرهان على أنّ عدد ما P ليس أوّليّاً (أو أنه مؤلّفاً) ، وذلك بإثبات أنّه يوجد عدد صحيح a بحيث $a^p \not\equiv a(mod\ p)$.
وبهذه الطّريقة سوف نعالج المثال الثالث القادم.
البرهان (على النتائج): (1)بما أنّ P أوّلي ، فإنّ φ(p)=p-1 ، وبما أنّ p†a فإنّ (p,a)=1 وبالتالي حسب مبرهنة أولر نجد أنّ
$a^{p-1} \equiv 1(mod\ p)$.
(2) إذا كان p|a فإنّ $a \equiv 0(mod\ p)$ وبالتالي $a^p \equiv 0(mod\ p)$ ومنه ينتج $a^p \equiv a(mod\ p)$ ، وذلك لأن علاقة التطابق هي علاقة تكافؤ، أمّا إذا كان p†a فإنّه حسب (1) نجد أنّ $a^{p-1} \equiv 1(mod\ p)$ ، ومنه $a^p \equiv a(mod\ p)$.
(3)بما أنّ (a,n)=1 فإنّنا نستطيع استخدام مبرهنة أولر ، ونكتب $a.a^{\varphi(n)-1} \equiv 1\ (mod\ n) \Rightarrow a^{\varphi(n)} \equiv 1(mod\ n)$ ، وحسب مفهوم النّظير الضّربي قياس n ، نجد أنّ $a^{\varphi n)-1}$ هو نظير ضربي للعدد a قياس n .

(4) بضرب طرفي التطابق $ax \equiv b\ (mod\ n)$ بالنظير الضربي لـ a الوارد في البند (3) نحصل على المطلوب .
أمثلة:
(1) أوجد باقي قسمة 5^{38} على العدد 11.
(2) أوجد مرتبتي الآحاد والعشرات للعدد 3^{256}.
(3)أثبت أنّ العدد 117 مؤلّف (ليس أوّلي) .

الأمثلة السابقة محلولة.

سؤال: إذا كان n عدداً مؤلّفاً ، هل يوجد عدد صحيح a أوّلي نسبيّاً مع n يحقّق $a^n \equiv a(mod\ n)$ ، الإجابة على السّؤال في التمرين :
برهن على أنّ $2^{341} \equiv 2(mod\ 341)$:

(الحل موجود).....

وهذا يبرر التعريف الآتي :
تعريف (عدد شبه أوّلي) ليكن b , n عددين صحيحين موجبين ، وحيث n عدد مؤلّف .
نقول عن العدد المؤلّف n إنّه عدد شبه أوّلي(Pseudoprime) للأساس b إذا كان $b^n \equiv b(mod\ n)$.

تعريف (أعداد كارمايكل)
عدد كارمايكل هو كلّ عدد مؤلّف n يحقّق $a^{n-1} \equiv 1(mod\ n)$ ، من أجل كلّ عدد صحيح a أوّلي نسبيّاً مع n .
أعداد كارمايكل موجودة وأصغرها العدد (561) ، والذي تمّ اكتشافه من قبل العالم كارمايكل العام 1910 . وقد تم البرهان على وجود عدد غير منته من هذه الأعداد في العام 1992 في الولايات المتّحدة من قبل ثلاثة علماء من جامعة جورجيا .
تمرين(محلول) : إذا كان p عدداً أوّليّاً أكبر من 2 فإنّه يتحقّق : $x^2 \equiv 1(mod\ p) \Leftrightarrow x \equiv \pm 1(mod\ p)$.
الحلّ: (⟸) بدهي بالتّربيع .
(⟹)بما أنّ $x^2 \equiv 1(mod\ p)$ ، فإنّ $p|x^2 - 1 = (x-1)(x+1)$ ، وبما أنّ P أوّلي فإنّ $P|x-1$ أو $p|x+1$ ، أي أنّ $x \equiv 1(mod\ p)$ أو $x \equiv -1(mod\ p)$ ، وبما أنّ $1 \not\equiv -1(mod\ p)$ ، فإنّ $x \equiv \pm 1(mod\ p)$.
مبرهنة (ويلسن Wilson's theorem)
إذا كان P عدداً أوّليّاً فإنّه يتحقّق : $(p-1)! \equiv -1(mod\ p)$.
البرهان: إذا كان p=2 ، فإنّ $(p-1)! = 1 = -1(mod\ 2)$ ، ويتحقق المطلوب في هذه الحالة . لنفرض الآن أنّ p>2 ، بما أنّ (a ,p)=1 لكلّ $1 \leq a \leq p-1$ ، فإنّه يوجد نظير ضربي b للعدد a قياس p بحيث $1 \leq b \leq p-1$ ، إن الأعداد a التي نظيرها الضربي نفس العد هي التي تحقّق : $a^2 \equiv 1(mod\ p)$ ، وحسب التمرين السابق ، لدينا التكافؤ $a^2 \equiv 1(mod\ p) \Leftrightarrow a \equiv \pm 1(mod\ p)$ ، ايّ أنّ الأعداد التي نظيرها الضّربيّ هو نفس العدد قياس p ، هي التي تحقق $a \equiv \pm 1(mod\ p)$ وحيث $1 \leq a \leq p-1$ ، وبالتالي فإنها فقط العددان 1 , p-1 وعليه نستطيع تكوين $\frac{p-3}{2}$ زوجاً من الأعداد بين 2 , p-2 ، بحيث يكون حاصل ضرب كلّ زوج منها يطابق 1 قياس p ، وبالتالي نحصل على أنّ :
$2 \times 3 \times \dots\dots \times (p-3)(p-2) \equiv 1(mod\ p)$ ، ومنه نجد أنّ
$(p-1)! \equiv 1 \times (p-1) \equiv -1(mod\ p)$ ، أي أنّ $1 \times 2 \times 3 \times \dots\dots \times (p-3)(p-2)(p-1) \equiv -1(mod\ p)$.
مبرهنة (عكس مبرهنة ويلسن)
إذا كان n عدداً صحيحاً موجباً ، بحيث $(n-1)! \equiv -1(mod\ n)$ ، فإنّ n عدد أولي .
البرهان: لنفرض جدلاً أنّ n عدد مؤلّف ،وبالتالي n = a b وحيث 1 < a , b <n ، بما أنّ a < n فإنّ (1) ... $a|(n-1)!$ ،

وبما أنّ $(n-1)! \equiv -1(mod\ n)$ ، فإن $n|(n-1)!+1$ ، ولدينا $a|n$ ، فإنه من خاصة التّعدي للقسمة ينتج أن (2) ... $a|(n-1)!+1$ ، من (1)و (2) نجد أنّ a يقسم أي تركيب خطي للعددين $(n-1)!+1$, $(n-1)!$ أي أن : $a|(n-1)!+1-(n-1)!=1 \Rightarrow a|1$ وهذا مستحيل ، أن a>1 ، (قواسم الواحد هي فقط ± 1)، إذاً الفرض الجدلي بأنّ n عدد مؤلّف غير صحيح ، ومنه n عدد أوّلي .

مبرهنة (برهانها تطبيق جيد لمبرهنتي ويلسن و اولر)

إذا كان P عدداً أوّليّاً فرديّاً ، فإنّه يتحقّق : يوجد حلّ للتطابق $p \equiv 1(mod\ 4) \Leftrightarrow x^2 \equiv -1(mod\ p)$

وعلاوة على ذلك إذا كان $p \equiv 1(mod\ 4)$ فإنّ $x = \left(\frac{p-1}{2}\right)!$ حلّ للتطابق .

البرهان:($\Longleftarrow$) نفرض أوّلاً أنّه يوجد حلّ x_0 للتطابق ، وبالتالي يتحقق $x_0^2 \equiv -1(mod\ p)$ ، فيكون $x_0^{p-1} = (x_0^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}(mod\ p)$.

بملاحظة أنّ $p \dagger x_0$ (لأنّ $x_0^2 \equiv -1(mod\ p)$) فإنّه باستخدام مبرهنة فيرما الصّغرى نجد $x_0^{p-1} \equiv 1(mod\ p)$ ، مما تقدّم نجد أنّ :

$(-1)^{\frac{p-1}{2}} \equiv 1(mod\ p) \Rightarrow p|1-(-1)^{\frac{p-1}{2}}$، ولكن العدد $1-(-1)^{\frac{p-1}{2}}$ إمّا أصغر أو يساوي 2 ، وبما أنّ العدد الأوّلي الفردي p لا يمكن أن يقسم 2 ، فإنّه من المحتّم أنّ $1-(-1)^{\frac{p-1}{2}} = 0$ ، وهذا يوجب أن يكون $\frac{p-1}{2}$ زوجيّاً ، أي أنّ $\frac{p-1}{2} = 2k$ ، وحيث k عدد صحيح ، ومنه p-1=4k وبالتالي $p \equiv 1(mod\ 4)$.

($\Longrightarrow$) لنفرض أن $p \equiv 1(mod\ 4)$ ، وبالتالي فإنّ p-1=4k ، وحيث k عدد صحيح ، إذاً $\frac{p-1}{2} = 2k$ زوجي . الآن لدينا :

$$(p-1)! = 1 \times 2 \times \dots\dots \times \frac{p-1}{2} \times \frac{p+1}{2} \dots\dots (p-2)(p-1)$$

$$\equiv 1 \times 2 \times \dots\dots \times \frac{p-1}{2}\left(-\frac{p-1}{2}\right)\dots.(-2)(-1)(mod\ p) \equiv (-1)^{\frac{p-1}{2}}\left(1 \times 2 \times \dots.\times \frac{p-1}{2}\right)^2 (mod\ p)$$

بما أنّ $\frac{p-1}{2}$ زوجي فإنّ $(-1)^{\frac{p-1}{2}} = 1$ $\Longleftarrow$ $(p-1)! \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 (mod\ p)$.

لكن باستخدام مبرهنة ويلسن، لدينا : $(p-1)! \equiv (-1)(mod\ p)$ ، ومن التطابقين الأخيرين ينتج أنّ $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1(mod\ p)$

أي أنّ $x = \left(\frac{p-1}{2}\right)!$ حلّاً للتطابق $x^2 \equiv -1(mod\ \ p)$.

مثال: بما أنّ $p = 17 \equiv 1(mod\ 4)$ ، فإنّ للتطابق $x^2 \equiv -1(mod\ 17)$ حلاً (حلول) ، وأحد هذه الحلول كما وجدنا في المبرهنة السّابقة .

$x = \left(\frac{p-1}{2}\right)! = 8!$، وبما أنّ $8! \equiv 13(mod\ 17)$ فإنّ $x = 13$ يكون حلّاً . كذلك $x = -13 \equiv 4(mod\ 17)$ يكون حلّاً آخر .

مثال: أوجد (إن أمكن) حلّاً للتطابق $x^2 \equiv -1(mod\ 11)$.

الحلّ: نعلم أنّه يكون للتطابق $x^2 \equiv -1(mod\ p)$ حلاً (وحيث p عدد أوّلي) $\Leftrightarrow p \equiv 1(mod\ 4)$. من أجل p=11 ، نلاحظ أنّ $11 \not\equiv 1(mod\ 4)$ ، إذاً ليس للتطابق المفروض حلّاً.

نتيجة: يوجد عدد غير منته من الأعداد الأوّليّة على الصّورة 4n+1 ، وحيث n عدد صحيح موجب .

البرهان: نفرض جدلاً أنّ عدد الأعداد الأوّليّة التي على الصّورة 4n+1 منته ، ولتكن هذه الأعداد $p_1 < p_2 < \dots < p_k$ ، ولنفرض أنّ العدد N معطى بالمساواة $N = (2p_1p_2 \dots p_k)^2 + 1$ ، بما أنّ N>1 فردي ، إذن يوجد قاسم أوّلي P>2 للعدد N (أي أنّ P|N) أي أنّ $N \equiv 0(mod\ p)$ ، ومنه $(2p_1p_2 \dots p_k)^2 \equiv -1(mod\ P)$وبالتالي فإنّ $x = 2p_1p_2 \dots p_k$ حلّا للمعادلة $x^2 \equiv -1(mod\ p)$ ، وحسب المبرهنة الأخيرة فإنّ ذلك يكافئ أنّ $p \equiv 1(mod\ 4)$ أيّ أنّ $p = 4n+1$ وبما أنّ $p_1, p_2, \dots., p_n$ هي جميع الأعداد الأوّليّة التي تكتب بالشّكل $4n+1$ فإنّ p يجب أن يكون مساوٍ لأحدها وليكن p_i ، حيث $1 \leq i \leq k$ ، وبما أنّ p | N ، وكذلك $P = p_i|(2p_1p_2 \dots p_k)^2$ ، فإنّ P يقسم أي تركيب خطّي لهما ، وينتج أنّ P|1 وهذا مستحيل ، إذاً الفرض الجدلي بوجود عدد منته من الأعداد الأوّليّة على الصّورة 4n+1 غير صحيح ، إذاً يوجد عدد غير منته من تلك الأعداد الأوّليّة.

تمارين(على التطابقات الخاصّة)

1) إذا كان n عدداً أوّليّاً يحقّق $n|2^n+1$ فأثبت أنّ n=3.

2) هل صحيح أنّ $(n-1)! \equiv 0(mod\ n)$ لأيّ عدد مؤلّف n ؟

3) إذا كان p , q عددين أوّليّن مختلفين بحيث $a^q \equiv a(mod\ p)$ و $a^p \equiv a(mod\ q)$ فأثبت أنّ $a^{p.q} \equiv a(mod\ pq)$.

4) إذا كان p , q عددين أوّليّين مختلفين وكان a عدداً صحيحاً فأثبت أنّ:

(a) $a^{p+q} - a^{p+1} - a^{q+1} + a^2 \equiv 0(mod\ pq)$.

(b) $a^{pq} - a^p - a^q + a \equiv 0(mod\ pq)$.

5) إذا كان P عدداً أوّليّاً فأثبت أنّ :

(a) $(m+n)^p \equiv m^p + n^p(mod\ p)$.

(b) $(m+1)^p \equiv (m+1)(mod\ p) \Leftrightarrow m^p \equiv m(mod\ p)$.

(c)لكل $m \geq 1$ أثبت $m^p \equiv m(mod\ p)$

- التطابقات الخطيّة (linear congruence):

تعريف: كلّ تطابق من الشّكل (1)... $ax \equiv b(mod\ n)$ ، يسمّى تطابقا خطيّا بالمجهول x ، وحيث a ,b أعداداً صحيحة . إن دراسة حلّ (حلول) للتطابق يعني البحث عن الأعداد الصّحيحة x (غير المتطابقة قياس n ، وبالتالي عن صفوف تطابق قياس n) التي تحقّق التطابق (1) . وهنا نقدّم ملاحظتين :

ملاحظة(1) إذا كان x_0 حلّاً للتطابق (1) (أي $ax_0 \equiv b(mod\ n)$) ، وكان $x_1 \equiv x_0(mod\ n)$ ، فإنّ $ax_1 \equiv ax_0 \equiv b(mod\ n)$ أي أنّ x_1 يكون أيضاً حلّا للتطابق (1) . من هنا ينتج أنّه إذا كان العدد x_0 حلّاً للتطابق (1)، فإنّ جميع عناصر صفّ التطابق $[x_0]$ ،تكون حلّاً لذلك التطابق ، وبالتالي من الطبيعي البحث عن صفوف التطابق المختلفة (من بين n صفّ) والتي كلّ منها يكون حلّاً للتطابق (1) ، وهذا مضمون المبرهنة الآتية :

(2) من تعريف التطابق يمكن كتابة التكافؤ : $ax \equiv b(mod\ n) \Leftrightarrow ax + ny = b$ ... (2) ... (1) ونلاحظ مايلي :

يوجد عدد صحيح x يحقّق التطابق (1) ⇔ يوجد عددان صحيحان x , y بحيث تتحقّق المعادلة الديوفنتيّة (2) ، وبالتالي البحث عن حلول التطابق (1) يكافئ البحث عن حلول المعادلة الديوفنتيّة (2) المعروف سابقاً ، ويكون ذلك بمثابة طريقة لحلّ التطابق (1) عند وجوده . علماً بأنّه يوجد طريقتان إضافيتان لإيجاد حلّ ، الأولى بالتّعويض عن x ، بعناصر أحد أنظمة الرواسب التامّة قياس n (مثل $\mathbb{Z}_n$) . والثانية باستخدام خواصّ التطابقات ، وهنا يجب الحذر واستخدام خواصّ التكافؤ (⇔) ، وليس خواصّ الاقتضاء (⇒) فقط .

مبرهنة: (a) يكون للتطابق (1).. $ax \equiv b(mod\ n)$ حلّاً ⇔ (a , n)| b .

(b) وإذا كان (a , n)|b ، وكان x_0 حلّاً للتطابق (1) ، فإنّه يوجد بالضّبط d=(a , n) حلّاً غير متطابق قياس n ، وهي:

$x = x_0 + \frac{n}{(a,n)}k \ ; 0 \le k \le d-1$.

البرهان: نعلم أنّ: (2)...$ax \equiv b(md\ n)$...(1)$\Leftrightarrow ax + ny = b$

ونعلم من مبرهنة سابقة أنّ للمعادلة الديوفنتيّة (2) حلّ ⇔ (a , n) | b ، وبالتالي يتحقّق : للتطابق (1) حلّ ⇔ (a , n) | b .

(b) ونعلم من مبرهنة سابقة ، أنّه إذا كان x_0, y_0 حلّاً للمعادلة الديوفنتيّة $ax + ny = b$ فإنّ جميع الحلول هي:

$x = x_0 + \frac{n}{d}k \ \ , \ \ y = y_0 - \frac{a}{d} \ \ \forall \ \ k \in \mathbb{Z}$.

لنأخذ قيم x التي توافق قيم k التالية k = 0 , 1 , 2 ,..., d-1 ، فنجد : $x_0 \ , x_0 + \frac{n}{d} \ , \ x_0 + \frac{2n}{d} \ , \ \dots \ , \ x_0 + \frac{(d-1)n}{d}$ ، ولنبرهن على :

أوّلاً: إنّ جميع هذه الأعداد غير متطابقة قياس n .

وثانياً: أي حلّ آخر(حتماً يوافق قيمة أخرى لـ k غير (0,1,2,....,d-1)) ، يجب أن يتطابق مع أحد هذه الأعداد قياس n .

1) لنفرض جدلاً أنّ $x_0 + \frac{n}{d}k_1 \equiv x_0 + \frac{n}{d}k_2(mod\ n) \Leftrightarrow \ 0 \le k_2 < k_1$ ، وحيث $\Leftrightarrow \frac{n}{d}k_1 \equiv \frac{n}{d}k_2(mod\ n)$

$k_1 \equiv k_2 \left(mod\ \frac{n}{(n,n/d)}\right) \equiv k_2 \left(mod\ \frac{n}{n/d}\right) \Leftrightarrow k_1 \equiv k_2(mod\ d) \Leftrightarrow d|\ (k_1 - k_2)$. والتكافؤ الأخير مستحيل لأن $0 < \ k_1 - k_2 < d$.

ثانياً: لنفرض الآن أنّ ، $x_0 + \frac{n}{d}k$ ، حلّاً للتطابق (1) . بتطبيق خوارزميّة القسمة على *k, d* ، نستطيع كتابة k على الصّورة :

$k = qd + r \ ; \ 0 \le r \le d-1$. ومنه نجد أن :

$x_0 + \frac{n}{d}k = x_0 + \frac{n}{d}(qd + r) = x_0 + nq + \frac{n}{d}r \equiv \left(x_0 + \frac{n}{d}r\right)(mod\ n); 0 \le r \le d-1 \Longrightarrow$ المطلوب .

نتيجة: إذا كان 1=(a,n) ، فإنّ للتطابق الخطيّ $ax \equiv b(mod\ n)$ حلّاً وحيداً قياس n (كفصل تطابق قياس n) .

مثال(1): أوجد (إن أمكن) جميع الحلول غير المتطابقة (قياس 29 للتطابق) $6x \equiv 15(mod 29)$ نلاحظ أنّ 15|1=(6,29)وبالتالي يوجد حلّ وحيد للتطابق المعطى قياس 29 . نحصل عليه(كما ذكرنا في الملاحظة (1) ؛ إمّا بكتابة المعادلة الديوفنتيّة الخطيّة المكافئة ، واستخدام خوارزميّة إقليدس لإيجاد أحد الحلول [أو]بالتجريب ، وذلك بالتعويض عنx بعناصر أحد أنظمة الرّواسب التامّة قياس 29(مثلاً {0,1,2,.....28}) [أو] باستخدام خواصّ التطابقات (وهنا يجب الحذر واستخدام التكافؤات فقط) فمثلاً لدينا : $6x \equiv 15(mod\ 29) \Leftrightarrow 30x \equiv 75(mod\ 29) \Leftrightarrow x \equiv 17(mod\ 29)$

طريقة ثانية: بالتجريب (الاستبدال عن x بـ (0,1,2,..,28)فيجب أن يحقّق بعضها هذا التطابق إن كان لها حل .

طريقة ثالثة:حلّ المعادلة الديوفنتيّة الخطيّة الموافقة : $6x + 29y = 15 \ \Leftrightarrow \ 6x \equiv 15(mod\ 29)$.

تمرين :(a)أوجد (إن أمكن) نظيراً ضربيّاً للعدد 12 قياس 28 ، ثمّ استنتج إذا كان للتطابق $12x \equiv 1(mod\ 28)$ حلّاً أم لا .

(b) أوجد (إن أمكن) حلّاً للمعادلة الديوفنتيّة $12x + 28y = 4$.

(c) أوجد (إن أمكن) جميع الحلول غير المتطابقة قياس 28 للتطابق الخطّي $12x \equiv 4(mod\ 28)$.

مثال(2): أوجد (إن أمكن) جميع حلول التطابق$14x + 18y = 10 \Leftrightarrow 14x \equiv 10\ (mod 18)$

نلاحظ أنّ 10|2=(14,18) وبالتالي يوجد للتطابق حلّين غير متطابقين قياس 18 . أحدهما $x_0 = 2$ (بالتجريب أو بالطّريقة المعروفة من خوارزميّة إقليدس) ، حصلنا عليه من الحلّ $y_0 = -15$, $x_0 = 20$ للمعادلة الديوفنتيّة $56x + 72y = 40 \xrightarrow{\div 4} 14x + 18y = 10$.

والحل الآخر يكون ، حسب المبرهنة الأخيرة ، $x = x_0 + \frac{n}{d}k \; ; 0 \le k \le d-1 \Rightarrow x = x_0 + \frac{18}{2}k = x_0 + 9k [(\equiv x_0 (mod\ 9)]$

$$(k = 0) \Rightarrow x_0 = 2 \;\wedge\; (k = 1) \Rightarrow x_1 = 2 + 9(1) = 11 \Rightarrow x_0 = 2 \wedge x_1 = 11$$

مثال (3): أوجد (إن أمكن) جميع الحلول غير المتطابقة قياس 15 للتطابق $27x \equiv 3(mod\ 15)$.

بما أنّ 3|3=(27,15) فإنّ للمعادلة المعطاة ثلاثة حلول غير متطابقة قياس 15 حسب النّظريّة الأساسيّة وهذه الحلول تعطى بدلالة حلّ x_0 كما يلي :

$$x = x_0 + \frac{n}{(a,n)}k \; ; 0 \le k \le d-1 \text{ (أي } 0 \le k \le 2)$$

لنوجد أوّلاً حلّاً x_0 (بالتّجريب مثلاً) ، نلاحظ أوّلاً أنّه بوضع $x_0 = -1$ ، نجد $-27 \equiv 3(mod\ 15)$ ، وبالتّالي تكون بقيّة الحلول غير المتطابقة قياس15هي:

$x_2 = 9$, $x_1 = 4$, $x_1 = x_0 + \frac{15}{3} = -1 + 5 = 4$ ، $x_2 = x_1 + \frac{2(15)}{3} = -1 + 10 = 9 x_0 = -1 \Rightarrow x_0 = -1$

إذاً صفوف التطابق المختلفة قياس 15والتي كلّ منها يمثّل حلاً هي : {[9],[4],[-1]} وهي نفسها{[9],[4],[14]} .

أنظمة التطابقات الخطيّة:

مثال(تمهيدي): لنرى إذا كان يوجد عدد صحيح x يحقّق كلّاً من التطابقين $(1)\begin{cases} x \equiv 2(mod\ 4) \\ x \equiv 4(mod 5) \end{cases}$

الحلّ: من التطابق الأوّل نجد أن $x \equiv 2\ (mod\ 4)$ ، نستطيع كتابة : $x = 2 + 4k \; ; k \in \mathbb{Z}$ .... (2) ، بالتّعويض في التطابق الثاني نجد :

$$2 + 4k \equiv 4(mod\ 5)$$

$$\Leftrightarrow 4k \equiv 2(mod\ 5) \xleftrightarrow{-5k \equiv 0} -k \equiv 2(mod\ 5) \Leftrightarrow k \equiv -2 \equiv 3(mod 5) \Leftrightarrow k = 3 + 5m \; ; m \in \mathbb{Z} \ldots (3)$$

بتعويض (3) في (2) نجد أنّ : $x = 2 + 4(3 + 5m) = 14 + 20m \Leftrightarrow x \equiv 14(mod\ 20)$ ،ونلاحظ أنّ x=14 تحقّق التطابقين معاً ، و بالعكس . أي أنّه لدينا التكافؤ : $x \equiv 4(mod\ 5) \;\wedge\; x \equiv 2(mod\ 4) \Leftrightarrow x \equiv 14(mod\ 20)$.

من الضروري في دراسة أنظمة التطابقات (كما هو الحال في أنظمة المعادلات) المعرفة المسبقة لوجود ، أو عدم وجود ، حلّ لهذا النّظام ، وفي حالة الوجود ، تقديم طريقة (أو خوارزميّة) لحساب هذا الحلّ (الحلول) وهو موضوع البند التالي .

تمهيدية: (تكافؤ بين نظامين أحدهما من الشّكل $a_i x \equiv c_i (mod\ m_i)$ والآخر من الشّكل $x \equiv x_i (mod \frac{m_i}{(a_i, m_i)})$)

ليكن لدينا نظام التطابقات الخطيّة التالي : (1)

$$\left.\begin{array}{l} a_1 x \equiv c_1 (mod\ m_1) \\ a_2 x \equiv c_2 (mod\ m_2) \\ \ldots\ \ldots\ \ldots \\ a_k x \equiv c_k (mod\ m_k) \end{array}\right\}$$

وليكن $d_i = (a_i, m_i)$ لكلّ 1≤i≤k ، وليكن x_i حلّاً للتطابق $a_i x \equiv c_i (mod\ m_i)$ لكلّ 1≤i≤k . عندئذٍ يتحقّق :

x حلّا للنظام (1) $\Leftrightarrow$ x حلّا للنظام (2)

$$\left.\begin{array}{l} x \equiv x_1 \left(mod\ \frac{m_1}{(a_1, m_1)}\right) \\ x \equiv x_2 \left(mod\ \frac{m_2}{(a_2, m_2)}\right) \\ \ldots\ \ldots\ \ldots \\ x \equiv x_k \left(mod\ \frac{m_k}{(a_k, m_k)}\right) \end{array}\right\}$$

مثال: ليكن نظام التطابقين $(1)\begin{cases} 6x \equiv 4(mod\ 8) \\ 3x \equiv 2(mod\ 5) \end{cases}$ إنّ للتطابق الأوّل حلّ $x_1 \equiv 2(mod\ 4)$ إنّ للتطابق الثّاني حلّ $x_2 \equiv 4(mod\ 5)$ ، وحسب التمهيديّة السابقة يتحقّق :

xحلّاً للنّظام $(1)\begin{cases} 6x \equiv 4(mod\ 8) \\ 3x \equiv 2(mod\ 5) \end{cases} \Leftrightarrow x$ حلاً للنّظام $(2)\begin{cases} x \equiv 2(mod\ 4) \\ x \equiv 4(mod\ 5) \end{cases}$

وبما أنّنا وجدنا أنّ $x \equiv 14(mod\ 20)$ حلّاً للنظام (2) ، فإنّه يكون حلّا للنّظام (1) ، لنتحقّق من ذلك :

$$x \equiv 14(mod\ 20) \Rightarrow x = 14 + 20k \xrightarrow{\text{بالتعويض الطرف الأيسر من(1)}} \begin{cases} 6(14 + 20k) = 84 + 120k \equiv 4(mod\ 8) \\ 3(14 + 20k) = 42 + 60k \equiv 2(mod\ 5) \end{cases}$$

ملاحظة: إنّ التكافؤ الذي تقدّم التمهيديّة السابقة يجعلنا نركّز اهتماماتنا على الأنظمة الخطيّة التي فيها معاملات x تساوي 1 .
المبرهنة التالية تقدّم لنا شرطاً كافيا لوجود حلّ لبعض **الأنظمة** .

مبرهنة: (الباقي الصّينيّة the Chinese remainder theorem)

إذا كانت الأعداد $m_1, m_2, \dots, m_k$ أوّليّة نسبيّاً مثنى مثنى ، فإنّه يوجد للنّظام : $\left.\begin{matrix} x \equiv c_1 (mod\ m_1) \\ x \equiv c_2 (mod\ m_2) \\ \dots\dots\dots \\ x \equiv c_k (mod\ m_k) \end{matrix}\right\}$ (1)

حلّ وحيد x_0 قياس العدد $M = m_1 . m_2 \dots m_k$ ، يعطى بالمساواة : $x_0 = c_1 M_1 y_1 + c_2 M_2 y_2 + \cdots + c_k M_k y_k$ ، وحيث $M_r = \frac{M}{m_r}$ و y_r هو نظير ضربي للعدد M_r قياس m_r .

البرهان: لإيجاد حلّ للنّظام نفرض أنّ $r = 1,2, \dots . k \quad ; M_r = \frac{M}{m_r} = m_1 . m_2 \dots . m_{r-1} . m_{r+1} \dots m_k$ ، بما أنّ $(m_r, m_s) = 1$ عندما $r \neq s$ ، فإنّه بالاعتماد على تمرين($(a_1, b) = (a_2, b) = \cdots = (a_n, b) = 1 \Rightarrow (a_1 . a_2 \dots . a_n, b) = 1$) نجد أنّ $(m_r, m_1 m_2 \dots m_{r-1} . m_{r+1} . . m_k) = 1$ أي أنّ $(m_r, M_r) = 1$ ، وبالتالي للعدد M_r نظير ضربي قياس m_r وليكن y_r (أي أنّ $M_r y_r \equiv 1 (mod\ m_r)$) ، لنبرهن الآن على أنّ $x_0 = c_1 M_1 y_1 + c_2 M_2 y_2 + \cdots + c_k M_k y_k$ حلّاً للنظام المفروض . وهذا يتمّ بإثبات أنّ $x_0 \equiv c_r (mod m_r)$ لكلّ 1≤r≤k ، بما أنّ $m_r | M_s$ عندما $r \neq s$ ، فإنّ $M_s \equiv 0 (mod m_r)$ لكلّ $r \neq s$ ومنه :

$$x_0 = c_1 M_1 y_1 + c_2 M_2 y_2 + \cdots + c_k M_k y_k \equiv c_r M_r y_r (mod m_r)$$

وقد وجدنا أنّ $M_r y_r \equiv 1 (mod m_r)$ ، ومنه نجد أنّ $\forall\ 1 \leq r \leq k \quad x_0 \equiv c_r (mod m_r)$. لبرهان الوحدانيّة ، نفرض أنّ x_0, x_1 حلّان للنّظام (1) (ولنبرهن على أنّهما متطابقان قياس $M = m_1 \dots m_k$) من تعريف الحلّ نجد أنّ $x_0 \equiv x_1 \equiv c_r (mod m_r)$ لكلّ 1≤r≤k ومنه :
$\forall\ 1 \leq r \leq k \quad m_r | (x_0 - x_1)$ ، وباستخدام نتيجة سابقة ، نجد $M = m_1 . m_2 . . m_k = [m_1 . m_2 . . m_k] | (x_0 - x_1)$. أي أنّ :
$x_0 = x_1 (mod M)$.

مثال: أوجد أصغر عدد موجب x بحيث إذا قسّم على 3 بقي 1 ، وإذا قسّم على 4 بقي 2 ، وإذا قسّم على 5 بقي 3 .

إنّ العدد المطلوب x يجب ان يحقق $\begin{cases} (1) \dots x \equiv 1 (mod\ 3) \\ (2) \dots . x \equiv 2 (mod\ 4) \\ (3) \dots x \equiv 3 (mod\ 5) \end{cases}$

إنّ الأعداد 3,4,5 أوّليّة نسبيّاً مثنى مثنى لأنّ 1=(4,5)=(3,5)=(3,4) وبالتالي حسب مبرهنة الباقي الصينية يوجد للنّظام السابق حلّ وحيد x_0 قياس العدد $M = m_1 . m_2 . m_3 = 3 \times 4 \times 5 = 60$ ، وهذا الحلّ يعطى بالمساواة : $x_0 = c_1 M_1 y_1 + c_2 M_2 y_2 + c_3 M_3 y_3$ وحيث (r=1,2,3) $M_r = \frac{M}{m_r}$ ، وحيث y_r هو نّظير ضّربي لـ M_r قياس m_r ، أي أنّ y_r هو حلّ للتطابق $y_r M_r \equiv 1 (mod\ m_r)$ ، $1 \leq r \leq k = 3$ ونلاحظ أنّه من كون $M = m_1 \times m_2 \times m_3 = 3 \times 4 \times 5 = 60$ فإنّ

$$M_1 = \frac{M}{m_1} = \frac{60}{3} = 20 \Longrightarrow 20\ y_1 \equiv 1 (mod\ 3) \Longrightarrow y_1 \equiv 2 (mod\ 3) \Longrightarrow y_1 = 2$$

$$M_2 = \frac{M}{m_2} = \frac{60}{4} = 15 \Longrightarrow 15\ y_2 \equiv 1 (mod\ 4) \Longrightarrow y_2 \equiv 3 (mod\ 4) \Longrightarrow y_2 = 3$$

$$M_3 = \frac{M}{m_3} = \frac{60}{5} = 12 \Longrightarrow 12\ y_3 \equiv 1 (mod\ 5) \Longrightarrow y_3 \equiv 3 (mod\ 5) \Longrightarrow y_3 = 3$$

وبالتالي الحلّ هو :

$$x_0 = c_1 M_1 y_1 + c_2 M_2 y_2 + c_3 M_3 y_3 = 1(20)(2) + 2(15)(3) + 3(12)(3)$$
$$= 40 + 90 + 108 = 238 \equiv 58 (\text{mod } 60) \Longrightarrow x_0 \equiv 58 (mod\ 60)$$

تمرين: أوجد (إن أمكن) حلّاً للنّظام : $\left.\begin{matrix} x \equiv 3 (mod\ 28) \\ x \equiv 4 (mod\ 5) \end{matrix}\right\}$

– الفهرس –

انتهى المقرّر بعونه تعالى

هذا المقرّر من أوراق الدكتور حيث يبدأ بالفصل الثاني وينتهي بالرّابع ، تمّ تفريغها في هذا الشّكل وقام الدكتور بتدقيق الفصل الرّابع والجزء الأوّل من الفصل الثّالث في حين لم تسنح الظّروف لإتمام التدقيق(لكنّها على أيّة حال من أوراقه)

نتمنّى لكم التوفيق دائماً

2013–12–24

قام بإعداده يمان سوّاس

بمساعدة الزّميلات : نوره عطار–قمر بوشي–فاطمة الزّهراء أدنى