جامعة دمشق

كلية العلوم

المرجع كتاب نظرية الاعداد – الدكتورة دعد الحسيني و الدكتور محمد بشير قابيل

محاضرات نظرية الأعداد
2020

محاضرات د. يحيى

الفهرس

مقدمة .....

تمهيد .....

الباب الأول

الفصل الأول قابلية القسمة في Z وتطبيقاتها .....

– قابلية القسمة في Z وتطبيقاتها .....

– خواص قابلية القسمة .....

– مبرهنة اقليدس .....

الفصل الثاني القواسم المشتركة والمضاعفات المشتركة .....

– القاسم المشترك الأعظم .....

– خواص القاسم المشترك الأعظم.....

– خوارزمية اقليدس .....

– القاسم المشترك الأعظم لمجموعة أعداد صحيحة.....

– المضاعف المشترك الأصغر.....

– تمارين .....

الفصل الثالث الأعداد الأولية

– بعض خواص الأعداد الأولية .....

– المبرهنة الأساسية في الحساب .....

– مبرهنة الأعداد الأولية.....

– التحليل إلى عوامل بطريقة فيرما.....

الفصل الرابع معادلات ديوفانتس

– معادلات ديوفانتس الخطية بمجهولين.....

– ثلاثيات فيثاغورث..... .....

– تمارين .....

الباب الثاني

الفصل الأول التطابيقات .....

– تعريف التطابق .....

– صفوف البواقي .....

– مجموعة البواقي التامة .....

– خواص التطابقات .....

الفصل الثاني التطابقات الخطية .....

– تعريف التطابق الخطي .....
– الكسور البسيطة المستمرة المنتهية .....
– النظير الصفري .....
– حل جملة تطابقات خطية .....
– مبرهنة الباقي الصينية .....
– مبرهنة فيرما الصغرى .....
– مبرهنة ويلسون .....
– عكس مبرهنة ويلسون .....
– تمارين .....

الفصل الثالث الدوال العددية وبعض الدوال الخاصة .....
– تعريف الدوال العددية .....
– الدالة العددية الضربية .....
– دالة الجزء الصحيح .....
– مجموعة البواقي المختزلة .....
– دالة أولر .....
– مبرهنة أولر .....
– الدالتان $\sigma(n)\ ,\tau(n)$ .....
– الأعداد التامة أو الأعداد الكاملة .....
– دالة موبياس .....
– صيغة موبياس للتعاكس .....
– الدالة ليوفيل $\lambda(n)$ .....
– الدالة مانجولد $\wedge\ (n)$ .....
– تمارين .....

الفصل الرابع المراتب والجذور الأولية والأدلة .....
– تعريف المرتبة .....
– الجذور الأولية والأدلة .....
– تعريف الجذر الأولي .....
– تعريف الدليل .....
– خواص الأدلة .....
– حل التطابقات غير الخطية باستخدام الأدلة .....
– تمارين .....

محاضرات د. يحيى

تمهيد

مبدأ الاستقراء الرياضي :

لا بد قبل البدء بموضـوعات المقرر من عرض مبدأين هامين يكثر اسـتخدامهما في إثبات مبرهنات هذا المقرر, الأول هو مبدأ الترتيب الحســـن أو (الجيد) *Well − ordering Principle* و**الثاني** هو مبدأ الاستقراء الرياضي المنتهي *Mathematical Induction* Principle.

1 – مبدأ الترتيب الحسن :

إذا كانت A مجموعة جزئية غير خالية من مجموعة الأعداد الصـــحيحة الموجبة Z^+ فإنه يوجد في A عنصر أصغر أي يوجد $a_0 \in A$ بحيث : $a_0 \le a \quad \forall\, a \in A$ ، " وهذا العنصر الأصغر وحيد " .

2 – مبدأ الاستقراء الرياضي المنتهي :

وهو وسيلة سهلة لإثبات الكثير من المبرهنات الرياضية ، وخاصة في نظرية الأعداد ، ولنشرح هذا المبدأ بالتمرين الممهد الآتي:

تمرين مُمهِّد :

إذا أشرنا بالرمز S_n للقضية الرياضية :

$$S_n : \quad 1^3 + 2^3 + ... + n^3 = (1 + 2 + ... + n)^2 = (\frac{n\,(n+1)}{2})^2$$

فيمكن أن نتحقق بسهولة أن S_1 صحيحة ذلك أن

$$1^3 = (1)^2 = (\frac{1\times 2}{2})^2$$

مساواة صحيحة

كذلك يمكن أن نتوثق من أن S_2 صحيحة ذلك أن القول هل المساواة الآتية صحيحة

$$1^3 + 2^3 \stackrel{?}{=} (1+2)^2 \stackrel{?}{=} (\frac{2\times 3}{2})^2$$

أي هل صحيح أن $1+8 \stackrel{?}{=} 9 \stackrel{?}{=} 9$

والجواب نعم إذن تم المطلوب .

ويمكن أن نتحقق أن S_3 صـحيحة أيضـاً ، ولكن هل S_n صـحيحة أياً كانت n ؟. وإذا ظننا ذلك فكيف نثبت ذلك ، علماً بأننا لا نسـتطيع أن نقوم بعمل ما لا نهاية له من التحقيقات ؟ أليس ثمة مخرج ؟ ... بلى ثمة مخرج هو مبدأ الاستقراء الرياضي الذي ينطلق من الفكرة البسيطة الآتية:

نحن نعلم أنه إذا أمكن أن نقف على درجة من درجات سـلم متتالية وإذا كان بالإمكان بعد ذلك المرور من درجة إلى الدرجة التي تليها فعندئذ يمكن أن نصـــل إلى الدرجة الثالثة فالرابعة ... وبالتالي يمكن أن نتسلق السلم حتى نهايته بل لنقل لأية درجة شئنا.

يمكن أن ينص مبدأ الآستقراء الرياضـي أو كما يسمى أحياناً مبدأ البرهان بالتدريج أو بالاستقراء على ما يلي:

إذا أردت إثبات صـحة قضـية رياضـية S_n تتعلق بالمتغير الطبيعي n من أجل أي عدد $n \geq 1$ ما عليك إلا أن تقوم بالخطوتين التاليتين:

- تتوثق بدايةً من صحة القضية من أجل $n = 1$ (خطوة البداية أو الخطوة الأساسية) .
- ثم نفترض أنها (صحيحة من أجل $n = k$) و تبرهن بعد ذلك صحتها من أجل ($n = k + 1$)، (خطوة الاستقراء)

لنستخدم ذلك الآن لإثبات القضية S_n التي وردت في بداية هذه الفقرة:

الخطوة الأولى (الخطوة الأساسية) نتوثق من أنها صحيحة من أجل $n = 1$ وقد فعلنا ذلك.

الخطوة الثانية (خطوة الاستقراء) لنفترض **أن** S_k صحيحة ، أي لنفترض أن :

$$S_k : \quad (1^3 + 2^3 + ... + k^3) = (\frac{k\,(k+1)}{2})^2 \qquad *$$

مساواة صحيحة ولنبرهن أن

$$S_{k+1} : \quad (1^3 + 2^3 + ... + k^3) + (k+1)^3 = (\frac{(k+1)(k+2)}{2})^2$$

صحيحة مستفيدين من * ذلك أن الطرف الأيسر يساوي :

$$(1^3 + 2^3 + ... + k^3) + (k+1)^3 = (\frac{k\,(k+1)}{2})^2 + (k+1)^3 =$$

$$= (\frac{k\,(k+1)}{2})^2 + (k+1)^3 \overset{?}{=} \frac{((k+1)(k+2))^2}{4}$$

ويكفي للتحقق من ذلك أن تفك الأقواس وتصلح لتجد المراد أو أن تكتب هل :

$$k^2\,(k+1)^2 + 4(k+1)^3 \overset{?}{=} (k+1)^2\,(k+2)^2$$

أو هل : $k^2 + 4(k+1) \overset{?}{=} (k+2)^2$ اختصرنا على $(k+1)^2$

أو هل : $k^2 + 4\,k + 4 \overset{?}{=} k^2 + 4k + 4$

والجواب نعم وتم المطلوب .

ثلاث ملاحظات هامة

ملاحظة (1) :

هنالك صيغ أخرى لمبدأ الاستقراء السابق مكافئة له منها :

❖ تكون القضية S_n المتعلقة بالمتغير الطبيعي n صحيحة لأجل $n \geq n_0$ إذا استطعنا فعل ما يلي :

1) خطوة البداية : التوثق من أن S_{n_0} صحيحة (تعديل في خطوة البداية)

2) خطوة الإســـتقراء : إثبات أن (كون S_k صـــــحيحة من أجل $k \geq n_0$) و نبرهن بعدها أن S_{k+1} صحيحة.

مثال (1) : أثبت أن العبارة $S_n: 2^n \leq n!$ صحيحة لكل $n \geq 4$.

(لاحظ أنها صحيحة من أجل $n = 4$)

الحل : الخطوة الأولى : $s_4: 2^4 \overset{?}{\leq} 4!$ **(الرمز $\overset{?}{\leq}$ يقرأ هل هو أصغر أو يساوي)**

نجد أن $2^4 = 16 \leq 24$ محققة.

والجواب نعم والخطوة الأولى قد أنجزت . لننتقل إلى الخطوة الثانية.

خطوة الاستقراء : لنفترض أن المتراجحة $2^k \leq k!$ صحيحة من أجل $k \geq 4$.

والطلب إثبات أن : $2^{k+1} \leq (k+1)!$

نقول إن : $2^{k+1} = 2.2^k \leq (k!).2 \overset{?}{\leq} (k+1)!$

أي $2(k!) \overset{?}{\leq} (k+1)(k!)$

أو هل $2 \overset{?}{\leq} k+1$

علماً بأن $k \geq 4$ والجواب نعم وتم المطلوب .

ملاحظة (2) :

مبدأ الاسقراء الثاني و يبرهن أنه مكافئ للأول:

❖ لإثبات صـحة قضـية S_n من أجل جميع قيم n المحققة للشـرط $n \geq n_0$ حيث n_0 معلومة. مثلاً قد نحتاج إلى :

1) التوثق من أنها صحيحة من أجل $n = n_0$

2) افتراض صحتها من اجل جميع قيم $n = k$ المحققة للشرط $n_0 \leq k$

ثم إثبات صحتها من أجل $n = k + 1$.

مثال (2) : لتكن لدينا المتتالية العددية الصحيحة المعرفة كما يلي :

$a_0 = 1, a_1 = 2, a_2 = 3, a_n = a_{n-1} + a_{n-2} + a_{n-3} \quad , \forall n \geq 3$

والمطلوب إثبات أن $a_n \leq 3^n$ من أجل جميع القيم $n \in N$

الإثبات : الخطوة الأساسية : نلاحظ أن :

$a_3 = a_2 + a_1 + a_0 += 3 + 2 + 1 = 6 \leq 3^3 = 27$ محققة

كذلك $a_4 = a_3 + a_2 + a_1 = 6 + 3 + 2 = 11 \leq 3^4 = 81$ محققة

فالعلاقة صحيحة .

خطوة الاستقراء :

لنفترض أن $a_n \leq 3^3$ من أجل كل $k \geq n$ (حيث $k \geq n \geq 3$)

ولنبرهن صحتها من أجل $n = k + 1$

لدينا $a_{k+1} = a_k + a_{k-1} + a_{k-2}$

أي $a_{k+1} \le 3^k + 3^{k-1} + 3^{k-2} \le 3^k + 3^k + 3^k = 3.(3^k) = 3^{k+1}$

وتم المطلوب . أي أن العلاقة $a_n \le 3^n$ صحيحة مهما تكن $n \in N$.

مثال (3) أثبت أن

$\forall n \in Z^+$ S_n : $\sum_{i=1}^{n} i = 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$

الحل : الخطوة الأساسية : $s_1 = 1 = \frac{1(2)}{2} = 1$ والعلاقة صحيحة

خطوة الاستقراء : نفترض S_k صحيحة $k \ge 1$ ولنثبت أن S_{k+1} صحيحة

لذا نكتب : $\sum_{i=1}^{k+1} i = 1 + 2 + 3 + \ldots + k + (k+1) = s(k) + (k+1)$

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

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

$\sum_{i=1}^{k+1} i = 1 + 2 + 3 + \ldots + k + (k+1) = \frac{(k+1)(k+2)}{2}$

والعلاقة S_{k+1} صحيحة أي أن S_n محققة $\forall n \in Z^+$.

ملاحظة (3) :

إن إثبات خطوة الاستقراء فقط لا يكفي لإثبات صحة علاقة رياضية كما أن إثبات الخطوة الأساسية من أجل قيمة معينة n_0 لا يكفي لإثبات صحة علاقة رياضية $\forall\, n \ge n_0$.

مثال هادف (4) : أثبت أنه إذا كانت العبارة S_k : $\sum_{i=1}^{k} i = 1 + 2 + 3 + \ldots + k = \frac{(k^2+k+2)}{2}$ صحيحة فإن S_{k+1} صحيحة أي أن : $S_{k+1} = \frac{(k+1)^2+(k+1)+2}{2}$ صحيحة

وهل يمكن أن تستنتج أن S_n صحيحة $\forall n \in Z^+$ ؟ ؟.

الحل : لنكتب :

S_{k+1} : $\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{k^2+k+2}{2} + (k+1)$

$\sum_{i=1}^{k+1} i = \frac{k^2+k+2+2k+2}{2} = \frac{k^2+3k+4}{2}$

أي أنه من أجل $k \in Z^+$ فإن $S_k \Rightarrow S_{k+1}$

لنحسب الآن S_1 فنجد عندما $n = 1$

$\frac{(n^2+n+2)}{2} = \frac{1+1+2}{2} = 2$ و $\sum_{i=1}^{1} 1 = 1$

ولما كان $2 \ne 1$ فإن S_1 غير صحيحة

لنتساءل هل يمكن إيجاد قيمة ابتدائية n_0 بحيث أن s_{n_0} محققة فنثبت صحة S_n , $\forall n \ge n_0$ ؟

من أجل ذلك و بالاستفادة من **المثال (3)** نكتب

$$\sum_{i=1}^{n_0} i = \frac{n_0(n_0+1)}{2} = \frac{n_0^2+n_0+2}{2} \Rightarrow n_0^2+n_0 = n_0^2+n_0+2 \Rightarrow 0 = 2$$

وهذا غير صحيح مما يدل على أنه لا توجد أي قيمة n_0 ابتدائية تصح من أجلها العلاقة S_n .

مثال (3) : أثبت أن

$$S_n \forall n \in Z^+ : \ \sum_{i=1}^{n}(2i-1) = 1+3+5+\ldots+(2n-1) = n^2$$

الحل : الخطوة الأساسية : نلاحظ أن

$$S_1: 1 = 1 = 1^2$$
$$S_2: 1+3 = 4 = 2^2$$
$$S_3: 1+3+5 = 9 = 3^2$$

خطوة الاستقراء : لنفترض أن S_k محققة ولنثبت صحة S_{k+1}

لنكتب :

$$\sum_{i=1}^{k+1}(2i-1) = \sum_{i=1}^{k}(2i-1) + [2(k+1)-1]$$
$$= k^2 + [2(k+1)-1] = k^2+2k+1 = (k+1)^2$$

فالعلاقة S_{k+1} محققة .

أي : S_n محققة $\forall n \in Z^+$

محاضرات د. يحيى

تمارين

أولاً : لنفترض أن $9)\ \sum_n i^2 = 1^2 + 2^2 + \ldots\ldots + n^2$

حيث n عدد طبيعي احسب

(a $\sum_1, \sum_2, \sum_3, \sum_4$

b) برهن بالاستقراء أن $\sum_n i^2 = \frac{n(n+1)(2n+1)}{6}$

ثانياً: أثبت ما يلي بطريقة الاستقراء الرياضي :

1) $\mathbf{1^2 + 3^2 + \ldots\ldots + (2n-1)^2 = n(2n-1)(2n+1)/3}$

2) $\mathbf{1.3 + 2.4 + 3.5 + \ldots\ldots + n(n+2) = (n)(n+1)(2n+7)/6}$

3) $\mathbf{\sum_{i=1}^{n} \frac{1}{i(i+1)} = 1 - \frac{1}{n+1}}$

ثم استفد من ذلك في حساب مجموع السلسلة $\mathbf{\sum_{i=1}^{\infty} \frac{1}{n(n+1)}}$

4) $\mathbf{\sum_{i=1}^{n} 2^{i-1} = 2^n - 1}$

5) $\mathbf{\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}}$

6) $\mathbf{\sum_{i=1}^{n} (i)(i!) = (n+1)! - 1}$

7) $\mathbf{\sum_{k=1}^{n} (2k+1)^3 = n(2n^3 + 8n^2 + 11n + 6)}$

8) $\mathbf{\sum_{k=1}^{n} k(k+1)(k+2) = \frac{n(n+1)(n+2)(n+3)}{4}}$

الباب الأول

الفصل الأول

قابلية القسمة في Z وتطبيقاتها

1-1 تعريف قابلية القسمة :

نقول إن العدد الصحيح $a \neq 0$ يقسم العدد الصحيح b ونكتب $a|b$ إذا وجد عدد صحيح c يحقق المساواة $b = c\,a$. ونسمي a قاسماً لـ b و نسمي b مضاعفاً له أو نقول إن b يقبل القسمة على a .

وإذا كان a لا يقسم b نكتب $a \nmid b$ وعلى سبيل المثال نكتب : $3|15$ ، $5 \nmid 12$

1-2 خواص قابلية القسمة :

1) أن العدد 1 هو قاسم لأي عدد صحيح ، وأن الصفر هو مضاعف لأي عدد صحيح .

2) إذا كان $a|b$ فإن $-a|b$

3) $\forall a \neq 0\ ,\ a|a$ لأن $a = 1.a$

4) $\boldsymbol{a|c \Rightarrow a|kc} \quad ,\forall \boldsymbol{k \in Z}$

5) $a|c \wedge c|d \Rightarrow a|d$ لأن $c = ab_1 \wedge d = cb_2 \Rightarrow d = ab_1b_2 = a(b_1b_2)$

6) $\boldsymbol{a|c \wedge a|d \Rightarrow a|(mc + nd)\forall m,n \in Z}$

لأن $c = ab_1 \wedge d = ab_2 \Rightarrow mc + nd = mab_1 + nab_2 = a(mb_1 + nb_2)$

2- ملاحظة :

يمكن تعميم هذه الخاصة كما يلي : إذا كان $a|b_i\ ,\ (i = 1,2,\ldots,k)$

فإنّ $a|b_1x_1 + b_2x_2 + \ldots\ldots + b_kx_k$ حيث $x_i \in Z$

7) $\boldsymbol{a|c \wedge c \neq 0 \Rightarrow |a| \leq |c|}$ لأن : $c = ab \neq 0 \Rightarrow |c| = |a|.|b| \Rightarrow |c| \geq |a|$

8) $|a| = |c|$ لأن حسب الخاصة **(7)** $\boldsymbol{a|c \wedge c|a \Leftrightarrow |a| = |c|}$ $|a| \leq |c| \wedge |c| \leq |a| \Leftrightarrow |a| = |c|$

نتيجة:

إن مجموعة القواسم الموجبة لأي عدد صحيح $a \neq 0$ تحوي عدداً منتهياً من العناصر كلها $\geq |a|$

3-1 المبرهنة الأساسية في الحساب (مبرهنة اقليدس) :

إذا كان $a,b \in Z$ و $a \neq 0$ فإنه يوجد عددان صحيحان r,q وحيدان يحققان المساواة $b = aq + r$ حيث $0 \leq r < |a|$

الإثبات : لتكن مجموعة الأعداد الصحيحة التالية : $S = \{x \geq 0 : x = b - ta; t \in Z\}$

من الواضح أن هذه المجموعة غير خالية ومرتبة فحسب مبدأ الترتيب الحسن يوجد فيها عنصر أصغر نسميه r . ولتكن قيمة t الموافقة لهذا العنصر هي q وعندها يمكن أن نكتب :

$$r = b - qa \in S \Rightarrow r \geq 0$$

ولنثبت أن $r < |a|$

من أجل ذلك نفترض جدلاً أن $r \geq |a|$ أي $r - |a| \geq 0$

فإذا كانت a موجبة فإن $r - |a| = r - a = b - qa - a$

ومنه $r - |a| = b - a(q + 1) \in S$

لأن $x = r - |a| \geq 0$ وهو من الشكل $x = b - ta$

وإذا كانت a سالبة فإن : $r - |a| = r + a = b - qa + a = b - a(q - 1) \in S$

ولكن $r - |a|$ عدد أصغر من r وينتمي إلى S وهذا تناقض لأن r هو العنصر الأصغر في S أي أن الافتراض الجدلي خاطىء و $r < |a|$.

لنثبت الآن أن العددين r, q وحيدان .

من أجل ذلك نفترض جدلاً أن r_1, q_1 عددان مختلفان عن q, r ويحققان العلاقة

$$b = q_1 a + r_1 \quad , 0 \leq r_1 \leq |a|$$

ولدينا $b = qa + r \quad , 0 \leq r \leq |a|$

أي أن $q_1 a + r_1 = qa + r \Rightarrow (q - q_1)a = r_1 - r$

ومنه فإن العدد $r_1 - r$ مضاعف لـ a ولكن قيمته العددية أصغر من $|a|$ وهذا لا يصح إلا إذا كان $r_1 - r = 0$ و $r_1 = r$ وبالتالي فإن $q_1 = q$ وهو المطلوب .

أمثلة :

من أجل $a=7, b=2$ نجد $2=7(0)+2$

" $a=3, b=23$ نجد $23=3(7)+2$

" $a=-3, b=7$ نجد $7=(-3)(-2)+1$

" $a=79, b=-3$ نجد $-3=(79)(-1)+76$

" $a=-6, b=0$ نجد $0=(-6)(0)+0$

من أجل $a=-7, b=-2$ نجد $-2=-7(1)+5$

" $a=-7, b=1$ نجد $1=(-7)0+1$

" $a=-7, b=56$ نجد $56=(-7)(-8)+0$

4-1 تطبيق هام :

إن مربع أي عدد فردي يزيد بالعدد 1 عن مضـــاعف للعدد 8 أي إذا كان b عدداً صـــحيحاً فردياً فإن $b^2=8M+1$.

الإثبات : إن باقي قســـمة أي عدد فردي على العدد 2 يســـاوي الواحد لذا يمكن دوماً كتابة العلاقة $b=2q+1$ وبتربيع الطرفين نجد : $b^2=4q^2+4q+1$

ومنه $b^2=4q(q+1)+1$

ولما كان q و $q+1$ عددان متتاليان فإن أحدهما زوجي والآخر فردي فجداءهما عدد زوجي ومنه $b^2=8M+1$.

تمرين (1) : أثبت أن $6|f(m)=5m^3+7m$ حيث $m\in N$

الحل : نكتب $f(m)=m(5m^2+7)$ ولنثبت أن $6|f(m)$ **بطريقة الاستقراء**

الخطوة الأساسية :

$f(0)=0 \rightarrow 6|0$ والعلاقة صحيحة ، وكذلك $f(1)=12 \rightarrow 6|12$ والعلاقة صحيحة .

خطوة الاستقراء : لنفترض صحة العلاقة من أجل $m=k>1$ ولنثبت صحتها من أجل $m=k+1$

لذا نكتب : $f(k)=5k^3+7k, f(k+1)=5(k+1)^3+7(k+1)$

ولنحسب $f(k+1)-f(k)=15k(k+1)+12$

نلاحظ أن $6|12$ وأن $15=3(5)$ و $k(k+1)$ عدد زوجي لأن أحد العددين المتتاليين عدد زوجي أي $k(k+1)=2n$ ومنه

$$15k(k+1)=3(5)(2)n=6(5)n \Rightarrow 6|15k(k+1)$$

وحسب الخاصة **(6)** فإن 6 تقسم المجموع $15k(k+1)+12$

أي أن $6|[f(k+1)-f(k)]$ وحسب الفرض $6|f(k)$ و منه نجد

$6|f(k+1)$ وخطوة الاستقراء صحيحة أي أن $6|f(m)$ مهما تكن $m\geq 0$.

تمرين (2) : أثبت أن $14|5^{2n+1}+3^{4n+2}$ حيث $n \geq 0$

نسمي $f(n)=5^{2n+1}+3^{4n+2}$ ولنثبت صحة العلاقة $14|f(n)$ $n \geq 0$

بطريقة الاستقراء :

1- الخطوة الأساسية : نلاحظ أن $14|14$, $f(0)=14$ والعلاقة صحيحة.

2- خطوة الاستقراء : إذا كانت $k>0$ لنثبت أن $f(k) \Rightarrow f(k+1)$

لذا نحسب المقدار :

$$f(k+1)-11f(k)=5^{2k+3}+3^{4k+6}-11(5^{2k+1}+3^{4k+2})$$

نصلح العلاقة الأخيرة فنجد :

$$f(k+1)-11f(k)=5^{2k}[125-11\times 5]+3^{4k}(3^6-11\times 9)$$

$$=5^{2k}.5(25-11)+3^{4k+2}(3^4-11)\ ,3^4-11=70=5\times 14$$

$$f(k+1)-11f(k)=14[5^{2k+1}+(5)3^{4k+2}] \Rightarrow 14|[f(k+1)-11f(k)]$$

ولما كانت $14|f(k)$ $\Leftarrow$ $14|11f(k)$

ينتج أن $14|f(k+1)$ وخطوة الاستقراء صحيحة أي أن : $14|f(n)$ عندما $n \geq 0$.

محاضرات د. يحيى

الفصل الثاني
القواسم المشتركة والمضاعفات المشتركة

2-1 القواسم المشتركة

1-2-1 تعريف : نقول إن العدد الصحيح d_1 هو قاسم مشترك للعددين الصحيحين a , b غير الصفريين معاً إذا تحقق ما يلي : $d_1|a \wedge d_1|b$

مثلاً :$3|30$, $3|12$

1-2-2 ملاحظات :

1) يلاحظ أنه إذا كان d_1 قاسماً مشتركاً لـ a , b فإن $(-d_1)$ يكون قاسماً مشتركاً لهما أيضاً

2) نعلم من خواص قابلية القسمة أن $|d_1| \leq |a|, |d_1| \leq |b|$ فإذا كان $a.b \neq 0$

فإن $|d_1|$ لا يتجاوز العدد الأصغر بين العددين $|a|$ و $|b|$

3) إن مجموعة القواسم المشتركة الموجبة لعددين صحيحين غير صفريين a , b هي تقاطع مجموعة القواسم الموجبة للعدد a مع مجموعة القواسم الموجبة للعدد b فهي مجموعة منتهية .

1-2-3 القاسم المشترك الأعظم :

تعريف: نقول إن d هو القاسم المشترك الأعظم للعددين الصحيحين a , b غير المعدومين معاً ونكتب $d = (a,b)$ أو $d = g.c.d(a,b)$

إذا تحقق ما يلي : **(1** $d > 0$

(2 $d|b \wedge d|a$

(3 إذا كان العدد الصحيح $c > 0$ و $c|b \wedge c|a$ فإن $c \leq d$.

على سبيل المثال :

$$(-3,-9) = 3 \ , (15,28) = 1 \ , (0,6) = 6 \ , (21,15) = 3$$

نتيجة : إن القاسم المشترك الأعظم لعددين a , b غير معدومين معاً دوماً موجود وهو وحيد

الإثبات : قلنا إن مجموعة القوا سم المشتركة لعددين a , b غير معدومين معاً هي مجموعة منتهية وعناصرها لا تتجاوز العدد الأصغر بين العددين $|a|, |b|$ فهي مجموعة محدودة من الأعلى فلها بالتالي عنصر أكبر هو القاسم المشترك الأعظم للعددين a , b . وهذا القاسم وحيد إذ لو افترضنا جدلاً أن d_1 و d_2 كل منهما قاسم مشترك أعظم فحسب الشرط **(3)** يمكن أن تكتب أن :

$$d_1 = d_2 \Leftarrow d_2 \leq d_1, d_1 \leq d_2$$ وهو المطلوب .

ملاحظة : إن مجموعة القوا ســـم المشـــتركة للعددين المعدومين$a = 0, b = 0$ هي مجموعة الأعداد الصحيحة الموجبة، فهي مجموعة غير منتهية، وليس لها عنصر أكبر ولا يوجد قاسم مشترك أعظم لهما.

4-2-1 مبرهنة : إذا كان a , b عددين صحيحين غير معدومين فإن القاسم المشترك الأعظم لهما $d = (a, b)$ هو تركيب خطي للعددين a , b . أي يوجد دوماً عددان صحيحان x_0, y_0 بحيث :

$$d = (a, b) = x_0 a + y_0 b$$

الإثبات : لنعرف مجموعة التراكيب الخطية لـ a , b كما يلي :

$$S = \{n = ax + by; x, y \in Z\}$$

إن المجموعة S غير خالية فهي تحوي :

$n = \pm a$ عندما $x = \pm 1, y = 0$

$n = \pm b$ عندما $x = 0, y = \pm 1$ أي أنها تحوي أعداداً موجبة وأعداداً سالبة.

لنعرف المجموعة الجزئية S_1 كما يلي : $S_1 = \{n > 0, n \in S\}$.

إن المجموعة S_1 غير خالية وضوحاً وحسب مبدأ الترتيب الحسن لها عنصر أصغر نسميه n_0 ونكتب $n_0 = x_0 a + y_0 b$ وحسب المبرهنة الأساسية في الحساب يمكن أن تكتب :

$$\boldsymbol{n = n_0 q + r : 0 \le r < n_0} \qquad \textbf{(1)}$$

أي $ax + by = (ax_0 + by_0)q + r \Rightarrow r = a(x - x_0 q) + b(y - y_0 q)$

ولما كان $r \ge 0$ وهو تركيب خطي لـ a , b فإن $r \in S$.

فإذا كان $r = 0$ فإن n_0 يقسم n .

وإذا كان $r > 0$ فإن $r \in S_1$ ولكن n_0 هو العنصر الأصغر في S_1

ولدينا من **(1)** $r < n_0$ وهذا تناقض إذاً لابد وأن تكون $r = 0$ و $n_0 | n$ أي أن n_0 تقسم جميع عناصـــر S أي : $n_0 | a$ و $n_0 | b \Leftarrow n_0$ قاســـم مشـــترك للعـددين a , b أي أن : $n_0 \le d = (a, b)$.

ومن جهة أخرى فإن العلاقة $n_0 = x_0 a + y_0 b$ تدل على أن كل قاسم لـ a , b يجب أن يقسم n_0 أي أن d يقسم n_0 و بالتالي $d \le n_0$ مما يثبت أن $d = n_0$ أي $d = x_0 a + y_0 b$.

ملاحظة (1) : يلاحظ مما ســبق أن القاســم المشــترك الأعظم لعددين غيرمعدومين معاً هو العنصــر الأصغر في مجموعة التراكيب الخطية الموجبة للعددين a , b .

ملاحظة (2) : إن تمثيل القاسم المشترك الأعظم لعددين كتركيب خطي ليس وحيداً .

فعلى سبيل المثال إن : $d = (15,24) = 3$

نكتب $3 = 15(-3) + 24(2)$ أو $3 = 15(-27) + 24(17)$

أو $3 = 15(5) + 24(-3)$ .....

نتيجة : إذا كان $d = (a,b)$ وكان c قاسماً مشتركاً لـ $a\ ,\ b$ فإن $c|d$

الإثبات : حسب **المبرهنة السابقة** نكتب $d = x_0a + y_0b$

فإذا كان $c|b \wedge c|a$ فأن $c|d$

1−2−5 تعريف : إذا كان القاسم المشترك الأعظم لعددين صحيحين $a\ ,\ b$ يساوي الواحد فإننا نسمي العددين عددين أولين نسبياً $(relatively\ prime)$

مثال : نلاحظ أن $(32,15) = 1$ فالعددان 32,15 أوليان نسبياً (أوليان معاً)

1−2−6 مبرهنة : يكون العددان $a\ ,\ b$ غير الصفريين معاً أوليين نسبياً فيما بينهما إذا وفقط إذا وجد عددان صحيحان $x\ ,\ y$ بحيث يكون : $ax + by = 1$

الإثبات : إذا كان $(a,b) = 1$ **فحسب المبرهنة (1−2−4)** نجد أن $1 = ax + by,\quad x,y \in Z$

ومن ناحية أخرى إذا كان $ax + by = 1$ حيث $x,y \in Z$ وكان $(a,b) = d$

فإن $d|b\ \wedge d|a$ بالتالي $d|ax + by$ أي $d|1$ ومنه $d = 1$

نتيجة : إذا كان $d = (a,b)$ وكان $b = b_0d$ و $a = a_0d$ فإن $(a_0,b_0) = 1$.

الإثبات : بما أن $(a,b) = d$ فيمكن كتابة العلاقة $ax + by = d$ وبتقسيم طرفي العلاقة على d نجد: $\frac{a}{d}x + \frac{b}{d}y = 1$

وحسب المبرهنة (1−2−6) يكون $(\frac{a}{d},\frac{b}{d}) = 1$ أي $(a_0,b_0) = 1$

1−2−7 بعض خواص القاسم المشترك الأعظم :

1) $(-a,-b) = (a,-b) = (-a,b) = (a,b) = (b,a) = (|a|,|b|)$ وضوحاً

2) $(0,a) = |a|$و$(a,1) = (1,a) = 1$ وضوحاً

3) $(a,m) = 1 \wedge (b,m) = 1 \Rightarrow (ab,m) = 1$

الإثبات : بما أن $(a,m) = 1$ يمكن إيجاد عددين صحيحين $x\ ,\ y$ بحيث $ax + my = 1$

نضرب طرفي العلاقة بـ b فنجد : $ab.x + mby = b$

لذا فإن أي قاسم d_1 لـ $a\ b$ و m يجب أن يقسم b أي $d_1|b \Leftarrow d_1|m \wedge d_1|ab$

أصبح لدينا $d_1|(b,m)$ أي $d_1|1$ و منه $d_1 = 1$.

4) إذا كان $(k,b)=1$ و $k|ab$ فإن $k|a$.

الإثبات : يمكن أن تكتب $1=kx+by$ نضرب الطرفين بـ a فنجد : $a=ak.x+aby$

لما كان k قاسماً لـ $a\,b$ وقاسما لـ $a\,k\,x$ فهو يقسم مجموعهما a .

ملاحظة: إذا كان $k|ab$ و $(k,b)\neq 1$ فإن k قد لا تقسم أياً من a , b .

مثال : $4|2\times 6=12$ في حين أن $4\nmid 6$, $4\nmid 2$.

5) إذا كان $(a,b)=1$ و $a|n$ و $b|n$ فإن $a.b|n$.

الإثبات : نكتب $n=an_0$ ولدينا $b|n$ أي $b|an_0$ ولكن $(a,b)=1$ ومنه $b|n_0$

بالتالي يمكن أن نكتب $n_0=bm$ أي $n=abm$ ومنه $ab|n$

6) إذا كان m عدد صحيح موجب وكان $(a,b)=d$ فإن $D=(ma,mb)=md$.

الإثبات : بما أن $(a,b)=d$ نكتب $d=ax+by$ نضرب الطرفين بـ m

فنجد : $md=max+mby$ ولدينا $D|ma\wedge D|mb$ ومنه نجد $D|md$ *

ومن جهة أخرى يمكن أن نكتب $D=max_1+mby_1$

ولدينا $d|a\wedge d|b\Leftarrow d|(ax_1+by_1)$ ،

ومنه $md|m(ax_1,by_1)$ و $md|D$ **

ومن * و** نجد أن $D=m\,d$.

تمهيدية : إذا كان $b=qa+r,\ 0\leq r<a$ فإن $(a,b)=(a,r)$

الإثبات : ليكن $(a,b)=d$ أي $d|\,b\wedge d|a$ ومنه $d|b-qa$ أي $d|r$

فهو قاسم مشترك لـ $r\,,a$. ليكن c قاسماً للعددين $r\,,a$ من الواضح أن $c|qa+r$ أي

$c|b\ ,\ c|\,a\Leftarrow c|d\Leftarrow c\leq d$ أي $d=(a,r)$.

خوارزمية اقليدس (*Euclidean algorithm*) :

هي وسيلة لإيجاد القاسم المشترك الأعظم لعددين صحيحين .

نعلم أن $(b,a)=(|a|,|b|)$ لذا نفترض أن $b\geq a>0$ ونشرح الخوارزمية كما يلي :

نجري عمليات القسمة المتتالية : $b=q_1a+r_1,\qquad 0\leq r_1<a$

فإذا كانت $r_1=0$ فإن $(b,a)=(a,0)=a$

وإذا كان $r_1\neq 0$ نتابع القسمة : $a=q_2r_1+r_2,\qquad 0\leq r_2<r_1$

فإذا كانت$r_2=0$ فإن $(a,b)=(a,r_1)=(r_1,0)=r_1$

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

.....

ونتابع حتى نحصل على باقي صفري ونكتب

$$r_{t-1} = q_{t+1} r_t + 0$$

عندئذ يكون

$$(a,b) = (a,r_1) = (r_1,r_2) = \ldots\ldots\ldots = (r_t,r_{t+1}) = (r_t,0) = r_t$$

حيث $b > r_1 > r_2 > \ldots\ldots\ldots > r_t > 0$

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

مثال : لنبحث عن القاسم المشترك الأعظم للعددين (3054 , 12378)

$$12378 = 4.(3054) + 162$$
$$3054 = 18.(162) + 138$$
$$162 = 1.(138) + 24$$
$$138 = 5.(24) + 18$$
$$24 = 1.(18) + 6$$
$$18 = 3.(6) + 0$$

أي $gcd\,(12378, 3054) = 6$

ملاحظة: يلاحظ من خوارزمية اقليدس أن البواقي المتتالية يمكن أن تكتب كتركيب خطي للعددين a , b حيث نجد :

$$r_1 = a - q_1 b$$
$$r_2 = b - r_1 q_2 = -q_2 a + (1 + q_1 q_2) b$$
$$r_3 = (1 + q_1 q_2) a - (q_1 + q_3 + q_1 q_2 q_3) b$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

وبالتالي يمكن استخدام هذه الخوارزمية لتعيين أمثال التركيب الخطي للقاسم المشترك الأعظم لعددين وذلك بأن نبدأ من الخطوة الأخيرة في الخوارزمية ونوضح ذلك في المثال السابق فنكتب :

$$6 = 24 - 18$$
$$= 24 - (138 - (5).(24))$$
$$= (6).(24) - 138 = 6(162 - 138) - 138$$
$$= (6).(162) - (7).(138) = (6).(162) - 7(3054 - (18).162)$$
$$= 9132).(162) - (7).(3054)$$
$$= 132(12378 - (4).(3054)) - (7).(3054)$$
$$= 132(12378) + (-535)(3054)$$

ومنه: $6 = gcd\,(12378, 3054) = x.12378 + y.3054$, $x = 132, y = -535$

ملاحظة (2) :

يمكن الاستفادة من خواص القاسم المشترك الأعظم بتبسيط خطوات خوارزمية اقليدس وعلى سبيل المثال يمكن أن نكتب :

$$g\,c\,d\,(12,30) = 3 \times g\,c\,d\,(4,10) = (3)\times(2)\times gcd\,(2,5) = 6$$

8-2-1 القاسم المشترك الأعظم لمجموعة أعداد صحيحة

- **تعريف :** لتكن $a_i, i = 1,2,3,\ldots,n$ أعداداً صحيحة ليست جميعها أصفاراً .

نقول إن d هو القاسم المشترك الأعظم لها ونكتب :

$$d = gcd(a_1 \ldots\ldots a_n) = (a_1, a_2, \ldots, a_n)$$

إذا وفقط إذا كان : (1) $d > 0$

(2) $1 \le i \le n d | a_i$

(3) إذا كان $c|a_i,\ 1 \le i \le n$ و $c>0$ فإن $c \le d$

مبرهنة : إذا كان $d = (a_1, a_2, \ldots, a_{n-1}, a_n)$

و $d_1 = (a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n))$ فإن $d = d_1$

الإثبات : من الفرض نلاحظ أن $i = 1,2,\ldots,n d|a_i$ أي $d|(a_{n-1}, a_n)$

ومنه $d|d_1$ ومن جهة أخرى $i = 1,2,\ldots\ldots,n-2 d_1|a_i$ و $d_1|(a_{n-1}, a_n)$

أي $d_1|a_{n-1} \wedge d_1|a_n$ ومنه $i = 1,2,\ldots,n,\ d_1|a_i$ ومنه $d = d_1 \Leftarrow d_1|d$

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

$$(256, 112, 72) = (256, (112, 72)) = (256, 8) = 8$$

تعريف : إذا كان القاسم المشترك الأعظم للأعداد غير الصفرية معاً $(a_1, a_2, \ldots, a_n)$ يساوي الواحد نقول إن الأعداد a_i أولية نسبياً فيما بينها .

تعريف : إذا كان $(a_i, a_j) = 1 \quad \forall i,j =< 1,n >$ فإننا نقول إن

الأعداد $a_i \quad i = 1,2,\ldots\ldots,n$ أولية نسبياً مثنى مثنى .

نتيجة : إذا كانت الأعداد غير الصفرية معاً a_i , $i = 1,2,\ldots\ldots,n$ أولية نسبياً مثنى مثنى فإنها أولية نسبياً والعكس غير صحيح .

مثال(1) : إن الأعداد 21 , 14 , 6 أولية نسبياً لأن : $(6, 14, 21) = 1$ ولكنها ليست أولية نسبياً مثنى مثنى لأن : $(14,21) = 7$, $(6,14) = 2$, $(6,21) = 3$

مثال(2) : إن الأعداد 6 , 25 , 77 أولية نسبياً مثنى حيث وهي أولية نسبياً لأن :

$$(6\ ,\ 25\ ,\ 77) = (6,\ (25\ ,\ 77)) = (6\ ,\ 1) = 1$$

1-2-9 المضاعف المشترك الأصغر (*least common multiple*)

تعريف : لتكن a_i أعداد صحيحة غير صفرية نقول إن m مضاعف لهذه الأعداد إذا كان $\forall i = 1,\dots,n \quad a_i|m$.

ونقول إن L هو المضاعف المشترك الأصغر لها ونكتب $lcm(a_1 \dots\dots a_n) = L$

إذا وفقط إذا كان :

$$L > 0 \qquad (1)$$

$$\forall i = 1,2,\dots,n, \quad a_i|L \qquad (2)$$

(3) إذا كان $m > 0$ و $a_i|m$, $i = 1,2,\dots,n$ فإن $L \leq m$.

في الحقيقة إذا كانت S مجموعة الأعداد الموجبة التي هي مضاعفات لكل من الأعداد غير الصفرية a_i $i = 1,\dots,n$ فإن هذه المجموعة غير خالية وحسب مبدأ الترتيب الحسن فيها عنصر أصغر يسمى هذا العنصر المضاعف المشترك الأصغر للأعداد a_i.

مثال : $l\,.\,c\,.\,m\,(9\,,8\,) = 72$ ، $l\,.\,c\,.\,m\,(6\,,15\,) = 30$

نتيجة : المضاعف المشترك الأصغر للأعداد غير الصفرية a_i يقسم أي مضاعف مشترك لها

الإثبات : ليكن $L = l.c.m(a_i)$ وليكن m مضاعف مشترك للأعداد a_i حسب خوارزمية القسمة نكتب: $\mathbf{0 \leq r < L}$: $m = q\,L + r$

ومنه $r = m - q\,L$ ، لدينا $\forall i = 1,2,\dots,n, \quad a_i|L, a_i|m$ و منه نجد

$a_i|r$ و $r < L$ وهذا تناقض لأن L هو العنصر الأصغر لمجموعة المضاعفات المشتركة الموجبة مما يدل على أن $r = 0$ حصراً و $L|m$

مبرهنة : إذا كان $a\ ,\ b$ عددان صحيحان موجبان وكان $d = gcd(a,b)$

و $L = l\,.\,c\,.\,m\,(\,a\,,b\,)$ فإن $L = \frac{a.b}{d}$

الإثبات : بما أن $d = (a,b)$ فيمكن أن تكتب $a = a_0.d, b = b_0.d$

حيث $(a_0, b_0) = 1$ ومنه $L = \frac{a.b}{d} = a_0 b = b_0 a$ هو مضاعف مشترك للعددين $a\ ,\ b$ ، ليكن m مضاعفاً مشتركاً لـ $a\ ,\ b$ فيمكن أن تكتب

$$\boldsymbol{m = a_1 a = a_1 a_0 d, b|m \Rightarrow b|a_1 a_0 d}$$

ومنه

$$\boldsymbol{b_0 d|a_1 a_0 d \Rightarrow b_0|a_1 a_0}$$

ولما كان $(a_0, b_0) = 1$ فإن $\boldsymbol{b_0 a|a_1 a = m \Leftarrow b_0|a_1}$

أي $\boldsymbol{L|m}$ و $\boldsymbol{L \leq m}$ ومنه $\boldsymbol{L}$ هو المضاعف المشترك الأصغر

نتيجة : إذا كان $gcd(a, b) = 1$ **فإن** $L = a.b$

مثال : المضاعف المشترك الأصغر للعددين 6 , 21 هو $L = \frac{6.21}{d}$

$d = (6,21) = 3$ ومنه $L = 42$

محاضرات د. يحيى

تمارين

1- استخدم طريقة الاستقراء الرياضي لإثبات ما يلي :

$$15|2^{4n}-1n\geq 0، \quad 7|2^{3n}-1n\geq 1$$
$$8|3^{2n}+7n\geq 0، \quad 8|3^{2n}+7n\geq 1$$
$$2304|7^{2n+2}-48n-49n\geq 0، \quad 3|2^{n}+(-1)^{n+1}n\geq 1$$

2- أثبت أنه إذا كان $3x+2$ مضاعفاً للعدد 7 فإن

$$14|15x^2-11x+14$$
$$49|24x^2+4x+41$$

3- إذا كان $(a,b)=1$ أوجد القيم الممكنة لكل من :

$$(a+b,a-b),(a+b,a^2+b^2),(2a+b,a+2b)$$

4- إذا كان $a\in Z$ فهل يقبل العدد a^2+2 القسمة على 4 أم لا ؟

5- هل العبارات التالية صحيحة أم خاطئة إن كانت صحيحة فأثبت صحتها

وإن كانت خاطئة فأعط مثالاً يبين ذلك :

1) إذا كان $a|b$ و $a|c \Rightarrow a^2|bc$

2) $ac|bc \Leftrightarrow a|b$ حيث $c\neq 0$

3) إذا كان $a|b+c$ فإن إما $a|b$ أو $a|c$

4) إذا كان $a|b^2+1$ فإن $a|b^4+1$

5) إذا كان $a^2|b^3$ فإن $a|b$

6) إذا كان $a^2\leq b^2 \wedge b^2|n \wedge a^2|n \Rightarrow a|b$

6- عين القاسم المشترك الأعظم :

$$(227,659),\quad (143,227),\quad (306,657),\quad (272,1479)$$
$$(25,72,175,168),\quad (227,659,454),\quad (272,24,306)$$

7- أوجد قيماً لـ x , y تحقق ما يلي : $g.c.d(56,72)=56x+72y$

$$g.c.d(119,272)=119x+272y$$
$$g.c.d(1769,2378)=1769x+2378y$$

8- أوجد $l\,c\,m\,(143,227)$ $\quad l\,c\,m\,(272,1479)$

9- أوجد أعداداً صحيحة x , y , z تحقق العلاقة :

$$g.c.d(198,288,512)=198x+288y+512z$$

الفصل الثالث

الأعداد الأولية

3-1 الأعداد الأولية (*Prime number*)

1-3-1 تعريف: نقول إن العدد الصحيح p عدد أولي إذا تحقق ما يلي :

1- $p > 1$

2- p لا يقبل القسمة إلا على نفسه وعلى 1

ونسمي العدد الصحيح الموجب غير الأولي عدداً مؤلفاً **(*composite number*)**

- **نتيجة :** إذا كان n عدداً مؤلفاً فيمكن أن يكتب كما يلي $n = a \ . \ b$

حيث $1 < b < n, 1 < a < n$.

مثال : العدد 35 عدد مؤلف ويمكن أن يكتب $35 = 5 \times 7$

2-3-1 بعض خواص الأعداد الأولية :

1) الأعداد الأولية هي أعداد أولية نسبياً مثنى مثنى .

2) إذا كان العدد الأولي p يقسم العدد الصحيح n فإن $p = (p , n)$ فيما عدا ذلك فإن $(p, n) = 1$.

3) إذا كان p عدداً أولياً وكان $p|ab$ فإن p يقسم أحدهما على الأقل أو بعبارة أخرى إذا كان $p \nmid a$ و $p|ab$ فإن $p|b$.

4) إذا كان $p|a_1.a_2.....a_n$ فإن p يقسم أحد الأعداد a_i على الأقل(تبرهن بطريقة الاستقراء) .

5) إذا كانت $p, p_1, p_2, ..., p_n$ أعداد أولية وكان $p|p_1.p_2.....p_n$ فإن p يساوي أحد الأعداد الأولية p_i .

الإثبات : بما أن p يقسم جدا ء الأعداد p_i فهو يقسم أحدهما على الأقل ولنفترض أن $p|p_k$ ولكن p_k عدد أولي لا يقبل القسمة إلا على نفسه وعلى الواحد فيجب أن يكون $p_k = p$

المبرهنة الأساسية في الحساب (*Fundamental Theorem of Arithmetic*)

إن أي عدد صحيح $n > 1$ هو إما عدد أولي أو هو جدا ء عدد منته من الأعداد الأولية وهذا التمثيل كجداء عوامل أولية تمثيل وحيد بغض النظر عن ترتيب الأوليات .

البرهان : لنستخدم طريقة الاستقراء الرياضي

الخطوة الأساسية : لدينا $n = 2$ هو عدد أولي ، $n = 3$ هو عدد أولي

$n = 4 = 2 \times 2$، $n = 5$ عدد أولي، $n = 6 = 2 \times 3$

خطوة الاستقراء : لنفترض أن المبرهنة صحيحة من أجل الأعداد حتى العدد k ولنثبت صحتها من أجل $n = k + 1$

- إن كان العدد $k+1$ أولياً فقد تم البرهان .

وإن كان $k+1$ عدداً مؤلفاً لأمكن كتابته على النحو : $a.b = k+1$ حيث

$$1 < b < k+1, \quad 1 < a < k+1$$

ولما كان كلّ من a وb أصغر من $k+1$ فهو يكتب كجداء عدد منته من العوامل أولية أي أن $k+1$ هو جداء عدد منته من العوامل الأولية والقضية صحيحة من أجل أي عدد صحيح $n > 1$. لنثبت الآن أن تمثيل العدد كجداء عوامل أولية هو تمثيل وحيد . ونستخدم أيضاً طريقة الاستقراء الرياضي في البرهان .

الخطوة الأساسية : نلاحظ أن $2 = 2$ ، $3 \ldots\ldots 2 = 6$ والعلاقة صحيحة

خطوة الاستقراء : لنفترض صحة العلاقة من أجل $n = k$ ولنثبت صحتها من أجل $n = k+1$

ولنفترض جدلاً أنه يمكن كتابة $k+1$ كجداء عوامل أولية بشكلين مختلفين ونكتب

$$k+1 = p_1.p_2 \ldots . p_s = q_1.q_2 \ldots . q_t$$ من العلاقة الأخيرة ينتج أن

$$p_1 | q_1.q_2 \ldots . q_t$$

أي أن p_1 تساوي أحد الأعداد الأولية q_i وليكن $p_1 = q_j$. نغير ترتيب العوامل q_i بحيث $q_j = q_1 = p_1$ ونكتب

$$k+1 = p_1(p_2.p_3 \ldots . p_s) = p_1(q_2.q_3 \ldots q_t)$$

نلاحظ أن $n_1 = p_2.p_3 \ldots . p_s = q_2.q_3 \ldots q_t$ $\quad n_1 < k+1,$

أي أن تمثيل n_1 كجداء عوامل أولية تمثيل وحيد مما يدل على أن $s = t$ وأن تمثيل $k+1$ كجداء عوامل أولية هو أيضاً تمثيل وحيد .

ملاحظة : يمكن أن تكون بعض العوامل الأولية لعدد صحيح $n > 1$ متساوية فإذا جمّعنا معاً العوامل المتساوية أمكننا كتابة العدد n كجداء عوامل أولية بالشكل القانوني كما يلي :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_s^{\alpha_s}$$

حيث p_i عوامل أولية مختلفة مرتبة $p_1 < p_2 < \ldots\ldots < p_s$ وα_i أعداد صحيحة موجبة . وتدعى عملية إيجاد هذه العوامل عملية تحليل العدد الصحيح $n > 1$.

مثال : $\mathbf{360 = 2^3.3^2.5}$

$$\mathbf{17640 = 2^3.3^2.5.7^2}$$

نتيجة (1) : كل عدد صحيح $n > 1$ له عامل أولي أي يوجد $p|n$ (p عدد أولي)

نتيجة (2) : إذا كان $n > 1$ عدداً مؤلفاً فله عامل أولي p بحيث يكون $\boldsymbol{p \le \sqrt{n}}$.

الإثبات : بما أن n عدد مؤلف فيمكن أن تكتب $n = a.b$

$$1 < a \le b < n \quad \text{ومنه} \quad n = a.b \ge a^2$$

أي أن $a \le \sqrt{n}$ ولما كان $a > 1$ فله عامل أولي وليكن p

أي $p|a \Leftarrow p|n, p \le a$ و $p \le \sqrt{n}$ و هو المطلوب.

نتيجة (3) : إذا كان $n > 1$ وليس له عامل أولي $\geq \sqrt{n}$ فإن n عدد أولي .

الإثبات : ذلك أنه إذا لم يكن n أولياً كان عدداً مؤلفاً و إذا كان n عدداً مؤلفاً فله عامل أولي $\geq \sqrt{n}$ وهذا تناقض . أي إذا كان $n > 1$ فهو إما عدد أولي أو له عامل أولي $p \leq \sqrt{n}$.

- كم هو عدد الأعداد الأولية ؟

شـــغلت هذه المســـألة أذهان علماء الرياضـــيات منذ القدم وقد وضـــعت براهين كثيرة تثبت أن عدد الأعداد الأولية غير منته ومن أقدم هذه البراهين وأبسطها البرهان الذي وضعه اقليدس وسنورد هذا البرهان فيما يلي :

لنفترض أن عدد الأوليات (الأعداد الأولية) منته ولنرتب هذه الأعداد كما يلي:

$$p_1 < p_2 < p_3 < \ldots\ldots < p_n$$

ولنكتب $N = p_1 p_2 p_3 \ldots . p_n + 1$

من الواضح أن $N > 1$ فله عامل أولي وليكن p أي أن $p|N$

فإذا كان p يساوي أحد الأوليات p_i لوجدنا $i = 1, 2, \ldots, n$

$$p|1 \Leftarrow p|N - p_1 p_2 \ldots . p_n \Leftarrow p|N, p|p_1 p_2 \ldots . p_n$$

وهذا تناقض أي أن p عدد أولي مختلف عن الأوليات p_i وهكذا فإن عدد الأوليات غير منته

يلاحظ أن الأعداد ذات الصيغة $p_1 p_2 \ldots . p_k + 1$ تعطي

$N_1 = 3$ ، $N_2 = 7$ ، $N_3 = 31$ ، $N_4 = 211$ ، $N_5 = 2311$ كلهـا أوليـة ولكن لســـوء الحظ $N_6 = 59 \times 509$ عدد مؤلف وتسمى هذه الأعداد أعداد اقليدس .

- هل يوجد صيغة معينة تعطي جميع الأوليات ؟

سؤال آخر حير علماء الرياضيات ، فوضعوا صيغاً ظن بعضهم أنها تعطي جميع الأوليات ثم ثبت أن حدسهم خاطىء ، من هذه الصيغ

1- الصيغة $x^2 - x + 41$ وجد أنها تعطي أعداداً أولية من أجل $x = 0,1,2, \ldots . ,40$ ولكنها تعطي عدداً مؤلفاً من أجل $x = 41$

2- الصيغة $x^2 - 79x + 1601$ تعطي أعداداً أولية من أجل $x = 0,1,2, \ldots . ,79$ فقط

ثم أثبت **غولدباخ (1752)** أنه لا يوجد أي حدودية صـــحيحة من أي درجة كانت تعطي أعداداً أولية من أجل جميع قيم x

و أثبت **دير خلية (1837)** أن الحدودية $a\,x + b$ حيث $(a , b) = 1$ تعطي عدداً غير منته من الأوليات عندما تأخذ x قيماً صحيحة موجبة .

3- وضع **فيرما (1601-1665) الصيغة** : $F_n = 2^{2^n} + 1$ وظن أنها تعطي أوليات من أجل جميع قيم .... $n = 0 , 1 , 2$ وأثبت **اولر (1732)** أن F_5 عدد مؤلف يقبل القسمة على 641 .

- كيف نعين الأعداد الأولية التي لا تتجاوز قيمة معينة N ؟

لما كان توزيع الأعداد الأولية غير منتظم وليس هناك صيغة رياضية تعطي فقط أعداداً أولية كان تعيين الأعداد الأولية عملية غير سهلة وخاصة إذا كان العدد N كبيراً ، ومن أبسط الطرق لتعيين الأعداد الأولية هي طريقة وضعها الرياضي اليوناني ايراتوستين تسمى مرشحة **ايراتوستين *(The sieve of Eratosthenes)*** في القرن الثالث قبل الميلاد وسنشرح هذه الطريقة فيما يلي :

تكتب جميع الأعداد من 1 إلى N ثم نبدأ بالعدد الأولي الأول وهو 2 يترك وتشطب جميع مضاعفاته ثم يترك أول عدد لم يتم شطبه وسيكون العدد 3 وتشطب جميع مضاعفات العدد 3 وهكذا ، وفي كل مرة يكون أول عدد لم يتم شطبه عدداً أولياً حتى تصل إلى العدد $p \leq \sqrt{N}$ وتكون الأعداد التي لم يتم شطبها هي الأعداد الأولية المطلوبة . وهذا تمثيل لمرشحة ايراتوستين من أجل $N = 101$:

	~~2~~	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
51	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101									

سنذكر أخيراً نص المبرهنة التي تحدد عدد الأعداد الأولية التي لا تتجاوز العدد الحقيقي الموجب x هذه المبرهنة التي كانت حدساً من قبل كل من **ليجاندر و غاوس** عام 1793 ولم يتم إثباتها بشكل كامل ومبسط حتى عام 1949 من قبل **سيليرغ *(A . Sellerg)*** **و ايردوس (*P. Erodes*)**

مبرهنة الأعداد الأولية :

إذا كان $\pi(x)$ هو عدد الأعداد الأولية p التي تحقق العلاقة $2 \leq p \leq x$ حيث x عدد حقيقي موجب ، فإن نسبة $\pi(x)$ إلى الدالة $x / \log x$ تنتهي إلى اللانهاية .

3-3-1 التحليل إلى عوامل بطريقة فيرما :

لقد أثبتنا أن أي عدد صحيح $n > 1$ يمكن أن يحلل إلى عوامل أولية ولكن طريقة التحليل تصبح شاقة عندما تكون الأعداد كبيرة . وقد شرح فيرما برسالة إلى صديقه العالم الرياضي ميرس في 1643 طريقة لتحليل أي عدد فردي إلى جداء عددين فرديين ولما كان حذف قوى العدد 2 من أي عدد زوجي عمل سهل فإن لتحليل الأعداد الفردية أهمية كبرى وقبل شرح طريقة التحليل سنثبت التمهيدية التالية :

تمهيدية : إذا كان n عدداً صحيحاً فردياً موجباً فيمكن كتابة n كحاصل ضرب عددين صحيحين موجبين a وb إذا وفقط إذا أمكن كتابة n كفرق بين مربعين .

البرهان: إذا كان $n = a\,b$ حيث $a\,,\,b$ عددان صحيحان موجبان فرديان حتماً فيمكن كتابة العلاقة :

$$n = ab = \frac{(a+b)^2}{2} - \frac{(a-b)^2}{2}$$

وبالعكس إذا كان $n = x^2 - y^2$ فإن من الممكن كتابة n على النحو :

$$.n = (x-y)(x+y) = a.b$$

طريقة فيرما لتحليل العدد الفردي n إلى جداء عاملين تكمن في البحث عن عددين $x\,,\,y$ يحققان المعادلة $n = x^2 - y^2$ أو المعادلة $x^2 - n = y^2$

لذا نبدأ بالبحث عن أصغر عدد صحيح k يحقق العلاقة : $k^2 \geq n$ ثم نبحث بين الأعداد $k^2 - n,\ \ (k+1)^2 - n, \ldots\ldots$ حتى نصل إلى قيمة m حيث $m \geq \sqrt{n}$ تجعل المقدار $m^2 - n$ مربعاً لعدد صحيح .

إن خطوات العمل من دون شك منتهية لأنه لابد وأن نصل إلى الخطوة الأخيرة

$$(\frac{n+1}{2})^2 - n = (\frac{n-1}{2})^2$$

وعندها نجد $n = n\,.\,1$ مما يدل على أن n عدد أولي وذلك إذا لم نحصل على $m^2 - n$ مربعاً لعدد صحيح في خطوة سابقة.

لقد استخدم فيرما هذه الطريقة لتحليل العدد $n = 2027651281$ ووجد أن

$n = 440201 \times 46061$ بعد 11 خطوة فقط . وإذا قورنت هذه الطريقة بطريقة التحليل العادية فإننا نجد أننا بحاجة لـ 2850 عملية قسمة على أعداد أولية متتالية لنحصل على العدد 44021 ..

كما نلاحظ هنا أننا لسنا بحاجة لمعرفة جميع الأعداد الأولية التي هي أصغر من $\sqrt{n}$ لإيجاد عوامل n الأولية .

مثال (1) : لتحليل العدد $n = 23449$ نجد أن $153^2 < n < 154^2$

لذا نكتب :

$$154^2 - 23449 = 267$$

$$155^2 - 23449 = 576 = 24^2$$

$$n = 23449 = (155 - 24)(155 + 24) = 131 \times 179$$

وهما عددان أوليان .

مثال (2) : لنحلل العدد $n = 315$ بطريقة فيرما

نلاحظ $17^2 < 315 < 18^2$ ونكتب

$$\mathbf{18^2 - n = 9 = 3^2}$$

ومنه $n = (18-3)(18+3) = 15 \times 21$

ونحلل كلاً من 15 و21 فنجد $n = 315 = 3^2.5.7$

مثال (3) : لنحلل العدد $\boldsymbol{n = 119143}$

نلاحظ أن $345^2 < 119143 < 346^2$

ونكتب :

$$346^2 - 119143 = 573 = 119716 - n$$
$$347^2 - n = 1266 = 120409 - n$$
$$348^2 - n = 1961 = 121104 - n$$
$$349^2 - n = 2658 = 121801 - n$$
$$350^2 - n = 3357 = 122500 - n$$
$$351^2 - n = 4058 = 123201 - n$$
$$352^2 - n = 4761 = 69^2 = 123904 - n$$

ومنه $n = (352 - 69)(352 + 69) = 283 \times 421$

وكلاهما عددان أوليان واحتجنا لسبع خطوات فقط .

محاضرات د. يحيى

تمارين

1- أثبت أن العدد الأولي الوحيد من الصيغة $n^3 - 1$ هو 7 .

2- أثبت أن الأولي الوحيد p الذي يحقق العلاقة $\boldsymbol{3p + 1 = n^2}$ هو $p = 5$.

3- لدينا p عدد أولي و $p|a^n$ أثبت أن $p^n|a^n$ وأن $p|a$.

4- إذا كان p عدداً أولياً فردياً و $p \neq 5$ أثبت أنه إما $p^2 - 1$ أو $p^2 + 1$ يقبل القسمة على 10 .

5- أوجد جميع الأعداد الأولية التي هي ≥ 30 .

6- أوجد جميع الأعداد الأولية في المجال 250 , 150 .

7- إذا كان p عدداً أولياً و $p \geq 5$ أثبت أن $p^2 + 2$ عدد مؤلف .

8- أثبت أنه إذا كان $n > 0$ فإن $2^{4n+2} + 1$ عدد مؤلف .

9- حلل الأعداد التالية إلى عواملها الأولية بطريقة فيرما :

$31623, 10541, 493, 2931, 977, 945, 430663, 2279, 38025, 81518057$

10- استخدم طريقة فيرما لتحليل العدد $2^{11} - 1$

الفصل الرابع
معادلات ديوفانتس

4-1 معادلات ديوفانتس *Diophantus Equations*

1-4-1 تمهيد : هي المعادلات التي سماها العرب المعادلات السيالة أي له عدد لانهائي من الحلول وهي معادلات بعدة متحولات تخرج بصوابات كثيرة . تنسب هذه المعادلات إلى العالم اليوناني ديوفانتس الذي عاش في حوالي 250 بعد الميلاد في الإسكندرية . وكان أثر المصريين والبابليين و الصومريون بارزاً جداً في أعماله . لم يضع ديوفانتس حلاً عاماً لهذه المعادلات بل كان يحل كل مسألة حلاً مستقلاً لا يستند إلى قاعدة عامة ، ويوجد الحلول الصحيحة لها .

سنقتصر في هذا الفصل على دراسة معادلات ديوفانتس الخطية بمجهولين ومعادلات ديوفانتس من الدرجة الثانية التي تعين ثلاثيات فيثاغورث .

2-4-1 معادلات ديوفانتس الخطية بمجهولين :

نكتب هذه المعادلات على النحو : $a\,x + b\,y = n$ حيث $a, b, n \in Z$ ونبحث عن الحلول الصحيحة لهذه المعادلات أي عن القيم الصحيحة للمتحولين $x\,, y$ التي تحقق هذه المعادلات

نلاحظ أولاً أنه قد يكون لمعادلة خطية من هذا النوع أكثر من حل وعلى سبيل المثال نلاحظ أن الثنائيات $(14,1), (-6,6), (10,-2)$ تحقق المعادلة $3\,x + 6\,y = 18$

وقد لا يكون لمثل هذه المعادلات أي حل ، فعلى سبيل المثال المعادلة

$2\,x + 10\,y = 17$ ليس لها أي حل لأن الطرف الأول من المعادلة عدد زوجي والطرف الثاني عدد فردي ولا يمكن تحقيق المساواة بين الطرفين مهما تكن قيم x و y .

3-4-1 مبرهنة : إذا كان لدينا المعادلة (1) $a\,x + b\,y = c$ حيث $a, b, c \in Z$ و $a\,,\ b$ غير صفريين معاً فإنه يكون لهذه المعادلة حل إذا وفقط إذا كان d القاسم المشترك الأعظم للعددين $a\,,\ b$ يقسم الطرف الثاني c . وإذا كان (x_0, y_0) حلاً خاصاً لهذه المعادلة فإن جميع الحلول تعطى بالعلاقات :

$$x = x_0 + \frac{b}{a}t$$
$$y = y_0 - \frac{a}{d}t$$

حيث t عدد صحيح ما .

البرهان : تعلم أنه إذا كان $d=(a,b)$ فيمكن إيجاد عددين صـــحيحين $r\ ,\ s$ بحيث يكون:

$(r,s)=1, a=rd, b=sd$. فإذا وجد للمعادلة (1) حل وليكن x_0,y_0 فإن :

$$ax_0+by_0=c=rdx_0+sdy_0=d(rx_0+sy_0)$$

أي أن $d|c$.

ومن جهة ثانية إذا كان $d|c$ فيمكن أن نكتب $c=td\ ,\ t\neq 0$

ولما كان $d=(a,b)$ فيوجد عددين صـحيحين $m\ ,\ n$ بحيث $d=a\,m+b\,n$ وبضـرب طرفي هذه العلاقة بـ t نجد : $t\,d=a\,(t\,m)+b\,(t\,n)=c$

أي يوجد عددان $x_0=tm, y_0=tn$ يحققان المعادلة : $a\,x+b\,y=c$ لنثبت الآن أنه إذا عرفنا الحل الخاص x_0,y_0 للمعادلة (1) فإن أي حل (x,y) لها يكتب على النحو :

$$x=x_0+(\frac{b}{d})t, y=y_0-(\frac{a}{d})t$$

لذا تكتب $ax_0+by_0=c=ax+by$

$$a(x-x_0)=b(y-y_0) \qquad (2)$$

ولما كان $d=(a,b)$ فإن $(a_0,b_0)=1$ نعوض $a=a_0d,\quad b=b_0d,$ في (2) فنجد :

$$a_0(x-x_0)=b_0(y_0-y) \qquad (3)$$

ومنه $a_0|b_0(y_0-y)$ ولكن

$$a_0|(y_0-y) \quad \Leftarrow \quad (a_0,b_0)=1$$

أي $y_0-y=a_0tt\in Z$

أو $y=y_0-a_0t=y_0-\frac{a}{d}t$

وبالتعويض في (3) نجد :

$$a_0(x-x_0)=b_0a_0t\Rightarrow x-x_0=b_0t$$

$$x=x_0+b_0t=x_0+\frac{b}{d}t$$ وهو المطلوب ،

وللمعادلة عدد غير منته من الحلول .

ملاحظة (1) : إذا كان $d=1$ فإن $x=x_0+bt,\ y=y_0-at$

هي جميع حلول المعادلة (والمعادلة لها حل دوماً) .

ملاحظة (2) : إن المبرهنة السـابقة مع خوارزمية اقليدس تزودنا بطريقة عملية لإيجاد حلول معادلة ديوفانتس الخطية (1) ومن أجل ذلك نبدأ بتعيين القاسـم المشـترك الأعظم للعددين $a\ ,\ b$ ثم كتابة هذا القاسم المشترك الأعظم كتركيب خطي لهما ومن ثم نعين حلول المعادلة (1) .

مثال (1) : لنوجد جميع حلول المعادلة $172x + 20y = 1000$ إن وجدت

لنثبت أولاً أن للمعادلة حل فنبدأ بتعيين القاسم المشترك الأعظم للعددين (20 , 172) ، نطبق من أجل ذلك خوارزمية اقليدس فنجد :

$$172 = 8 \times 20 + 12$$
$$20 = 1 \times 12 + 8$$
$$12 = 1 \times 8 + 4$$
$$8 = 2 \times 4 + 0 \Rightarrow 4 = (172,20)$$

تلاحظ أن $4|1000$ فللمعادلة حل ، لإيجاد الحل نكتب :

$$4 = 12 - 8 = 12 - (20 - 12)$$
$$= 2 \times 12 - 20 = 2(172 - 8 \times 20) - 20$$
$$4 = 2(172) + (-17)20$$

ومنه $1000 = 4 \times 250 = 250[2 \times 172 + (-17)20]$

$$= (500) \times 172 + (-4250) \times 20$$

أي $y_0 = -4250\ ,\ x_0 = 500$

والحل الكامل للمعادلة :

$$x = 500 + \frac{20}{4}t = 500 + 5t$$
$$y = -4250 - \frac{172}{4}t = -4250 - 43t$$

ملاحظة : قد يطلب منا تعيين الحلول الموجبة لمعادلة ما . من أجل ذلك نعين قيم t التي تحقق الشرط $x > 0$, $y > 0$ في المثال السابق نكتب :

$$-43\,t - 4250 > 0 \qquad 5\,t + 500 > 0$$

ومنه $-98\frac{36}{43} > t > -100$

ولما كان t عدد صحيح فإن $t = -99$ ويكون الحل الوحيد الموجب للمعادلة السابقة هو :

$$x = 5 \qquad , \qquad y = 7$$

مثال (2) : لنوجد حلول المعادلة $6\,x + 51\,y = 22$ إن وجدت

نلاحظ أنّ : $(6\ ,\ 51) = 3$ ولكن $3 \nmid 22$ وليس للمعادلة أي حل .

مثال (3) : لنوجد حلول المعادلة : $7\,x + 9\,y = 5$ إن وجدت

نلاحظ أنّ $d = (7\ ,\ 9) = 1$ وللمعادلة حل

نكتب : $9 = 1 \times 7 + 2$

$$7 = 3 \times 2 + 1$$
$$2 = 1 \times 2 + 0$$
$$d = 1 = 7 - (2 \times 3) = 7 - (9 - 7) \times 3 = 7\,(4) + 9\,(-3)$$

نضرب الطرفين بـ 5 :

$$5 = 7(20) + 9(-15) \Rightarrow x_0 = 20, y_0 = -15$$

والحل الكامل $x = 20 + 9t, \quad y = -15 - 7t$

1-4-3 ثلاثيات فيثاغورث (*Pythagorean triple*)

اكتشـــف البابليون (حوالي2000 ق.م) العلاقة التي تربط بين أضـــلاع المثلث القائم أي العلاقة $x^2 + y^2 = z^2$ وعينوا أطوال أضلاع عدد من هذه المثلثات منها

$$(4961, 6480, 8161), (169, 120, 119)$$

ولم يعثر على برهان ذلك ولا على شـرح لطريقة الوصـول إلى هذه الأرقام الكبيرة . وقد قدم برهان لوجود حلول صـــحيحة للمعادلة $x^2 + y^2 = z^2$ الرياضـــي اليوناني فيثاغورث حوالي 500 ق. م وهذه المعادلة هي صـنف من المعادلات ديوفانتس التربيعية . وتسـمى الأعداد الصـحيحة (x , y , z) التي تحقق هذه المعادلة ثلاثيات فيثاغورث ولنبحث في إيجاد حلول هذه المعادلة .

تعريف : الثلاثي x , y , z الذي يحقق معادلة فيثاغورث ويحقق العلاقة 1= (x , y , z) يدعى ثلاثي فيثاغورث الأولي .

مثال (5 , 4 , 3) هو ثلاثي فيثاغورث أولي وكذا الثلاثي(13 , 12 , 5) . في حين الثلاثي (10 , 8 , 6) هو ثلاثي فيثاغورث غير أولي .

تمهيدية (1) : لنفترض أن (x , y , z) ثلاثي فيثاغورث أولي أي 1= (x , y , z) ولنثبت أن الأعداد x, y, z هي أولية نسبياً مثنى مثنى.

البرهان : إذا كان $(x , y) = d > 1$ فإنه يوجد عدد أولي مثل $p|d$ ولما كان $d|x \wedge d|y$ ينتج أن $p|x \wedge p|y$

ومنه $p|x^2 \wedge p|y^2$ ومنه $p|x^2 + y^2 = z^2$ وهذا يقتضي :

$p|z^2$ وهذا يناقض كون 1= (x , y , z) أي أن :1 = (x , y) وبالطريقة ذاتها نثبت أن :

$(x , z) = (z , y) = 1$.

تمهيدية (2) : إذا كان (x , y , z) ثلاثي فيثاغورث وكان $d =$ (x , y , z)

فإن (x_0, y_0, z_0) هو ثلاثي فيثاغورث أولي حيث $x = x_0 d, y = y_0 d, z = z_0 d$

الإثبات : لما كان $d|x, d|y, d|z$ يمكن إيجاد x_0, y_0, z_0 بحيث

$x = x_0 d, y = y_0 d, z = z_0 d$ ولما كان $d \neq 0$ و $x^2 + y^2 = z^2$ فإن

$$(x_0^2 + y_0^2)d^2 = z_0^2 d \Rightarrow x_0^2 + y_0^2 = z_0^2$$

و(x_0, y_0, z_0) هو ثلاثي فيثاغورث ولنثبت $(x_0, y_0, z_0) = 1$

لذلك نكتب :

$$(x_0d, y_0d, z_0d) = ((x_0d, y_0d), z_0d) = (d(x_0, y_0), z_0d)$$

ومنه :

$$(x\ ,\ y\ ,z\ ) = d\ \ (x_0, y_0, z_0) \Rightarrow (x_0, y_0, z_0) = 1 = d$$

ملاحظة : إذا كان ثلاثي فيثاغورث (x_0, y_0, z_0) أولياً وإذا كان k عدداً صحيحاً أكبر من الصفر فإن (kx_0, ky_0, kz_0) هو ثلاثي فيثاغورث.

ينتج مما سبق أنه لإيجاد جميع ثلاثيات فيثاغورث يكفي البحث عن ثلاثيات فيثاغورث الأولية .

تمهيدية (3): إذا كان ثلاثي فيثاغورث (x, y, z) أولياً فإن العددين $x\ ,\ y$ أحدهما فردي والآخر زوجي .

البرهان : لقد أثبتنا أن $(x\ ,\ y\ ) = 1$ مما يدل على أن $x\ ,\ y$ لا يمكن أن يكونا زوجيين معاً ، لنفترض جدلاً أنهما فرديان ، عندها يمكن أن نكتب

$y^2 = 8M_2 + 1, x^2 = 8M_1 + 1$ وبالتالي $z^2 = x^2 + y^2 = 8M + 2$ وهذا غير ممكن لأنه لو كان z عدداً فردياً لكان $z^2 = 8n + 1$ ولو كان z عدداً زوجياً لكان $z^2 = 4n^2$.

تمهيدية (4) : إذا كان $a.b = c^n$ حيث $(a\ ,\ b\ ) = 1$ فإنه يوجد b_1, a_1 بحيث $b = b_1^n, a = a_1^n$.

البرهان : لنفترض أن $a > 1\ ,\ b > 1$ ونحلل كلاً منها إلى عوامله الأولية فنكتب

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_{k_1}^{\alpha_{k_1}}, b = q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots q_{k_2}^{\beta_{k_2}}$$

ولما كان $a\ ,\ b$ أوليان نسبياً فإن جميع الأوليات $p_i^{\alpha_i}, q_j^{\beta_j}$ مختلفة (فهي أولية نسبياً مثنى مثنى فيما بينها) وبالتالي فإن تحليل $a\ .\ b$ إلى عوامله الأولية يكتب على النحو :

$$a.b = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_{k_1}^{\alpha_{k_1}} q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots q_{k_2}^{\beta_{k_2}}$$

ومن جهة ثانية لنحلل العدد c إلى عوامله الأولية فنكتب

$$c = u_1^{\gamma_1} u_2^{\gamma_2} \ldots\ldots u_t^{\gamma_t}$$

فيكون

$$c^n = u_1^{n\gamma_1} u_2^{n\gamma_2} \ldots\ldots u_t^{n\gamma_t}$$

ولما كان $a.b = c^n$ ولما كان التحليل إلى العوامل يتم بشكل وحيد فقط فإن المساواة

$$p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_{k_1}^{\alpha_{k_1}} q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots q_{k_2}^{\beta_{k_2}} = u_1^{n\gamma_1}\, u_2^{n\gamma_2} \ldots\ldots u_t^{n\gamma_t}$$

تدل على أن كل عامل $u_k^{n\gamma_k}$ يقابل عاملاً واحداً فقط من الطرف الثاني مما يعني أن $k_1 + k_2 = t$ (عدد العوامل المختلفة في الطرف الأول يســـاوي عدد العوامل المختلفة في الطرف الثاني) وقوة أي عامل أي β_j أو α_i تساوي $n\gamma_k$ أي يمكن كتابة المقدار $a\ .\ b$ بعد إعادة ترتيب العوامل على النحو

$$a.b = p_1^{n\gamma_1} \dots\dots p_{k_1}^{n\gamma_{k_1}} q_1^{n\gamma_{k_1+1}} \dots\dots q_{k_2}^{n\gamma_t} = a_1^n . b_1^n$$

حيث $k_1 + k_2 = t$ و $a_1 = p_1^{\gamma_1} \dots\dots p_{k_1}^{\gamma_{k_1}}, b_1 = q_1^{\gamma_{k_1+1}} \dots\dots q_{k_2}^{\gamma_t}$

مبرهنة : إن جميع الحلول الصحيحة غير الصفرية لمعادلة فيثاغورث $x^2 + y^2 = z^2$

حيث y عدد زوجي و $1 = (x , y , z)$ تعطى بالعلاقات

$$x = (r^2 - s^2) , \quad y = 2rs, \quad z = (r^2 + s^2)$$

حيث s , r أعداد صحيحة غير صفرية و $1 = (s , r)$, s , r أحدهما فردي والآخر زوجي .

البرهان : بما أن y عدد زوجي فإن x عدد فردي وبالتالي z عدد فردي .

لنكتب $y = 2y_1$

ومن معادلة فيثاغورث نكتب $y^2 = 4y_1^2 = z^2 - x^2$

أي $y_1^2 = \frac{z+x}{2} . \frac{z-x}{2}$

إن $\frac{z+x}{2} , \frac{z-x}{2}$ أوليان نسبياً إذ لو فرضنا أن

$$(\frac{z+x}{2} , \frac{z-x}{2}) = d > 1$$

فإن d سيقسم مجموعهما وفرقهما أي يقسم z , x وهذا غير ممكن لأن $1 = (x , z)$ فإذا افترضنا أن x, y ,z غير سالبة ولاحظنا أن جداء العددين الصحيحين $\frac{z+x}{2} , \frac{z-x}{2}$ يساوي y_1^2 وطبقنا **التمهيدية (4)** أمكننا أن نكتب :

$$\frac{z+x}{2} = r^2, \frac{z-x}{2} = s^2$$

ومنه نجد أن :

$$x = r^2 - s^2, y = 2y_1 = 2rs, z = r^2 + s^2$$

وأخيراً ولما كان كل من z , x فردياً فإن s , r الأوليان نسبياً أحدهما فردي والآخر زوجي حتماً .

أي أمكن إيجاد ثلاثي فيثاغورث أولي بين الأعداد الصحيحة غير السالبة يحقق معادلة فيثاغورث بشرط $r^2 > s^2$ ومن جهة ثانية إذا عوضنا قيم x, y ,z في المعادلة (1) نجد :

$$x^2 + y^2 = (r^2 - s^2)^2 + 4r^2s^2 = (r^2 + s^2)^2 = z^2$$

أي أنها محققة من أجل جميع الأعداد الصحيحة s , r

وأخيراً إذا ضربنا قيم x, y ,z بالعدد الصحيح $k \neq 0$ فإننا نحصل على جميع ثلاثيات فيثاغورث وهو المطلوب .

مثال (1) : لنوجد جميع ثلاثيات فيثاغورث الأولية علماً أن : $x = 15$

الحل: لدينا $x = r^2 - s^2 = 15$ أي $(r - s)(r + s) = 15$

وقيم r , s الممكنة التي تحقق الطلب هي التي تحقق ما يلي :

$r+s=15$ و $r-s=1$ أو $r+s=5$ و $r-s=3$

بحل المجموعتين نجد :

$r=8$ و $s=7$ أو $r=4$ و $s=1$

وثلاثيات فيثاغورث المطلوبة هي : (15 , 8 , 17) و (15 , 112 , 113)

مثال (2): أثبت أنه إذا كان $(x\ ,y,z)$ ثلاثي فيثاغورث أولي فإن أحد الأعداد $x,y\ ,z$ يقبل القسمة على 3 .

الحل: بما أن الأعداد $x,y\ ,z$ هي ثلاثي فيثاغورث أولي فيمكن أن نكتب

$$x=r^2-s^2,\quad y=2rs,\quad z=r^2+s^2$$

حيث $r\ ,s$ عددان أوليان نسبياً أحدهما زوجي والثاني فردي فإننا نلاحظ أنه إذا كان $3|y$ تم المطلوب وإذا كان y ł 3 فإن 3 لا تقسم أياً من r أو s أي يمكن أن نكتب حسب خوارزمية القسمة :

$$r=3q+1 \quad \text{أو} \quad r=3q+2$$

$$s=3q_1+1 \quad \text{أو} \quad s=3q_1+2 \qquad \text{وَ}$$

ومنه فإن :

$$x=r^2-s^2=(9q^2+12q+4)-(9q_1^2+6q_1+1)=3M+3 \quad \text{و} \quad 3|x$$

أو $x=r^2-s^2=(9q^2+6q+6)-(9q_1^2+6q_1+1)=3M$ و $3|x$

مثال (3) : أثبت أن نصف قطر الدائرة الماسة داخلاً لأضلاع مثلث فيثاغورث هو عدد صحيح دوماً .

الحل: ليكن R نصف قطر الدائرة ، $x\ ,y$ طولا الضلعين القائمين في المثلث و z طول الوتر .

نحسب مساحة المثلث بطريقتين ونكتب :

$$S=\frac{1}{2}xy=\frac{1}{2}R(x+y+z) \qquad (1)$$

نعوض قيم $x,y\ ,z$ التالية :

$$x=k(r^2-s^2), y=2krs, z=k(r^2+s^2)$$

في العلاقة (1) ثم نحسب R فنجد :

$$R=\frac{xy}{x+y+z}=\frac{2k^2rs(r^2-s^2)}{2kz^2+2krs}=\frac{krs(r^2-s^2)}{r^2+rs}$$

$$R=\frac{krs(r-s)(r+s)}{r(r+s)}=ks(r-s)$$

وهو عدد صحيح دوماً .

تمارين

1) أوجد حلول المعادلات :

$56x + 72y = 40$
$24x + 138y = 18$
$221x + 91y = 117$
$84x - 438y = 165$

2) أوجد الحلول الموجبة للمعادلات

$30x + 17y = 300$
$158x - 57y = 7$
$54x + 21y = 906$
$123x + 360y = 99$

3) أوجد الحل الكامل للمعادلات

$2x + 11y = 5$
$18x - 21y = 15$
$2x + 12y = 6$

4) أوجد جميع ثلاثيات فيثاغورث التي فيها $y = 28$.

5) أثبت أنه إذا كان (x , y , z) ثلاثي فيثاغورث أولي فإن $12|x.y.z$

6) أوجد جميع الحلول الأولية الموجبة للمعادلة $x^2 + y^2 = z^2$ إذا كان y عدد زوجي وَ $0 < z < 90$.

7) أوجد دستور لتعيين ثلاثيات فيثاغورث الأولية التي تحقق ما يلي : y عدد زوجي و :

(a $z - x = 1$ أو $z - y = 1$

(b $z - x = 2$ أو $z - y = 2$

(c $z - x = p$ حيث p عدد أولي فردي

8) أوجد ثلاثيات فيثاغورث الأولية في الحالات :

(a $y = 24$ ***(b*** $x = 21$

(c $z = 125$ ***(d*** $y = 16$

الباب الثاني

الفصل الأول : التطابقات

الفصل الثاني : التطابقات الخطية

الفصل الثالث : التطابقات العددية وبعض الدوال الخاصة

الفصل الرابع : المراتب الجذور الأولية والأدلة

محاضرات د. يحيى

الفصل الأول

التطابقات

2-1 التطابقات (*Congruence*)

إن أول من تعرض لفكرة التطابق ووضع رمزها هو الرياضي الألماني فريدريك غاوس **(*F . gauss*)** (1855 - 1771 م) في كتاب الحساب .

وكان يقول : الرياضيات ملكة العلوم ونظرية الأعداد ملكة الرياضيات .

2-1-1 تعريف التطابق : ليكن $M, a, b \in Z$ و $m \in Z^+$ نقول إن العدد a يطابق العدد b بالمقاس m ونكتب $a \equiv b(modm)$ إذا كان $m|a-b$ أو $a - b = M.m$.

أما إذا كان $m \nmid a-b$ فإنا نقول إن a لا يطابق b بالمقاس m ونكتب $a \not\equiv b(modm)$.

2-1-2 صفوف البواقي :

رأينا أنه إذا كان m عدداً صحيحاً أكبر من الواحد و $n \in Z$ فإنه يوجد عددان وحيدان q , r بحيث يكون $n = mq + r, \ 0 \leq r < m$ إن الباقي r يمكن أن يأخذ أيا من القيم $r_i = 0,1,2,\dots,m-1$ لنضع جميع الأعداد الصحيحة التي باقي قسمها على m يساوي أحد الأعداد r_i في صف واحد نسميه صف الباقي r_i ، فنحصل بالتالي على m من هذه الصفوف ، ونلاحظ أنه إذا كان الفرق بين عددين صحيحين مضاعفاً لـ m فإنهما يقعان في صف واحد وأن الفرق بين أي عددين من صف واحد هو مضاعف لـ m . نسمي هذه الصفوف صفوف البواقي للعدد m .

مثال : ليكن $m = 6$ إن مجموعة بواقي القسمة على العدد 6 هي

$\{r = 0,1,2,3,4,5\}$ أي أن للعدد 6 ستة صفوف بواقي .

وصف الباقي $r = 0$ يحوي العناصر

$\{\dots\dots, -12, -6, 0, 6, 12, 18, \dots\dots\}$

وصف الباقي $r = 1$ هو :

$\{\dots\dots, -11, -5, 1, 7, 13, 19, \dots\dots\}$

وهكذا ...

ونلاحظ أن كل عدد صحيح يمكن أن ينتمي إلى باقي واحد فقط من هذه الصفوف .

فالعدد 31 مثلاً ينتمي إلى صف الباقي ($r = 1$) .

والعدد 500- ينتمي إلى صف الباقي $r = 4$ لأن $4 + (-84)\ 6 = -500$.

2-1-3 مجموعة البواقي التامة :

تعريف: نسمي مجموعة الأعداد الصحيحة A التي عدد عناصرها يساوي m والتي ينتمي كل عنصر منها إلى صف واحد فقط من صفوف بواقي العدد m مجموعة البواقي التامة بالمقاس m ، فالمجموعة $A = \{0,1,2,3,4\}$ هي مجموعة بواقي تامة بالمقاس 5 وكذا المجموعة $A_1 = \{0,6,-8,8,4\}$ حيث نلاحظ أن الصفر ينتمي إلى مجموعة البواقي $r = 0$ و 6 إلى مجموعة البواقي لـ $r = 1$ و -8 إلى مجموعة البواقي $r = 2$ و 8 إلى مجموعة البواقي $r = 3$ و 4 إلى مجموعة البواقي $r = 4$.

ويلاحظ أن مجموعة البواقي التامة بالمقاس m التي عناصرها $\{0,1,2,\ldots\ldots,m-1\}$ هي أبسط مجموعات البواقي التامة بالمقاس m ويطلق عليها أحياناً مجموعة البواقي التامة الصغرى .

نتيجة : من تعريف التطابق ينتج أنه إذا كان $a \equiv b(modm)$ فهذا يعني أن $a\ ,\ b$ ينتميان إلى صف واحد من صفوف البواقي بالمقاس m في حين $a \not\equiv b(modm)$ تعني أن $a\ ,\ b$ ينتميان إلى صفين مختلفين من صفوف بواقي m .

نتيجة : إن أي عدد صحيح n يطابق باقي قسمته على العدد m لأن :

$$n = mq + r \Rightarrow n - r = mq \Rightarrow m|n - r \Rightarrow n \equiv r(modm)$$

2-1-4 خواص التطابقات :

نفترض الأعداد $a_i, b_i, c, d, \ldots . \in Z$ و $m \in Z^+$

1) إن علاقة التطابق هي علاقة تكافؤ على مجموعة الأعداد الصحيحة .

البرهان :

- إذا كان $a\ ,b,c \in Z$ و $m \in Z^+$ فإن $a \equiv a(modm)$ لأن $m|a - a$.
- و $a \equiv b(modm) \Rightarrow b \equiv a(modm)$ لأنه إذا كان $m|a - b \Rightarrow m|b - a$
- و $a \equiv b(modm) \wedge b \equiv c(modm) \Rightarrow a \equiv c(modm)$

لأنه إذا كان $a - b = k_1 m \wedge b - c = k_2 m \Rightarrow a - c = (k_1 + k_2)m$

2) إذا كان $a \equiv b(modm)$ و $k \in Z$ فإن $ka \equiv kb(modm)$

لأن $a - b = M\ m$ فإذا ضربنا الطرفين بالعدد k نجد $k\ a - k\ b = (k\ M)\ m$

3) إذا كان $c \equiv d(modm) \wedge a \equiv b(modm)$

فإن $(modm) a \pm c \equiv b \pm d$

البرهان : لما كان $c-d=M_1m, a-b=M_2m$

فإن $(a-b)\pm(c-d)=(M_2\pm M_1)m$

أي $(a\pm c)-(b\pm d)=Mm, M=M_1\pm M_2$

ويمكن تعميم هذه الخاصـــة فنكتب : إذا كان $a_i\equiv b_i(modm)$ من أجل جميع القيم $i=1,2,\ldots,n$ فإن $\sum_1^n a_i\equiv\sum^n b_i(modm)$ ويمكن إثبات ذلك بطريقة الاستقراء الرياضي .

4) مبرهنة: إذا كان $c\equiv d(modm)\wedge a\equiv b(modm)$ فإن $ac\equiv bd(modm)$

البرهان : لدينا $a\equiv b(modm)\Rightarrow ac\equiv bc(modm)$

و $c\equiv d(modm)\Rightarrow bc\equiv bd(modm)$

أي $ac\equiv bd(modm)$ وهو المطلوب .

5) إذا كان $a\equiv b(modm)$ فإن $a^n\equiv b^n(modm)$ حيث $n\geq 0$.

البرهان : الخطوة الأساسية في الاستقراء : من أجل $n=0$ و $n=1$ العلاقة محققة

خطوة الاستقراء : لنفترض صحتها من أجل $n=k$ ولنثبت صحتها من أجل $n=k+1$

لذا نكتب : $a^k\equiv b^k(modm)$

وحسب الخاصة (4) نكتب : $a.a^k\equiv b.b^k(modm)$

الأمر الذي يثبت صحة العلاقة $a^{k+1}\equiv b^{k+1}(modm)$ المطلوبة.

أي أن العلاقة صحيحة $\forall n\geq 0$.

6) إذا كان $a\equiv b(modm)$ وإذا كان $f(x)=\sum_{i=0}^n a_ix^i$ حيث $0\leq i\leq n, a_i\in Z$

فإن : $f(a)\equiv f(b)(modm)$

البرهان :

بما أن $a\equiv b(modm)$ فإن $a^i\equiv b^i(modm)$ حســـب الخاصـــة (5) وكذا $a_ia^i\equiv a_ib^i(modm)$ أي $\sum_{i=0}^n a_ia^i\equiv\sum_{i=0}^n a_ib^i(modm)$ أي $f(a)\equiv f(b)(modm)$.

مثال : لدينا $2\equiv -4(mod6)$ فإذا كان $f(x)=x^2-x+5$ فإن

$f(2)=7, f(-4)=25, 7\equiv 25(mod6)\Rightarrow f(2)\equiv f(-4)(mod6)$.

7) مبرهنة : إذا كان $ka\equiv kb(modm)$ وإذا كان $d=(k,m)$ فإن $a\equiv b(mod\frac{m}{d})$.

البرهان : بما أن $d=(k,m)$ فيمكن أن نكتب : $k=k_0d, m=m_0d$

و $(k_0,m_0)=1$ وبما أن $ka\equiv kb(modm)$ فإن

$$k_0 d(a-b) = Mm_0 d \Leftarrow k(a-b) = Mm$$

ومنه $k_0(a-b) = Mm_0$ أي أن $m_0 | k_0(a-b)$ ولما كان $(k_0, m_0) = 1$

ينتج أن : $m_0 | a-b$ أي $a \equiv b(mod m_0)$ حيث $m_0 = \frac{m}{d}$

نتيجة (1) : ينتج من الخاصة السابقة أنه إذا كان $ka \equiv kb(modm)$ وكان $(k,m) = 1$ فإن $a \equiv b(modm)$ أي يمكن اختصار العامل المشترك بين طرفي تطابق إذا كان هذا العامل أولياً نسبياً مع المقاس .

مثال : $10 \equiv 6 mod 4$ ولكن $5 \not\equiv 3 mod 4$ لأن : $(10,6) = 2 \wedge (2,4) \neq 1$

في حين $77 \equiv -28(mod 15) \Leftarrow 11 \equiv -4(mod 15)$ لأن :

$$(-77, -28) = 7 \wedge (7,15) = 1$$

نتيجة (2) : إذا كان $ca \equiv cb(modp)$ حيث p عدد أولي لا يقسم c فإن $a \equiv b(modp)$ وذلك لأن $(a,p) = 1$ في هذه الحالة .

ملاحظة (1): إذا كان العامل المشترك $k \equiv 0(modm)$ فإن $(k,m) = m$ والاختصار يؤدي إلى النتيجة $a \equiv b(mod 1)$ وهي علاقة صحيحة مهما تكن الأعداد a , b .

ملاحظة (2): إذا كان $ab \equiv a.0(modm)$ و $(a,m) = 1$ فإن المبرهنة السابقة تعطي $b \equiv 0(modm)$. وإذا كان $ab \equiv a.0(modp)$ حيث p عدد أولي فإما أن يكون

$a \equiv 0(modp)$ أو $b \equiv 0(modp)$.

8) إذا كان $a \equiv b(modm)$ وكان $n|m$ فإن $a \equiv b(modn)$.

البرهان : لدينا $m|a-b$ و $n|m \Leftarrow n|a-b$ ومنه $a \equiv b(modn)$.

9) مبرهنة : إذا كان $a, b \in Z$ و $m_i \in Z^+$ حيث $i = 1,2,\ldots,k$

وإذا $a \equiv b(modm_i)$ فإن $a \equiv b(modm)$ حيث $m = lcm(m_1, m_2, \ldots, m_k)$

البرهان : لدينا $m_i | a-b$ ولما كان $m_i | m$ من أجل $1 \leq i \leq k$

فإن $a - b$ مضاعف مشترك للأعداد m_i فهو مضاعف للمضاعف المشترك الأصغر m أي $m|a-b$ و $a \equiv b(modm)$.

نتيجة : إذا كانت m_i أولية نسبياً مثنى مثنى فإنها أولية نسبياً و $m = m_1.m_2.\ldots.m_k$ و $a \equiv b(modm_i)$ من أجل $i = 1,2,\ldots,k \Leftarrow a \equiv b(modm_1.m_2.\ldots.m_k)$.

وبحالة خاصة إذا كان $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ هو الشكل القانوني لـ m فإن :

$a \equiv b(modm) \Leftarrow a \equiv b(modp_i^{\alpha_i})$ حيث $i = 1,2,\ldots,k$

10) مبرهنة : إذا كان $r \geq 1$ و $a \equiv b(mod p^r)$ ، a , b , r أعداد صحيحة و $r \geq 1$ و p عدد أولي ، فإن : $a^{p^s} \equiv b^{p^s}(mod p^{r+s})$ حيث $s \geq 0$.

البرهان : بطريقة الاستقراء الرياضي على s :

الخطوة الأساسية : من أجل $s = 0$ نجد أن العلاقة صحيحة

خطوة الاستقراء : لنفترض أن العلاقة صحيحة من أجل $s = k > 0$ ولنثبت صحتها من أجل $s = k+1$ فنكتب : $a^{p^k} \equiv b^{p^k}(mod p^{r+k}) \Rightarrow a^{p^k} = b^{p^k} + Mp^{r+k}$

نرفع الطرفين إلى القوة p فنجد :

$$(a^{p^k})^p \equiv a^{p^{k+1}} = (b^{p^k} + Mp^{r+k})^p$$

$$= b^{p^{k+1}} + \frac{p}{1}(b^{p^k})^{p-1}(Mp^{r+k}) + \frac{p(p-1)}{2!}(b^{p^k})^{p-2}(Mp^{r+k})^2 +$$

$$+\ldots. + M^p(p^{r+k})^p$$

ولما كانت قوى p بدءاً من الحد الثاني هي $r + k + 1$، $2r + 2k + 1$,.... وكلها أكبر أو تساوي $r + k + 1$ فإن جميع الحدود تطابق الصفر بالمقاس p^{r+k+1} أي :

$a^{p^{k+1}} = b^{p^{k+1}}(mod p^{r+k+1})$ أي أن المبرهنة صحيحة من أجل $s \geq 0$.

مثال(1) : لنثبت أن الفرق بين أي عدد صحيح N بالنظام العشري ومجموع أرقامه يقبل القسمة على 9

الإثبات : إن العدد N يكتب بالنظام العشري كما نعلم على النحو :

$$N = a_n 10^n + a_{n-1}10^{n-1} + \ldots\ldots + a_1 10 + a_0$$

ولما كان $10 \equiv 1(mod 9)$ فإن $10^k = 1^k \equiv 1(mod 9)$ من أجل $k \geq 0$

وبالتالي : $\sum_{k=0}^{n} a_k 10^k \equiv \sum_{0}^{n} a_k . 1(mod 9)$

أي $N = a_n + a_{n-1} + \ldots\ldots + a_2 + a_1 + a_0 (mod 9)$

ومنه $9 | N - \sum_{0}^{n} a_k \quad \Rightarrow \quad N - (\sum_{0}^{n} a_k) = 0(mod 9)$

وعلى سبيل المثال : 3741 - (3+7+4+1) = 3726 = 9 . (414)

تمرين(2) : من أجل $n \in Z^+$ أثبت أن $15 | 2^{4n} - 1$

الحل: لدينا $2^4 \equiv 16 \equiv 1(mod 15) \Leftarrow (2^4)^n \equiv 1(mod 15)$

أي $15 | 2^{4n} - 1$

تمرين(3) : من أجل $n \geq 0$ أثبت أن $8 | 3^{2n} + 7$

الحل: إن $3^2 \equiv 9 \equiv 1(mod\ 8) \Leftarrow 3^{2n} \equiv 1(mod\ 8) \Leftarrow 3^{2n} + 7 \equiv 1 + 7(mod 8)$

$3^{2n} + 7 \equiv 0(mod 8)$ أي $8 | 3^{2n} + 7$

تمرين(4) : أوجد أصغر عدد صحيح موجب k يحقق العلاقة :

$$31|33(26)^2 - k$$

الحل: العدد المطلوب هو k باقي قسمة $33(26)^2$ على 31 لذا نكتب :

$$33(26)^2 \equiv k(mod31)$$

ولما كان $33 \equiv 2(mod31)$ و $26 \equiv -5(mod31)$

فإن $(26)^2 \equiv 25(mod31)$

أي أن $33(26)^2 \equiv 50(mod31)$

وأخيراً $33(26)^2 \equiv 19(mod31)$ و $k = 19$

تمرين (5) : أوجد باقي قسمة $\sum_1^{1000} k!$ على 24

الحل: نعلم أن $4! = 24$ و $5! = 5 (4!)$ ..... لذا نكتب

$$\sum_1^{1000} k! = 1 + 2! + 3! + 4! + 5! + \ldots\ldots + 1000!$$

ولما كانت الحدود بدءاً من $4!$ تطابق الصفر بالمقاس 24 نجد :

$$\sum_1^{1000} k! = 1 + 2 + 6 \equiv 9(mod24)$$

وباقي القسمة هو 9 .

الفصل الثاني
التطابقات الخطية

2-2 التطابقات الخطية *Linear congruences*

2-2-1 تعريف : التطابق الخطي هو معادلة من الشكل :

$$ax \equiv b(modm) \qquad (1)$$

حيث a , b أعداد صحيحة معلومة x عدد صحيح مجهول و m عدد صحيح أكبر من الواحد وحل التطابق الخطي هو إيجاد قيمة العدد الصحيح x_0 الذي يحقق المعادلة $ax_0 \equiv b(modm)$ ومن تعريف التطابق نعلم أن هذا التطابق يتحقق إذا وفقط إذا كان $m|ax_0 - b$ أي إذا وفقط إذا وجد عدد y_0 بحيث $ax_0 - b = my_0$ أي أن مسألة حل تطابق خطي تؤول إلى مسألة إيجاد الحلول الكاملة لمعادلة ديوفانتس الخطية $ax - my = b$.

ملاحظة : نعد الحلول المتطابقة بالمقاس m للتطابق الخطي حلاً واحداً

فعلى سبيل المثال : إن $x = 3$ و $x = -9$ كل منهما يحقق التطابق $3x \equiv 9(mod12)$ و $3x \equiv -9(mod12)$ لذا نعدهما حلاً واحداً ونعني بعدد حلول تطابق عدد الحلول غير المتطابقة بالمقاس m .

2-2-2 مبرهنة : يكون للتطابق الخطي $ax \equiv b(modm)$ حلاً إذا وفقط إذا كان $d|b$ حيث $d = g\,c\,d(a,m)$ ، وإذا كان $d|b$ فإن للتطابق d من الحلول غير المتطابقة بالمقاس m.

البرهان : لقد بينا أن حل التطابق الخطي يكافىء حل معادلة ديوفانتس الخطية

وقد أثبتنا أن الشرط اللازم والكافي كي يكون للمعادلة حل هو أن يكون $d|b$ كما أثبتنا أنه إن كان x_0, y_0 هو حل خاص لمعادلة ديوفانتس فإن الحل الكامل لها هو :

$$x = x_0 + \frac{m}{d}t \quad y = y_0 - \frac{m}{d}dt \in Z$$

لنأخذ الحلول المقابلة لقيم t التالية : $t = 0,1,2,\ldots,d-1$

أي لنكتب : $x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots\ldots\ldots\ldots\ldots, x_0 + \frac{(d-1)}{d}m$

ولنثبت أن هذه الحلول كلها غير متطابقة بالمقاس m إذ لو تطابق حلان موافقان للقيمتين t_2, t_1 لأمكن أن نكتب : $x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2(modm) 0 \leq t_1 < t_2 \leq d-1$

ومنه $\frac{m}{d}t_1 \equiv \frac{m}{d}t_2(modm)$

ولدينا $(\frac{m}{d}, m) = \frac{m}{d}$ وحسب خواص التطابقات يمكن اختصار العامل المشترك لنحصل على $t_1 \equiv t_2 (mod d)$ وهذا تناقض لأن قيم t أي الأعداد $t = 0,1,2,\ldots,d-1$ كلها غير متطابقة بالمقاس d .

لنثبت أخيراً أن أي حل من الحلول $(x_0 + \frac{m}{d}t)$ حيث t أكبر أو تساوي d يطابق بالمقاس m واحداً من الحلول السابقة والتي عددها يساوي d .

في الحقيقة بما أن $t \geq d$ فهي تكتب على النحو $t = qd + r$ حيث $0 \leq r < d$

أي $0 \leq r \leq d-1$ ، نعوض في عبارة الحل فنجد :

$$x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}(qd + r) = x_0 + mq + \frac{m}{d}r$$

ومنه $x_0 + \frac{m}{d}t \equiv (x_0 + \frac{m}{d}r)(mod m)$

و $x_0 + \frac{m}{d}r$ هو أحد الحلول المذكورة ، وهو المطلوب .

نتيجة : إذا كان $(a\ ,\ m) = 1$ فإن للتطابق الخطي $ax \equiv b(mod m)$ حل وحيد .

وإذا كان المقاس عدداً أولياً p وكان $p \nmid a$ فإن للتطابق $ax \equiv b(mod p)$ حل وحيد أيضاً .

تمرين (1) : أوجد حلول التطابق $6x \equiv 2(mod 9)$

الحل: نلاحظ أن $(6,9) = 3$ و $3 \nmid 2$ وليس للتطابق أي حل .

تمرين (2) : أوجد حلول التطابق $6x \equiv 21(mod 30)$

الحل: لدينا: $(9,30) = 3$ و $3|21$ أي أن للتطابق ثلاثة حلول غير متطابقة بالمقاس 30

طريقة أولى : نختصر طرفي التطابق على 3 فنجد : $3x \equiv 7(mod 10)$

ولما كان $(3,10) = 1$ فلهذا التطابق حل وحيد بالمقاس 10 ، وبتعويض x بأحد الأعداد من 0 إلى 9 نجد أن : $x = 9$ يحقق التطابق أي

$x_0 \equiv 9(mod 10)$ وهو يحقق التطابق الأصلي $9x \equiv 21(mod 30)$

ونحصل على الحلول الثلاثة بكتابة $x \equiv x_0 + 10t$ حيث $t = 0,1,2$

وتكون الحلول : $x \equiv 9(mod 30)$ و $x \equiv 19(mod 30)$ و $x \equiv 29(mod 30)$

طريقة ثانية : يمكن إيجاد الحل بالعودة إلى حل معادلة ديوفانتس المكافئة

للتطابق فنبحث عن حلول المعادلة : $9x - 30y = 21$ بتطبيق خوارزمية القسمة فنجد :

$$30 = 9 \times 3 + 3$$
$$9 = 3 \times 3 + 0$$

وبالتالي

$$3 = 30 - 9 \times 3$$
$$21 = 9(-21) - 30(-7)$$

أي $x_0 = -21$ هو حل خاص والحلول الكاملة هي :

$$x = -21 + \frac{30}{3}t = -21 + 10t, t = 0,1,2$$

أي الحلول غير المتطابقة بالمقاس 30 هي :

$$x \equiv -1(mod30) \text{ و } x \equiv -11(mod30) \text{ و } x \equiv -21(mod30)$$

وهي تطابق الحلول الموجبة (9,19,29) حيث $-1 \equiv 29$ و $-11 \equiv 19$ و $-21 \equiv 9$ بالمقاس 30.

2-2-3 الكسور البسيطة المستمرة المنتهية :

إن إيجاد حلول التطابقات الخطية باستخدام خوارزمية اقليدس أو بالتجريب تصبح طويلة أو متعذرة حين يكون المقاس عدداً كبيراً لذا تستخدم طريقة الكسور البسيطة المستمرة التي ستشرحها في هذه الفقرة لحل التطابقات الخطية وحل معادلات ديوفانتس الخطية .

- **تعريف** : الكسور البسيطة المستمرة المنتهية هي كسور تكتب كما يلي :

$$\frac{A}{B} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}}$$

حيث $a_2, a_3, \ldots, a_n \in Z^+, a_i \in Z$

ويرمز : $\frac{A}{B} =< a_1, \ldots, a_n >$

مثال (1) : $-2 + \frac{1}{1+\frac{1}{3}} = -2 + \frac{1}{\frac{4}{3}} = -2 + \frac{3}{4} = -\frac{5}{4} =< -2,1,3 >$

مثال (2) :

$$\frac{32}{19} = 1 + \frac{13}{19} = 1 + \frac{1}{\frac{19}{13}} = 1 + \frac{1}{1+\frac{6}{13}} = 1 + \frac{1}{1+\frac{1}{\frac{13}{6}}}$$

$$= 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6}}} =< 1,1,2,6 >$$

يسمى العدد a_k النسبة الجزئية من المرتبة k وإذا توقفنا بالكسر عند النسبة الجزئية فإننا نحصل على التقريب من المرتبة k : c_k ونكتب :

$$c_1 = a_1, c_2 = a_1 + \frac{1}{a_2} \ldots\ldots\ldots c_k = a_1 + \frac{1}{a_2 + \ldots\ldots + \frac{1}{a_k}}$$

ففي المثال (2) يمكن أن نكتب :

$$c_1 = 1, c_2 = 1 + \frac{1}{1} = 2, c_3 = 1 + \frac{1}{1+\frac{1}{2}} = \frac{5}{3}$$

$$c_4 =< 1,1,2,6 >= \frac{32}{19}$$

2-2-4 مبرهنة : إذا كان لدينا الكسر المستمر المنتهي $< a_1, a_2, \ldots, a_n >$ وأدخلنا الرموز التالية :

$$q_1 = 1\,, \quad p_1 = a_1$$
$$q_2 = a_2, \quad p_2 = a_1 a_2 + 1$$
$$q_3 = a_3 q_2 + q_1, \; p_3 = a_3 p_2 + p_1$$
$$\ldots\ldots \qquad \ldots\ldots$$
$$q_i = a_i q_{i-1} + q_{i-2}, p_i = a_i p_{i-1} + p_{i-2}$$

فإن التقريب من المرتبة n أي c_n للكسر يساوي : $c_n = \frac{p_n}{q_n}$ عندما $n \geq 1$

الإثبات : نتبع طريقة الاستقراء الرياضي :

1- الخطوة الأساسية : نلاحظ أن

$c_1 = \frac{p_1}{q_1} = \frac{a_1}{1}$, $c_2 = \frac{p_2}{q_2} = \frac{a_2 a_1 + 1}{a_2}$ والعلاقة صحيحة .

2- لنفترض أن العلاقة صحيحة من أجل $n = k$

أي لنفترض أن $c_k = \frac{p_k}{q_k}$

ولنثبت صحتها من أجل $n = k + 1$ أي لنثبت أن : $c_{k+1} = \frac{p_{k+1}}{q_{k+1}}$:

نعلم أن : $c_k = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ldots\ldots + a_k}}}$

و

$$c_{k+1} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ldots\ldots\ldots + a_k + \frac{1}{a_{k+1}}}}}$$

أي أن c_{k+1} يختلف عن c_k بأن الحد الأخير في الكســـر هو $a_k + \frac{1}{a_{k+1}}$ بدلاً عن a_k لذا نعوض في عبارة c_k كل a_k بـ $a_k + \frac{1}{a_{k+1}}$ فنجد :

$$c_{k+1} = \frac{\left(a_k + \frac{1}{a_{k+1}}\right)p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right)q_{k-1} + q_{k-2}} = \frac{\{(a_k.a_{k+1}+1)p_{k-1} + a_{k+1}p_{k-2}\} \quad /_{a_{k+1}}}{\{(a_k.a_{k+1}+1)q_{k-1} + a_{k+1}q_{k-2}\} \quad /_{a_{k+1}}}$$

$$c_{k+1} = \frac{a_{k+1}(a_k.p_{k-1}+p_{k-2})+p_{k-1}}{a_{k+1}(a_k.q_{k-1}+q_{k-2})+q_{k-1}} = \frac{a_{k+1}p_k+p_{k-1}}{a_{k+1}q_k+q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}$$

أي أنه إذا كانت المبرهنة صحيحة من أجل $n = k$ فهي صحيحة من أجل $n = k + 1$ وبالتالي فهي صحيحة من أجل الأعداد الصحيحة الموجبة

2-2-5 مبرهنة : من أجل $n \geq 2$ فإن $p_n q_{n-1} - p_{n-1}q_n = (-1)^n$.

البرهان : بالاستقراء الرياضي :

الخطوة الأساسية : لما كان : $q_1 = 1, q_2 = a_2, p_1 = a_1 \quad , p_2 = a_2a_1 + 1$

فإننا نلاحظ أن المبرهنة صحيحة من أجل $n = 2$ لأن :

$$p_2q_1 - p_1q_2 = (a_2a_1 + 1)(1) - a_1a_2 = 1 = (-1)^2$$

خطوة الاستقراء : لنفترض أن المبرهنة صحيحة من أجل $n = k \geq 2$ ولنثبت صحتها من أجل $n = k + 1$ لذا نكتب :

$$p_{k+1}q_k - p_kq_{k+1} = (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k-1})$$
$$= -(p_kq_{k-1} + p_{k-1}q_k) = -(-1)^k = (-1)^{k+1}$$

أي أن المبرهنة صحيحة من أجل $n \geq 2$.

نتيجة : إن p_n و q_n أوليان نسبياً .

الإثبات : إذا كان $(p_n, q_n) = d > 1$ أي إذا كان : $d|p_n \ \wedge \ d|q_n$

فإن $d|p_nq_{n-1} - p_{n-1}q_n$ أي $d|1$ وبالتالي $d = 1$

- سنوضح عملياً كيفية الاستفادة من الكسور البسيطة في إيجاد حلول التطابقات الخطية :

تمرين (1): لنوجد حل التطابق $79x \equiv 3(mod103)$ بطريقة الكسور المستمرة .

إن إيجاد حلول التطابق يكافىء البحث عن حلول معادلة ديوفانتس التالية :

$$79x + 103y = 3$$

لذا نبحث أولاً عن حل المعادلة $79x + 103y = 1$ فنكتب الكسر $\frac{79}{103}$ على شكل كسر بسيط مستمر :

$$\frac{79}{103} = 0 + \frac{1}{1+\frac{24}{79}} = 0 + \frac{1}{1+\frac{1}{3+\frac{7}{24}}} = 0 + \frac{1}{1+\frac{1}{3+\frac{1}{\frac{24}{7}}}} = 0 + \frac{1}{1+\frac{1}{3+\frac{1}{3+\frac{1}{2+\frac{1}{3}}}}}$$

أي أن $\frac{79}{103} =< 0,1,3,3,2,3 >$

و $a_1 = 0, a_2 = 1, a_3 = 3, a_4 = 3, a_5 = 2, a_6 = 3$

$$p_1 = 0,\ p_2 = 1,\ q_1 = 1,\ q_2 = 1$$

و $c_1 = \frac{p_1}{p_2} = 0\ ,\ c_2 = \frac{p_2}{q_2} = 1$

$$c_3 = \frac{a_3p_2+p_1}{a_3q_2+q_1} = \frac{3}{4} = \frac{p_3}{q_3},\quad c_4 = \frac{a_4p_3+p_2}{a_4q_3+q_2} = \frac{10}{13} = \frac{p_4}{q_4}$$
$$c_5 = \frac{a_5p_4+p_3}{a_5q_4+q_3} = \frac{23}{30} = \frac{p_5}{q_5},\quad c_6 = \frac{a_6p_5+p_4}{a_6q_5+q_4} = \frac{79}{103} = \frac{p_6}{q_6}$$

نطبق المبرهنة الثانية فنجد :

$$p_6q_5 - p_5q_6 = 79 \times 30 - 103 \times 23 = 1$$

أي $79(90) + 103(-69) = 3 \Rightarrow x_0 = 90, y_0 = -69$

والحل الكامل للتطابق هو: $x = x_0 + 103t = 90 + 103t$

أي : $x \equiv 90(mod103)$.

تمرين (2) : لنوجد حل التطابق : $187x \equiv 2(mod503)$

نوجد الكسر البسيط المستمر للكسر $\frac{187}{503}$ فنجد : $\frac{187}{503} =< 0,2,1,2,4,2,6 >$

نوجد التقريبات المتتالية :

$$c_1 = \frac{0}{1} = 0,\quad c_2 = \frac{1}{2}\qquad c_3 = \frac{1}{3}\ c_4 = \frac{3}{8}$$
$$c_5 = \frac{13}{35} = \frac{p_5}{q_5},\quad c_6 = \frac{29}{78} = \frac{p_6}{q_6}\ ,\quad c_7 = \frac{187}{503} = \frac{p_7}{q_7}$$

وبالتالي $p_7q_6 - p_6q_7 = (-1)^7 \Rightarrow 187(78) - 503(29) = -1$

أي $187(-156) + 503(58) = 2$

والحل المطلوب هو : $x \equiv -156(mod503) \equiv 347(mod503)$

2-2-6 النظير الضربي

تعريف : نقول إن a^* هو النظير الضربي للعدد الصحيح a بالمقاس m إذا كان $a.a^* \equiv 1(modm)$ نلاحظ أنه ليس بالضرورة أن يوجد لكل عدد صحيح نظير ضربي بالمقاس m إذ مثلاً لا يوجد نظير ضربي للعدد 2 بالمقاس 4 لأن التطابق $2x \equiv 1(mod4)$ ليس له حل لأن $(2,4) = 2$ و $2 \nmid 1$ وبشكل عام لا يوجد نظير ضربي لأي عدد زوجي إذا كان المقاس زوجياً .

2-2-7 مبرهنة : يكون للعدد a نظير ضربي بالمقاس m إذا وفقط إذا كان $(a, m) = 1$.

الإثبات : في الحقيقة نعلم أن الشرط اللازم والكافي كي يكون للتطابق $ax \equiv 1(modm)$ حل هو أن يكون d القاسم المشترك الأعظم للعددين a , m قاسما للواحد وهذا لا يصح إلا عندما $d = 1$ أي $(a, m) = 1$.

تمرين (1) : عين النظير الضربي للعدد 17 بالمقاس 25 :

الحل : لنوجد حل التطابق $17x \equiv 1mod25$ فنجد

$$1 = 17(3) + 25(-2) \Rightarrow 17 \times 3 \equiv 1mod25$$

والعدد 3 هو النظير الضربي المطلوب .

تمرين (2) : أوجد النظير الضربي للعدد 71 بالمقاس 55 :

الحل : لنوجد حل التطابق $71x \equiv 1(mod55)$ بطريقة الكسور البسيطة المستمرة فنكتب :

$$\frac{71}{55} = 1 + \frac{1}{3+\frac{1}{2+\frac{1}{3+\frac{1}{2}}}} =< 1,3,2,3,2 >$$

ونحسب c_k فنجد :

$$c_1 = 1, c_2 = \frac{4}{3}, c_3 = \frac{9}{7}, c_4 = \frac{31}{24} = \frac{p_4}{q_4}, c_5 = \frac{71}{55} = \frac{p_5}{q_5}$$

ومنه $71(24) - 55(31) = -1 \Rightarrow 71(-24) + 55(31) = 1$

والنظير للعدد 71 بالمقاس 55 هو -24 أي : $71^* \equiv -24(mod55)$

2-2-8 حل جملة تطابقات خطية :

تكتب جملة التطابقات الخطية على النحو : $b_i x \equiv a_i(modm_i)$

نقول إن العدد الصحيح x هو حل مشترك لجملة التطابقات إذا حقق جميع هذه التطابقات معاً .

ونلاحظ ما يلي :

1- إذا لم يكن لأحد التطابقات ، حل فليس لجملة التطابقات حل .

2- إذا كان لكل من التطابقات حل فليس بالضرورة أن يكون لجملة التطابقات حل مشترك .

على سبيل المثال :

إن لكلٍ من التطابقين $3x \equiv 2(mod4)$ و $9x \equiv 3(mod12)$ حل ،

ونلاحظ أن $x \equiv 2(mod4)$ يحقق التطابق الأول ولا يحقق التطابق الثاني كما أن $x \equiv 3(mod4)$ يحقق التطابق الثاني $3x \equiv 1(mod4)$ ولا يحقق التطابق الأول وليس للتطابقين حل مشترك .

2- 2-9 مبرهنة الباقي الصينية : (*The Chinese remainder theorem*)

هي وسيلة لحل مسألة إيجاد عدد صحيح علمت بواقي قسمته على عدة أعداد معلومة وظهرت هذه المسألة عند علماء الصين في الألف الأول قبل الميلاد كما وجدت في أعمال بعض اليونانيين من حوالي 100 قبل الميلاد ونص المبرهنة هو :

المبرهنة : إذا كانت المقاسات $m_1 , m_2, \ldots, m_k$ أولية نسبياً مثنى مثنى فإنه

يوجد لجملة التطابقات الخطية :

$$x \equiv a_1(modm_1)$$
$$x \equiv a_2(modm_2)$$
$$\ldots\ldots\ldots\ldots$$
$$x \equiv a_k(modm_k)$$

حل وحيد بالمقاس $m = m_1.m_2.\ldots\ldots m_k$

البرهان : نكتب $M_i = \frac{m}{m_i}, i = 1,2,\ldots\ldots,k$

إن $(M_i, m_i) = 1$ لذا يوجد للتطابق $M_i m_i^{/} \equiv 1(modm_i)$ حل من أجل $i = 1,2,\ldots,k$.

أي يوجد للعدد M_i نظير ضربي بالمقاس m_i نسميه $m_i^{/}$.

لنكتب العدد x على النحو :

$$x = m_1^{/}M_1a_1 + m_2^{/}M_2a_2 + \ldots\ldots\ldots + m_k^{/}M_ka_k$$

إن العدد x هو حل لكل من التطابقات في الجملة المدروسة لأن $m_i | M_j$ عندما $i \neq j$ أي أن $M_j \equiv 0(modm_i)$ من أجل كل $i \neq j$ وبالتالي نجد :

$$x = m_i^{/}M_ia_i \equiv a_i(modm_i), \quad 1 \leq i \leq k$$

وx بالتالي هو حل مشترك لجملة التطابقات .

لنثبت الآن أن x هو الحل الوحيد بالمقاس m لذا نفترض أن $x^{/}$ و x حلان مختلفان لجملة التطابقات أي أن :

$x \equiv x' \equiv a_i(mod m_i)$ من أجل كل i ، $1 \le i \le k$ أي أن : $m_i | x - x'$ ولما كان m هو المضاعف المشترك الأصغر للأعداد m_i فإن $m | x - x'$ و $x = x'(mod m)$.

مثال (1) : أوجد أصغر عدد صحيح باقي قسمته على 6 يساوي 2 وباقي قسمته على 5 يساوي 3 وباقي قسمته على 11 يساوي 7 .

الحل: إن العدد المطلوب هو الحل المشترك للتطابقات :

$$x \equiv 2(mod 6$$
$$x \equiv 3(mod 5)$$
$$x \equiv 7(mod 11)$$

نلاحظ أن المقاسات 11 , 5 , 6 أولية نسبياً فيما بينها مثنى مثنى ولجملة التطابقات حل وحيد .

نكتب

$$m = (6)(5)(11) = 330 \Rightarrow M_1 = (5)(11), M_2 = (6)(11), M_3 = (6)(5) = 30$$

نوجد النظائر الضربية لـ M_1, M_2, M_3 بحل التطابقات .

$$55m_1' \equiv 1(mod 6), \quad 66m_2' \equiv 1(mod 5), \quad 30m_3' \equiv 1(mod 11)$$
$$m_1' \equiv 1(mod 6), \quad m_2' \equiv 1(mod 5), \quad m_3' \equiv -4(mod 11)$$

والحل المشترك لجملة التطابقات هو :

$$x \equiv 1(55)(2) + 1(66)(3) + (-4)(30)(7)(mod 330)$$
$$x \equiv 128(mod 330)$$

مثال (2) : أوجد حل التطابق $19x \equiv 1(mod 140)$ باستخدام مبرهنة الباقي الصينية :

الحل: لما كان $x = 140 = (4)(5)(7)$ فإن التطابق المعطي يكافىء جملة التطابقات :

$$19x \equiv 1(mod 4)$$
$$19x \equiv 1(mod 5)$$
$$19x \equiv 1(mod 7)$$

والمقاسات 4 , 5 , 7 أولية نسبياً مثنى مثنى ولهذه الجملة حل لإيجاده نكتب :

$$M_3 = 20, M_2 = 28, M_1 = 35$$

وحلول التطابقات :

$$35m_1' \equiv 1(mod 4) \Rightarrow m_1' = -1$$
$$28m_2' \equiv 1(mod 5) \Rightarrow m_2' = 2$$
$$20m_3' \equiv 1(mod 7) \Rightarrow m_3' = -1$$

والحل المشترك :

$$x \equiv (35)(-1)(3) + (28)(2)(4) + (20)(-1)(3) \equiv 59(mod 140)$$

وهو حل التطابق المطلوب .

مثال (3) : المطلوب إيجاد الحل المشترك لجملة التطابقات التالية :

$$x \equiv 10(mod24)$$
$$x \equiv 50(mod88)$$
$$x \equiv 28(mod99)$$

الحل : نلاحظ أن المقاسات غير أولية نسبياً ونلاحظ أن :

$$24 = (3)(8) \ ، \ 88 = (8)(11) \ ، \ 99 = (9)(11)$$

أي $(88,99) = 11, (24,99) = 3, (24,88) = 8$

إن حل التطابق الأول يكافىء حل جملة التطابقين $x \equiv 10(mod3)$ (1)

(2) $x \equiv 10(mod8)$

كما أن حل التطابق الثاني يكافىء حل جملة التطابقين $x \equiv 50(mod8)$ (3)

(4) $x \equiv 50(mod11)$

و حل التطابق الثالث يكافىء حل جملة التطابقين $x \equiv 28(mod9)$ (5)

(6) $x \equiv 28(mod11)$

وحل جملة التطابقات الأولى يكافىء حل جملة التطابقات الست الأخيرة ولكن نلاحظ :

أن $2 \equiv 10 \equiv 50(mod8)$ أي أن التطابق (2) هو ذات التطابق (3)

وأن $6 \equiv 50 \equiv 28(mod11)$ أي أن التطابق (4) هو ذات التطابق (6)

كما نلاحظ أن $1 \equiv 10 \equiv 28(mod9)$. وكل حل للتطابق (5) يحقق التطابق (1) لأن $3|9$

أي أن إيجاد حل جملة التطابقات المعطاة يؤول إلى إيجاد حل جملة التطابقات الثلاث :

$$x \equiv 2(mod8)$$
$$x \equiv 6(mod11)$$
$$x \equiv 1(mod9)$$

نلاحظ الآن أن 11 , 9 , 8 أولية نسبياً مثنى مثنى لذا يمكن إيجاد الحل الوحيد لجملة التطابقات فنجد :

$$m = (8)(11)(9) = 792 \quad , \quad M_1 = 99, M_2 = 72, M_3 = 88$$

ومنه $m_1' \equiv 3(mod8), \ m_2' \equiv 2(mod11), \ m_3' \equiv 4(mod9)$

والحل المشترك المطلوب :

$$x \equiv (3)(99)(2) + (2)(72)(6) + (4)(88)(1) \equiv 1810(mod792)$$
$$x \equiv 226(mod792)$$

وأخيراً سنورد المبرهنة التالية دون برهان

مبرهنة : يوجد لجملة التطابقات :

$$x \equiv a_1(modm_1)$$
$$x \equiv a_2(modm_2)$$
$$\ldots\ldots\ldots\ldots$$
$$x \equiv a_k(modm_k)$$

حل مشترك إذا وفقط إذا كان : $a_i \equiv a_j(modd_{ij})$ حيث : $d_{ij} = (m_i, m_j)$

و $i < j$ و $j = 1,2,\ldots\ldots\ldots,k, i = 1,2,\ldots\ldots\ldots,k$

وتسمى جملة التطابقات التي تحقق الشرط $a_i \equiv a_j(modd_{ij})$: جملة منسجمة .

10-2-2 مبرهنة فيرما الصغرى : ((***Fermat's theorem***))

لقد وضـــع فيرما ((*Pierre de Fermat* (1601-1665))).هذه المبرهنة عام 1640 و أول إثبات لها تم من قبل اولر بعد مئة عام .

نص المبرهنة : إذا كان p عدداً أولياً و $p \nmid a$ فإن $a^{p-1} \equiv 1(modp)$.

البرهان : لنكتبِ مضاعفات العدد الصحيح a التالية :$A_1 = \{1a, 2a, 3a, \ldots., (p-1)a\}$

نلاحظ أن هذه الأعداد غير متطابقة فيما بينها بالمقاس p ،

إذ لو كان : $ra \equiv sa(\ modp)$, $1 \leq r < s \leq p-1$ لاســـتطعنا اختصـــار a لأن $(a,p) = 1$ مما يؤدي إلى العلاقة $r \equiv s(modp)$ وهذا مســـتحيل ، كما أن عناصـــر المجموعة A_1 أولية نســـبياً مع p لذا فإن كل عنصـــر من عناصـــر المجموعة A_1 يطابق بالمقاس p عنصـراً واحداً من عناصـر المجموعة : $A = \{1,2,3,\ldots., p-1\}$ مما يدل على أن جداء عناصـر A_1 يساوي جداء عناصر المجموعة A الأمر الذي يعطي :

$$a.2a.3a.\ldots\ldots(p-1)a \equiv 1.2.3.\ldots\ldots(p-1)(modp)$$

ولما كان العدد الأولي p لا يقسم أياً من الأعداد $1,2,\ldots\ldots,(p-1)$ فهو لا يقسم جداءها لذا يمكن اختصار $(p-1)!$ من الطرفين لنحصل على : $a^{p-1} \equiv 1(modp)$

- **نتيجة (1) :** يمكن صياغة المبرهنة السابقة كما يلي :

إذا كان p عدداً أولياً فإن $a^p \equiv a(modp)$ من أجل أي عدد صحيح a .

الإثبات : إذا كان $p \nmid a$ فإن $(p,a) = 1$ ونختصر الطرفين على a لنحصل

على$a^{p-1} \equiv 1(modp)$ والعلاقة صحيحة .

أما إذا كان $p|a$ فإن $a^p \equiv 0 \equiv a(modp)$ والعلاقة صحيحة .

– **ملاحظة :** إن لمبرهنة فيرما هذه تطبيقات شتى وتعد أساساً لكثير من بحوث نظرية الأعداد .

تمرين : أثبت أن : $5^{38} \equiv 4(mod11)$

الحل: لدينا : $38 = 10(3) + 20(4) \Rightarrow 5^{38} = (5^{10})^3(5^2)^4$

ولدينا : $5^2 \equiv 25 \equiv 3(mod11)$ و $5^{10} \equiv 1(mod11) \Leftarrow$

$$5^{38} \equiv (1)^3(3)^4 \equiv 81(mod11) \equiv 4(mod11)$$

– **نتيجة (2) :** إذا كان $q\ ,p$ عددين أوليين مختلفين وكان :

$a^p \equiv a(modq)$ و $a^q \equiv a(modp)$ و $(a,pq) = 1$ فإن :

$$a^{pq} \equiv a(modpq)$$

البرهان : حسب مبرهنة فيرما نكتب : $(a^q)^p \equiv a^q(modp)$

ولما كان $a^q \equiv a(modp)$ فإن $(a^q)^p \equiv a(modp)$

وبشكل مشابه نجد أن $(a^p)^q \equiv a(modq)$ أي أن :

$p|a^{pq} - a$ و $p|a^{pq} - a$ و $(p,q) = 1$ ومنـه ينتج أن $pq|a^{pq} - a$ أي $a^{pq} \equiv a(modpq)$.

تمرين : أثبت أن $2^{340} \equiv 1(mod341)$

لنثبت صحة هذه العلاقة بطريقتين بعد ملاحظة أن $341 = (31)(11)$

طريقة أولى : بما أن $(2,11) = 1$ فحسب فيرما نكتب $2^{10} \equiv 1(mod11)$

وحسب خواص التطابقات نجد:

$$2^{31} \equiv 2^{30}.2 \equiv (2^{10})^3.2 \equiv 2(mod11)$$

ومن جهة أخرى لدينا : $2^{10} \equiv (2^5)^2 \equiv (1)^2(mod31)$

أي أن : $2^{11} \equiv 2(mod31)$

فحسب النتيجة (2) السابقة نجد أن :

$$2^{31\times11} \equiv 2(mod31 \times 11)$$

طريقة ثانية : كتبنا حسب فيرما $2^{10} \equiv 1(mod11)$ ويمكن أن نكتب

$$2^{340} \equiv (2^{10})^{34} \equiv 1(mod11) \Rightarrow 11|2^{340} - 1$$

ولدينا أن $(31,2) = 1$ لذا نكتب حسب فيرما : $2^{30} \equiv 1(mod31)$

وحسب خواص التطابقات نكتب :

$$2^{340} \equiv (2^{30})^{11}.2^{10} \equiv 1(mod31) \Rightarrow 31|2^{340} - 1$$

ولما كان $(31,11) = 1$ فإن $341 = (31)(11)|2^{340} - 1$ وهو المطلوب .

– **ملاحظة :** نلاحظ من التمرين السابق أن مبرهنة فيرما محققة من أجل العدد 341 غير أولي مما يدل عكس مبرهنة فيرما غير صحيح . أي إذا كان $a^n \equiv a(modn)$ فليس بالضرورة أن يكون العدد n أولياً .

– **تعريف :** تسمى الأعداد الصحيحة غير الأولية n التي تحقق العلاقة

$2^n \equiv 2(modn)$ أشباه الأوليات (*Pseudoprimes*) .

وقد أثبت أنه يوجد عدد غير منته منها . وأصغر هذه الأعداد هو العدد 341 ويليه العدد 561 .

تمرين (1) : إذا كان $(a,35) = 1$ أثبت أن $a^{12} \equiv 1(mod35)$

الحل : لدينا

$$(a,7) = 1, (a,5) = 1 \Leftarrow (a,35) = 1,35 = (5)(7)$$

نطبق مبرهنة فيرما فنجد $a^{12} \equiv 1(mod7) \Leftarrow a^6 \equiv 1(mod7)$

أي $7|a^{12} - 1$ ومن جهة أخرى :

$$5|a^{12} - 1 \Leftarrow a^{12} \equiv 1(mod5) \Leftarrow a^4 \equiv 1(mod5)$$

ولما كان $(5,7) = 1$ فإن $5.7 = 35|a^{12} - 1$

تمرين (2) : إذا كان $(a.b,42) = 1$ أثبت أن $a^6 - b^6 \equiv 0(mod168)$

الحل : لدينا

$(a.b,42) = 1,168 = (3)(7)(8) \Leftarrow (a,3) = 1, (a,7) = 1, (a,8) = 1$ وكذلك

$(b,3) = 1, (b,7) = 1, (b,8) = 1$ نطبق مبرهنة فيرما فنجد :

$$a^6 \equiv 1(mod7), b^6 \equiv 1(mod7), a^2 \equiv 1(mod3) \Rightarrow a^6 \equiv 1(mod3)$$

وَ $b^2 \equiv 1(mod3) \Rightarrow b^6 \equiv 1(mod3)$ ولما كان a , b فرديان لأن $(a.b,8) = 1$ يمكن أن تكتب $\Leftarrow b^2 \equiv 1(mod8), a^2 \equiv 1(mod8)$

$b^{12} \equiv 1(mod8), a^{12} \equiv 1(mod8)$. أي أن كل من 7 , 8 , 3 يقسم $a^6 - b^6$ ولما كان $(3,7,8) = 1$ ينتج $168|a^6 - b^6$.

2– 2–11 مبرهنة ويلسون : (*Wilson's theorem*)

إذا كان p عدداً أولياً فإن $p|(p-1)! + 1$ أو $(p-1)! \equiv -1(modp)$

البرهان : نلاحظ أنه إذا كان $p = 2$ فإن $2|1 + 1$ والعلاقة محققة

إذا كان $p = 3$ فإن $3|2 + 1$ والعلاقة محققة .

لنثبت صحة العلاقة من أجل $P > 3$

ليكن العـدد a هو أحـد عنـاصـــر المجموعـة $A = \{2,3,\ldots\ldots,(p-2)\}$ ، من الواضـــح أن $(a,p) = 1$ أي أن لكل عنصر a نظير ضربي واحد بالمقاس p يحقق العلاقة : $aa^* \equiv 1(modp)$ وينتمي إلى مجموعة البواقي التامة للعدد p : $A_1 = \{0,1,2,\ldots\ldots,(p-1)\}$.

ولكن من الواضح أن $a^* \not\equiv 0(modp)$. كما أن $a^* \not\equiv \pm 1(modp)$ لأنه لو كان

$a^* \equiv \pm 1(modp)$ لنتج أن $a \equiv \pm 1(modp)$ وهذا غير ممكن لأن $a \in A$ وكلا العددين 1 و $-1 \equiv p-1(modp)$ لا ينتميان إلى A ، مما يبين أن a^* ينتمي إلى المجموعة A . ومن جهة أخرى فإن $a \not\equiv a^*(modp)$ لأن هذا يقتضي أن يكون $a.a^* \equiv a^2 \equiv 1(modp)$ الأمر الذي يقود إلى العلاقة $a^2 - 1 \equiv (a-1)(a+1) \equiv 0(modp)$ التي تعطي $a \equiv \pm 1(modp)$ وهذا مستحيل كما ذكرنا . أي أن a^* هو أحد عناصر A ويختلف عن a ،

وبالتالي فإن عناصر المجموعة A– والتي عددها p-3 – ،وهو عدد زوجي ، يمكن أن تصنف مثنى بـ $\frac{p-3}{2}$ زوجاً ، جداء كل ثنائي منها يطابق الواحد بالمقاس p أي أن :

$$2.3.\ldots\ldots(p-2) \equiv 1(modp)$$

وبضرب طرفي التطابق بـ p -1 نجد :

$$1.2.3.\ldots\ldots(p-2)(p-1) \equiv (p-1)! \equiv (p-1)(modp)$$

أي $$(p-1)! \equiv -1(modp)$$

2– 2–12 عكس مبرهنة ويلسون :

إذا كان $n \geq 2$ و $(n-1)! \equiv -1(modn)$ فإن n عدد أولي .

البرهان : إذا لم يكن n أولياً فله قاسم d حيث : $1 < d < n$ أي

$1 < d \leq n-1$ أي أن d هو أحد عوامل $(n-1)!$ و $d|(n-1)!$ (1)

ومن جهة أخرى فإن $d|n$ و $p|(p-1)! + 1 \Leftarrow d|(n-1)! + 1$ (2)

ومن العلاقتين (1) و(2) ينتج أن $d|1$ أي $d = 1$ مما يدل على أن n عدد أولي .

– **ملاحظة :** يمكن صياغة مبرهنة ويلسون وعكسها معاً على النحو :

يكون العدد الصحيح $n > 1$ أولياً إذا كان $(n-1)! \equiv -1(modn)$.

ولكن من سوء الحظ أن هذا المعيار للأعداد الأولية معيار نظري بسبب سرعة تزايد $(n-1)!$ عندما يكون n كبيراً .

تمرين (1) : أثبت أن $18! \equiv -1(mod437)$.

الحل : لدينا $437 = 19 \times 23$ وحسب مبرهنة ويلسون نكتب :

$$18! \equiv -1 mod(19), 22! = -1(mod 23)$$

ولكن $22! = 18!(19)(20)(21)(22)$

أي : $22! \equiv 18!(-4)(-3)(-2)(-1)(mod 23)$

أو $18! \equiv -1(mod 23)$

مما سبق يمكن أن تكتب : $19|18! + 1$ و $23|18! + 1$

و $\Leftarrow (19,23) = 1(23)(19) = 437|18! + 1$

تمرين (2) : أثبت أن العدد 127 يقسم $7(125!) + 5!$

الحل : بما أن 127 عدد أولي فحسب ويلسون نكتب $126! \equiv -1(mod 127)$.

ولدينا

$126! \equiv 125!(126)$ و $126 \equiv -1(mod 127)$ أي $125! \equiv 1(mod 127)$

ومنه :

$(125!)7 + 5! \equiv 127 \equiv 0(mod 127)$ وهو المطلوب .

تمرين (3) : لنوضح مبرهنة ويلسون بالمثال التالي : ليكن p =13 ولنعرف المجموعة $A = \{2,3,4,\ldots.,11\}$ ولنرتب عناصر A وفق ثنائيات عددها $\frac{13-3}{2} = 5$ فنجد :

$(2)(7) \equiv 1(mod 13)$ ، $(3)(9) \equiv 1(mod 13)$ ، $(4)(10) \equiv 1(mod 13)$

$(5)(8) \equiv 1(mod 13)$ ، $(6)(11) \equiv 1(mod 13)$

وبالتالي فإن :

$11! = (2 \times 7)(3 \times 9)(4 \times 10)(5 \times 8)(6 \times 11) \equiv 1(mod 13)$

و $12! \equiv 12 \equiv -1(mod 13)$

– **ملاحظة** : يمكن التعبير عن مبرهنة ويلسون أيضاً كما يلي :

$(p-1)! \equiv p - 1(mod p)$ أو $(p-2)! \equiv 1(mod p)$

حيث p عدد أولي .

تمارين

1- أعط مثالاً يبين أنه إذا كان $a^2 \equiv b^2(modn)$ فليس من الضروري أن يكون $a \equiv b(modn)$.

2- أعط مثالاً يبين أنه إذا كان $a^k \equiv b^k(modn)$ و $k \equiv j(modn)$ فليس من الضروري أن يكون $a^j \equiv b^j(modn)$.

3- أثبت أنه إذا كان $(a,n) = 1$ فإن الأعداد $c, c+a, c+2a, \ldots\ldots, c+(n-1)a$ تؤلف مجموعة بواقي تامة بالمقاس n مهما تكن $c \in Z$.

4- أثبت بطريقة الاستقراء أنه إذا كان a عدداً صحيحاً فردياً فإن $a^{2^n} \equiv 1(mod2^{n+2})$

5- إذا كان n عدداً صحيحاً فردياً لا يقبل القسمة على 3 فبرهن أن $72|5n^6 + 3n^4 - 3n^2 - 5$

6- أثبت أنه إذا كان العدد الصحيح a لا يقبل القسمة على أي من الأعداد : $2\ ,\ 3\ ,\ 5\ ,\ 7$ كان : $840|a^{12} - 1$.

7- إذا كان $(a,35) = 1$ أثبت أن $n^{12} \equiv (mod35)$.

8- أثبت أنه إذا كان k عدداً صحيحاً فردياً و $(k,3) = 1$ فإن $k^2 \equiv 1(mod24)$

9- أوجد باقي قسمة الأعداد 2^{50} و 41^{65} على العدد 7

10- أوجد باقي قسمة المجموع $1^5 + 2^5 + 3^5 + \ldots\ldots + 99^5 + 100^5$ على العدد 4 .

11- إذا كان $(n,30) = 1$ أثبت أن 240 يقسم $n^4 + 239$.

12- إذا كان $(n,42) = 1$ أثبت أن 504 يقسم $n^6 - 1$.

13- أثبت أن باقي قسمة ! 255 على الأولي 257 يساوي 1 .

14- أوجد الكسور البسيطة المستمرة من أجل كل من الكسور التالية :

$$\frac{119}{32}, \frac{118}{303}, -\frac{503}{187}, -\frac{125}{198}$$

15- أوجد الكسر المقابل لـ $< 3,1,1,4,1,3 >$

16- أوجد الحل الكامل لكل من :

$187x \equiv 2(mod503)$ ، $18x \equiv 30(mod42)$

$79x \equiv 2(mod153)$ ، $9x \equiv 21(mod30)$

$182x \equiv 7(mod203)$ ، $17x \equiv 9(mod276)$

$4x \equiv 9(mod51)$ ، $140x \equiv 133(mod301)$

17- أوجد أصغر عدد صحيح موجب باقي قسمته على 13 يساوي 5 وباقي قسمته على 12 يساوي 3 وباقي قسمته على 35 يساوي 2 .

18- أوجد الحل المشترك لكل من جمل التطابقات التالية :

$(a$ $x \equiv 3(mod6)$ ، $x \equiv -1(mod25)$ ، $x \equiv 1(mod7)$

$(b$ $x \equiv -2(mod11)$، $x \equiv 13(mod28)$، $x \equiv 7(mod45)$

$(c$ $5x \equiv 2(mod13)$ ، $x \equiv 2(mod35)$

$3x \equiv 13(mod77)$ ، $x \equiv 7(mod20)$

$(d$ $17x \equiv 3(mod7)$، $17x \equiv 3(mod5)$،

$17x \equiv 3(mod2)$ ، $17x \equiv 3(mod3)$

19- أوجد أصغر عدد صحيح $a > 2$ بحيث تتحقق العلاقات :

$5|a+36|a+4$, $3|a+1$, $4|a+2$, $2|a$

20- أوجد باقي قسمة $2(26!)$ على 29 .

21- رتب الأعداد 21 , ... , 4 , 3 , 2 وفق ثنائيات (a , b) بحيث $a.b \equiv 1(mod23)$.

22- أثبت أن $18! \equiv -1(mod437)$.

23- إذا كان p عدداً أولياً أثبت أن :

$p|a^p + (p-1)!\,a$ و $p|(p-1)!\,a^p + a$

24- أوجد العدد الصحيح x بحيث يكون :

$5^2|x+2$, $4^2|x+1$, $3^2|x$

الفصل الثالث

الدوال العددية وبعض الدوال الخاصة

2 –3 الدوال العددية وبعض الدوال الخاصة في نظرية الأعداد

2–3–1 تعريف : الدوال العددية أو الدوال الحسابية ((*arithmetic functions*))

هي الدوال التي مجال تعريفها الأعداد الصـــحيحة الموجبة ، ولهذه الدوال أهمية عظمى في نظرية الأعداد وسندرس في هذا الفصل عدداً من هذه الدوال التي قيمها أعداد صحيحة وندرس خواصها .

2–3–2 الدالة العددية الضربية : نقول إن الدالة العددية $f(n)$ دالة ضربية إذا حققت الشرطين :

1– $f(n)$ غير صفرية

2– $\forall a,b \in Z^+$ و $(a,b)=1$ فإن $f(a.b)=f(a).f(b)$.

ونقول إن الدالة $f(n)$ ضربية تماماً إذا حققت الشروط السابقة دون الشرط $(a,b)=1$.

مثال : الدالة $f_\alpha(n)=n^\alpha$ (حيث $\alpha, n \in Z^+$) . ضربية تماماً ، لأن :

1– $f(n) \neq 0$ مهما تكن $n>0$.

2– إذا كان $n_1,n_2 \in Z^+$ فإن $f_\alpha(n_1.n_2)=(n_1.n_2)^\alpha=n_1^\alpha.n_2^\alpha=f_\alpha(n_1).f_\alpha(n_2)$.

2–3–3 مبرهنة : إذا كانت $f(n)$ دالة ضربية فإن $f(1)=1$

البرهان : بما أن الدالة $f(n)$ ضـــربية فإنها غير صـــفرية أي يوجد عدد n بحيث يكون .

$f(n) \neq 0$ ولما كان $(n,1)=1$ و $f(n.1)=f(n).f(1) \Leftarrow f(1)=1$

– **تعريف :** يمكن أن نعرف الدالة العددية الضربية بأنها الدالة العددية التي تحقق الشرطين :

1– $f(1)=1$

2– $f(a.b)=f(a).f(b)$ حيث $a,b \in Z^+,(a,b)=1$.

– **نتيجة :** إذا كانت الدالة $f(n)$ دالة عددية ضربية وكانت الأعداد $n_1,n_2,\ldots,n_k$ أولية نسبياً مثنى مثنى ، فإن $f(n_1.n_2.\ldots.n_r)=f(n_1).f(n_2).\ldots\ldots.f(n_r)$

البرهان : نبرهن صحة هذه النتيجة بطريقة الاستقراء :

1– من أجل r =2 نجد أن $(n_1,n_2)=1$ و $f(n_1.n_2)=f(n_1).f(n_2)$

2– لنفترض أن العبارة صحيحة عندما $r=k$ ولنثبت صحتها من أجل $r=k+1$

بما أن $((n_1.n_2.\ldots.n_k),n_{k+1})=1$ وبما أن :

$$f(n_1.n_2.\ldots.n_k)=f(n_1).f(n_2).\ldots\ldots.f(n_k)$$

نجد : $f\big((n_1.n_2 \ldots\ldots n_k), n_{k+1}\big) = f(n_1.n_2 \ldots\ldots n_k).f(n_{k+1})$

$= f(n_1).f(n_2).\ldots\ldots\ldots f(n_k)$

أي العبارة صحيحة من أجل $r>1$

– **نتيجة :** إذا كانت f دالة ضربية و كانت العبارة القانونية للعدد n هي:

$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}$ فإن $f(n) = f(p_1^{\alpha_1}).f(p_2^{\alpha_2}).\ldots\ldots f(p_k^{\alpha_k})$

وذلك لأن $p_i^{\alpha_i}$ أولية نسبياً فيما بينها مثنى مثنى .

– **تعريف :** إن العبارة $\sum_{d|n}$ تعني أن المجموع مأخوذ على جميع قواسم العدد n الموجبة .

مثال : $\sum_{d|15} f(d)$ تعني : $\sum_{d|15} f(d) = f(1) + f(3) + f(5) + f(15)$

2–3–4 تمهيدية (1) : إذا كانت f , g دالتين عدديتين فإن :

$$\sum_{\substack{d|m \\ e|n}} f(d)\, g(e) = \left(\sum_{d|m} f(d)\right)\left(\sum_{e|n} g(e)\right)$$

البرهان : لنفترض أن $d_1, d_2, \ldots, d_s$ هي جميع قواسم العدد m الموجبة

و $e_1, e_2, \ldots, e_t$ هي جميع قواسم العدد n الموجبة

ونكتب : $\sum_{\substack{d|m \\ e|n}} f(d)\, g(e) = \sum_{\substack{j=1,\ldots,s \\ k=1,\ldots,t}} f(d_j)\, g(e_k)$

$= \sum_{j=1}^{s} f(d_j)g(e_1) + \sum_{j=1}^{s} f(d_j)g(e_2) + \ldots + \sum_{j=1}^{s} f(d_j)g(e_t)$

$= \left(\sum_{j=1}^{s} f(d_j)\right)\left(\sum_{k=1}^{t} g(e_k)\right) = \sum_{d|m} f(d) \cdot \sum_{e|n} g(e)$

وهو المطلوب .

2–3–5 تمهيدية (2) : إذا كان n , m عددين صحيحين موجبين وكان $(m,n) = 1$ فإن أي قاسم لـ $m.n$ يكتب بشكل وحيد كجداء قاسم لـ m مثل d_1 وقاسم لـ n مثل d_2 حيث $(d_1, d_2) = 1$.

البرهان : لنحلل كلاً من n , m إلى عوامله الأولية ونكتب

$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_s^{\alpha_s}$ و $n = q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots q_r^{\beta_r}$

نعلم أن الأوليات p_i و q_j مختلفة لأن $(m,n) = 1$

ونكتب : $m.n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_s^{\alpha_s} q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots q_r^{\beta_r}$

إن أي قاسم لـ $m\,.\,n$ يكتب على النحو: $d = p_1^{c_1} p_2^{c_2} \ldots\ldots p_s^{c_s} q_1^{t_1} q_2^{t_2} \ldots\ldots q_r^{t_r}$

حيث $0 \le c_i \le \alpha_i$, $0 \le t_i \le \beta_i$ أي يمكن أن نكتب : $d = d_1.d_2$

حيث $d_1 = p_1^{c_1} p_2^{c_2} \ldots\ldots p_s^{c_s}, d_2 = q_1^{t_1} q_2^{t_2} \ldots\ldots q_r^{t_r}$

إن $d_2|n, d_1|m$ ولايوجد أي عامل مشترك بين d_2 و d_1 أي أنّ : $(d_1, d_2) = 1$.

2-3-6 مبرهنة : إذا كانت الدالة العددية f دالة ضربية وإذا عرفت الدالة العددية F على النحو :

$F(n)=\sum_{d|n} f(d)$ فإن F هي دالة ضربية .

البرهان : لنفترض $n\ ,\ m$ عددان صحيحان موجبان وأن $(m,n)=1$ ونكتب :

$$F(m.n)=\sum_{d|mn} f(d)=\sum_{\substack{d_1|m\\ d_2|n}} f(d_1 d_2)$$

لأن أي قاسم d للجداء $m\ .\ n$ يكتب بشكل وحيد كجداء قاسم لـــ $d_1 : m$ وقاسم لـــ $d_2 : n$ حيث $(d_1,d_2)=1$ ولما كان f دالة ضربية فإن $f(d_1.d_2)=f(d_1).f(d_2)$

نعوض في عبارة $F(m.n)$ فنجد :

$$F(m.n)=\sum_{\substack{d_1|m\\ d_2|n}} f(d_1).f(d_2)=\left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|n} f(d_2)\right)$$

$$F(m.n)=F(m)F(n)$$

مثال : لنوضـح المبرهنة السـابقة بالمثال التالي : حيث نأخذ $n=3$ ، $m=8$ و $m\,n=24$ ، فتكون قواسم n هي $\{1,3\}$ وقواسم m هي $\{1,2,4,8\}$

$$F(8\times 3)=\sum_{d|24} f(d)$$

$$F(8\times 3)=f(1)+f(2)+f(3)+f(4)+f(6)+f(8)+f(12)+f(24)$$
$$=[f(1)+f(2)+f(4)+f(8)][f(1)+f(3)]$$

تمرين : لتكن الدالة g المعرفة على النحو التالي :

$$g(n)=\begin{cases}0 & n \text{ زوجي}\\ 1 & n \text{ فردي}\end{cases}$$

ولتكن $G(n)=\sum_{d|n} g(d)$

1- برهن أن g و G دالتان ضربيتان : إن : $g\ (1\ )=1$ و إذا كان $(m\ ,\ n)=1$ فإن

$g(n.m)=\begin{cases}0 & \text{أحدهما زوجي}\\ 1 & \text{كلاهما فردي}\end{cases}$ أي $g(n.m)=g(n)g(m)$

و g دالة ضربية وكذلك G حسب المبرهنة السابقة .

2- أوجد قيمة $G(p^k)$ حيث p عدد أولي فردي : لدينا

$$G(p^k)=\sum_{d|p^k} g(d)=g(1)+g(p)+g(p^2)+\ldots\ldots+g(p^k)=k+1$$

لأن قوى أي عدد فردي هي أعداد فردية .

3- احسب $G(220):G(20)$

$G(20)=\sum_{d|20} g(d)=g(1)+g(2)+g(4)+g(5)+g(10)+g(20)=2$

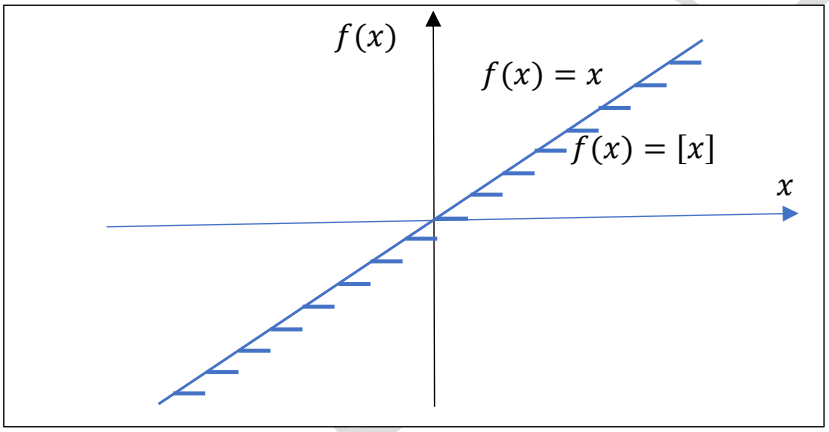
- إن القواسم الفردية لـ 220 هي 55 , 11 , 5 وبالتالي فإن $G(220)=3$.

2-3-7 دالة الجزء الصحيح *The greatest integer function* أو *(Floor)*

تلعب دالة الجزء الصحيح أهمية كبرى في نظرية الأعداد لذا سنورد تعريفها وأهم خواصها فيما يلي:

- **تعريف** : تعرف دالة الجزء الصحيح للعدد الحقيقي α وترمز $[\alpha]$

بأنها أكبر عدد صحيح لا تتجاوز قيمته قيمة العدد α (يرمز أحياناً $\lfloor\alpha\rfloor$ ليتميز عن العدد الصحيح الذي هو أكبر مباشرة من α والذي يرمز $[\alpha]$) . ويمكن تمثيل هذه الدالة في المستوي على النحو :



شكل(1)

ينتج من تعريف هذه الدالة أن :

$$[\alpha]\le\alpha<[\alpha]+1$$

ويعبر عن هذه الدالة كما يلي :

$$\alpha=[\alpha]+\theta 0\le\theta<1$$

ويسمى العدد θ الجزء الكسري من α .

أمثلة :

$$[-\sqrt{10}]=-4,[2.5]=2,\left[-\tfrac{12}{5}\right]=-3,[\sqrt{10}]=3,[-0.5]=-1$$

2-3-8 خواص دالة الجزء الصحيح

1) إذا كان $a\in Z,\alpha\in\Re$ فإن : $[a+\alpha]=a+[\alpha]$

البرهان : لدينا : $[a+\alpha]\le a+\alpha<[a+\alpha]+1$

$$([a+\alpha]-a)\le\alpha<([a+\alpha]-a)+1$$

أي أن $[\alpha]=[a+\alpha]-a$ وبالتالي : $[a+\alpha]=[\alpha]+a$

2) إذا كان $n\in Z^+,\alpha\in\Re$ فإن : $\left[\frac{[\alpha]}{n}\right]=\left[\frac{\alpha}{n}\right]$

البرهان : لدينا : $\frac{\alpha}{n} = \left[\frac{\alpha}{n}\right] + \theta : 0 \le \theta < 1$

ومنه $\alpha = n\left[\frac{\alpha}{n}\right] + n\theta$

$[\alpha] = n\left[\frac{\alpha}{n}\right] + [n\theta] : 0 \le n\theta < n$

أي $\frac{[\alpha]}{n} = \left[\frac{\alpha}{n}\right] + \frac{[n\theta]}{n} : 0 \le [n\theta] < n\theta < n$

و منه $\left[\frac{[\alpha]}{n}\right] = \left[\frac{\alpha}{n}\right] + 0 \ , \ 0 \le \frac{[n\theta]}{n} < 1$

- **نتيجة :** إن $\left[\frac{[\alpha/n]}{m}\right] = \left[\frac{\alpha}{n.m}\right]$ حيث $a, n, m \in Z^+$

3) إذا كان n عدداً صحيحاً أكبر من الواحد و α عدد حقيقي أكبر أو يساوي الواحد فإن: $[\alpha] > \left[\frac{\alpha}{n}\right]$

البرهان : نكتب : $\frac{\alpha}{n} = \left[\frac{\alpha}{n}\right] + \theta : 0 < \theta < 1$

ومنه : $\alpha = n\left[\frac{\alpha}{n}\right] + n\theta : 0 \le n\theta < n$

ولما كان $n\left[\frac{\alpha}{n}\right]$ عدداً صحيحاً فإن : $[\alpha] = n\left[\frac{\alpha}{n}\right] + [n\theta]$

و $[\alpha] > \left[\frac{\alpha}{n}\right]$ لأن $n > 1 \ , \ 0 < [n\theta]$

4) إذا كان $a, b, n \in Z^+$ فإن $\left[\frac{ab}{n}\right] \ge a\left[\frac{b}{n}\right]$

البرهان : لدينا من تعريف دالة الجزء الصحيح :

$$\frac{b}{n} = \left[\frac{b}{n}\right] + \theta : 0 < \theta < 1$$

$$\frac{ab}{n} = a\left[\frac{b}{n}\right] + a\theta : 0 \le a\theta < a$$

$$\left[\frac{ab}{n}\right] = a\left[\frac{b}{n}\right] + [a\theta] \ge a\left[\frac{b}{n}\right]$$

5) إذا كانت الأعداد $\alpha_i \in \Re$ و $\alpha = \sum_1^k [\alpha_i]$ فإن: $[\alpha] \ge \sum_1^k [\alpha_i]$

البرهان : نكتب $\alpha_1 = [\alpha_1] + \theta_1 0 \le \theta_1 < 1$

$\alpha_i = [\alpha_i] + \theta_i 0 \le \theta_i < 1$

$\alpha_n = [\alpha_n] + \theta_n 0 \le \theta_n < 1$

بالجمع نجد $\alpha = \sum_1^n [\alpha_i] + \sum_1^n \theta_i \Rightarrow [\alpha] = \sum_1^n [\alpha_i] + [\sum_1^n \theta_i]$

ولما كانت θ_i كلها أعداد موجبة فإن $[\alpha] \ge \sum_1^n [\alpha_i]$

- **نتيجة :** ينتج من الخاصة الأخيرة مباشرة أن: $\left[\frac{n}{p}\right] \ge \left[\frac{n_1}{p}\right] + \left[\frac{n_2}{p}\right] + \ldots + \left[\frac{n_k}{p}\right]$

حيث p عدد صحيح غير الصفر و n_i أعداد صحيحة و $n = \sum_1^k n_i$

2-3-9 مبرهنة : إذا كان $n \in Z^+$ و p عدداً أولياً فإن أس أكبر قوة لـــ p تقسم $n!$ وترمز $H_p(n!)$ يساوي : $H_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots\ldots + \left[\frac{n}{p^k}\right] = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$

حيث $\left[\frac{n}{p^k}\right] \geq 1$ و $\left[\frac{n}{p^{k+1}}\right] = 0$ وبقية الحدود التالية معدومة .

البرهان :

لنرتب الأعداد من 1 إلى n أي نرتب مضاريب $n!=1.2...n$ كما يلي:

$$1,2,\ldots,p,p+1,\ldots,2p,\ldots,3p,\ldots\ldots\ldots,pp,p^2+1,\ldots,2p^2,\ldots pp^2,\ldots,n$$

لنفترض أن الأعداد التي تقبل القسمة على p من بين هذه الأعداد هي : $p, 2p, \ldots, t_1 p$ حيث t_1 هو أكبر عدد صحيح يحقق العلاقة $t_1 p \leq n$ أي أن t_1 هو أكبر عدد صحيح أصغر أو يساوي $\frac{n}{p}$ أي $t_1 \leq \frac{n}{p} < (t_1 + 1)$ ومنه $t_1 = \left[\frac{n}{p}\right]$ أي أن هناك $\left[\frac{n}{p}\right]$ مضاعفاً لـ p بين مضاريب $n!$ ألا وهي: $p, 2p, 3p, \ldots, \left[\frac{n}{p}\right] p$.

وبمحاكمة شـــبيهة نجد أن عدد الأعداد التي تقبل القســـمةعلى p^2 من بين مضـــاريب $n!$ هو $t_2 = \left[\frac{n}{p^2}\right]$ وهي: $p^2, 2p^2, \ldots, \left[\frac{n}{p^2}\right] p^2$

ومن بين هذه الأعداد يوجد $\left[\frac{n}{p^3}\right]$ عدداً يقبل القســـمة ثانية على p أي يقبل القســـمة على p^3 ، وهكذا بعد تكرار هذه المحاكمة عدداً منتهياً من المرات نجد أن عدد المرات التي يقسـم بها p العدد $n!$ هو :

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots\ldots + \left[\frac{n}{p^k}\right] = t_1 + t_2 + \ldots + t_k$$

أي أن $n!$ تقبل القسمة على $p^{t_1+t_2+\ldots+t_k}$ ومنه $H_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$

مثال (1) : لنوضـــح المبرهنة الســـابقة بالمثال التالي : إذا كان $p = 3$ و $n = 19$

فإن $19! = 1.2.3 \ldots 6..9 \ldots 12 \ldots 15..18.19$

مضاعفات العدد 3 من بين مضاريب $19!$ هي $\{3,6,9,12,15,18\}$ و عددها $\left[\frac{19}{3}\right] = 6$.

مضـاعفات العدد 3^2 هي $\{9,18\}$ عددها $\left[\frac{19}{9}\right] = 2$ وعدد مضـاعفات العدد $3^3 = 27$ صـفر

أي $H_3(19!) = 6 + 2 = 8$ و $3^8 | 19!$ في حين $3^9 \nmid 19!$.

تمرين : ما هو عدد الأصفار في نهاية العدد $50!$

الحل: لتعيين عدد الأصفار في نهاية $50!$ نبحث عن أكبر قوة للعدد 10

تقسم $50!$ ولكن $10 = 2 . 5$ لذا نبحث عن $H_2(50!)$ و $H_5(50!)$ فنجد :

$$H_2(50!) = \left[\frac{50}{2}\right] + \left[\frac{50}{4}\right] + \left[\frac{50}{8}\right] + \left[\frac{50}{16}\right] + \left[\frac{50}{32}\right] + \left[\frac{50}{64}\right]$$

$$= 25 + 12 + 6 + 3 + 1 + 0 = 47 \quad \Rightarrow$$

$$2^{47} | 50! \quad \text{و} \quad 2^{48} \nmid 50!$$

$$H_5(50!) = \left[\frac{50}{5}\right] + \left[\frac{50}{25}\right] + 0 = 10 + 2 = 12 \Rightarrow 5^{12} | 50! \text{ و } 5^{13} \nmid 50!$$

بما كان $(2,5) = 1$ فإن أس أكبر قوة للعدد 10 تقسم $50!$ هو 12 وعدد الأصفار في نهاية $50!$ هو 12.

2-3-10 مبرهنة : إذا كتب العدد الصحيح m بالنظام الذي أساسه العدد الأولي p فإن أس أكبر قوة للعدد p تقسم $m!$ هي : $H_p(m!) = \frac{m - \sum_0^r a_i}{p-1}$

حيث $m = \sum_{i=0}^{r} a_i p^i = a_r p^r + a_{r-1} p^{r-1} + \ldots\ldots + a_1 p + a_0$

البرهان : نكتب حسب المبرهنة السابقة :

$$\begin{aligned} H_p(m!) &= \left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \ldots + \left[\frac{m}{p^r}\right] \\ &= a_r p^{r-1} + a_{r-1} p^{r-2} + \ldots\ldots\ldots\ldots + a_1 + \\ &\quad + a_r p^{r-2} + a_{r-1} p^{r-3} + \ldots + a_2 + \\ &\quad + \ldots\ldots\ldots\ldots \\ &\quad \ldots\ldots\ldots\ldots \\ &\quad + a_r p + a_{r-1} \\ &\quad + a_r \end{aligned}$$

ومنه

$$H_p(m!) = a_r(1 + p + p^2 + \ldots + p^{r-1}) + a_{r-1}(1 + p + p^2 + \ldots + p^{r-2}) + \ldots + a_1$$

$$H_p(m!) = a_r \frac{p^r - 1}{p-1} + a_{r-1} \frac{p^{r-1} - 1}{p-1} + \ldots + a_2 \frac{p^2 - 1}{p-1} + a_1$$

$$H_p(m!) = \frac{a_r p^r + a_{r-1} p^{r-1} + \ldots + a_1 p + a_0 - (a_r + a_{r-1} + \ldots + a_2 + a_1 + a_0)}{p-1}$$

$$H_p(m!) = \frac{m - \sum_0^r a_i}{p-1}$$

مثال : اكتب العدد 347 بنظام العد الذي أساسه 7 ثم احسب $H_7(347!)$

الحل : $347 = \mathbf{1}(\mathbf{7^3}) + \mathbf{0}(\mathbf{7^2}) + \mathbf{0}(\mathbf{7}) + \mathbf{4} = (\mathbf{1004})_7$

وبتطبيق المبرهنة الأخيرة نجد : $H_7(347!) = \frac{347 - (5)}{7-1} = 57$

2-3-11 مبرهنة : إذا كان n و r عددين صحيحين وكان $1 \leq r < n$

فإن : $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ هو عدد صحيح

محاضرات د. بهي

البرهان (غير مطلوب): من أجل البرهان يكفي أن نثبت أن أس أكبر قوة لأي عدد أولي p يقسم المقام أصغر أويساوي أس أكبر قوة لهذا العدد الأولي p تقسم البسط لذا نكتب حسب الخاصة (5) من خواص دالة الجزء الصحيح نكتب : $\left[\frac{n}{p^k}\right] \geq \left[\frac{r}{p^k}\right] + \left[\frac{n-r}{p^k}\right]$

وبالجمع على k نجد : $\sum_{k\geq 1}\left[\frac{n}{p^k}\right] \geq \sum_{k\geq 1}\left[\frac{r}{p^k}\right] + \sum_{k\geq 1}\left[\frac{n-r}{p^k}\right]$

ومنه $H_p(n!) \geq H_p(r!\,(n-r)!)$

أي أن أي عامل للمقام يقسم البسط والناتج عدد صحيح .

– **نتيجة :** إن جداء n من الأعداد الصحيحة المتتالية الموجبة يقبل القسمة على $n!$

البرهان :نجد أن: عدد صحيح $= \frac{(k+1)(k+2).....(k+n)}{n!} = \frac{k!(k+1).....(k+n)}{k!.n!} = \frac{(k+n)!}{k!n!}$

– **ملاحظة :** يمكن ببساطة إثبات العلاقة التالية

$\frac{n!}{n_1!n_2!.....n_k!}$ هو عدد صحيح علماً أن : $n = n_1 + n_2 + ... + n_k$

تمرين : أثبت أن إذا كان $m,n \in Z^+$ فإن $\frac{(2m)!(3n)!}{(m!)^2(n!)^3}$ هو

عدد صحيح .

الحل : لدينا $2\,m = m + m$ و $3\,n = n + n + n$ $\Leftarrow$

$\frac{(2m)!}{m!m!}$ و $\frac{(3n)!}{(n!)(n!)(n!)}$ عددان صحيحان جداؤهما عدد صحيح .

2-3-12 مبرهنة : إذا كانت f , F دالتين عددتين وكان $F(n) = \sum_{d|n} f(d)$

فإن : $\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$. من أجل أي عدد صحيح موجب N .

البرهان(غير مطلوب): بما أن $F(n) = \sum_{d|n} f(d)$ فإن : $\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N}\sum_{d|n} f(k)$

لنجمع الحدود التي تحوي قيماً متساوية لـ $f\,(\,d\,)$ في المجموع المضاعف السابق . نلاحظ أنه إذا كان العدد k عدداً صحيحاً $\geq N$ فإن هذا العدد k يظهر في المجموع $\sum_{d|n} f(d)$ إذا وفقط إذا كان k قاسماً لـ n (إن مجموعة الأعداد $\sum_{d|n} f(d)$ غير خالية لأن كل عدد هو قاسم لنفسه على الأقل) ، فلحساب عدد المجاميع $\sum_{d|n} f(d)$ التي يظهر فيها الحد $f\,(\,k\,)$ ، يكفي أن نحسب عدد الأعداد الصحيحة من بين الأعداد $1\,,\,2\,,\,.....\,,\,N$ التي تقبل القسمة على k . إن هذا العدد كما سبق ورأينا يساوي $\left[\frac{N}{k}\right]$. وهذه الأعداد هي $k\,,\,2\,k\,,\,3\,k\,,\,...,\left[\frac{N}{k}\right]k$ وهكذا نجد أنه من أجل كل عدد k حيث $1 \leq k \leq N$ فإن $f\,(\,k\,)$ هو حد في المجموع $\sum_{d|n} f(d)$ وذلك من أجل $\left[\frac{N}{k}\right]$ من الأعداد الصحيحة الموجبة المختلفة والتي هي أصغر أوتساوي N مما يمكننا من كتابة المجموع المضاعف على النحو : $\sum_{n=1}^{N}\sum_{d|n} f(k) = \sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$ وهو المطلوب .

- **تعريف** :إذا كان $\alpha \in \Re$ و $f(n)$ دالة عددية فإن: $\sum_{n=1}^{\alpha} f(n) = \sum_{n=1}^{[\alpha]} f(n)$

- **نتيجة** : ينتج من المبرهنة الأخيرة مباشرة أنه إذا كان f , F دالتين عددتين وكان $F(n) = \sum_{d|n} f(d)$ و $\alpha \in \Re$ فإن $\sum_{n=1}^{\alpha} F(n) = \sum_{n=1}^{[\alpha]} \sum_{d|n} f(n)$.

2-3-13 تعريف مجموعة البواقي المختزلة

إذا كانت A مجموعة بواقي تامة بالمقاس m فإن المجموعة الجزئية T من A التي تحوي الأعداد الأولية نسبياً مع m تسمى مجموعة بواقي مختزلة بالمقاس m أي أن

$T = \{a \in A: (a, m) = 1\}$ ، حيث $A = \{0,1,2,\ldots\ldots, m-1\}$

مثال (1) : إن المجموعة $A = \{0,1,2,3,4,5\}$ هي مجموعة بواقي تامة بالمقاس 6 والمجموعة $T = \{1,5\}$ هي مجموعة بواقي مختزلة بالمقاس 6 .

مثال (2) : إن المجموعة $A(12) = \{0, \pm1, \pm2, \pm3, \pm4, \pm5,6\}$ هي مجموعة بواقي تامة بالمقاس 12 والمجموعة $T(12) = \{\pm1, \pm5\}$ هي مجموعة بواقي مختزلة بالمقاس12. ومن الواضح أن عدد عناصر أي مجموعتي بواقي مختزلة بالمقاس m متساوٍ.

2-3-14 دالة اولر . ϕ ***Euler's - Function***

- **تعريف:** من أجل أي عدد صحيح موجب m فإن دالة أولر $\varphi(m)$ هي عدد العناصر التي لا تتجاوز m وأولية نسبياً مع m ، أي هي عدد عناصر أي مجموعة بواق مختزلة بالمقاس m .

مثال : $\varphi(3) = 2, \varphi(2) = 1, \varphi(1) = 1$ لأن الأعداد التي هي ≥ 3 والأولية نسبياً مع 3 هي 1 , 2 ، حيث : $T(3) = \{1,2\}$ وعدد العناصر =2 $= \varphi(3)$ ،

لإيجاد $\varphi(5)$ نكتب : $A(5) = \{0,1,2,3,4\}$ و $T(5) = \{1,2,3,4\}$

وعدد العناصر $T(5)$ هي 4 أي : $\varphi(5) = 4$.

2-3-15 مبرهنة : إن دالة اولر دالة عددية ضربية .

البرهان (غير مطلوب) : **1-** إن $\varphi(1) = 1$ حسب تعريف الدالة .

2 - إذا كان a , b عددين صحيحين موجبين وكان $(a, b) = 1$ فعلينا أن نثبت أن $\varphi(a.b) = \varphi(a)\varphi(b)$

نلاحظ أنه إذا كان أحد العددين a أو b مســـاوياً للواحد فالمبرهنة صـــحيحة لذا لنفترض أن $a > 1$ و $b > 1$ و لنرتب الأعداد من 1 إلى $a\,b$ كما يلي :

$0.a+1$	2	3	....	r	....	a
$1.a+1$	$a+2$	$a+3$	....	$a+r$	....	$2a$
$2.a+1$	$2a+2$	$2a+3$	....	$2a+r$	....	$3a$
....	....	....	....	....	....	....
$qa+1$	$qa+2$	....	....	$qa+r$	....	$(q+1)a$
....	....	....	....	....	....	....
$(b-1)a+1$	$(b-1)a+2$	....	....	$(b-1)a+r$	....	ba

نلاحظ أن عناصـر كل سطر في هذه المصـفوفة تشكل مجموعة بواق تامة بالمقاس a وأن عناصـر كل عمود تشكل مجموعة بواق تامة بالمقاس b إذ نلاحظ أن عدد عناصر كل سطر يساوي a وأن أي عنصـــرين مختلفين غير متطـابقين بـالمقـاس a لأنـه لو كـان :$qa+s \equiv qa+t(moda)$ لنتج $s \equiv t(moda)$ وهذا غير ممكن إن كان العنصـران مختلفين،وبشـكل مشـابه نجد أن عدد عناصـر كل عمود يساوي b وأنه لو كان : $qa+r \equiv q_1a+r(modb)$

لنتج $qa \equiv q_1a(modb)$ ولما كان $(a,b)=1$ فإن هذا يؤدي إلى :

$q \equiv q_1(modb)$ وهذا غير ممكن من أجل أي عنصرين مختلفين من العمود .

ومن جهة أخرى نعلم أن عدد العناصـر الأولية نسـبياً مع a في كل سـطر يسـاوي$\varphi(a)$ وأن العنصـر $((qa+r),a)=1$ إذا وفقط إذا كـان $(r,a)=1$ لـذا نـأخـذ أي عمود r يحقق الشـــرط $(r,a)=1$ ونلاحظ أن عدد عناصـر هذا العمود الأولية نسـبياً مع b يسـاوي $\varphi(b)$ مما يدل على أن عدد العناصـر من المصـفوفة السـابقة التي هي أولية نسـبياً مع a ومع b بآن واحد أي التي هي أولية نسبياً مع $a\,.\,b$ يساوي $\varphi(a)\varphi(b)$ مما يثبت أخيراً أن $\varphi(a.b)=\varphi(a)\varphi(b)$.

مثال :

$$\varphi(12)=\varphi(3).\varphi(4)=(2)(2)=4$$
$$\varphi(15)=\varphi(3).\varphi(5)=(2)(4)=8$$

2-3-16 مبرهنة : إن $\varphi(p)=p-1$ حيث p عدد أولي .

الإثبات: نعلم أن مجموعة البواقي التامة الصغرى للعدد الأولي p هي: $A=\{0,1,2,3.....,p-1\}$ و مجموعة البواقي المختزلة بالمقاس p هي : $T=\{1,2,3.....,p-1\}$

وعدد عناصر $T(p)$ يساوي p-1 أي : $\varphi(p)=p-1$

2-3-17 مبرهنة : إذا كان p عدداً أولياً فإن :

$$\varphi(p^{\alpha}) = p^{\alpha-1}(p-1) = p^{\alpha} - p^{\alpha-1} \quad \text{حيث} \quad \alpha > 0$$

البرهان : إن مجموعة البواقي التامة للعدد p^{α} هي :

$$A = \{1,2,\ldots,p,p+1,\ldots,2p,\ldots,p^2\ldots\ldots,p^{\alpha-1},2p^{\alpha-1},\ldots,p.p^{\alpha-1}\}$$

وعناصر A التي لها عامل مشترك مع p^{α} هي $p,2p,\ldots,p^{\alpha-1}p$ وعددها $p^{\alpha-1}$ أي أن عدد العناصر من A الأولية نسبياً مع p^{α} هي :

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^{\alpha}(1-\frac{1}{p})$$

مثال : $\varphi(8) = \varphi(2^3) = 2^3(2-1) = 4$

2-3-18 مبرهنة : إذا كان n عدداً صحيحاً موجباً $n>1$ وكان : $n = p_1^{\alpha_2}p_2^{\alpha_2}\ldots.p_r^{\alpha_r}$

حيث $p_1,p_2,\ldots,p_r$ أوليات مختلفة فإن : $\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots\ldots(1-\frac{1}{p_r})$

البرهان : بما أن $p_i^{\alpha_i}$ أعداد أولية نسبياً مثنى مثنى وبما أن دالة أولر دالة عددية ضربية فإن :

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\ldots\varphi(p_r^{\alpha_r})$$
$$= p_1^{\alpha_2}p_2^{\alpha_2}\ldots.p_r^{\alpha_r}(1-\frac{1}{p_1})\ldots\ldots(1-\frac{1}{p_r})$$
$$\varphi(n) = n(1-\frac{1}{p_1})\ldots\ldots(1-\frac{1}{p_r})$$

مثال : $\varphi(360) = \varphi(2^3.3^2.5) = 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 96$

2-3-19 مبرهنة أولر : إذا كان $(a,m) = 1$ فإن : $a^{\varphi(m)} \equiv 1(modm)$

البرهان : إذا كانت $T = \{a_1,a_2,\ldots\ldots,a_{\varphi(m)}\}$ مجموعة بواق مختزلة بالمقاس m ، فإن المجموعة

$$T_1 = \{a_1a,a_2a,\ldots\ldots,a_{\varphi(m)}.a\}$$

هي أيضاً مجموعة بواق مختزلة بالمقاس m ، إذ أن كل عنصر من T_1 أولي نسبياً مع m وضوحاً كما أن أي عنصـــرين من T_1 غير متطابقين بالمقاس m ، لأنه لو كان $a_i.a \equiv a_j.a(modm)$ لكان $a_i \equiv a_j(modm)$ وهذا مستحيل لأنها عناصر من T . وبالتالي فإن كل عنصر من T يطابق عنصر واحد فقط من T_1 الأمر الذي يؤدي إلى أن جداء عناصر T يطابق جداء عناصر T_1 بالمقاس m ونكتب

$$a_1.a_2\ldots\ldots a_{\varphi(m)} \equiv a_1.a_2\ldots\ldots a_{\varphi(m)}.a^{\varphi(m)}(modm)$$

ولما كان $(a_1.a_2\ldots\ldots a_{\varphi(m)},m) = 1$ فإن :

$$a^{\varphi(m)} \equiv 1(modm)$$

مثال : $a^{\varphi(15)} \equiv 2^8 \equiv 1(mod15)$

2-3-20 نتيجة : إن مبرهنة فيرما الصغرى هي حالة خاصة من مبرهنة أولر إذ لو كان المقاس m عدداً أولياً لحصلنا على : $a^{\varphi(p)} \equiv a^{p-1} \equiv 1(modp)$.

تمرين : أوجد رقمي الآحاد والعشرات للعدد 2^{256}.

الحل: إن العدد المؤلف من رقمي الآحاد والعشرات يساوي باقي قسمة 2^{256} على العدد 100 ولما كان (3, 100) = 1 فإن $3^{\varphi(100)} \equiv 1(mod100)$ نحسب $\varphi(100)$ فنجد :

$$\varphi(100) = \varphi(2^2.5^2) = 100(1-\frac{1}{2})(1-\frac{1}{3}) = 40$$

أي : $3^{40} \equiv 1(mod100)$

ولدينا 16 + (6)(40) = 256 لذا نكتب :

$$3^{256} \equiv (3^{40})^6.3^{16} \equiv 3^{16}(mod100) \equiv (81)^4 \equiv (-19)^4(mod100)$$
$$3^{256} \equiv (361)^2 \equiv (61)^2 \equiv 21(mod100)$$

والرقمين المطلوبين 21 .

2-3-21 تطبيق هام : يمكن استخدام مبرهنة اولر في إيجاد حلول التطابقات الخطية

مثال (1) : لنوجد حلول التطابق $6x \equiv 15(mod21)$

نلاحظ أن $3|15, (6,21) = 3$ أي أن للتطابق ثلاثة حلول غير متطابقة بالمقاس 21 .

نختصر طرفي التطابق على 3 فنجد : $2x \equiv 5(mod7)$

ولدينا $\varphi(7) = 6$ ، نضرب طرفي التطابق بـ 2^5 فنجد : $2^6.x \equiv 5.2^5(mod7)$

وحسب مبرهنة أولر $2^6 \equiv 1(mod7)$ مما يعطي

$$x \equiv 5.2^5(mod7) \equiv 5.2^3.2^2(mod7) \equiv 5.2^2(mod7)$$
$$x \equiv 20(mod7) \equiv 6(mod7)$$

وجميع حلول التطابق غير المتطابقة بالمقاس 21 هي: $x = 6 + 7t \ ; t = 0,1,2$

أي هي : 20 , 13 , 6 .

مثال (2) : لنوجد حل التطابق $6x \equiv 15(mod29)$

الحل : إن العدد 29 عدد أولي فللتطابق حل وحيد يعطى بالعلاقة : $x \equiv 15.6^{\varphi(29)-1}(mod29)$

ولما كان $\varphi(29) = 28$ فالحل هو $x \equiv 6^{28}.15(mod29)$

$$x \equiv (36)^{14}.15(mod29) \equiv (7)^{14}.15(mod29) \equiv (49)^7.15(mod29)$$
$$\equiv (20)^7.15(mod29) \equiv 2^6.(2.15).10^7(mod29) \equiv 2^6.10^7(mod29)$$

$$x \equiv 6.10^7(mod29) \equiv 2.10^6(mod29)$$

ما تجدر ملاحظته أن الحل بهذه الطريقة يصعب كلما كانت قيمة المقاس كبيرة .

– **تمهيدية :** إذا مسح العدد d جميع قواسم n فإن $\frac{n}{d}$ يمسح أيضاً جميع قواسم n لأنه من أجل كل $d|n \Leftarrow d_1 = \frac{n}{d}|n, n = dd_1$.

مثال : إن قواسم العدد 12 هي $\{1,2,3,4,6,12\}$ وقيم $\frac{n}{d}$ المقابلة لهذه القواسم هي : $\{12,6,4,3,2,1\}$ أي هي جميع قواسم n .

2-3-22 مبرهنة : إذا كان $n \geq 1$ فإن $n = \sum_{d|n} \varphi(d)$.

البرهان (غير مطلوب): لنوزع الأعداد من 1 إلى n إلى صفوف كما يلي : إذا كان d أحد قواسم n فإن : $S_d = \{m: d = (m,n), 1 \leq m \leq n\}$

ونعلم أنه إذا كان $(m,n) = d$ فإن , $n = n_0 d$ $m = m_0 d$ ، $(n_0, m_0) = 1$,

ويقابل كل قيمة لـ m قيمة واحدة d وقيمة واحدة m_0 لذا فإن عدد عناصر كل مجموعة من S_d يساوي عدد الأعداد $m_0 = \frac{m}{d}$ الأولية نسبياً مع $n_0 = \frac{n}{d}$ التي لا تتجاوز n_0 أي أن عدد عناصر المجموعة S_d يساوي عدد الأعداد الموجبة التي لا تتجاوز $\frac{n}{d}$ وأولية نسبياً معها أي يساوي $\varphi(\frac{n}{d})$.

ولما كان كل من الأعداد $\{1,2,\ldots\ldots,n\}$ ينتمي إلى صف واحد فقط من الصفوف S_d فإننا نجد أن $n = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$

مثال (1) : لنوضح طريقة إثبات المبرهنة السابقة بالمثال التالي :

لتكن $n = 10$ إن قواسم n هي بالتالي $\{1,2,5,10\}$ لنحسب S_d :

$$S_1 = \{m: (m,10) = 1, 1 \leq m \leq 10\} = \{1,3,7,9\}$$

عدد عناصر S_1 $= \varphi\left(\frac{10}{1}\right) = \varphi(2 \times 5) = 1 \times 4 = 4$

$$S_2 = \{m: (m,10) = 2, 1 \leq m \leq 10\} = \{2,4,6,8\}$$

عدد عناصر S_2 $= \varphi(\frac{10}{2}) = \varphi(5) = 4$

$$S_5 = \{m: (m,10) = 5, 1 \leq m \leq 10\} = \{5\}$$

عدد عناصر S_5 $= \varphi(\frac{10}{5}) = 1$

$$S_{10} = \{m: (m,10) = 10, 1 \leq m \leq 10\} = \{10\}$$

عدد عناصر S_{10} $= \varphi(\frac{10}{10}) = \varphi(1) = 1$

وبالتالي :

$$n = \varphi(10) + \varphi(5) + \varphi(2) + \varphi(1) = 4 + 4 + 1 + 1 = 10$$

مثال (2) : إذا كان $n = 25$ فإن قواسم العدد 25 هي $\{25,5,1\}$

$$S_1 = \{m: (m,25) = 1, 1 \leq m \leq 25\} \Rightarrow \varphi(25) = \varphi(5^2)$$

عدد عناصر $= 5(5-1) = 20 = S_1$

$S_5 = \{m: (m,25) = 5, 1 \le m \le 25\} \Rightarrow \varphi(\frac{25}{5}) = \varphi(5) = 4$

عدد عناصر $S_5 = 4$

$S_{25} = \{25\} \Rightarrow \varphi(\frac{25}{25}) = \varphi(1) = 1 =$ عدد عناصر S_{25}

$\varphi(25) + \varphi(5) + \varphi(1) = \sum_{d|25} \varphi(d) = 20 + 4 + 1 = 25$

تمرين : أثبت أن $f(n) = 3^{10n+2} + 5^{10n+3} - 2$ يقبل القسمة على 22 علماً أن $n \ge 0$.

الحل: نلاحظ أن $(3,22) = 1$ و $(5,22) = 1$ فحسب مبرهنة أولر نكتب :

$\varphi(22) = \varphi(11).\varphi(2) = 10$ و $3^{\varphi(22)} \equiv 5^{\varphi(22)} \equiv 1 \ (mod\ 22)$

ومنه : $(3^{10})^n \equiv 1(mod22)$و$(5^{10})^n \equiv 1(mod22)$

نعوض في عبارة $f(n)$ فنجد :

$$f(n) \equiv 3^{10n+2} + 5^{10n+3} - 2 \equiv 3^2 + 5^2 - 2 \equiv 132 \equiv 0(mod22)$$

2-3-26 الدالتان $\sigma(n), \tau(n)$:

- **تعريف :** الدالة $\tau(n)$ دالة عددية قيمتها عدد القواسم الموجبة المختلفة للعدد $n \in Z^+$ ،

ومن تعريف الدالة $\tau(n)$ يمكن أن نكتب : $\tau(n) = \sum_{d|n} 1$

وعلى سبيل المثال فإن القواسم الموجبة للعدد 12 هي : $1, 2, 3, 4, 6, 12$ وعددها $\tau(12) = 6$

مبرهنة : الدالة $\tau(n)$ دالة ضربية .

في الحقيقة إن الدالة $f(d)$ دالة ضربية لأن :

$$f(1) = 1 \quad \text{و} \quad f(d_1.d_2) = f(d_1).f(d_2) = 1.1 = 1$$

ونعلم أنه إذا كانت f دالة ضربية فإن الدالة المعرفة بالمساواة $F(n) = \sum_{d|n} f(d)$ هي دالة ضربية

أي الدالة المعرفة بالمساواة $\tau(n) = \sum_{d|n} 1$ هي دالة ضربية .

2-3-27 تعيين الدالة $\tau(n)$:

1) إذا كانت $n = p^a$ حيث p عدد أولي و $a \ge 1$ فإن قواسم n الموجبة

هي $1, p, p^2, \ldots, p^a$ وعددها $a+1$ أي $\tau(p^a) = a+1$

2) إذا كانت $n > 1$ و كتبت n بالشكل القانوني أي: $n = p_1^{a_1} p_1^{a_1} \ldots p_k^{a_k}$

فإنّ : $\tau(n) = (a_1+1)(a_2+1) \ldots \ldots (a_k+1)$

الإثبات : بما أن $\tau(n)$ دالة ضربية وبما أن $p_1^{a_1}, p_2^{a_2}, \ldots\ldots, p_k^{a_k}$ أولية نسبياً مثنى مثنى فإن

$$\tau(n) = \tau(p_1^{a_1})\tau(p_2^{a_2})\ldots\ldots\tau(p_k^{a_k})$$

أي $\tau(n) = (a_1+1)(a_2+1) \ldots\ldots \ldots\ldots (a_k+1)$

أمثلة :

1) لنحسب $\tau(p)$ حيث p عدد أولي:

$\tau(p) = 1 + 1 = 2$ وبالتالي : $\tau(5) = \tau(11) = 2$

2) لنحسب $\tau(4), \tau(63)$

$\tau(4) = \tau(2^2) = 2 + 1 = 3$ ، $\tau(63) = \tau(3^2.7) = (2+1)(2) = 6$

2-3-28 : تعريف الدالة σ: هي دالة عددية قيمتها عند العدد n هي $\sigma(n)$ تساوي مجموع القواسم الموجبة المختلفة للعدد n حيث $n \in Z^+$.

فعلى سبيل المثال : $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$

$\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 4$, $\sigma(4) = 7$

ينتج من تعريف الدالة $\sigma(n)$ أنه بالامكان كتابتها على النحو : $\sigma(n) = \sum_{d|n} d$

2-3-29 : مبرهنة : الدالة σ هي دالة ضربية .

الإثبات : إن الدالة $f(d) = d$ لكل d هي دالة ضربية تماماً لأن :

$f(1) = 1$ و $f(d_1.d_2) = d_1.d_2 = f(d_1).f(d_2)$

ولما كانت $\sigma(n) = \sum_{d|n} f(d)$ و $f(d)$ دالة ضربية فإن $\sigma(n)$ هي دالة ضربية .

2-3-30 : حساب قيمة الدالة $\sigma(n)$:

1) إذا كان $n = p^a$ فإن جميع القواسم الموجبة لـــــ n هي : $1, p, p^2, \ldots\ldots, p^a$ ومجموعها

$\sigma(n) = 1 + p + p^2 + \ldots\ldots + p^a$ أي $\sigma(n) = \frac{p^{a+1}-1}{p-1}$

2) إذا كان $n > 1$ و كتب بالشكل القانوني $n = p_1^{a_1}p_1^{a_1}\ldots p_k^{a_k}$ بما أن $\sigma(n)$ دالة ضربية نجد :

$$\sigma(n) = \sigma(p_1^{a_1})\sigma(p_1^{a_1})\ldots\ldots\sigma(p_k^{a_k}) = \frac{p_1^{a_1+1}-1}{p_1-1}\ldots\ldots\frac{p_k^{a_k+1}-1}{p_k-1}$$

ويمكن كتابة عبارة $\sigma(n)$ كما يلي : $\sigma(n) = \prod_1^k \frac{p_i^{a_i+1}-1}{p_i-1}$

أمثلة : $\sigma(p) = \frac{p^2-1}{p-1} = p + 1$ حيث p عدد أولي ومنه :

$$\sigma(5) = 6, \sigma(11) = 12, \sigma(3) = 4$$

$$\sigma(180) = \sigma(2^2).\sigma(3^2).\sigma(5) = \frac{2^3-1}{1}.\frac{3^3-1}{2}.6 = 546$$

- **ملاحظة :** إن الدالتين $\sigma(n), \tau(n)$ ليستا ضربيتين تماماً إذ نلاحظ أن:

$$\tau(2).\tau(10) = 2.4 = 8, \quad \tau(20) = \tau(2^2.5) = 3.2 = 6$$

وبالتالي $$\tau(2.(10)) = \tau(20) \neq \tau(2).\tau(10)$$

وكذلك فإن $$\sigma(20) = \sigma(2^2.5) = 42$$

$$\sigma(2).\sigma(10) = 3.18 = 54$$

أي أن $$\sigma(2.(10)) = \sigma(20) \neq \sigma(2).\sigma(10)$$

2-3-31 : تمرين هام :

إن جداء القواسم الموجبة لعدد $n > 1$ يساوي $n^{\tau(n)/2}$

الحل : إذا كان d قاسماً ما لـ n فإن $n = d.d'$

ولما كان عدد القواسم الموجبة لـ n = $\tau(n)$ فإنه لدينا $\tau(n)$ من العلاقات $n = d.d'$ وحاصل ضرب هذه العلاقات معاً يعطي : $n^{\tau(n)} = \prod_{d|n} d \prod_{d'|n} d'$

ونعلم أنه إذا مسحت d جميع قواسم n فإن $d' = \frac{n}{d}$ تمسح أيضاً جميع قواسم n مما يدل على أن $\prod_{d|n} d = \prod_{d'|n} d'$

الأمر الذي يعطي : $n^{\tau(n)} = (\prod_{d|n} d)^2$

ومنه $n^{\tau(n)/2} = \prod_{d|n} d$

مثال (1) : إن قواسم العدد 16 هي $\{1,2,4,8,16\}$ و $\tau(16) = 5$

وجداء هذه القواسم : $\prod_{d|16} d = 16^{\tau(16)/2} = (16)^{5/2} = (4)^5 = 1024$

مثال (2) : أثبت أن $\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}$

الحل: نعلم أن $\sigma(n) = \sum_{d|n} d$ وأن $\sum_{d|n} d = \sum_{d|n} \frac{n}{d}$

فإذا كانت جميع قواسم n الموجبة هي $\{d_1, d_2, .., d_k\}$

فإن $\sigma(n) = \frac{n}{d_1} + \frac{n}{d_2} + \ldots + \frac{n}{d_k} = n(\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_k})$

أي $\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}$

مثال (3) : أوجد العدد الصحيح n الذي يحقق العلاقة :

$$\tau(10n) = 10$$

لدينا $10 = 2.5$ فهو جداء عددين أوليين فقط لذا فإن $10n$ يلزم أن تكون من الشـــكل

$10n = 2^a.5^b$ وعندها يكون

$$\tau(10n) = (a+1)(b+1) = 10$$

ومنه نجد أنه إما $a = 1, b = 4 \Leftarrow b+1 = 5, a+1 = 2$

ومنه فإن $n = 5^3 = 125 \Leftarrow 10n = 2.5^4$

أو $b = 1, a = 4 \Leftarrow b+1 = 2, a+1 = 5$

و $n = 2^3 = 8 \Leftarrow 10n = 2^4.5$

2-3-32 : الأعداد التامة أو الأعداد الكاملة (*Perfect Numbers*)

- تعاريف :

- نقول إن العدد الصحيح n هو عدد كامل إذا كان $\sigma(n) = 2n$.

إن أصغر عددين كاملين معروفين هما $n = 6$ حيث $\sigma(6) = \sigma(2).\sigma(3)$

$\sigma(6) = 12 = (2)(6)$ أي $\sigma(6) = \frac{2^2-1}{2-1}\frac{3^2-1}{3-1} = \frac{3(8)}{2} = 12$

والعدد $n = 28$ حيث $\sigma(28) = \sigma(2^2).\sigma(7) = (7)(8) = 56 = (2)(28)$

- ونقول إن العدد الصحيح n فوق الكامل إذا كان $\sigma(n) > 2n$.

مثال ذلك العدد 12 حيث $\sigma(12) = \sigma(2^2).\sigma(3) = 28 > (2)(12)$

- ونقول إن العدد الصحيح n تحت الكامل إذا كان $\sigma(n) < 2n$.

مثال ذلك العدد 8 إذ أن $\sigma(8) = \sigma(2^3) = 15 < (2)(8)$

- نقول إن العددين m, n عددان متحابان إذا كان:

$$\sigma(n) = \sigma(m) = n + m$$

أو إذا كان $\sigma(n) - n = m \wedge \sigma(m) - m = n$

مثال ذلك : 284 و 220

وقد وجد العلماء عدداً من الأعداد الكاملة وكلها زوجية ، هل يوجد عدد كامل فردي ؟ مسـألة مفتوحة ، هل يوجد عدد غير منته من الأعداد الكاملة ؟ لقد وجد أن العدد االخامس هو $p_5 = 33.550336$ وأن العدد الســادس مؤلف من عشـرة أرقام مما يدل على ندرة هذه الأعداد . ولم يعرف حتى عام 1968

ســـوى 23 عدداً كاملاً وكلها زوجية ، وقد تبين أنه إن وجد عدد كامل فردي فهو أكبر حتماً من العدد 10^{200}.

إن مســـألة البحث عن صـــيغة للأعداد الكاملة مســـألة قديمة وقد أثبت اقليدس أنه إذا كان المجموع $1 + 2 + 2^2 + \ldots\ldots + 2^{k-1} = p$ عدداً أولياً فإن العدد $2^{k-1}.p$ هو عدد كامل وعلى ســـبيل المثال إن : $1 + 2 + 4 = 7$ هو عدد أولي و $28 = (7)(4)$ هو عدد كامل ، وقد أثبت أولر بعد 2000 سنة أن جميع الأعداد الكاملة الزوجية لها هذا الشكل الأمرالذي سنوضحه في المبرهنة التالية:

2-3-33 مبرهنة : إذا كان العدد $2^k - 1$ حيث $k > 1$ أولياً فإن :

$n = 2^{k-1}(2^k - 1)$ هو عدد كامل وكل عدد كامل زوجي هو من الشكل السابق.

البرهان : لنفترض أن العدد $2^k - 1 = p$ عدد أولي ولنكتب $n = 2^{k-1}.p$

نلاحظ أن $(2^k, p) = 1$ لأن p عدد فردي ولأن عوامل 2^{k-1} هي قوى العدد 2 حصـــراً لذا يمكن أن نكتب :

$$\sigma(n) = \sigma(2^{k-1})\sigma(p) = (2^k - 1)(p + 1)$$
$$\sigma(n) = (2^k - 1)2^k = 2(2^k - 1)2^{k-1} = 2n$$

و n بالتالي هو عدد كامل .

العكس : لنفترض أن العدد n عدد كامل زوجي. إن أي عدد زوجي n يمكن أن يكتب على النحو $n = 2^{k-1}.q$ حيث q عدد فردي و $k \geq 2$ ولما كان $(2^{k-1}, q) = 1$ فإن :

$$\sigma(n) = \sigma(2^{k-1})\sigma(q) = (2^k - 1)\sigma(q)$$

ومن جهة أخرى فإن $\sigma(n) = 2n = 2^k q$

والعلاقة $2^k q = (2^k - 1)\sigma(q)$ تدل على أن $2^k - 1 \mid 2^k.q$

ولما كان $(2^k - 1, 2^k) = 1$ فإن : $2^k - 1 \mid q$

لذا يمكن أن نكتب $q = (2^k - 1)M$ نعوض هذه القيمة لـ q في العلاقة $2^k q = (2^k - 1)\sigma(q)$ ونختصر على $(2^k - 1)$ فنجد أن: $2^k M = \sigma(q)$

وبما أن M و q كلاهما يقسم q و $M < q$ فإن : $\sigma(q) \geq q + M$

ولكن : $q + M = 2^k M$ أي أن $\sigma(q) = q + M$ مما يدل على أن للعدد q قاســـمان فقط هما M و q ينتج من ذلك أن q عدد أولي وأن $M = 1$. نعوض في قيمة q لنجد أخيراً أن : $q = 2^k - 1$ وهو المطلوب .

2-3-34 مبرهنة : إذا كان العدد $a^k - 1$ عدداً أولياً عندما $a > 0\ ,\ k \geq 2$

فإن : $a = 2$ و k عدد أولي .

الإثبات : نعلم أن : $a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \ldots\ldots + a + 1)$

ولما كان $a>0$ و $k \geq 2$ فإن المقدار $a^{k-1} + a^{k-2} + \ldots\ldots + a + 1 \geq a + 1 > 1$

وحسب الفرض فإن $a^k - 1$ عدد أولي أي أنّ العامل الثاني لـ $a^k - 1$ يجب أن يساوي الواحد ومنه

a-1 = 1 و $a = 2$

ومن جهة ثانية إذا كان k عدداً مؤلفاً لأمكن كتابته على النحو :

$k = r.s$ حيث s >1 و r >1 وبالتالي فإن :

$$a^k - 1 = (a^r)^s - 1 = (a^r - 1)(a^{r(s-1)} + a^{r(s-2)} + \ldots\ldots + a^r + 1)$$

ولكن وجدنا أن $a = 2$ و $r > 1$ مما يدل على أن قيمة كل من العاملين في الطرف الثاني أكبر من الواحد وهذا يناقض كون $a^k - 1$ عدداً أولياً مما يثبت أن k لا بد وأن يكون أولياً .

- ملاحظة:

نلاحظ أنه من أجل k = 2 فإن $2^2 - 1 = 3$ عدد أولي والعدد $2(2^2 - 1) = 6$ عدد كامل .

ومن أجل k = 3 فإن $2^3 - 1 = 7$ عدد أولي والعدد $2^2\,(2^3 - 1) = 28$ عدد كامل

ومن أجل k = 5 فإن $2^5 - 1 = 31$ عدد أولي والعدد $2^4\,(2^5 - 1) = 496$ عدد كامل

ظن الرياضـــيون القدماء أن الصـــيغة $2^p - 1$ تعطي دوماً أعداداً أولية ، إلى أن تم في عام 1536 إثبات أن العدد $2^{11} - 1 = 2047 = (23)(89)$

- ملاحظة :

تسمى الأعداد $M_k = 2^k - 1$ حيث $k \geq 2$ أعداد ميرسن(($Mersenne\ numbers$))

وتدعى الأعداد الأولية $M_p = 2^p - 1$ أوليات ميرسن ، وقد كتب ميرسن عام (1644) أن M_p أعداد أولية من أجل القيم : $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$

ومؤلفة من أجل بقية الأوليات $p < 257$. وقد تحقق أولرعام 1772 من أن M_{31} عدد أولي . ثم أثبت لوكاس عام 1876 أن M_{67} عدد مؤلف ، مخالفا لتوقع ميرسن ، ولكن دون أن يعين عوامله الأولية التي عينها بعد ذلك الرياضي الأمريكي غريدريك نلسون كول عام 1903 .

2-3-35 دالة موبياس (*Mobius - function*) :

تعريف : نعرف الدالة $\mu(n)$ حيث n عدد صحيح موجب كما يلي :

$$\mu(n)=\begin{cases}1 & n=1 \text{ عندما} \\ 0 & p^2 \mid n \text{ إذا وجد عدد أولي } p \text{ بحيث} \\ (-1)^r & \text{إذا كان } n=p_1p_2\dots p_r \text{ و } p_i \text{ مختلفة أوليات}\end{cases}$$

من التعريف ينتج أن $\mu(1)=1,\mu(2)=-1,\mu(3)=-1$

$\mu(4)=0,\mu(5)=-1,\mu(6)=1$

لاحظ أن :

$\mu(p)=-1$ دوماً عندما p عدد أولي

$\mu(p^k)=0$ من أجل p عدد أولي و $k\geq 2$

2-3-36 مبرهنة دالة موبياس ضربية :

الإثبات : إن $\mu(1)=1$ كما مر معنا ولنثبت أن $\mu(m.n)=\mu(m).\mu(n)$

عندما $(m\ ,n)=1$ نلاحظ أنه إذا كان p عدداً أولياً وكان

$p^2|m$ أو $p^2|n$ فإن $p^2|m.n$ وبالتالي :

$$\mu(m.n)=0=\mu(m).\mu(n)$$

لنفترض الآن أن $m=p_1p_2\dots p_r$ وأن $n=q_1q_2\dots q_s$

حيث p_i,q_j أوليات مختلفة . فعندها نكتب

$$\mu(m.n)=\mu(p_1p_2\dots p_rq_1q_2\dots q_s)=(-1)^{r+s}=(-1)^r(-1)^s=\mu(m)\mu(n)$$

2-3-37 مبرهنة : من أجل أي عدد صحيح $n\geq 1$ فإن :

$$G(n)=\sum_{d|n}\mu(d)=\begin{cases}1 & n=1 \text{ عندما} \\ 0 & n>1 \text{ عندما}\end{cases}$$

الإثبات (غير مطلوب): نلاحظ أن $\sum_{d|1}\mu(d)=\mu(1)=1$ لنفترض أن $n>1$ ولنحسب $G(n)$

1) إذا كان $n=p^k$ نكتب :

$$G(n) = G(p^k) = \sum_{d|n} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^k)$$
$$G(p^k) = \mu(1) + \mu(p) = 1 + (-1) = 0$$

2) إذا كان $n = p_1^{k_1} p_2^{k_2} \ldots\ldots\ldots p_r^{k_r}$ فإن

$$G(n) = G(p_1^{k_1} p_2^{k_2} \ldots\ldots\ldots p_r^{k_r}) = G(p_1^{k_1}).\, G(p_2^{k_2}) \ldots\ldots G(p_r^{k_r})$$

ولما كانت الدالة $\mu(d)$ ضربية فإن $G(n)$ دالة ضربية وينتج من ذلك أن : $G(n) = 0$

مثال : لتكن $n = 10$ ، إن قواسم n هي $1\ ,\ 2\ ,\ 5\ ,\ 10$ ومنه

$$G(10) = \sum_{d|10} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10) = 1 + (-1) + (-1) + 1 = 0$$

2-3-38 صيغة موبياس للتعاكس : (*Mobius inversion formula*)

إذا كانت : F , f دالتين عدديتين وكان : $F(n) = \sum_{d|n} f(d)$

فإن : $f(n) = \sum_{d|n} \mu(d)\, F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d})\, F(d)$

الإثبات (غير مطلوب): نلاحظ أولاً أن الدالة $f(n)$ تتعين بشكل وحيد بدلالة $F(n)$ لأن :

$$f(2) = F(2) - F(1) \Leftarrow F(2) = f(2) + f(1) \quad , \quad F(1) = f(1)$$
$$f(3) = F(3) - F(1) \Leftarrow F(3) = f(1) + f(3)$$

وهكذا نوجد قيم f بشكل تدريجي بدلالة F. ولحساب المقدار $\sum_{d|n} \mu(d)\, F(\frac{n}{d})$ نكتب من تعريف الدالة F :

$$F(\frac{n}{d}) = \sum_{m|\frac{n}{d}} f(m)$$

نضرب الطرفين بـ $\mu(d)$ ونجمع على قواسم n الموجبة فنجد :

$$* \sum_{d|n} \mu(d)\, F(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{m|\frac{n}{d}} f(m) = \sum_{d|n} \sum_{m|\frac{n}{d}} \mu(d) f(m)$$

ولكن القول إن d تمسح جميع قواسم n و m تمسح جميع قواسم $\frac{n}{d}$ يكافىء القول إن m تمسح جميع قواسم n و d تمسح جميع قواسم $\frac{n}{m}$ لذا يمكن أن نكتب العلاقة * على النحو :

$$\sum_{d|n} \mu(d)\, F(\frac{n}{d}) = \sum_{m|n} f(m) \sum_{d|\frac{n}{m}} \mu(d)$$

ولكن قيمة المجموع $\sum_{d|\frac{n}{m}} \mu(d)$ **حسب المبرهنة 2-3-37** تساوي الواحد عندما $\frac{n}{m} = 1$ أي عندما $m = n$ وتساوي الصفر فيما عدا ذلك الأمر الذي يبين أن :

$$\sum_{d|n} \mu(d)\, F(\frac{n}{d}) = \sum_{m=n} f(m) \,.\, 1 = f(n)$$

- **ملاحظة:** نعلم أن إذا مسحت d جميع قواسم n فإن $\frac{n}{d}$ تمسح أيضاً قواسم n لذا يمكن أن نكتب :

$$f(n) = \sum_{d|n} \mu(d)\, F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d})\, F(d)$$

وعلى سبيل المثال نأخذ $n = 10$ فتكون قواسم n هي $1\ ,\ 2\ ,\ 5\ ,\ 10$ ونكتب

$$\sum_{d|10}\sum_{m|\frac{10}{d}}\mu(d)f(m)=\mu(1)[f(1)+f(2)+f(5)+f(10)]+$$
$$+\mu(2)[f(1)+f(5)]+\mu(5)[f(1)+f(2)]+\mu(10)f(1)$$

$$=f(1)[\mu(1)+\mu(2)+\mu(5)+\mu(10)]+f(2)[\mu(1)+\mu(5)]+$$
$$+f(5)[\mu(1)+\mu(2)]+f(10)\mu(1)=\sum_{m|10}\sum_{d|\frac{10}{m}}f(m)\mu(d)$$

39−3−2 تطبيقات

1− نعلم أن $\tau(n)=\sum_{d|n}1$ و $\sigma(n)=\sum_{d|n}d$

باستخدام صيغة موبياس للتعاكس نجد أن

$n=\sum_{d|n}\mu(\frac{n}{d})\sigma(d)$ و $1=\sum_{d|n}\mu(\frac{n}{d})\tau(d)$

عندما $n\geq 1$

40−3−2 مبرهنة : إذا كانت f , F دالتين عدديتين وكان $F(n)=\sum_{d|n}f(d)$

وإذا كانت $F(n)$ دالة ضربية فإن f دالة ضربية .

البرهان(غير مطلوب)

ونهاية هذا الفصل سنورد تعريفاً لدالتين عدديتين دون التعرض لخواصهما

تعريف (1) : دالة ليوفيل $\lambda(n)$ (*Liouville's Function*)

نعرف دالة ليوفيل كما يلي :

$$\lambda(n)=\begin{cases}1 & n=1 \text{ عندما}\\ (-1)^{\alpha_1+\alpha_2+\dots+\alpha_r} & n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r} \text{ عندما}\end{cases}$$

$$\boldsymbol{\lambda(1)=1,\lambda(2)=\lambda(3)=\lambda(5)=-1}$$

مما يدل على أن

$$\boldsymbol{\lambda(4)=\lambda(6)=1,\lambda(7)=\lambda(8)=-1,\lambda(9)=\lambda(10)=1}$$

ويلاحظ مباشرة من التعريف أنها دالة ضربية .

تعريف (2) : دالة مانجولد $\wedge(n)$ (*Mangoldt Function*)

نعرف دالة مانجولد كما يلي :

$$\wedge(n)=\begin{cases}\log p & \text{عندما } n=p^k \text{ و } p \text{ أولي و } k\geq 1\\ 0 & \text{فيما عدا ذلك}\end{cases}$$

تمرين : برهن أن

1. $\sum_{d|n}\wedge(n)=\log n$
2. $\wedge(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)\log d$

تمارين

1) أثبت أنه إذا كان $\alpha,\beta\in\Re$ فإن :

1) $[4\alpha]+[4\beta]\geq 2[\alpha]+2[\beta]+[\alpha+\beta]$
2) $[4\alpha]+[4\beta]\geq 3[\alpha]+3[\beta]+[\alpha+\beta]$
3) $[3\alpha]+[3\beta]\geq [\alpha]+[\beta]+2[\alpha+\beta]$

2) إذا كان $n\ ,\ m$ عددين صحيحين فأثبت أن :

1) $\frac{(4m)!(4n)!}{(m!)^2(n!)^2[(m+n)!]^2}$ هو عدد صحيح

2) $\frac{(4m)!(4n)!}{(m!)^3(n!)^3(m+n)!}$ هو عدد صحيح

3) $\frac{(3m)!(3n)!}{m!n![(m+n)!]^2}$ هو عدد صحيح

3) أثبت أن أس اكبر قوة للعدد 7 تقسم $(7^n-3)!$ هي $(7^n-6n-1)/_6$

4) أثبت أن أس اكبر قوة للعدد 5 تقسم $(5^n-4)!$ هي $(5^n-4n-1)/_4$

5) أوجد أس أكبر قوة للعدد 3 تقسم $80\ !$.

6) أوجد أس أكبر قوة للعدد 7 تقسم $2400\ !$.

7) إذا كان n عدداً صحيحاً موجباً فأثبت أن : $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3)=0$

8) إذا كان $n \geq 3$ أثبت أن $\sum_{k=1}^{n} \mu(k!) = 1$.

9) إذا كان $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ حيث $p_1, p_2, \dots, p_r$ أوليات مختلفة وإذا كانت الدالة f دالة ضربية فأثبت أن :

1) $\sum_{d|n} \mu(d)\, f(d) = (1 - f(p_1))(1 - f(p_2)) \dots\dots (1 - f(p_r))$

2) $\sum_{d|n} \mu(d)\, \tau(d) = (-1)^r$

3) $\sum_{d|n} \mu(d)\, \sigma(d) = (-1)^r p_1 p_2 \dots\dots p_r$

4) $\sum_{d|n} d\, .\mu(d) = (1 - p_1)(1 - p_2) \dots\dots (1 - p_r)$

10) إذا كان $\lambda(n)$ دالة ليوفيل و $n > 0$ فأثبت أن :

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{إذا وجد عدد صحيح } m \text{ بحيث } n = m^2 \\ 0 & \text{فيما عدا ذلك} \end{cases}$$

11) إذا كان $(a, 30) = 1$ أثبت أن $240 \mid a^4 - 1$.

12) إذا كان $n \geq 0$ أثبت أن $f(n)$ $240 \mid$ حيث $f(n) = 6.17^{4n} - 5.13^{4n^2} - 1$

13) إذا كان a عدداً فردياً و $(a, 3) = 1$ أثبت أن: $192 \mid a^4 + 14a^2 - 96a + 81$

14) أثبت أن $\tau(n)$ يكون عدداً فردياً إذا وفقط إذا كان n مربعاً كاملاً .

15) أثبت أن $\sigma(n)$ يكون عدداً فردياً إذا وفقط إذا كان $n = m^2$ أو $n = 2m^2$ من أجل عدد ما m.

16) أوجد صيغة n حتى يكون $\tau(n) = 10$ ، هل يوجد عدد n يحقق العلاقة: $\sigma(n) = 10$ ؟

17) إذا كان $k \geq 0$ أثبت ما يلي : $n = 2^{k-1} \Rightarrow \sigma(n) = 2n - 1$

18) احسب : 1) $\psi(3025)$ علماً أن $e_1 = 1, e_2 = 4, e_3 = 7$

2) $\psi(50)$ علماً أن $e_1 = 0, e_2 = 3, e_3 = 4$

3) $\psi(168)$ علماً أن $e_1 = 0, e_2 = 1, e_3 = 9$

19) أثبت أن قوة عدد أولي لا يمكن أن يكون عدداً كاملاً .

20) أثبت أن n^2 لا يمكن أن يكون عدداً كاملاً .

21) جداء أي عددين أوليين فرديين ليس عدداً كاملاً .

22) إذا كان n عدداً كاملاً أثبت أن $\sum_{d|n} \frac{1}{2} = 2$

23) من أجل أي عدد كامل $n > 6$ أثبت أن مجموع أرقام n يطابق الواحد بالمقاس 9 .

24) أثبت أنه لا يمكن لأي قاسم لعدد كامل أن يكون كاملاً .

25) استخدم مبرهنة اولر لإثبات ما يلي :

$1) a^{37} \equiv a(mod 1729)$

$2) a^{13} \equiv a(mod 2730)$

$3) a^{33} \equiv a(mod 4080)$ علماً أن a عدد صحيح فردي

26) أثبت أنه إذا كان $(a,n) = (a-1,n) = 1$ فإن :

$$1 + a + a^2 + \ldots\ldots + a^{\varphi(n)-1} \equiv 0(mod n)$$

27) إذا كان $(m,n) = 1$ حيث n و m عددان صحيحان موجبان

فأثبت أن: $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1(mod mn)$

28) أثبت أن المجموعة $\{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ هي مجموعة بواقي مختزلة بالمقاس 14 .

29) أثبت أن المجموعة $\{2, 2^2, 2^3, \ldots\ldots, 2^{16}\}$ هي مجموعة بواقي مختزلة بالمقاس 27 .

30) إذا كان $n > 1$ لا يحوي عوامل أولية مكررة فأثبت أن $\tau(n^2) = n$ إذا

وفقط إذا كان $n = 3$.

31) أثبت أن $3|\sigma(3n+2)$ و $4|\sigma(4n+3)$ من أجل أي عدد صحيح موجب n .

الفصل الرابع

المراتب والجذور الأولية والأدلة

4-1 المراتب والجذور الأولية والأدلة

4-2-1 تعريف المرتبة : إن مرتبة العدد a بالمقاس m (أو الأس الذي ينتمي إليه العدد الصحيح a بالمقاس m) حيث $(a , m) = 1$ هوأصغر عدد صحيح موجب e يحقق العلاقة $a^e \equiv 1(modm)$ ، ونقول إن e هو الدليل الذي ينتمي إليه العدد a بالمقاس m ونكتب $e \equiv Inda(modm)$

مثال : نلاحظ أن :

- مرتبة العدد 2 بالمقاس7 هي3 لان: $2^3 \equiv 1(mod7)$, $2^2 \equiv 4(mod7)$ $2^1 \equiv 2(mod7)$,
- مرتبة العدد 2 بالمقاس 6 هي 5 لان: $2^5 \equiv 1(mod6)$

كذلك نقول إن2 هو دليل العدد 5 بالمقاس 6 .

- مرتبة العدد 3 بالمقاس 14 هي 6 ذلك أن :

$3^1 \equiv 3(mod14)$, $3^2 \equiv 9(mod14)$, $3^3 \equiv -1(mod14)$,
$3^4 \equiv 11(mod14)$, $3^5 \equiv 5(mod14), 3^6 \equiv 1(mod14)$,

- **4-2-2 مبرهنة :** إذا كانت مرتبة العدد الصحيح a تساوي e بالمقاس m فإن $a^k \equiv 1(modm)$ إذا وفقط إذا كان $e|k$

الإثبات : إذا كان $e|k$ فإن $k = ee_1$ وبالتالي

$$e^k = (e^e)^{e_1} \equiv (1)^{e_1} \equiv 1(modm)$$ فإن

وبالعكس إذا كان k عدداً صحيحاً موجباً يحقق العلاقة $a^k \equiv 1(modm)$

فحسب خوارزمية القسمة نكتب $k = eq + r 0 \leq r < e$

$$a^k \equiv (a^e)^q . a^r (modm)$$

ولما كان كل من a^k و a^e يطابق الواحد بالمقاس m فإن العلاقة الأخيرة تعطي $a^r \equiv 1(modm)$ ولكن حسب تعريف المرتبة فإن e هي أصغر عدد صحيح موجب يحقق التطابق السابق و $0 \leq r < e$

إذاً $r = 0$, $k = e\,q$ أي $e|k$

– **نتيجة :** نعلم من مبرهنة أولر أن $a^{\varphi(m)} \equiv 1(modm)$ مما يدل على أنه إذا كانت e مرتبة a بالمقاس m فإن e يجب أن تقســـم $\varphi(m)$ وبالتالي يكفي أن تبحث عن مرتبة العدد a بالمقاس m بين قواسم $\varphi(m)$

فعلى سبيل المثال إذا أردنا البحث عن مرتبة العدد 2 بالمقاس 13 نحسب $\varphi(13) = 12$ ونبحث عن المرتبة بين قواسم العدد 12 أي بين الأعداد $1 , 2 , 3 , 4 , 6 , 12$ فنكتب

$2^{12} \equiv 1(mod13)$, $2^6 \equiv 12$,$2^4 \equiv 3$,$2^2 \equiv 4$, $2^3 \equiv 8$,

أي أن مرتبة العدد 2 هي 12 بالمقاس 13

– **تمرين :** هل يوجد عدد a مرتبته بالمقاس $\varphi(12)$ بالمقاس 12 ؟ أي هل للمعادلة $a^4 \equiv 1(\ mod\ 12)$ حل؟

نعلم من التعريف أن العددa إن وجد يجب أن يكون أولياً نســبياً مع 12 و يصــغره لذا نبحث عن العدد a ضمن مجموعة البواقي المختزلة للعدد 12 أي ضمن المجموعة $\{1,5,7,11\}$ و هنا نرى أن :

$$1^2 = 5^2 = 7^2 = 11^2 \equiv 1(mod12)$$

إذاً لا يوجد للمعادلة المعطاة حل.

4–2–3 مبرهنة : إذا كانت مرتبة a بالمقاس m هي e فإن $a^t \equiv a^s(modm)$ إذا وفقط إذا كان $t \equiv s(mode)$

الإثبات : لنفترض أولاً أن $a^t \equiv a^s(modm)$ حيث $t \geq s$. و نعلم أن $(\ a\ ,\ m\ ) = 1$ لذا يمكن اختصار a^s من الطرفين لنجد : $a^{t-s} \equiv 1(modm)$

وحسب ماسبق فإن $e|t-s$ أي $t \equiv s(mode)$

وبالعكس إذا كان $t \equiv s(mode)$ لأمكننا أن نكتب : $t = s + qe$

ولدينا $a^e \equiv 1(modm)$ أي $a^t \equiv a^s.(a^e)^q \equiv a^{s+qe} \equiv a^s(modm)$

– **نتيجة:** إذا كانت مرتبة a بالمقاس m هي e فإن الأعداد $a, a^2, \ldots, a^e$ غير متطابقة بالمقاس m .

البرهان : لو كان $a^t \equiv a^s(modm)$ حيث $1 \leq s \leq t \leq e$

فإن المبرهنة السابقة تؤكد أن $t \equiv s(mode)$ وهذا غير ممكن من أجل القوى المختلفة لـ a السابقة .

4–2–4 مبرهنة : إذا كانت مرتبة العدد a تساوي e بالمقاس m وكان $k > 0$ **فإن مرتبة** a^k بالمقاس m هي $\frac{e}{d}$ حيث $d = (k, e)$

الإثبات : لما كان $d = (k, e)$ فإن : $k = k_0 d$, $e = e_0 d$ و $(k_0, e_0) = 1$

فإذا افترضنا أن r هي مرتبة a^k بالمقاس m لكان :

$$e|kr \Rightarrow e_0|k_0 r(a^k)^r \equiv a^{kr} \equiv 1(modm) \Rightarrow$$

ولما كان $(k_0, e_0) = 1$ ينتج أن $e_0|r$ (1)

ومن جهة أخرى نكتب : $e|kr \Rightarrow e_0|k_0 r(a^e)^{k_0} \equiv a^{ek_0} \equiv a^{edk_0} \equiv (a^k)^{e_0} \equiv 1(modm)$

ولما كانت r هي مرتبة a^k بالمقاس m فإن $r|e_0$ (2)

ومن العلاقتين (1) و(2) ينتج أن $r = e_0 = \frac{e}{d}$

– **نتيجة :** إذا كان $(k, e) = 1$ فإن مرتبة a^k تساوي مرتبة a بالمقاس m

تمرين : عين مراتب الأعداد من 1 إلى 12 بالمقاس 13

الحل : بالاعتماد على المبرهنات السابقة يمكن أن نرتب الجدول التالي :

العدد	1	2	3	4	5	6	7	8	9	10	11	12
المرتبة	1	12	3	6	4	12	12	4	3	6	12	2

يلاحظ من الجدول أن مرتبة العدد 2 بالمقاس 13 تساوي 12

ومرتبة $2^2 = 4$ تساوي $\frac{12}{2} = 6$

ومرتبة $2^3 = 8$ تساوي $\frac{12}{3} = 4$

ومرتبة $2^4 \equiv 3(mod13)$ تساوي $\frac{12}{4} = 3$

ومرتبة $2^5 \equiv 6(mod13)$ تساوي 12 لأن $(5,12) = 1$

ومرتبة $2^6 \equiv 12(mod13)$ تساوي $\frac{12}{6} = 2$ لأن $(6,12) = 6$

ومرتبة $2^7 \equiv 11(mod13)$ تساوي 12 لأن $(7,12) = 1$

ومرتبة $2^8 \equiv 9(mod13)$ تساوي $\frac{12}{4} = 3$ ويمكن أن نكتب $9 = 3^2$, $(2,3) = 1$ فمرتبة 9 تساوي مرتبة 3 بالمقاس 13 أي = 3

ومرتبة $2^9 \equiv 5(mod13)$ تساوي $\frac{12}{(9,12)} = 4$

ومرتبة $2^{10} \equiv 10(mod13)$ تساوي $\frac{12}{(10,12)} = 6$

ومرتبة $2^{11} \equiv 7(mod13)$ تساوي $\frac{12}{(11,12)} = 12$

4–2–5 مبرهنة : إذا كانت مرتبة العدد a تساوي e بالمقاس m ومرتبة العدد b تساوي f بالمقاس m وكان $(e, f) = 1$ فإن مرتبة $a.b$ بالمقاس m تساوي $e.f$

الإثبات : لنفترض أن مرتبة $a\,.\,b$ بالمقاس m هي k أي أن

$(a.b)^k \equiv 1(modm)$ وبرفع الطرفين إلى القوة e نجد :

$$((ab)^k)^e \equiv (a^e)^k b^{ke} \equiv b^{ke} \equiv 1(modm)$$

ولما كانت مرتبة b هي f فإن $f|ke$ ولكن $(f,e)=1$ الأمر الذي يعطي $f|k$

وبمناقشة مماثلة يمكن أن نكتب : $((ab)^k)^f \equiv a^{kf}.(b^f)^k \equiv a^{kf} \equiv 1(modm)$

ولما كانت مرتبة a هي e بالمقاس m فإن $e|kf$ و$(f,e)=1$ أي

$e|k$ وبالتالي فإن $e.f|k$ (1)

ومن جهة أخرى نجد أن $(ab)^{e.f} \equiv (a^e)^f.(b^f)^e \equiv 1(modm)$

ولما كانت مرتبة $a.b$ هي k فإن $k|e.f$ (2)

من العلاقتين (1) و (2) نجد أن $k = e.f$

مثال : نلاحظ أن مرتبة العدد 2 بالمقاس 7 تساوي 3 ومرتبة العدد 6 بالمقاس 7تساوي 2 و $(2,3)=1$ ، وبالتالي فإن مرتبة العدد الناتج عن ضربهما بالمقاس7

$2.6 = 12 \equiv 5(mod7)$ تساوي $3\,.\,2 = 6$ أي: $5^6 \equiv 1(mod7)$

والعدد 6 هو أصغر عدد يحقق هذا التطابق .

4-2 الجذور الأولية والأدلة ((*Primitive roots , Indices*))

4-2-1 تعريف الجذر الأولي : إذا كان $(a,m)=1$ وكانت مرتبة a بالمقاس m تساوي $\varphi(m)$ فإن a يدعى الجذر الأولي للعدد m.

أي إذا كان العدد $\varphi(m)$ هو أصغر عدد صحيح موجب يحقق العلاقة $a^{\varphi(m)} \equiv 1(modm)$ وكان $(a,m)=1$ فإن a هو جذر أولي للعدد m .

يمكن أن يكون لعدد ما عدة جذور أولية بالمقاس m وقد لا يوجد لعدد ما أي جذر أولي .

مثال : رأينا سابقاً أن مرتبة كل عدد من الأعداد $\{2,6,7,11\}$ تساوي $\varphi(13)=12$ فللعدد 13 أربعة جذور أولية أو نقول أن للمعادلة $a^{12} \equiv 1(mod13)$ أربعة حلول.

كما رأينا أنه لا يوجد أي عدد مرتبته تساوي 4 بالمقاس 12 ونعلم أن $\varphi(12)=4$ أي ليس للعدد 12 أي جذر أولي .

4-2-2 مبرهنة : إذا كان $(a,m)=1$ وإذا كان a جذراً أولياً للعدد m فإن مجموعة الأعداد $\{a, a^2, \ldots\ldots, a^{\varphi(m)}\}$ هي بواقي مختزلة بالمقاس m.

الإثبات : بما أن a جذر أولي لـ m فإن $a^{\varphi(m)} \equiv 1(modm)$ وحسب نتيجة المبرهنة **8−2−3** فإن الأعداد التالية التي عددها $\varphi(m)$: $a, a^2, \ldots\ldots, a^{\varphi(m)}$ غير متطابقة بالمقاس m . ولدينا من جهة ثانية $(a,m) = 1$ مما يدل على أن قوى a هي أولية نسبياً أي أن المجموعة $T_m = \{a, a^2, \ldots\ldots, a^{\varphi(m)}\}$ هي مجموعة بواقي مختزلة بالمقاس m .

4−2−3 مبرهنة : إذا وجد جذر أولي للعدد m وكان هذا الجذر هو a حيث $(a,m) = 1$ فإن العدد m يملك $\varphi(\varphi(m))$ جذراً أولياً .

الإثبات : لنفترض أن a هو جذر أولي للعدد m أي $(a,m) = 1$ ومرتبة $\varphi(m) = a$ بالمقاس m . إن أي جذر أولي لـــ m يجب أن يكون أولياً نسبياً مع m فهو أحد عناصر مجموعة البواقي المختزلة بالمقاس m أي هو أحد عناصر المجموعة $T_m = \{a, a^2, \ldots\ldots, a^{\varphi(m)}\}$.

ونعلم أن مرتبة a^k بالمقاس m تساوي مرتبة a بالمقاس m إذا كان $(\varphi(m), k) = 1$ أي أن عدد العناصـــر التي مرتبتها هي $\varphi(m)$ من المجموعة $T(m)$ (أي عدد الجذور الأولية للعدد m) يساوي عدد العناصر الأولية نسبياً مع $\varphi(m)$ من بين عناصر $T(m)$ فهو يساوي $\varphi(\varphi(m))$.

– **نتيجة :** إذا كان p عدداً أولياً وإذا كان r جذراً أولياً لـــــ p أي إذا كانت مرتبة r هي $\varphi(p) = p - 1$ فإن عدد الجذور الأولية للعدد p يساوي $\phi(p-1)$.

وعلى سبيل المثال إذا كان p= 7 فإن $\varphi(7) = 6$ و $\varphi(6) = 2$ فإنه يوجد للعدد 7 جذران أوليان هما 3 , 5 , ذلك أن أس أصغر قوة للعدد 3 يحقق التطابق $3^e \equiv 1(mod7)$ هو 6 أي أن العدد 3 هو الجذر أولي للعدد 7 و $3^6 \equiv 1(mod7)$ كذلك نجد أن 3^e حيث $(e,6) = 1$ يحقق $e = 5$ أي هو 3^5 ولدينا $3^5 \equiv 5(mod7)$ ومنه $5^6 \equiv 1(mod7)$ أي العدد 5 جذراً أولياً ثاني للعدد 7 .

سنورد فيما يلي المبرهنة الهامة التالية دون سرد لإثباتها .

4−2−4 مبرهنة : يوجد للعدد m جذر أولي إذا وفقط إذا كان m=2 أو m=4 أو من الشـــكل $m = p^n$ أو $m = 2p^n$ حيث p عدد أولي فردي و n عدد صحيح موجب .

تمرين : أوجد الجذور الأولية للعدد 9 .

الحل : إن مجموعة البواقي المختزلة للعدد 9 هي : $T(9) = \{1,2,4,5,7,8\}$

والجذور الأولية إن وجدت تساوي قوى عناصر المجموعة $T(9)$.

ونلاحظ أن: $2^2 = 4\,, 2^3 = 8\,, 2^4 \equiv 7(mod9)\,, 2^5 \equiv 5(mod9), 2^6 \equiv 1(mod9)$

أي أن العدد 2 هو جذر أولي للعدد 9 . ونعلم أن $\varphi(9) = \varphi(3^2) = 6$,

$\varphi(\varphi(9)) = \varphi(6) = 2$ أي أن عدد الجذور الأولية = 2

ولنبحث عن الجذر الأولي الثاني بين الأعداد 2^k بحيث يكون k أولياً نسبياً مع 6 . أي $k = 5$,

$2^5 \equiv 5(mod9)$ والعدد 5 هو الجذر الأولي الثاني . في الحقيقة فإن

$5^2 \not\equiv 1(mod9),\ 5^3 \equiv -1(mod9) \Rightarrow 5^6 \equiv 1(mod9)$.

3-4 الأدلة (Indices):

4-3-1 تعريف الدليل : إذا كان r جذراً أولياً للعدد m وإذا كان b أولياً نسبياً مع m فإن أصغر عدد صحيح موجب k: $1 \le k \le \varphi(m)$ يحقق العلاقة $b \equiv r^k(modm)$ يسمى دليل أولر للعدد b أو لغاريتم أولر للعدد b أو أختصاراً دليل b بالأساس r والمقاس m ونكتب

$$k = \underset{r}{Ind}a \Leftrightarrow r^{\underset{r}{Inda}} \equiv a(modm)$$

مثال : بما أن $r = 2$ هو جذر أولي للعدد 5 و $\varphi(5) = 4$ و أن قوى العدد 2 فنجد :

$$2^1 \equiv 2(mod5)\ , 2^2 \equiv 4(mod5), 2^3 \equiv 3(mod5), 2^4 \equiv 1(mod5)$$

لذا نقول إن $\underset{2}{Ind}1 = 4$, $\underset{2}{Ind}3 = 3$, $\underset{2}{Ind}4 = 2$, $\underset{2}{Ind}2 = 1$

ونلاحظ أن الدليل يلعب دور اللغارتيم وأن الجذر الأولي يلعب دور أساس اللغارتيم المعروفة لذا قد يقرأ في بعض الأحيان دليل عدد معطى لغاريتم أولر لذلك العدد.

4-3-2 خواص الأدلة : إذا كان r جذراً أولياً للعدد m وإذا كان M , N عددين صحيحين وكان $(M.N, m) = 1$ فإن

(1 $$\underset{r}{IndM} = \underset{r}{IndN}(mod\varphi(m)) \Leftrightarrow M \equiv N(modm)$$

البرهان : من تعريف الأدلة نكتب

$$M = r^{\underset{r}{IndM}}(modm) \wedge N = r^{\underset{r}{IndN}}(modm)$$
$$M \equiv N(modm) \Leftrightarrow r^{\underset{r}{IndM}} \equiv r^{\underset{r}{IndN}}(modm)$$

وحسب المبرهنة 4-1-3 فإن :

$$r^{\underset{r}{IndM}} \equiv r^{\underset{r}{IndN}}(modm) \Leftrightarrow \underset{r}{IndM} \equiv \underset{r}{IndN}(mod\varphi(m))$$

(2 $$\underset{r}{IndM.N} \equiv (\underset{r}{IndM} + \underset{r}{IndN})(mod\varphi(m))$$

البرهان (غير مطلوب): لدينا

$MN = r^{\underset{r}{IndMN}}$, $M = r^{\underset{r}{IndM}}$, $N = r^{\underset{r}{IndN}} \Rightarrow M.N = r^{\underset{r}{IndM}+\underset{r}{IndN}}$ ومنه

$$r^{\underset{r}{IndMN}} \equiv r^{\underset{r}{IndM}+\underset{r}{IndN}}(modm) \Leftrightarrow \underset{r}{IndMN} \equiv \underset{r}{IndM} + \underset{r}{IndN}(mod\varphi(m))$$

(3 $$\underset{r}{IndM^k} \equiv k\ \underset{r}{IndM}\big(mod\varphi(m)\big)\ \ , k > 0$$

البرهان (غير مطلوب): لدينا $M^k \equiv r^{\underset{r}{IndM^k}}(modm)$

ومن جهة أخرى $M^k \equiv \left(r^{Ind_r M}\right)^k \equiv r^{k Ind_r M}(mod m)$

ومنه فإن $Ind_r M^k \equiv k\, Ind_r M(mod\varphi(m))$

نتيجة لما سبق نلاحظ أن $Ind_r 1 \equiv 0(mod\varphi(m))$

$Ind_r r \equiv 1(mod\varphi(m))$

4) إذا كان s , r جذرين أوليين مختلفين للعدد m فإن :

$$Ind_r N \equiv (Ind_s N)(Ind_r S)(mod\varphi(m))$$

البرهان (غير مطلوب): لدينا $N \equiv r^{Ind_r N} = S^{Ind_s N}(mod m)$

ولكن $S \equiv r^{Ind_r S}(mod m)$

ومنه $N \equiv r^{Ind_r N} \equiv r^{(Ind_r S) Ind_s N}(mod m)$

الأمر الذي يكافىء :

$$Ind_r N \equiv (Ind_s N)(Ind_r S) mod(\varphi(m))$$

– **نتيجة :** إذا كان $N = r$ نجد :

$$Ind_r r \equiv 1 \equiv (Ind_s r)(Ind_r S) \equiv 1(mod\varphi(m))$$

تمرين : لقد وجدنا أن العدد 2 هو جذر أولي للعدد $m = 13$ لذا فإن جدول الأدلة بالنسبة للأساس 2 والمقاس 13 هو :

N	1	2	3	4	5	6	7	8	9	10	11	12
Ind_2	12	1	4	2	9	5	11	3	8	10	7	6

4–4 حل التطابقات غير الخطية باستخدام الأدلة :

تستخدم الأدلة في إيجاد حلول بعض التطابقات غير الخطية وسنبين ذلك في الأمثلة التالية :

تمرين (1) : لنوجد حلول التطابق : $7x^3 \equiv 3(mod 13)$

الحل : رأينا أن العدد 2 هو جذر أولي للعدد 13 ، لنأخذ الدليل لطرفي التطابق بالنسبة للأساس 2 فنجد حسب خواص الأدلة : حيث $\varphi(13) = 12$

$$Ind_2 7 + 3\left(Ind_2 x\right) \equiv Ind_2 3(mod 12)$$

وباستخدام جدول الأدلة السابق للعدد 13 بالنسبة للأساس 2 نجد :

$$11 + 3(Ind_2 x) \equiv 4(mod12)$$

وبفرض $Ind_2 x \equiv y$ نجد $3y \equiv 5(mod12)$ ولما كان $(3,12) = 33\not|5$,

فليس للتطابق الخطي الأخير حل مما يدل على أنه ليس للتطابق الأصلي حل .

تمرين (2) : لنوجد حلول التطابق : $7x^3 \equiv 4(mod13)$

باســتخدام الطريقة المســتخدمة في التمرين (1) نجد أنه لحل التطابق يكفي إيجاد حلول التطابق الخطي : $3y \equiv 3(mod12)$

لدينا هنا $(3,12) = 33|3$, أي يوجد للتطابق الخطي ثلاث حلول غير متطابقة بالمقاس 12 ،

ويمكن ببساطة التأكد أن حلول التطابق هي : $y = 1,5,9$

وبالعودة إلى الجدول السابق والبحث عن x التي تقابل قيم $y = Ind_2 x$

نجد أن حلول التطابق هي : $x \equiv 5(mod13), x \equiv 6(mod13), x \equiv 2(mod13)$

تمارين

1- أوجد مراتب الأعداد 5 , 3 , 2 بالمقاسات التالية

أ - بالمقاس 17 ب - بالمقاس 19 جـ - بالمقاس 23

2- أثبت أن مرتبة العدد 2 تساوي 3 بالمقاس 7 و أثبت أن مرتبة العدد 6 تساوي 2 بالمقاس 7 ثم أوجد مرتبة العدد 5 بالمقاس 7

3- أوجد مرتبة كل من العددين 19 , 11 بالمقاس 36 .

4- أثبت أن 2 هو جذر أولي للعدد 19 وأنه ليس جذراً أولياً للعدد 17

5- أثبت أنه لا يوجد للعدد 15 أي جذر أولي .

6- أوجد جذرين أوليين للعدد 10 .

7- أوجد جميع الجذور الأولية للعدد 17 علماً أن 3 هو جذر أولي له .

8- أوجد حلول التطابقات

$3x^6 \equiv 4(mod11)$, $x^8 \equiv 10(mod11)$, $3x^3 \equiv 3(mod11)$

9- اكتب جدول الأدلة للعدد 17 بالنسبة للجذرالأولي 3 ثم أوجد حلول التطابقات :

$x^{12} \equiv 13(mod17)$, $9x^8 \equiv 8(mod17)$, $7^x \equiv 7(mod17)$